Panorama 管理員指南

Version 10.0 (EoL)

docs.paloaltonetworks.com

techDOCS paloalto NETWORKS

Contact Information

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

About the Documentation

- To ensure you are viewing the most current version of this document, or to access 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

© 2020-2020 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

December 4, 2020

Table of Contents

Panorama 概要介紹 9
關於 Panorama 10
Panorama 型號 11
集中管理防火牆組態與更新 13
內容切換—防火牆或 Panorama 13
Panorama 的總設定大小 13
範本與範本堆疊 14
裝置群組 15
集中記錄日誌與報告 19
受管理的收集器和收集器群組 19
本機和分散式日誌收集 20
警告有收集器群組擁有多個日誌收集器 20
日誌轉送選項 22
集中報告 23
使用 Panorama 重新散佈資料 24
以角色為基礎的存取控制 25
管理角色 25
驗證設定檔和順序 26
存取網域 26
管理驗證 27
Panorama 認可、驗證和預覽操作 28
規劃 Panorama 部署 29
部署 Panorama：工作概要 31

設定 Panorama 33
確定 Panorama 日誌儲存要求 34
設定 Panorama 虛擬設備 36
設定 Panorama 虛擬設備的先決條件 36
安裝 Panorama 虛擬設備 38
執行 Panorama 虛擬設備的初始設定 64
設定 Panorama 虛擬設備作為日誌收集器 66
設定具備本機日誌收集器的 Panorama 虛擬設備 71
在 Panorama 模式下設定 Panorama 虛擬設備 75
在僅管理模式下設定 Panorama 虛擬設備 75
擴展 Panorama 虛擬設備的日誌儲存容量 76
在 Panorama 虛擬設備上增加 CPU 和記憶體 93
在 Panorama 虛擬設備上增加系統磁碟 98
完成 Panorama 虛擬設備設定 103
設定 M-Series 設備 104
M-Series 設備介面 104
執行 M-Series 設備的初始設定 105
M-Series 設定概觀 108
將 M-Series 設備設定為日誌收集器 110
增加 M-Series 設備的儲存容量 115
設定 Panorama 來使用多個介面 122
註冊 Panorama 與安裝授權 128
註冊 Panorama 128
啟動 Panorama 支援授權 129
在 Panorama 虛擬設備與網際網路連線時，啟動/擷取防火牆管理授權 130

在 Panorama 虛擬設備並未與網際網路連線時，啟動/擷取防火牆管理授權 130
在 M-Series 設備上啟動/擷取防火牆管理授權 132
安裝 Panorama 裝置憑證 134
安裝 Panorama 的內容與軟體更新 136
Panorama、日誌收集器、防火牆和 WildFire 版本相容性 136
在 HA 組態中為 Panorama 安裝更新 136
為有網際網路連線的 Panorama 安裝更新 137
為沒有連線至網際網路的 Panorama 安裝更新 141
為沒有網際網路連線的 Panorama 自動安裝更新 144
將 Panorama 日誌移轉為新的日誌格式 148
轉移至不同的 Panorama 型號 150
從 Panorama 虛擬設備移轉至 M-Series 設備 150
將 Panorama 虛擬設備移轉至不同的 Hypervisor 152
從 M-Series 設備移轉至 Panorama 虛擬設備 155
從 M-100 設備移轉至 M-500 設備 159
存取並導覽 Panorama 管理介面 162
登入 Panorama 網頁介面 162
導覽 Panorama 網頁介面 162
登入 Panorama CLI 163
設定對 Panorama 的管理存取權 165
設定管理員角色設定檔 165
設定存取網域 165
設定管理帳戶和驗證 166
設定使用自訂憑證進行驗證 176
SSL/TLS 連線如何相互驗證？ 176
在 Panorama 上設定使用自訂憑證進行驗證 177
在受管理的裝置上設定使用自訂憑證進行驗證 178
新增用戶端裝置 180
變更憑證 180

管理防火牆 183
將防火牆新增為受管理的裝置 184
安裝受管理防火牆的裝置憑證 188
安裝受管理防火牆的裝置憑證 188
安裝多個受管理防火牆的裝置憑證 190
設定零接觸佈建 193
ZTP 概要 193
安裝 ZTP 外掛程式 194
設定 ZTP 安裝程式管理員帳戶 200
新增 ZTP 防火牆至 Panorama 200
使用 CLI 以進行 ZTP 工作 204
解除安裝 ZTP 外掛程式 206
管理裝置群組 208
新增裝置群組 208
建立裝置群組階層 209
建立共用或裝置群組原則中使用的物件 210
還原至繼承的物件值 211
管理未使用的共用物件 211
管理繼承物件的優先順序 212
移動或複製原則規則或物件至不同的裝置群組 213
在 Panorama 上選取 URL 篩選廠商 214
將原則規則推送至防火牆子集 217
管理規則階層 219

管理範本與範本堆疊 221
範本功能與例外狀況 221
新增範本 221
設定範本堆疊 223
設定範本或範本堆疊變數 225
匯入及覆寫現有範本堆疊變數 227
取代範本或範本堆疊值 228
停用/移除範本設定 230
從 Panorama 管理主要金鑰 232
設定企業資料遺失防護 (DLP) 235
企業資料遺失防護 (DLP) 概要介紹 235
企業資料遺失防護 (DLP) 支援什麼？ 236
預先定義的資料篩選設定檔 239
安裝企業資料遺失防護 (DLP) 外掛程式 239
建立資料模式 241
建立資料篩選設定檔 242
啟用企業資料遺失防護 (DLP) 245
檢視企業資料遺失防護 (DLP) 日誌詳細資料 247
啟用現有資料模式和篩選設定檔 249
編輯企業資料遺失防護 (DLP) 設定 249
解除安裝企業資料遺失防護 (DLP) 外掛程式 252
重新散佈資料到受管理防火牆 255
移轉防火牆至 Panorama 進行管理 257
計劃移轉至 Panorama 進行管理 257
移轉防火牆至 Panorama 進行管理 258
移轉防火牆 HA 配對至 Panorama 進行管理 261
載入部分防火牆組態至 Panorama 中 263
Panorama 上的裝置監控 266
監控裝置健康 266
監控原則規則使用狀況 267
使用案例：使用 Panorama 設定防火牆 272
此使用案例中的裝置群組 272
此使用案例中的範本 273
設定您的中央設定與原則 274

管理大規模防火牆部署 279
確定最佳大規模防火牆部署解決方案 280
為 M-600 和 Panorama 虛擬設備增加設備管理容量 281
增加的設備管理容量需求 281
為增加的設備管理部署 Panorama 282
Panorama Interconnect 284
Panorama Interconnect 概要 284
Panorama Interconnect 需求 285
啟用 Panorama 控制器與節點間驗證 287
設定 Panorama Interconnect 外掛程式 291
同步 Panorama Interconnect 293
管理 Panorama Interconnect 的防火牆 295
升級 Panorama Interconnect 外掛程式 303

管理日誌收集 305
設定受管理收集器 306
為專用日誌收集器設定驗證 309

為專用日誌收集器設定管理帳戶 309
為專用日誌收集器設定 RADIUS 驗證 310
為專用日誌收集器設定 TACACS+ 驗證 312
為專用日誌收集器設定 LDAP 驗證 314
管理收集器群組 318
設定收集器群組 318
以日誌收集器間的自訂憑證，來設定驗證 320
移動日誌收集器至不同的收集器群組 321
從收集器群組移除防火牆 322
設定日誌轉送至 Panorama 323
設定 Syslog 轉送至外部目的地 326
轉送日誌至 Cortex 資料湖 329
確認日誌轉送至 Panorama 330
修改日誌轉送及緩衝預設值 331
設定日誌從 Panorama 轉送至外部目的地 333
日誌收集部署 335
部署具備專用日誌收集器的 Panorama 335
部署具備本機日誌收集器的 Panorama M-Series 設備 340
部署具備本機日誌收集器的 Panorama 虛擬設備 344
部署具備本機日誌收集的傳統模式 Panorama 虛擬設備 349

管理 WildFire 設備 351
新增獨立 WildFire 設備給 Panorama 管理 352
在 Panorama 上進行 WildFire 設備基本設定 355
為 WildFire 設備設定驗證 355
使用 WildFire 設備和叢集上的自訂憑證進行驗證 364
設定 Panorama 管理的 WildFire 設備的自訂憑證 364
以單一自訂憑證設定 WildFire 叢集驗證 366
將自訂憑證套用在透過 Panorama 設定的 WildFire 設備 367
移除 WildFire 設備不要由 Panorama 管理 369
管理 WildFire 叢集 370
在 Panorama 上集中設定叢集 370
使用 Panorama 檢視 WildFire 叢集狀態 387
在有網際網路連線的情況下在 Panorama 上集中升級叢集 388
在沒有網際網路連線的情況下在 Panorama 上集中升級叢集 390

管理授權與更新 393
使用 Panorama 管理防火牆上的授權 394
使用 Panorama 將升級部署至防火牆、日誌收集器和 WildFire 設備 395
支援的更新 395
使用 Panorama 排程內容更新 396
當 Panorama 連線至網際網路時升級日誌收集器 397
當 Panorama 未連線至網際網路時升級日誌收集器 399
當 Panorama 連線至網際網路時升級防火牆 402
當 Panorama 未連線至網際網路時升級防火牆 407
升級 ZTP 防火牆 410
從 Panorama 復原內容更新 411

監控網路活動 413
使用 Panorama 增強可見度 414
使用應用程式監測中心及應用程式層面以監控網路 414

分析日誌資料 415
產生、排程及以電子郵件傳送報告 416
為排程報告設定金鑰限制 418
在 Panorama 上擷取陷阱 ESM 日誌 421
使用案例：使用 Panorama 監控應用程式 423
使用案例：使用 Panorama 回應事件 426
事件通知 426
檢閱 ACC 內的 Widget 426
檢閱威脅日誌 426
檢閱 WildFire 日誌 427
檢閱資料篩選日誌 427
更新安全性規則 428

Panorama 高可用性 429
Panorama HA 先決條件 430
HA 中 Panorama 上的優先順序與容錯移轉 432
故障復原觸發程序 433
HA 活動訊號輪詢與您好訊息 433
HA 路徑監控 433
Panorama HA 中的日誌記錄注意事項 434
傳統模式 Panorama 虛擬設備上的日誌記錄容錯移轉 434
M-Series 設備或 Panorama 模式 Panorama 虛擬設備上的日誌記錄容錯移轉 434
Panorama HA 端點之間同步化 436
管理 Panorama HA 配對 437
在 Panorama 上設定 HA 437
設定在 HA 對等之間使用自訂憑證進行驗證 438
測試 Panorama HA 故障復原 439
Panorama 故障復原後切換優先順序以恢復 NFS 日誌記錄 440
將主要 Panorama 還原至主動狀態 441

管理 Panorama 443
預覽、驗證或提交組態變更 444
啟用自動提交復原 446
管理 Panorama 和防火牆組態備份 448
排程組態檔案匯出 448
儲存及匯出 Panorama 和防火牆組態 449
還原 Panorama 組態變更 451
設定 Panorama 上的最大組態份數 453
載入受管理防火牆上的組態備份 453
比較 Panorama 組態中的變更 454
管理限制組態變更的鎖定 455
將自訂標誌新增至 Panorama 457
使用 Panorama 工作管理員 458
管理日誌和報告儲存配額和到期日期 459
日誌和報告儲存 459
日誌和報告到期日期 459
設定日誌和報告儲存配額和到期日期 460
設定 Panorama 報告的執行階段 461
監控 Panorama 462
Panorama 系統與組態日誌 462
透過 SNMP 監控 Panorama 和日誌收集器統計資料 462
重新啟動或關閉 Panorama 465

設定 Panorama 密碼設定檔及複雜性 466

Panorama 外掛程式 467
關於 Panorama 外掛程式 468
安裝 Panorama 外掛程式 469
VM-Series 外掛程式和 Panorama 外掛程式 471
在 Panorama 上安裝 VM-Series 外挂程式 471

疑難排解 473
疑難排解 Panorama 系統問題 474
產生 Panorama 診斷檔案 474
診斷 Panorama 暫停狀態 474
監控檔案系統完整性檢查 474
管理 Panorama 儲存軟體與內容更新 475
從 Panorama HA 部署中的腦分裂復原 475
疑難排解儲存與連線問題 477
驗證 Panorama 連接埠的使用 477
解決收集器群組的零日誌儲存容量問題 479
更換 M-Series 設備的故障磁碟 479
更換 ESXi 伺服器上的虛擬磁碟 479
更換 vCloud Air 上的虛擬磁碟 480
移轉日誌至日誌收集器模式內的新 M-Series 設備 480
移轉日誌至 Panorama 模式內的新 M-Series 設備 485
移轉日誌至高可用性 Panorama 模式內的新 M-Series 設備型號 490
移轉日誌至高可用性 Panorama 模式內的新 M-Series 設備型號 496
非 HA Panorama 故障/ RMA 後轉移日誌收集器 501
重新產生 M-Series 設備 RAID 配對的中繼資料 504
檢視日誌查詢作業 504
更換 RMA 防火牆 506
為防火牆產生部分裝置狀態 506
開始 RMA 防火牆更換前 506
更換後還原防火牆組態 507
疑難排解提交失敗 510
疑難排解註冊或序號錯誤 511
疑難排解報告錯誤 512
疑難排解裝置管理授權錯誤 513
疑難排解自動復原防火牆組態 514
當 Panorama HA 對等關閉時，完成內容更新 516
檢視工作成功或失敗狀態 518
為受管理裝置測試原則比對和連線 519
疑難排解原則規則流量匹配 519
疑難排解網路資源連線 520
從 Panorama 10.0 降級 521

Panorama 概要介紹

Panorama™ 管理伺服器可集中監控和管理多個 Palo Alto Networks 新世代防火牆，以及 WildFire 設備和設備叢集。它提供單一位置，從該位置能讓您監控您網路周遊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原則，以保護及控制網路。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。使用 Panorama 來集中管理 WildFire 設備和 WildFire 設備叢集可增加單一網路支援的防火牆數目、提供容錯高可用性，以及提升管理效率。

> 關於 Panorama
> Panorama 型號
> 集中管理防火牆組態與更新
> 集中記錄日誌與報告
> 使用 Panorama 重新散佈資料
> 以角色為基礎的存取控制
> Panorama 認可、驗證和預覽操作
> 規劃 Panorama 部署
> 部署 Panorama：工作概要

關於 Panorama

Panorama 可讓您透過中央監督，有效地設定、管理和監控您的 Palo Alto Networks 防火牆。以下是 Panorama 發揮價值的三個主要領域：

- 中央設定和部署—若要簡化中央管理及快速部署網路上的防火牆和 WildFire 設備，請使用 Panorama 以預先規劃防火牆和 WildFire 設備的部署階段。您接著可以將防火牆組合成群組，並建立範本以套用基礎網路和裝置設定，及使用裝置群組以全域地管理共用和本機原則規則。請參閱集中管理防火牆組態與更新。
- 藉由中央監控分析與報告，以執行彙總日誌記錄—跨網路的所有受管理防火牆收集活動資訊，並集中分析、調查和報告資料。藉助此廣泛的網路流量、使用者活動和相關風險檢視，您可以在網路上使用豐富的原則集以安全地啟用應用程式，從而回應潛在的威脅。請參閱集中日誌記錄與報告。
- 分散式管理—可讓您委派或限制存取全域和本機防火牆的設定與原則。請參閱以角色為基礎的存取控制，瞭解如何為分散式管理委派適當的存取層級。

有四個可用的 Panorama 型號：Panorama 虛擬設備、M-600 設備、M-500 設備和 M-200 設備在 PAN-OS 10.0 中受支援。Panorama 集中管理說明如何在高可用性 (HA) 設定中部署 Panorama 來管理防火牆。

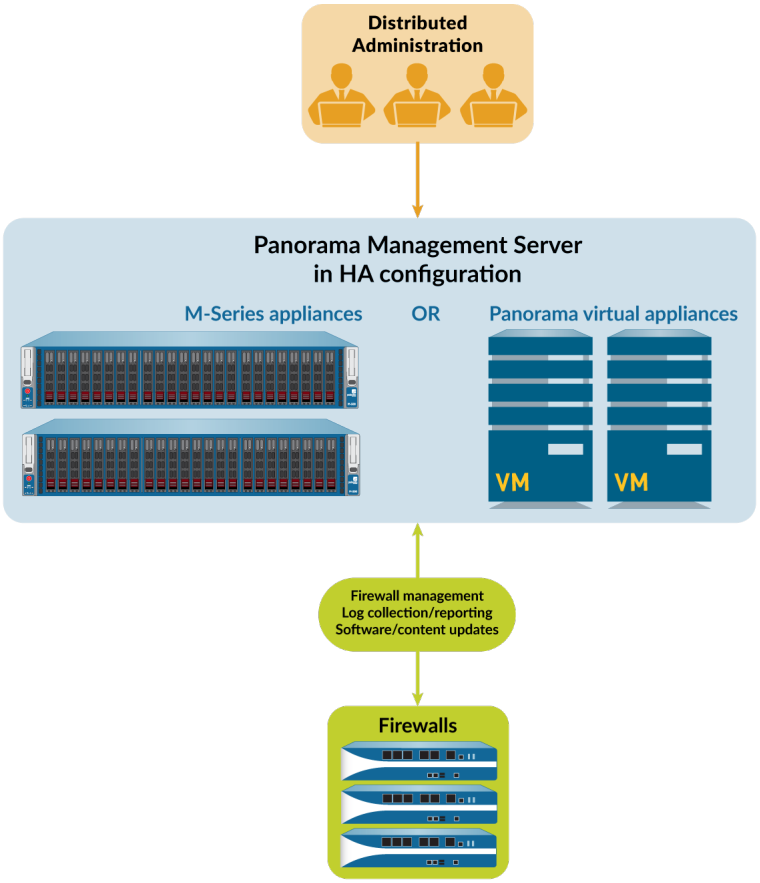


圖 1: Panorama 集中管理

© 2019 Palo Alto Networks, Inc.

Panorama 型號

Panorama 的形式有下列其中一種虛擬或實體設備，各支援授權來管理最多 25、100或 1,000 個防火牆。此外，M-600 設備，以及類似資源 Panorama 虛擬設備也支援管理多至 5000 個防火牆的授權：

- **Panorama** 虛擬設備—針對需要虛擬管理設備的網站，此型號安裝簡單，也有助於伺服器彙總。您可以在 Amazone Web Services (AWS)、AWS GovCloud、Microsoft Azure、Google Cloud Platform (GCP)、KVM、Hyper-V、VMware ESXi 伺服器或 VMare vCloud Air 上安裝 Panorama。虛擬設備能夠以高達每秒 10,000 個日誌的速率在本機收集日誌，還能管理專用日誌收集器以達到更快的日誌記錄速率。虛擬設備可以作為專用管理伺服器使用，Panorama 管理伺服器擁有本機日誌收集能力，或可作為專用日誌收集器使用。如需支援的介面、日誌儲存容量和最大日誌收集速率的資訊，請參閱 設定 Panorama 虛擬設備的先決條件。您可以將虛擬設備部署成下列模式：
  - **Panorama** 模式—在此模式中，Panorama 虛擬設備支援具備 1 至 12 個虛擬日誌記錄磁碟的本機日誌收集器（請參閱部署具備本機日誌收集器的 Panorama 虛擬設備）。在單一虛擬設備上，每個日誌記錄磁碟的儲存容量為 2TB，合計最多 24TB，而在高可用性 (HA) 配對上最多 48TB。只有 Panorama 模式可讓您新增多個虛擬日誌記錄磁碟，而不會遺失現有磁碟上的日誌。Panorama 模式還有更快產生報告的優點。在 Panorama 模式中，虛擬設備不支援 NFS 儲存空間。

    最佳作法是以 *Panorama* 模式部署虛擬設備，才會以最佳方式儲存日誌和產生報告。
  - 傳統模式（僅限 ESXi 和 vCloud Air）—在此模式中，Panorama 虛擬設備接收和儲存防火牆日誌時，並不使用本機日誌收集器（請參閱部署具備本機日誌收集的傳統模式 Panorama 虛擬設備）。依預設，傳統模式的虛擬設備有一個磁碟分割區用於儲存所有資料。此分割區大約配置 11GB 來儲存日誌。如果需要更多本機日誌儲存空間，您可以在 ESXi 5.5 及更新版本或 vCloud Air 上新增一個最多 8TB 的虛擬磁碟。較早 ESXi 版本支援一個最多 2TB 的虛擬磁碟。如果需要超過 8TB 的空間，您可以將傳統模式的虛擬設備掛載至 NFS 資料存放，但僅限於 ESXi 伺服器上，而不是 vCloud Air 中。此模式僅可在 Panorama 虛擬設備在傳統模式中升級至 PAN-OS 10.0 時使用。升級至 PAN-OS 9.0 和更新版本後，如果您變更至任何其他模式，傳統模式將不再可用。如果您將 Panorama 虛擬設備從傳統模式變更為可用模式之一，則您將不再能夠將其改回傳統模式。

    雖然傳統模式受支援，但是建議不要在生產環境中使用，其仍可用于實驗室或示範環境中。
  - 僅管理模式—在此模式下，Panorama 虛擬設備為您受管理裝置和專用日誌收集器的專用管理設備，並且在此模式下，相應資源的 Panorama 虛擬設備可管理多至 5,000 個防火牆。除了組態和系統日誌外，Panorama 虛擬設備沒有任何日誌收集功能，同時還需要專用日誌收集器以儲存日誌。依預設，處於僅管理模式的虛擬設備僅有一個磁碟分割區用於儲存所有資料，所以所有轉送至處於僅管理模式下的 Panorama 虛擬設備的日誌都會被丟棄。因此，若要儲存來自來自您受管理設備的日誌資料，您必須 configure log forwarding（設定日誌轉送）才能儲存來自您受管理裝置的日誌資料。如需詳細資訊，請參閱增加的設備管理容量需求。
  - 日誌收集器模式—Panorama 虛擬設備充當專用日誌收集器。如果有多個防火牆轉送大量的日誌資料，處於日誌收集器模式的 Panorama 虛擬設備可提升規模及效能。此模式中，設備沒有用於進行管理存取的 web 介面，僅有命令行介面 (CLI)。不過，您可以使用 Panorama 管理伺服器的網頁介面來管理設備。只有在初始設定與偵錯時，才需要以 CLI 存取日誌收集器模式的 Panorama 虛擬設備。關於設定的詳細資訊，請參閱部署具備專用日誌收集器的 Panorama。
- **M-Series** 設備—M-200、M-500 和 M 600 設備是大規模部署專用的硬體設備。在具有高日誌記錄速率（超過 10,000 個日誌每秒）和日誌保留需求的環境中，此類設備可調整日誌收集基礎結構的規模。如需支援的介面、日誌儲存容量和最大日誌收集速率的資訊，請參閱 M-Series 設備介面。所有 M-Series 型號共用下列屬性：
  - RAID 磁碟機：儲存防火牆日誌；RAID 1 鏡像：避免受磁碟故障所影響
  - SSD：儲存 Panorama 和日誌收集器產生的日誌
  - MGT、Eth1、Eth2 和 Eth3 介面：支援 1Gbps 輸送量

© 2019 Palo Alto Networks, Inc.

- 備援的熱插拔電源
- 由前至後的氣流

M-600 和 M-500 設備還有下列額外屬性，使之變得更適合資料中心：

- Eth4 和 Eth5 介面：支援 10Gbps 輸送量

此外，以下屬性使 M-600 設備更適合大規模防火牆部署：

- Management Only（僅管理模式）下的 M-600 設備可管理多至 5000 個防火牆。

您可以 M-Series 設備部署成下列模式：

- **Panorama** 模式—設備充當 Panorama 管理伺服器來管理防火牆和專用日誌收集器。設備也支援本機日誌收集器來彙總防火牆日誌。Panorama 模式是預設模式。關於設定的詳細資訊，請參閱部署具備本機日誌收集器的 Panorama M-Series 設備。
- **Management Only mode**（僅管理模式）—Panorama 虛擬設備為您受管理裝置和專用日誌收集器的專用管理設備。除了組態和系統日誌外，Panorama 設備沒有任何日誌收集功能，同時您的部署還需要專用日誌收集器以儲存這些日誌。依預設，處於僅管理模式的 Panorama 設備僅有一個磁碟分割區用於儲存所有資料，所以所有轉送至處於僅管理模式下的 Panorama 虛擬設備的日誌都會被丟棄。因此，若要儲存來自來自您受管理設備的日誌資料，您必須 configure log forwarding（設定日誌轉送）才能儲存來自您受管理裝置的日誌資料。
- 日誌收集器模式—設備充當專用日誌收集器。如果有多個防火牆轉送大量的日誌資料，日誌收集器模式的 M-Sereis 設備可提升規模及效能。此模式中，設備沒有用於進行管理存取的 web 介面，僅有命令行介面 (CLI)。不過，您可以使用 Panorama 管理伺服器的網頁介面來管理設備。只有在初始設定與偵錯時，才需要以 CLI 存取日誌收集器模式的 M-Series 設備。關於設定的詳細資訊，請參閱部署具備專用日誌收集器的 Panorama。

如需 M-Series 設定的更多詳細資訊和規格，請參閱 M-Series 設備硬體參考指南。

© 2019 Palo Alto Networks, Inc.

集中管理防火牆組態與更新

Panorama™ 使用裝置群組和範本，將防火牆分組成（需要類似的設定）的邏輯集合。您可使用裝置群組和範本集中管理受管理防火牆上的所有設定元件、原則和物件。Panorama 還讓您可以集中管理授權、軟體（PAN-OS® 軟體、SSL-VPN 用戶端軟體、GlobalProtect™ 代理程式/應用程式軟體）和內容更新（應用程式、威脅、WildFire® 和防毒）。

- 內容切換—防火牆或 Panorama
- Panorama 的總設定大小
- 範本與範本堆疊
- 裝置群組

內容切換—防火牆或 Panorama

Panorama™ 網頁介面可讓您使用位於各頁籤左上角的 **Context**（內容）下拉式清單，在以 Panorama 為中心的檢視與以防火牆為中心的檢視之間切換。設定 **Context**（內容）至 **Panorama** 以集中管理防火牆或切換內容至特定防火牆的網頁介面以執行本機設定。Panorama 和防火牆網頁介面的相似度讓您可以在二者之間無縫移動，從而監控和管理防火牆。

Context（內容）下拉式清單僅列出連線至 Panorama 的防火牆。對於裝置群組和範本管理員，下拉式清單僅列出已連線的防火牆，此類防火牆位於被指派至該管理員的存取網域內。若要搜尋長清單，使用下拉式清單中的篩選器。

對於有高可用性 (HA) 設定的防火牆，圖示帶有彩色背景以顯示 HA 狀態（如下）。在選取防火牆內容時，瞭解 HA 狀態非常有效。例如，您通常在主動防火牆上對特定防火牆組態進行變更。

- 綠色—主動。
- 黃色—被動或已啟動防火牆（啟動後，啟動狀態會持續最多 60 秒）。
- 紅色—防火牆處於非作用（錯誤狀態）、暫停（管理員已停用防火牆）或暫訂（針對主動/主動 HA 設定中的連結或路徑監控事件）狀態。

Panorama 的總設定大小

在確定您需要在 Panorama 虛擬設備上配置哪個 M-Series 設備或最小數量的虛擬資源以確保滿足安全性要求時，Panorama™ M-Series 和虛擬設備的總設定檔案大小是效能指標的重要部分。執行設定變更、提交和推送到受管理防火牆時，超過 Panorama 管理伺服器支援的總設定檔案大小會導致效能降低。

對於所有範本、裝置群組和 Panorama 特定設定，Panorama 模式中的 Panorama 管理伺服器支援的總設定檔案大小為 80MB。「僅管理」模式中的 Panorama 最多支援 120MB 或 150MB 的總設定檔案大小，具體取決於 Panorama 型號或您配置給 Panorama 虛擬設備的資源。請參閱以下表格，瞭解基於 Panorama M-Series 設備型號或配置給 Panorama 虛擬設備的資源建議的最大設定檔案大小。

Panorama 型號	所需虛擬資源	推薦的 Panorama 最大設定檔案大小
M-200	不適用	120MB
M-500		120MB
M-600		150MB
Panorama 虛擬設備	• 16 vCPU • 128GB 記憶體	120MB

© 2019 Palo Alto Networks, Inc.

Panorama 型號	所需虛擬資源	推薦的 Panorama 最大設定檔案大小
請參閱 設定 Panorama 虛擬設備的先決條件 獲取更多設定資訊。	• 56 vCPU • 256GB 記憶體	150MB

範本與範本堆疊

您可以使用範本和範本堆疊來設定啟用防火牆在網路上操作的設定。範本為您用來設定 Panorama™ 上 **Network**（網路）和 **Device**（裝置）頁籤的基本建置組塊。您可以使用範本定義介面與區域設定，以管理日誌記錄和系統日誌存取的伺服器設定檔，或定義 VPN 設定。範本堆疊讓您能夠將多個範本分層，並建立結合的設定。範本堆疊簡化了管理，因為它們能讓您為所有連接至範本堆疊的裝置定義常用基礎設定，並讓您可以將範本分層，以建立結合的設定。它可以讓您以位置或功能特定設定來定義範本，然後依優先次序的降序來堆疊範本，好讓防火牆能依據範本在堆疊中的順序繼承設定。

範本與範本堆疊兩者都支援變數。變數讓您可以依據設定需求，以範本或範本堆疊中特定的值來建立占位符物件。建立範本或範本堆疊變數以取代 IP 位址、分組 ID 和設定中的介面。範本變數由範本堆疊繼承，您可以取代它們以建立範本堆疊變數。不過，範本無法繼承在範本堆中定義的變數。當在範本或範本堆疊中定義變數並推送至防火牆時，變數定義的值會顯示在防火牆上。

若要滿足唯一設定的防火牆您可以使用範本來取代範本堆疊設定。或者，您可以推送一個更廣泛、常用的基本設定，然後以個別防火牆上的特定防火牆值來取代某些推送的設定。當您取代防火牆的設定時，防火牆儲存設定至其本機設定，且 Panorama 不再管理該設定。若要在取代它們之後還原範本值，則使用 Panorama 以強制範本或範本堆疊設定至防火牆。例如，在您定義範本內的普通 NTP 伺服器並取代防火牆上的 NTP 伺服器設定以協調其本機時區後，您可以隨後還原至範本中定義的 NTP 伺服器。

當定義範本堆疊時，請考慮將硬體機型類似、且需要存取類似網路資源（例如閘道和系統日誌伺服器）的防火牆進行指派。這讓您可以避免新增各種設定備援至各範本堆疊。下圖所示示例設定中，您指派亞太地區資料中心防火牆至帶有全域設定的範本、亞太特定設定範本和資料中心特定設定範本的堆疊。如欲管理亞太公司的防火牆，可以重複使用全域及亞太專屬範本，此時只要將其新增至包含分公司專屬設定範本的另一個堆疊中。堆疊內的範本有可設定的優先級順序，確保 Panorama 僅為任何重複設定推送一個設定。Panorama 從上至下評估堆疊設定內所列的範本，位置較高的範本優先級也較高。下圖所示資料中心堆疊中的範本比全域範本優先級高：Panorama 推送來自資料中心範本的閒置逾時值，並忽略來自全域範本的值。

© 2019 Palo Alto Networks, Inc.

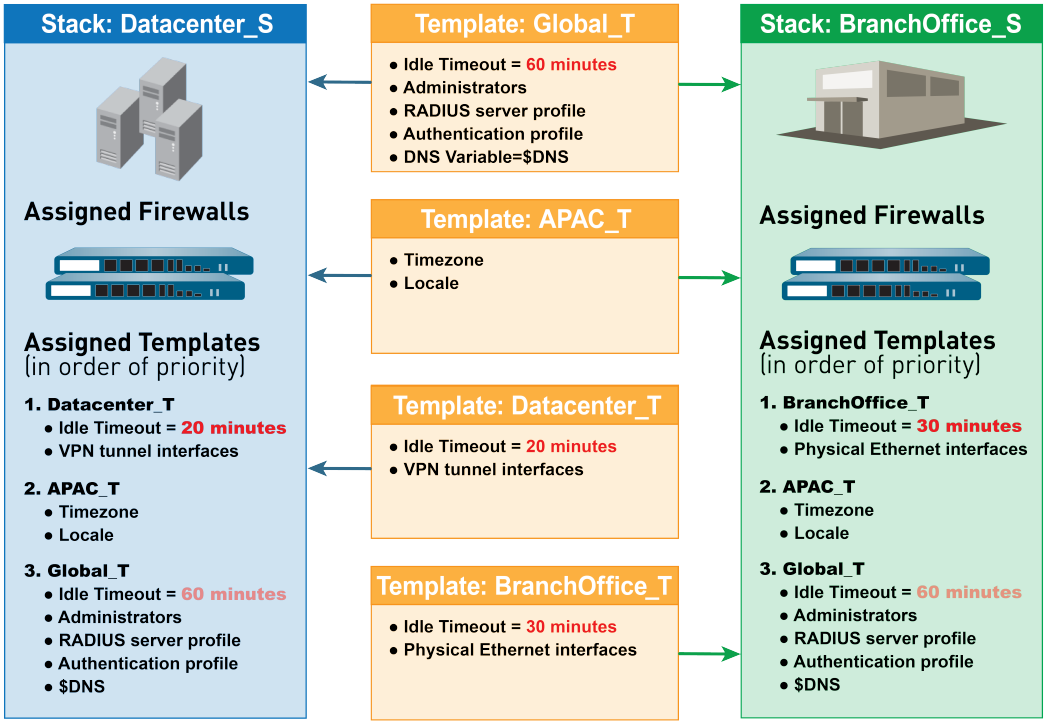


圖 2: 範本堆疊

您無法使用範本或範本堆疊設定防火牆模式：虛擬私人網路（VPN）模式、多虛擬系統（multi-vsys）模式或操作模式（一般或 FIPS-CC 模式）。詳細資訊，請參閱範本功能與例外狀況。但是，您可以指派帶有不匹配模式的防火牆至相同的範本或堆疊。這種情況下，Panorama 只會將模式特定設定套用至支援這些模式的防火牆。有一種例外情況，您可以設定 Panorama 推送範本內的預設 vsys 設定至不支援虛擬系統或沒有任何設定的虛擬系統。

相關程序，請參閱管理範本與範本堆疊。

裝置群組

若要有效使用 Panorama，您必須將網路上的防火牆分組為邏輯單位，稱為裝置群組。裝置群組啟用的分組基於網路區段、地理位置、組織功能或防火牆任何其他普通方面（需要類似原則設定）。透過裝置群組，您可以設定政策規則及其參考的物件。透過頂部共用的規則和物件，以及裝置群組特定規則和後續層級的物件，您可以按階層組織裝置群組。這讓您可以建立規則階層，強制防火牆處理流量的方式。例如，您可以定義一套共用規則作為企業可接受的使用政策。接下來，若只要允許地區辦事處存取點對點流量（例如 BitTorrent），您可以定義裝置群組規則，讓 Panorama 僅推送至地區辦事處（或定義共用安全規則並將其目標設為地區辦事處）。對於相關程序，請參閱 管理裝置群組。下列主題詳細說明裝置群組概念和每個元件：

- 裝置群組階層
- 裝置群組原則
- 裝置群組物件

裝置群組階層

您現在可以 建立裝置群組階層，以在（最多四層的）樹狀階層建立巢狀裝置群組，其中低層群組將繼承高層群組設定（政策規則和物件）。在底端層級，裝置群組可以具有父項（上層）、上一層和上二層的裝置群組（統稱為父系）。在頂端層級，裝置群組可以具有子項（下層）、下一層和下二層的裝置群組（統稱為子系）。所有從共用位置（該位置是設定階層頂端位置的容器）繼承設定的裝置群組，其設定是所有裝置群組的共同設定。

© 2019 Palo Alto Networks, Inc.

建立裝置群組階層讓您可以根據共同原則要求組織防火牆，且無備援設定。例如您可設定對所有防火牆通用的共用設定，在第一層級設定具有功能專屬設定的裝置群組，以及在下端層級設定具有位置專屬設定的裝置群組。如果沒有階層，您可能就需要在「共用」之下的單一層級，針對每個裝置群組設定功能和位置專屬設定。

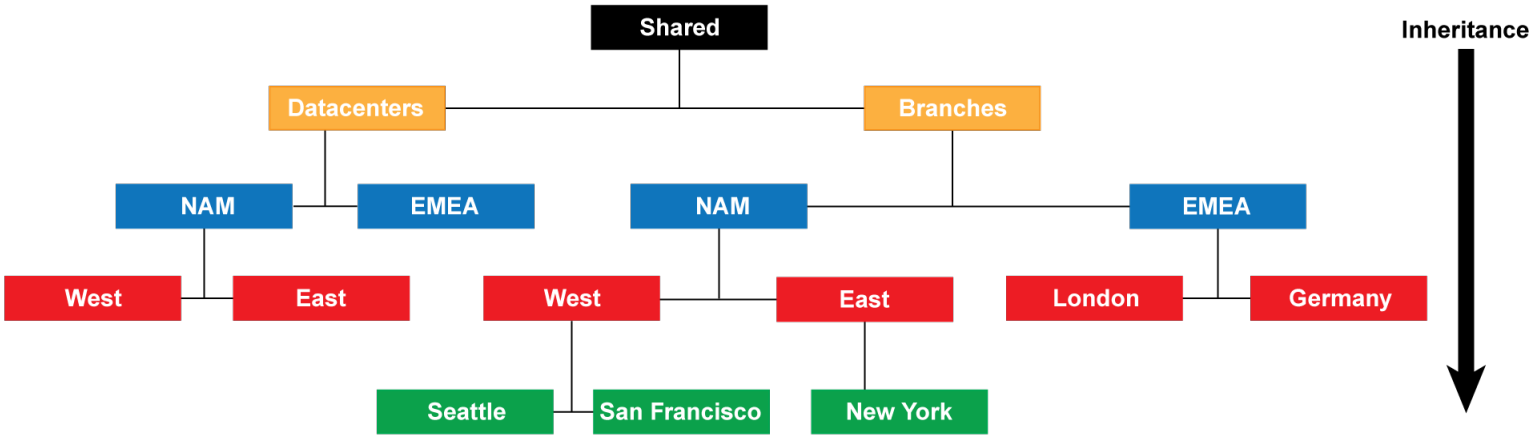
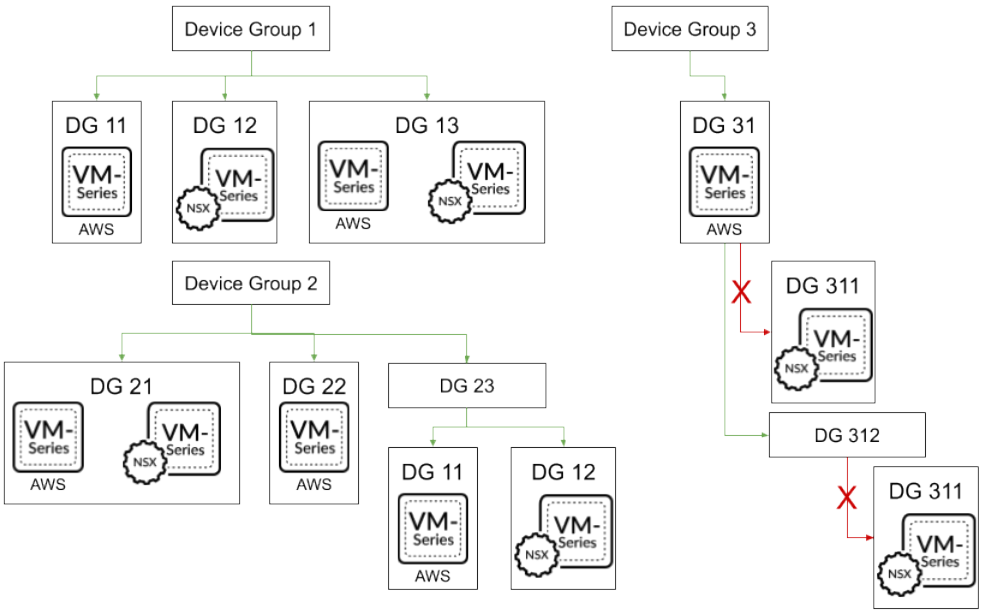


圖 3: 裝置群組階層

防火牆在裝置群組階層內評估原則規則的順序詳細資訊，請參閱 裝置群組原則。裝置群組從父系裝置群組繼承的物件值取代詳細資訊，請參閱 裝置群組物件。

在要執行的多 Panorama 外掛程式部署中，包含部署在特定超管理器中的防火牆的裝置群組不能是包含部署在其他超管理器中的防火牆的裝置群組的子系或父系。例如，如果 Panorama 從 VMware NSX-V 和 AWS 接收 IP 位址更新，則不能建立作為 AWS VM-Series 防火牆裝置群組子系的 NSX-V VM-Series 防火牆裝置群組。



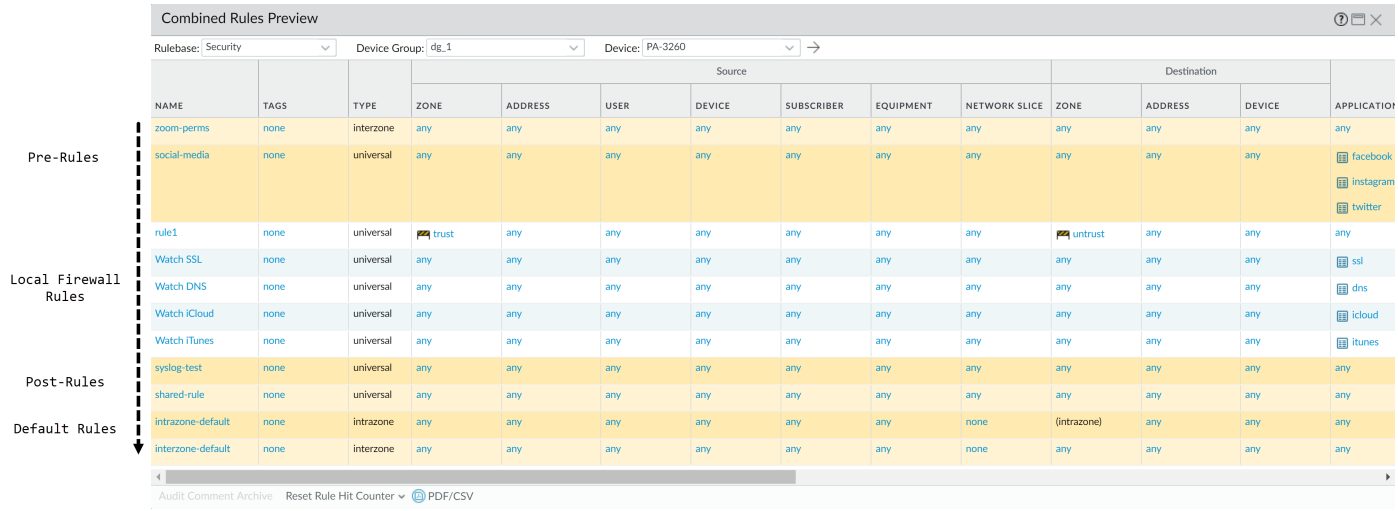
裝置群組原則

裝置群組提供了分層方法的實作方式，可用來管理受管理的防火牆網路之間的原則。防火牆依據層級（共用、裝置群組和本機）和類型（預先規則、後續規則和預設規則），按下列順序從上到下評估原則規則。當防火牆接收流量時，其執行首個評估規則中定義的動作，首個評估規則與流量相符，且放棄所有後續規則。

© 2019 Palo Alto Networks, Inc.

若要變更特定層級、類型和規則庫內的規則評估順序（例如，共用安全性預先規則），請參閱管理規則階層。

無論在防火牆或 Panorama 內檢視規則，web 介面都按照評估順序顯示。所有共用的裝置群組以及防火牆從 Panorama 繼承的預設規則均以帶陰影的橙色顯示。本機防火牆規則顯示為預先規則和後續規則。



評估順序	規則範圍和描述	管理裝置
共用預先規則 裝置群組預先規則	Panorama 將共用的預先規則推送至所有裝置群組內的所有防火牆中。Panorama 將特定裝置群組預先規則推送至特定裝置群組及其子系裝置群組內的所有防火牆中。 如果防火牆從裝置群組階層多個層級的裝置群組繼承了規則，其按照層級的從高到低對預先規則進行評估。這表示防火牆會首先評估共用規則，最後評估無子系的裝置群組規則。 您可以使用預先規則強制執行組織的可接受使用政策。例如，預先規則可能封鎖對特定 URL 類別的存取，或允許所有使用者的網域名稱系統 (DNS) 流量。	這些規則在防火牆上可見，但您僅可在 Panorama 中管理。
本機防火牆規則	本機規則是對單一防火牆或虛擬系統 (vsys) 的特定規則。	本機防火牆管理員或切換至本機防火牆內容的 Panorama 管理員，都可以編輯本機防火牆規則。
裝置群組後續規則 共用後續規則	Panorama 將共用的後續規則推送至所有裝置群組內的所有防火牆中。Panorama 將特定裝置群組後續規則推送至特定裝置群組及其子系裝置群組內的所有防火牆中。 如果防火牆從裝置群組階層多個層級的裝置群組繼承了規則，其按照層級的從低到高對後續規則進行評估。這表示防火牆會	這些規則在防火牆上可見，但您僅可在 Panorama 中管理。

© 2019 Palo Alto Networks, Inc.

評估順序	規則範圍和描述	管理裝置
	首先評估無子系的裝置群組規則，最後評估共用規則。 後續規則通常包含規則來根據 App-ID™ 簽章、User-ID™ 資訊（使用者或使用者群組）或服務，以拒絕存取流量。	
內區域-預設 內區域-預設	預設規則僅套用至安全性規則庫，並在 Panorama（共用層級處）和防火牆（各 vsys 內）上預先定義。這些規則規定 PAN-OS 處理不與任何其他規則相符的流量的方式。 內區域-預設規則允許區域內的所有流量。內區域-預設規則拒絕區域間的所有流量。 如圖取代預設規則，優先順序會從最低的內容執行到最高的內容：在防火牆層級被取代的設定會優先於在裝置群組層級的設定，而裝置群組層級的設定會優先於共用層級的設定。	預設規則一開始是唯讀的，因為預設規則是預先定義設定的一部分，或因為 Panorama 已將這些規則推送至防火牆。然而，您可以覆寫標籤、動作、日誌記錄及安全性設定檔的規則設定。內容會決定您可取代規則的層級： • Panorama——在共用或裝置群組層級，您可以取代作為預先定義設定一部分的預設規則。 • 防火牆——您可以取代防火牆或 vsys 上預先定義部分的預設規則，或 Panorama 從共用位置或裝置群組推送的預設規則。

裝置群組物件

物件是原則規則中參考的設定元件，例如：IP 位址、URL 類別、安全性設定檔、使用者、服務和應用程式。任何類型（預先規則、後續規則、預設規則和防火牆上本機定義的規則）和任何規則庫（安全、NAT、QoS、基於原則的轉送、解密、應用程式取代、網頁認證和 DoS 保護）都可參考物件。您可以在任意規則數量中重複使用某物件，前提是需要與該物件在裝置群組階層中的範圍一致。例如，如果您新增一個物件至共用位置，階層內所有規則可參考該共用物件，因為所有裝置群組都是從共用位置繼承物件的。如果您新增一個物件至特定裝置群組，僅該裝置群組及其子系裝置群組內的規則可以參考該裝置群組物件。如果裝置群組內的物件值與繼承自父系裝置群組的物件值必須不同，您可以取代繼承的物件值（請參閱步驟取代繼承的物件值）。您還可以隨時還原至繼承的物件值。當您一次建立共用或裝置群組原則中使用的物件並多次使用時，減少管理額外負荷並確保防火牆原則的一致性。

您可以設定 Panorama 處理系統物件的方式：

- **Pushing unused objects**（推送未使用的物件）——依預設，無論任何共用或裝置群組原則規則是否參考物件，Panorama 都將推送所有物件至防火牆。或者，您可以設定 Panorama 僅推送參考的物件。詳細資訊，請參閱管理未使用的共用物件。
- **Precedence of ancestor and descendant objects**（父系和子系物件優先順序）——依預設，當階層內多等級的裝置群組擁有相同名稱的物件，但值不同時（例如，由於發生取代），子系裝置群組中的原則規則適用該子系裝置中的物件值，而非從上階裝置群組或共用群組中繼承的物件值。或者，您可以還原優先順序以將含有物件的共用或最高上階值推送至所有子系裝置群組。詳細資訊，請參閱管理繼承物件的優先順序。

© 2019 Palo Alto Networks, Inc.

集中記錄日誌與報告

Panorama 可彙總所有受管理防火牆的日誌，並提供跨網路所有流量的可見度。它同時針對受管理的防火牆，提供對該防火牆進行的所有原則修改和設定變更的稽核記錄。除了彙總日誌外，Panorama 還可以利用 SNMP 設陷、電子郵件通知、syslog 訊息和 HTTP 承載，將日誌轉送至外部伺服器。

在集中記錄日誌和報告方面，您還可以選擇使用與 Panorama 完美結合的雲端式 Cortex Data Lake（Cortex 資料湖）。Cortex Data Lake（Cortex 資料湖）可讓受管理的防火牆將日誌轉送至 Cortex Data Lake（Cortex 資料湖）基礎結構，而不是 Panorama，或轉送至受管理的日誌收集器，您不必投入時間和精力，就能擴大現有分散式日誌收集設定，或調整目前的記錄日誌基礎結構。

Panorama 上的應用程式命令中心 (ACC) 提供跨所有防火牆的統一報告單一的窗格。讓您可以集中監控網路活動，以分析、調查和報告流量和安全事件。在 Panorama 上，您可以檢視日誌、從轉送至 Cortex Data Lake（Cortex 資料湖）、Panorama 或受管理日誌收集器（如果設定）的日誌中產生報告，或者直接查詢受管理的防火牆。例如，您可以根據 Panorama（及受管理的收集器）上儲存的日誌，或藉由存取受管理的防火牆本機或 Cortex Data Lake（Cortex 資料湖）上儲存的日誌，產生受管理網路中的流量、威脅和/或使用者活動的相關報告。

如果您不設定日誌轉送至 Panorama 或 Cortex Data Lake（Cortex 資料湖），您可以排程在每個受管理的防火牆上執行報告，再將結果轉送至 Panorama，以形成使用者活動和網路流量的整合檢視。雖然報告無法提供特定資訊及活動的深入細節，但仍提供一致的監控方法。

- 受管理的收集器和收集器群組
- 本機和分散式日誌收集
- 警告有收集器群組擁有多個日誌收集器
- 日誌轉送選項
- 集中報告

受管理的收集器和收集器群組

Panorama 使用日誌收集器彙總來自受管理防火牆的日誌。產生報告時，Panorama 會向日誌收集器查詢日誌資訊，讓您洞察防火牆監控的所有網路活動。由於您使用 Panorama 設定與管理日誌收集器，因此這些收集器也就是所謂的受管理收集器。Panorama 可以管理兩種日誌收集器：

- 本機日誌收集器—這種日誌收集器在 Panorama 管理伺服器的本機執行。只有 Panorama 模式的 M-600、 M-500 設備、M-200、M-100 設備或 Panorama 虛擬設備才支援本機日誌收集器。

  如果您將日誌轉送至傳統模式的 *Panorama* 虛擬設備，此設備會在本機儲存日誌，而不使用日誌收集器。
- 專用日誌收集器 - 這是日誌收集器模式的 M-600、M-500、M-200、M-100 設備或 Panorama 虛擬設備。您可以使用 Panorama 模式的 M-Series 設備，或使用 Panorama 或傳統（ESXi 和 vCloud Air）模式的 Panorama 虛擬設備，以管理專用日誌收集器。若要使用 Panorama 網頁介面來管理專用日誌收集器，您必須將其新增為受管理的收集器。否則，只能透過 CLI 並使用預先定義的管理使用者（管理員）帳戶，才能對專用日誌收集器進行管理存取。專用日誌收集器不支援額外的管理使用者帳戶。

您可以使用任一種日誌收集器或兩種都使用，為您的環境打造更好的日誌記錄解決方案（請參閱本機和分散式日誌收集）。

收集器群組是 1 至 16 個受管理的收集器，以單一邏輯日誌收集單元的形式運作。如果收集器群組包含專用日誌收集器，Panorama 會將日誌均勻散佈於每個日誌收集器中的所有磁碟，以及群組中的所有日誌收集器。此散佈充分善用可用的儲存空間。若要讓日誌收集器接收日誌，您必須將其新增至收集器群組。您可以透過指派多個日誌收集器至收集器群組，以啟用日誌備援（請參閱警告有收集器群組擁有多個日誌收集器）。收集器群組設定指定哪些受管理防火牆可將日誌傳送給群組中的日誌收集器。

若要設定日誌收集器和收集器群組，請參閱管理日誌收集。

© 2019 Palo Alto Networks, Inc.

本機和分散式日誌收集

在設定將日誌轉送至 Panorama 之前，您必須決定要使用本機日誌收集器、專用日誌收集器或兩者。

部署本機日誌收集器很容易，因為不需要額外硬體或虛擬機器實例。在高可用性 (HA) 設定中，您可以將日誌傳送至兩個 Panorama 對等上的本機日誌收集器；被動 Panorama 不會等待容錯移轉才開始收集日誌。

若為本機日誌收集，您也可以將日誌轉送至傳統模式的 *Panorama* 虛擬設備，此裝置儲存日誌時不使用日誌收集器作為邏輯容器。

專用日誌收集器是日誌收集器模式的 M-600、M-500、M-200 或 Panorama 虛擬設備。專用日誌收集器僅執行日誌收集，不管理防火牆，因此可形成比本機日誌收集器更強固的環境。專用日誌收集器提供下列優點：

- 可讓 Panorama 管理伺服器將更多資源投入管理功能，而非記錄日誌。
- 在專用硬體裝置上提供高容量的日誌儲存空間。
- 啟用更高的日誌記錄速率。
- 使用 RAID 1 儲存裝置提供水平式的延展性和備援。
- 最佳化網路中的頻寬資源，有更多頻寬可供防火牆用於將日誌傳送至附近的日誌收集器，而非遠端 Panorama 管理伺服器。
- 讓您符合當地的法規要求（例如，法規可能不允許日誌離開特定地區）。

在分散式日誌收集所展現的拓撲中，HA 設定中的 Panorama 對等會管理防火牆和專用日誌收集器的部署和設定。

在 *HA* 設定中，您可以部署 *Panorama* 管理伺服器，但無法部署專用日誌收集器。

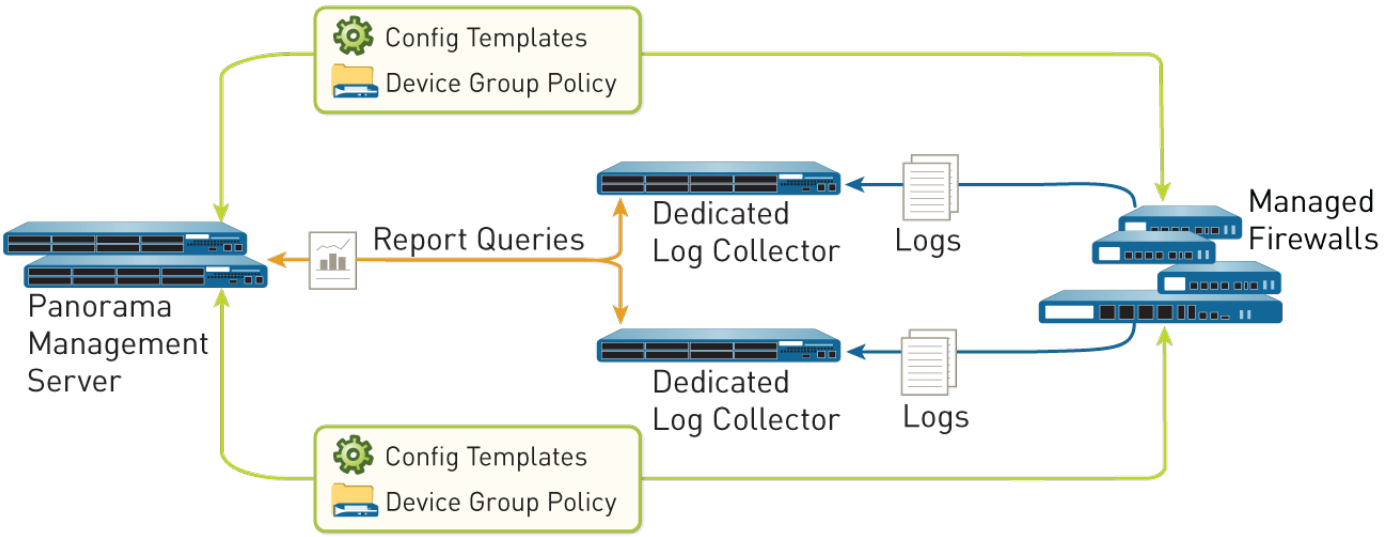


圖 4: 分散式日誌收集

警告有收集器群組擁有多個日誌收集器

您可以設定收集器群組來包含多個日誌收集器（最多 16 個），以確保日誌備援、延長日誌保留期間及協調超出單一日誌收集器容量的日誌記錄速率（關於容量的資訊，請參閱 Panorama 型號）。在任何單一收集器群組中，所有日誌收集器都必須在相同 Panorama 型號上執行：全部是 M-600 設備、全部都是 M-500 設備、全部都是 M-200 設備，或全部是 Panorama 虛擬設備。例如，如果單一受管理的防火牆產生 48TB

© 2019 Palo Alto Networks, Inc.

的日誌，接收這些日誌的收集器群組至少需要六個是 M-200 設備的日誌收集器，或兩個是 M-500 設備或 Panorama 虛擬設備的日誌收集器。

帶有多個日誌收集器的收集器群組將可用的儲存空間作為一個邏輯單元，並在其所有日誌收集器上均勻散佈日誌。日誌是根據日誌收集器的磁碟容量（請參閱 Panorama 型號）及雜湊演算法（可動態決定哪些日誌收集器擁有日誌，並將日誌寫入磁碟）予以散佈。雖然 Panorama 使用偏好設定清單，排定受管理防火牆將日誌轉送到的日誌收集器清單優先順序，但 Panorama 不一定會將日誌寫入偏好設定清單中指定的第一個日誌收集器。例如，請考量下列偏好設定清單：

受管理防火牆	收集器群組中定義的日誌轉送偏好設定清單
FW1	L1,L2,L3
FW2	L4,L5,L6

根據此清單，只要主要日誌收集器可用，FW1 就會將日誌轉送至 L1。但是，根據雜湊演算法，Panorama 可能選擇 L2 當作擁有者而將日誌寫入磁碟。如果 L2 變成無法存取或發生機殼故障，FW1 並不會知道，因為它仍然連接至 L1。

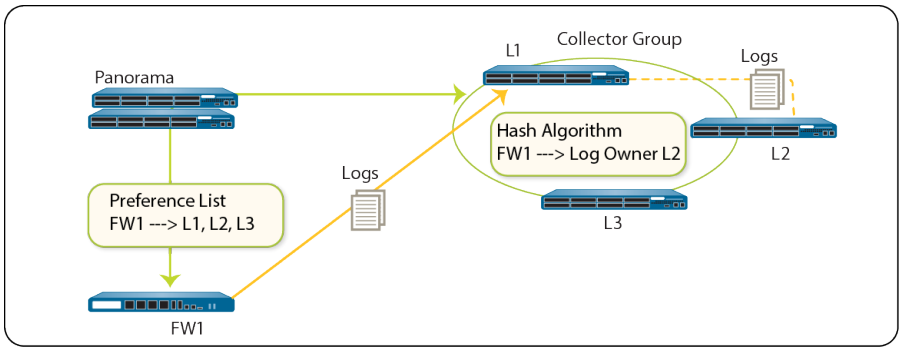


圖 5: 範例 - 一般日誌收集器群組設定

如果收集器群組只有一個日誌收集器，而且日誌收集器故障，防火牆會將日誌儲存至 HDD/SSD（可用儲存空間視防火牆型號而異）。當日誌收集器的連線恢復時，防火牆會立即從故障發生前中斷的地方繼續轉送日誌。

如果收集器群組有多個日誌收集器，假設只有一個日誌收集器停止運作，防火牆並不會將日誌緩衝到本機儲存空間。在 L2 停止運作的範例案例中，FW1 會繼續將日誌傳送至 L1，而 L1 會儲存將被傳送至 L2 的日誌資料。當 L2 重新運作時，L1 不再儲存 L2 的日誌資料，而是按預期進行散佈。如果收集器群組內的一個日誌收集器停止運作，則要被寫入停止運作的日誌收集器的日誌將被重新散佈至偏好設定清單中的下一個日誌收集器。

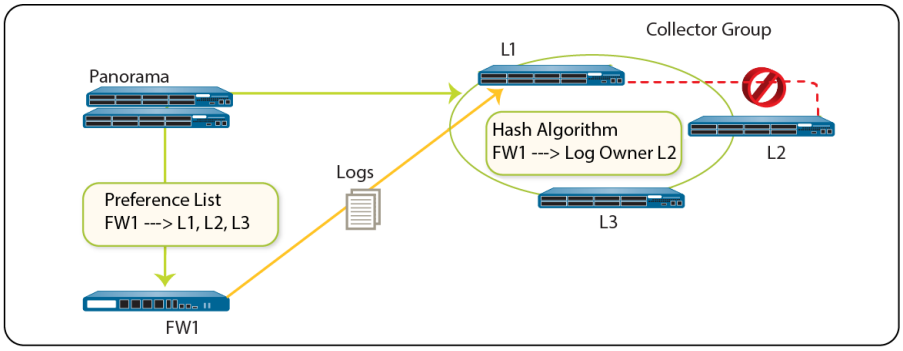


圖 6: 範例 - 日誌收集器故障時

© 2019 Palo Alto Networks, Inc.

如果在某個收集器群組中使用多個日誌收集器，則 Palo Alto Networks 建議採用下列方式減輕風險：

- 在設定收集器群組時，啟用日誌備援。這確保了如果日誌收集器群組內的某個日誌收集器不可用時，不會有日誌丟失。每個日誌將有兩個副本，每個副本都將保留在不同的日誌收集器上。只有當每一個日誌收集器都具有相同數量的日誌磁碟時，日誌備援才可用。

  由於啟用備援會建立更多日誌，因此此設定需要更多儲存容量。收集器群組空間用盡時，其會刪除較舊的日誌。

  由於每個日誌收集器都必須散佈每個接收的日誌複本，因此啟用備援會讓收集器群組中的日誌處理流量加倍，並讓最大日誌記錄速率減半。
- 取得現場備件 (OSS)，以便在日誌收集器故障時能立即更換。
- 除了將日誌轉送至 Panorama 外，還能設定轉送至外部服務作為備份儲存。外部服務可以是 syslog 伺服器、電子郵件伺服器、SNMP 設陷伺服器或 HTTP 伺服器。

日誌轉送選項

依預設，各防火牆本機儲存其日誌檔案。若要使用 Panorama 集中監控日誌與產生報告，您必須設定日誌轉送至 Panorama。Panorama 支援轉送日誌至日誌收集器、Cortex Data Lake（Cortex 資料湖）或兩者並行。您也可以直接從防火牆或從 Panorama 將日誌轉送至外部服務，以利用這些服務來封存、通知或分析。外部服務包括 syslog 伺服器、電子郵件伺服器、SNMP 設陷伺服器或基於 HTTP 的服務。除了轉送防火牆日誌，您還可以轉送 Panorama 管理伺服器和日誌收集器所產生的日誌。轉送日誌的 Panorama 管理伺服器、日誌收集器或防火牆會將日誌轉換成適合目的地的格式（syslog 訊息、電子郵件通知、SNMP 設陷或 HTTP 承載）。

Palo Alto Networks 防火牆和 Panorama 支援下列日誌轉送選項。在選取其中一個選項前，請考慮您的 Panorama 型號並決定 Panorama 日誌儲存需求。

- 將日誌從防火牆轉送至 Panorama，並從 Panorama 轉送至外部服務—此設定適合防火牆與外部服務之間的連線頻寬不足，無法維持記錄速率的部署（此情況在遠端連線時較為常見）。此設定會將某些處理卸載到 Panorama，藉此改善防火牆效能。

  您可以設定各收集器群組以轉送日誌至不同的目的地。

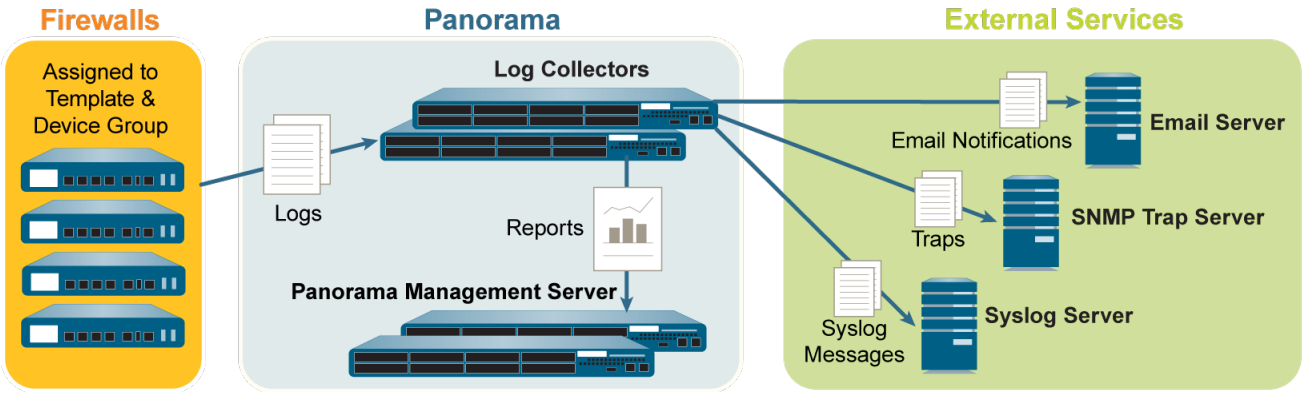


圖 7: 將日誌轉送至 **Panorama** 再轉送至外部服務

- 將日誌從防火牆轉送至 Panorama，同時轉送至外部服務—在此設定中，Panorama 與外部服務皆為不同日誌轉送流量的端點；防火牆不依賴 Panorama 將日誌轉送外部服務。此設定適合防火牆與外部服務之間的連線頻寬充足，可維持記錄速率的部署（此情況在本機連線時較為常見）。

© 2019 Palo Alto Networks, Inc.

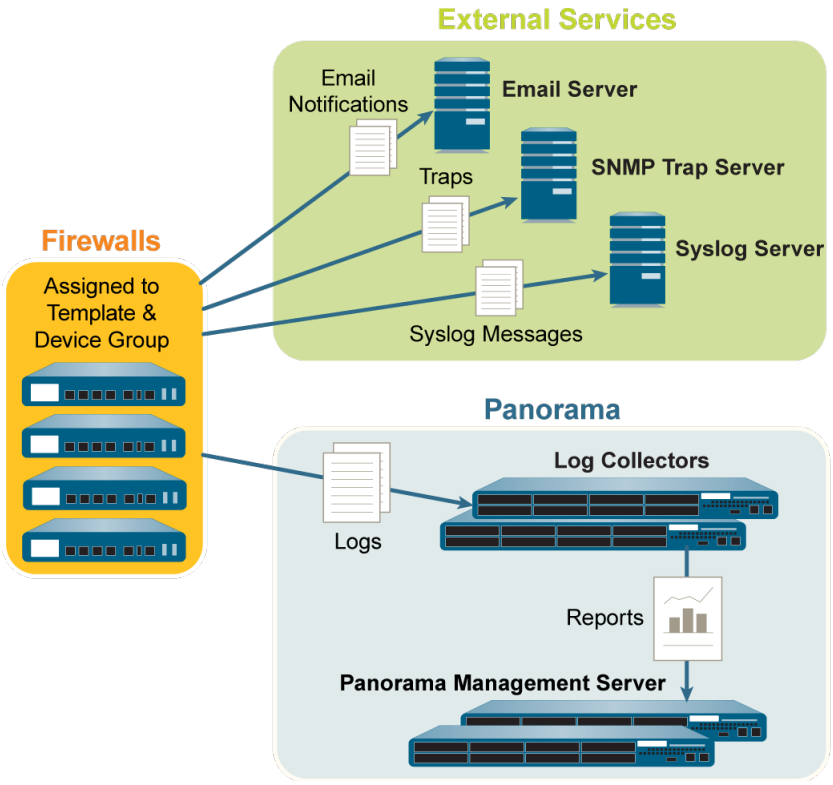


圖 8: 將日誌同時轉送至外部服務與 **Panorama**

集中報告

Panorama 可彙總所有受管理防火牆的日誌，並以寬廣的視野，彙總跨整個網路的應用程式使用、使用者活動及流量模式資料。將防火牆新增至 Panorama 後，ACC 會立即顯示周遊您網路的所有流量。啟用日誌記錄後，按一下 ACC 中的日誌項目可直接存取應用程式精確的詳細資料。

產生報告時，Panorama 會使用兩個來源：本機 Panorama 資料庫及其管理的遠端防火牆。Panorama 資料庫指的是 Panorama 上配置的本機儲存空間，目的是儲存摘要的日誌及某些詳細的日誌。如果您擁有散佈日誌收集部署，Panorama 資料庫會在 Panorama 及所有受管理的日誌收集器上加入本機儲存空間。Panorama 會每隔 15 分鐘，即會針對所有從受管理防火牆所收集的資訊進行摘要，即流量、應用程式、威脅。使用本機 Panorama 資料庫可加快回應時間，不過，如果您不想將日誌轉送給 Panorama，Panorama 可直接存取遠端防火牆，並執行受管理的設備防火牆所儲存的資料報告。

Panorama 提供 40 種以上的預先定義報告，您可以依原狀使用這些報告，或藉由結合其他報告的元件來產生自訂的報告，並且可儲存報告群組。您可視需要或依週期性排程來產生報告，並可排程以電子郵件傳送報告。這些報告提供使用者和內容的相關資訊，如此您即可產生事件的關聯，並且識別模式、趨勢和可能感興趣的領域。利用整合的日誌記錄和報告方法，ACC 可連結相同事件的多個相關日誌項目之間的關聯。

如需詳細資訊，請參閱監控網路活動。

© 2019 Palo Alto Networks, Inc.

使用 Panorama 重新散佈資料

使用資料重新散佈，您只需設定每個來源一次，然後就可根據需要將多種資料類型重新散佈到任意數量的用戶端。這有助於您擴展網路，以便根據網路需求的變更輕鬆新增或移除來源和用戶端。

資料重新散佈還能透過僅將資訊類型重新散佈給您指定的防火牆或 Panorama 管理系統，進行精確的控制。您可以使用子網路、範圍和區域來進一步減少網路流量並最大化裝置容量。

Palo Alto Networks 防火牆的主要優點之一是可以根據使用者名稱和標籤來執行原則和產生報告，而非根據 IP 位址。大型網路的挑戰在於確保每個執行原則和產生報告的防火牆都具有適用於全部原則規則的對應和標籤。此外，每個執行驗證原則的防火牆都要求使用者群必須有一組完整、相同的驗證時間戳記。每當使用者驗證來存取服務和應用程式時，個別防火牆會記錄相關聯的時間戳記，但不會自動透露給其他防火牆以確保一致性。資料重新散佈可讓您重新散佈必要資料，為大型網路克服這些挑戰。但是，您無需建立額外的連線來在防火牆之間重新散佈資料，而是可以利用 Panorama 基礎結構來 重新散佈資料到受管理防火牆。基礎結構提供現有連線，可讓您將資料重新散佈到各層，從防火牆到 Panorama。然後，Panorama 就可以將資訊重新散佈至執行原則和產生報告的防火牆。

每個防火牆或 Panorama 管理伺服器可以從最多 100 個重新散佈點接收資料。重新散佈點可以是其他防火牆或 Panorama 管理伺服器。不過，您也可以使用 Windows 型 User-ID 代理程式來執行對應，並將資訊重新散佈至防火牆。只有當使用者流量符合驗證原則規則時，防火牆才會記錄驗證時間戳記。

© 2019 Palo Alto Networks, Inc.

以角色為基礎的存取控制

以角色為基礎的存取控制 (RBAC) 可讓您定義每位管理使用者（管理員）應有的權限與責任。每位管理員必須有一個指定角色和驗證方法的使用者帳戶。管理角色 定義對 Panorama 和防火牆內容中特定設定、日誌和報告的存取。對於裝置群組和範本管理員，您可以對應角色至 存取網域，並透過其定義對特定裝置群組、範本和防火牆的存取（通過內容切換）。透過將各存取網域與管理員角色結合，以便在組織的職務區域或地區區域之間分隔資訊。例如，您可以限制管理員監控資料中心防火牆的活動，但允許該管理員設定測試實驗室防火牆的原則。依預設，各 Panorama 裝置（虛擬設備或 M-Series 設備）都有預先定義的管理帳戶（管理員），提供完整讀寫權限（超級使用者權限），可存取所有功能區域及所有裝置群組、範本和防火牆。對於各管理員，您可以定義驗證設定檔，以決定 Panorama 如何驗證使用者存取認證。

最佳作法是為每個需要在 *Panorama* 上存取管理或報告功能的人員，建立單獨的管理帳戶，而非使用所有管理員的預設帳戶。如此能更有效地防範未經授權的設定變更，並能夠讓 *Panorama* 記錄和識別每個管理員的動作。

- 管理角色
- 驗證設定檔和順序
- 存取網域
- 管理驗證

管理角色

您設定管理員帳戶的方式取決於組織的安全性需求、網路使用的任何現有驗證服務，以及所需的管理角色。角色可定義管理員可用的系統存取權類型。您可以視需要（依據您組織的安全性需求），廣泛或精細地定義與限制存取權。例如，您可以決定資料中心管理員能擁有所有設備和網路設定的存取權；安全性管理員可控制安全性原則定義，而其他關鍵人員可擁有限制的 CLI 或 XML API 存取權。角色的類型為：

- 動態角色—此內建角色可提供 Panorama 和受管理防火牆的存取權。當新增新功能時，Panorama 會自動更新動態角色的定義，您永遠不用手動更新這些定義。下表列出與動態角色相關的存取權限。

動態角色	權限
超級使用者	完整的 Panorama 讀取/寫入存取權限
超級使用者（唯讀）	Panorama 的唯讀存取權限。
Panorama 管理員	Panorama 的完整存取權，但不包括下列動作： • 建立、修改或刪除 Panorama 或防火牆管理員及角色。 • 在 **Device**（設備）> **Setup**（設定）> **Operations**（操作）頁面中匯出、驗證、還原、儲存、載入或匯入設定。 • 在 **Panorama** 頁籤上設定 **Scheduled Config Export**（已排程的設定匯出）功能。

- 管理員角色設定檔—若要能夠更精確的存取控制 Web 介面、CLI 及 XML API 的功能區，您可以建立自訂角色。當新功能新增至產品時，您必須以對應的存取權限更新角色：Panorama 不會自動將新功能新增至自訂的角色定義。當您 設定管理員角色設定檔.時，選取以下設定檔類型之一。

© 2019 Palo Alto Networks, Inc.

管理員角色設定檔	說明
Panorama	針對這些角色，您可以將讀取-寫入存取權、唯讀存取權或無存取權指派給所有可供超級使用者動態角色使用的 Panorama 功能，唯 Panorama 管理員與 Panorama 角色的管理功能除外。針對最後兩個功能，您可以指派唯讀存取權或無存取權，但您無法指派讀取-寫入存取權。 舉例來說，Panorama 角色的使用適用於需要存取 Panorama 上安全性原則定義、日誌與報告的安全性管理員。

裝置群組與範本	針對這些角色，您可以將讀取-寫入存取權、唯讀存取權或無存取權指派給裝置群組、範本和防火牆內容中的特定功能區域。透過將角色與 存取網域 結合，以便在組織的職務區域或地區區域之間分隔資訊。裝置群組和範本角色有下列限制：
	• 不可存取 CLI 或 XML API
	• 不可存取設定或系統日誌
	• 不可存取 VM 資訊來源
	• 在 **Panorama** 頁籤中，存取權被限制為：
	  • 設備部署功能（讀取-寫入、唯讀或無存取）
	  • 管理員帳戶中指定的裝置群組（讀取-寫入、唯讀或無存取）
	  • 管理員帳戶中指定的範本和受管理的防火牆（唯讀或無存取）
	
	舉例來說，在需要存取 Web 介面上設備與網路設定區中特定裝置群組和/或範本的操作工作人員中的管理員便適合使用此角色。

驗證設定檔和順序

驗證設定檔中定義驗證服務，可在管理員存取 Panorama 時驗證其登入憑證。該服務可能是本機驗證或外部驗證服務。某些服務（SAML、TACACS+ 和 RADIUS）提供選項在外部伺服器上為管理帳戶同時管理驗證和授權，而不是在 Panorama。除了驗證服務，驗證設定檔還定義如 Kerberos single sign-on（單一登入 - SSO）和 SAML single logout（單一登出 - SSO）這些選項。

一些網路針對不同使用者和使用者群組擁有多個資料庫（如 TACACS+ 和 LDAP）。如果要在此情況下驗證管理員，請設定驗證順序—在登入期間，供 Panorama 比對管理員的驗證設定檔先後順序。Panorama 會按順序檢查每個設定檔，直到有一個設定檔成功驗證管理員。唯有當序列中的所有設定檔都驗證失敗時，才會拒絕管理員存取。

存取網域

存取網域可控制對特定裝置群組和範本的管理存取，還可控制能否切換內容至受管理防火牆的 Web 介面。存取網域僅套用至帶有裝置群組和範本角色的管理員。將管理角色對應至存取網域，可以對管理員在 Panorama 上存取的資訊進行非常細微的控制。例如，請考慮以下案例：您設定的存取網域包含您的資料中心防火牆的所有裝置群組，而您將該存取網域指派給能夠監控資料中心流量但不能設定防火牆的管理員。在此情況下，您會將存取網域對應至某個角色，該角色已啟用所有監控權限，但會停用裝置群組設定的存取權。此外，裝置群組和範本管理員可以在其存取網域中對受管理防火牆執行管理工作，例如檢視設定和系統日誌、執行設定稽核、檢閱擱置中的工作，以及直接存取防火牆操作（如重新啟動、產生技術支援檔案、執行統計資料傾印以及匯出核心檔案）。

您可以在本機 Panorama 組態中設定存取網域，然後指派給管理帳戶和角色。您可以在本機執行指派，或使用外部 SAML、TACACS+ 或 RADIUS 伺服器。使用外部伺服器可讓您透過目錄服務，快速重新指派存取網域，而不必在 Panorama 上重新設定。若要使用外部伺服器，您必須定義可讓 Panorama 存取伺服器的伺服器設定檔。您也必須在 RADIUS 或 TACACS+ 伺服器上定義廠商特定屬性 (VSA)，或在 SAML IdP 伺服器上定義 SAML 屬性。

© 2019 Palo Alto Networks, Inc.

例如，如果您使用 RADIUS 伺服器，您就會為每個管理員定義 VSA 號碼和值。定義的值必須符合 Panorama 上設定的存取網域。當管理員嘗試登入 Panorama 時，Panorama 會在 RADIUS 伺服器中查詢管理員的存取網域和屬性號碼。根據 RADIUS 伺服器的回應，管理員會得到存取授權，並且限制為存取網域中指定的防火牆/虛擬系統、裝置群組和範本。

關於相關程序，請參閱：

- 設定存取網域。
- 為 Panorama 管理員設定 RADIUS 驗證。
- 為 Panorama 管理員設定 TACACS+ 驗證。
- 為 Panorama 管理員設定 SAML 驗證。

管理驗證

您可以為 Panorama 管理員設定以下類型的驗證及授權（管理角色和存取網域）：

驗證方法	授權方法	說明
本地	本地	管理帳戶認證與驗證機制屬於 Panorama 本機。請使用 Panorama 將管理角色和存取網域指派給帳戶。若要進一步保護帳戶，您可以建立密碼設定檔來定義密碼有效期間，以及設定 Panorama 全域密碼複雜度設定。詳細資訊，請參閱為 Panorama 管理員設定本機或外部驗證。
SSH 金鑰	本地	管理帳戶屬於 Panorama 本機，但 CLI 的驗證基於 SSH 金鑰。請使用 Panorama 將管理角色和存取網域指派給帳戶。詳細資訊，請參閱設定管理員以基於 SSH 金鑰的驗證來存取 CLI。
憑證	本地	管理帳戶屬於 Panorama 本機，但網頁介面的驗證基於用戶端憑證。請使用 Panorama 將管理角色和存取網域指派給帳戶。詳細資訊，請參閱設定 Panorama 管理員以基於憑證的驗證來存取網頁介面。
外部服務	本地	您在 Panorama 本機定義的管理帳戶用於參考外部多因素驗證、SAML、Kerberos、TACACS+、RADIUS 或 LDAP 伺服器上定義的帳戶。外部伺服器將執行驗證。請使用 Panorama 將管理角色和存取網域指派給帳戶。詳細資訊，請參閱為 Panorama 管理員設定本機或外部驗證。
外部	外部服務	僅在 SAML、TACACS+ 或 RADIUS 伺服器上定義管理帳戶。伺服器將執行驗證和授權。對於授權，您需在 TACACS+ 或 RADIUS 伺服器上定義廠商特定屬性 (VSA)，或在 SAML 伺服器上定義 SAML 屬性。Panorama 會將屬性對應至您在 Panorama 上定義的管理員角色和存取網域。如需詳細資訊，請參閱： • 為 Panorama 管理員設定 SAML 驗證 • 為 Panorama 管理員設定 TACACS+ 驗證 • 為 Panorama 管理員設定 RADIUS 驗證

© 2019 Palo Alto Networks, Inc.

Panorama 認可、驗證和預覽操作

在準備好啟動您對 Panorama 上的候選設定所做的變更時，或將變更推送至 Panorama 所管理的裝置時（防火牆、日誌收集器及 WildFire 設備和設備叢集），您可以 預覽、驗證或提交組態變更。例如，如果您將日誌收集器新增至 Panorama 組態，在您將變更提交至 Panorama，並將變更推送至包含該日誌收集器的收集器群組之前，防火牆無法將日誌傳送至該日誌收集器。

您可依管理員或位置篩選變更，然後只提交、推送、驗證或預覽這些變更。位置可能是特定裝置群組、範本、收集器群組、日誌收集器、共用設定或 Panorama 管理伺服器。

當您認可變更時，該變更會成為執行中組態的一部分。您尚未認可的變更是候選組態的一部分。Panorama 會將認可要求排入佇列，以便您在之前的認可正在進行中時，啟動新的認可。Panorama 會依啟動順序執行認可，但優先處理由 Panorama 啟動的自動認可（例如 FQDN 重新整理）。然而，如果佇列已達到管理員啟動提交的數目上限 (10)，您必須等候 Panorama 完成處理擱置的提交，才能啟動新的提交。您可以使用 Panorama 工作管理員（Tasks），以取消擱置中的提交，或查看擱置中、進行中、已完成或失敗提交的詳細資訊。若要查看提交將啟動的變更，您可以執行提交預覽。

啟動提交後，Panorama 將會檢查變更的有效性後再啟動。驗證輸出顯示封鎖提交的條件（錯誤）或務必知曉的條件（警告）。例如，驗證可能會指示您需要修復無效路由目的地，才能提交成功。驗證程序可讓您在認可前找出錯誤並加以修正（此程序並不會變更執行中的組態）。如果您使用固定認可視窗，而想要確定認可將成功而不發生錯誤，驗證程序將有所幫助。

依預設，自動認可復原已啟用，使受管理的防火牆能夠在本機測試從 Panorama 推送的組態，以確認新變更不會中斷 Panorama 與受管理防火牆之間的連線。如果所認可的組態會中斷 Panorama 與受管理防火牆之間的連線，則防火牆會自動使認可失效，且組態會還原至之前執行的組態，同時 Shared Policy（共用原則）或 Template Status（範本狀態）（**Panorama** > **Managed Devices**（受管理裝置）> **Summary**（摘要））將不同步，具體取決于推送的組態物件。此外，受管理防火牆會每 60 分鐘測試一次與 Panorama 的連線，如果受管理防火牆偵測到其無法再成功連線至 Panorama，則會將其組態還原至之前執行的組態。



如需候選組態與執行中組態的詳細資訊，請參閱 管理 Panorama 和防火牆組態備份。

若要防止多個管理員在並行工作階段中做出組態變更，請參閱 管理限制組態變更的鎖定。

將組態推送至受管理防火牆時，*Panorama* 會推送執行中的組態。因此，您必須先向 *Panorama* 認可變更，*Panorama* 才會讓您將變更推送至受管理防火牆。

© 2019 Palo Alto Networks, Inc.

規劃 Panorama 部署

- 決定管理方法。您是否計劃使用 Panorama 以集中設定和管理原則；集中管理軟體、內容和授權更新；及/或跨網路的受管理防火牆以集中執行日誌記錄與報告？

  如果您已經在網路上部署和設定 Palo Alto Networks 防火牆，請決定是否將防火牆轉移至中央管理。此程序需要將所有設定和原則，從您的防火牆移轉至 Panorama。詳細資訊，請參閱移轉防火牆至 Panorama 進行管理。
- 確認 Panorama 和防火牆軟體版本。Panorama 可管理運行版本與 Panorama 版本相符或早於 Panorama 版本的 PAN-OS 的防火牆。例如，Panorama 8.0 無法管理運行 PAN-OS 8.1 的設備。另外，Panorama 8.1 無法透過 6.0.3 管理執行 PAN-OS 6.0.0 的防火牆，且無法管理執行比 Panorama 版本更新的 PAN-OS 版本的防火牆。
- 請規劃在所有受管理防火牆之間使用相同的 URL 篩選資料庫（BrightCloud 或 PAN-DB）。如果部分防火牆使用 BrightCloud 資料庫，其他防火牆使用 PAN-DB，Panorama 只能管理其中一個 URL 篩選資料庫的安全性規則。另一個資料庫的 URL 篩選規則必須在使用該資料庫的防火牆本機上管理。
- 決定 Panorama 與其受管理的裝置和高可用性對等之間的驗證方法。依預設，Panorama 使用預先定義的憑證來驗證 SSL 連線，此連線用於管理和裝置間通訊。不過，您可以設定基於自訂憑證的驗證，以增強 Panorama、防火牆和日誌收集器之間的 SSL 連線安全。您可以使用自訂憑證建立唯一的信任鏈，以確保 Panorama 與其管理的裝置之間的相互驗證。您可以從企業公開金鑰基礎結構 (PKI) 匯入憑證，或在 Panorama 上產生憑證。
- 請在高可用性設定中規劃使用 Panorama；將其設定為主動/被動的高可用性配對。請參閱 Panorama 高可用性。
- 規劃在大規模部署中如何兼顧網路分段和安全性需求。依預設，在 M-Series 設備上執行的 Panorama 會使用管理 (MGT) 介面對 Panorama 進行管理存取，也用來管理裝置（防火牆、日誌收集器，以及 WildFire 設備和設備叢集）、收集日誌、與收集器群組通訊，以及將軟體和內容更新部署至裝置。不過，若要改善安全性和啟用網路分段，您可以將 MGT 介面保留給管理存取，並將專用的 M-Sereis 設備介面（Eth1、Eth2、Eth3、Eth4 和 Eth5）用於其他服務。
- 如需取得有意義的網路流量報告，請規劃日誌記錄解決方案：
  - 驗證部署在AWS 或 Azure 上日誌收集器模式下的 Panorama 虛擬設備的資源配置。Panorama 虛擬設備如果重新調整大小，則不會保留日誌收集器模式。因此會造成資料流失。
  - 估計網路需要的日誌儲存容量，以符合安全性與遵從需求。請考量下列因素：Panorama 型號的日誌記錄容量、網路拓撲、傳送日誌的防火牆數目、日誌流量的類型（例如，URL 篩選和威脅日誌與流量日誌）、防火牆產生日誌的速率，以及要在 Panorama 上儲存日誌的天數。詳細資訊，請參閱確定 Panorama 日誌儲存要求。
  - 除了將日誌轉送至 Panorama，是否還需要轉送至外部服務（例如 syslog 伺服器）？請參閱 日誌轉送選項。
  - 您是否想要擁有或管理自己內部部署的日誌儲存，或是否想要使用 Palo Alto Networks 所提供的 Cortex Data Lake（Cortex 資料湖）？
  - 如果需要長期儲存解決方案，您是否擁有可以將日誌轉送到其中的安全性資訊和事件管理 (SIEM) 解決方案，例如 Splunk 或 ArcSight？
  - 您是否需要在日誌記錄中備援？

    如果您設定具備多個日誌收集器的收集器群組，您可以啟用備援，以確保如果有任何一個日誌收集器變成無法使用，並不會遺失日誌（請參閱 警告有收集器群組擁有多個日誌收集器）。

    如果您在 HA 設定中部署傳統模式的 Panorama 虛擬設備，受管理的防火牆可以將日誌傳送至兩個 HA 對等，讓每個對等上都有每個日誌的複本。此備用選項預設為啟用（請參閱修改日誌轉送及緩衝預設值）。
  - 您要將日誌記錄至網路檔案系統 (NFS)？如果 Panorama 虛擬設備是傳統模式，且不管理專用日誌收集器，則 NFS 儲存空間是唯一可將日誌儲存容量增加到超過 8TB 的選項。只有當 Panorama 在 ESXi 伺服器上執行時，才可使用 NFS 儲存空間。如果您使用 NFS 儲存空間，記住，防火牆只能將日誌傳送至 HA 配對中的主要對等；只有主要對等會掛載至 NFS 和寫入 NFS。

© 2019 Palo Alto Networks, Inc.

- 決定管理員需要哪些角色型存取權限，才能存取受管理的防火牆和 Panorama。請參閱設定對 Panorama 的管理存取權。
- 規劃必要的設備群組。考慮要根據功能、安全性原則、地理位置，或是網路區段來分組防火牆。例如，功能式設備群組包含研發團隊使用的所有防火牆。考慮是否建立基於通用性的小型設備群組，易於擴展的大型設備群組，或簡化管理複雜分層的設備群組階層。
- 規劃管理原則的分層策略。考慮防火牆如何繼承及評估設備群組階層內的原則規則，及如何最完善地實作共享規則、設備群組規則及防火牆特定規則，以符合您的網路需求。對於可見度和集中式原則管理，請考慮使用 Panorama 來管理原則，即使您想要針對共享/設備群組規則建立防火牆特有的例外情況也是如此。若有必要，您可以在設備群組內將原則規則推送至防火牆子集。
- 根據防火牆從範本和範本堆疊繼承網路設定的方式，規劃防火牆的組織。例如，根據硬體型號、地理鄰近程度，以及時區、DNS 伺服器和介面設定的類似網路需求，考慮將防火牆指派給範本。

© 2019 Palo Alto Networks, Inc.

部署 Panorama：工作概要

下列工作清單摘要了開始使用 Panorama 的步驟。如需如何使用 Panorama 進行中央管理的範例，請參閱 使用案例：使用 Panorama 設定防火牆。

STEP 1 | （僅限 M-Series 設備）在機架中安裝設備。

STEP 2 | 執行初始設定以啟用 Panorama 的網路存取。請參閱 設定 Panorama 虛擬設備 或 設定 M-Series 設備。

STEP 3 | 註冊 Panorama 與安裝授權。

STEP 4 | 安裝 Panorama 的內容與軟體更新。

STEP 5 | （建議）在高可用性設定中設定 Panorama。請參閱Panorama 高可用性。

STEP 6 | 將防火牆新增為受管理的裝置。

STEP 7 | 新增裝置群組 或 建立裝置群組階層、新增範本 以及（如適用）設定範本堆疊。

STEP 8 | （選用）設定將日誌轉送至 Panorama 和/或外部服務。請參閱管理日誌收集。

STEP 9 | 監控網路活動 在 Panorama 上使用可見度和報告工具。

© 2019 Palo Alto Networks, Inc.

設定 *Panorama*

若要在網路上的所有防火牆之間進行集中報告及一致的原則管理，您可以將 Panorama™ 管理伺服器部署為虛擬設備或硬體設備（M-200、M-500 或 M-600 設備）。

下列主題說明如何在網路上設定 Panorama：

> 確定 Panorama 日誌儲存要求
> 設定 Panorama 虛擬設備
> 設定 M-Series 設備
> 註冊 Panorama 與安裝授權
> 安裝 Panorama 裝置憑證
> 安裝 Panorama 的內容與軟體更新
> 轉移至不同的 Panorama 型號
> 存取並導覽 Panorama 管理介面
> 設定對 Panorama 的管理存取權
> 設定使用自訂憑證進行驗證

確定 Panorama 日誌儲存要求

當您規劃 Panorama 部署時，請估計 Panorama 所需的日誌儲存容量，以決定部署哪些 Panorama 型號、是否在這些設備上將儲存空間擴展超出其預設容量、是否部署專用日誌收集器，以及是否設定日誌從 Panorama 轉送至外部目的地。當日誌儲存空間達到最大容量時，Panorama 會自動刪除較舊的日誌，以騰出空間給新的日誌。

執行以下步驟，確定 Panorama 大概需要的日誌儲存容量。如需瞭解詳細資訊和使用案例，請參閱 Panorama 大小與設計指南。

STEP 1 | 確定您組織的日誌記錄保留要求。

影響日誌保留要求的因素包括：

- 組織的 IT 原則
- 日誌備援—如果您在收集器群組時啟用了日誌備援，則每個日誌將有兩個副本，這將是所需的日誌儲存容量翻倍。
- 法規要求，例如支付卡產業資料安全標準 (PCI DSS)、薩班斯-奧克斯利法案 (Sarbanes-Oxley Act) 以及健康保險可攜性和責任法案 (HIPAA) 的規定。



如果您的組織需要在特定的一段時間後移除日誌，您可以設定各日誌類型的到期日期。如果需要按照類型優先日誌記錄保留，您也可以設定各日誌類型的儲存配額在總空間內的百分比。詳細資訊，請參閱管理日誌和報告儲存配額和到期日期。

STEP 2 | 確定平均每日日誌記錄速率。

在每天的高峰時期和非高峰時期執行數次以估算平均值。速率取樣越多，估算結果越準確。

1. 按日誌每秒顯示目前日誌產生速率：
   - 如果 Panorama 尚未收集日誌，存取各防火牆 CLI，執行下列命令，然後計算所有防火牆的總速率。此命令會顯示最後一秒接收的日誌數。

```
> debug log-receiver statistics
```

   - 如果 Panorama 已接收日誌，請在每個接收日誌的設備（Panorama 管理伺服器或專用日誌收集器）的 CLI 執行下列命令，並計算總速率。此命令給出了最後五分鐘的平均日誌速率。

```
> debug log-collector log-collection-stats show incoming-logs
```



您也可以使用 *SNMP* 管理員，判斷日誌收集器（查看 *panLogCollector MIB, OID 1.3.6.1.4.1.25461.1.1.6*）和防火牆（查看 *panDeviceLogging, OID 1.3.6.1.4.1.25461.2.1.2.7*）的日誌記錄速率。

2. 計算取樣速率的平均值。
3. 透過將平均每秒日誌乘以 86,400 以計算每日日誌記錄速率。

STEP 3 | 估算所需的儲存容量。



此算式提供的僅是估值；所需儲存容量的準確值與算式結果不同。

使用算式：

<required_storage_duration> x <average_log_size> x <average_logging_rate>

© 2019 Palo Alto Networks, Inc.

由於日誌類型的不同，日誌平均大小有很大的差異。但是，您可以 500 位元作為近似日誌平均大小。

例如，如果 Panorama 必須儲存日誌 30 天，所有防火牆的平均總日誌記錄速率為 21,254,400 個日誌每天，那麼所需的日誌儲存容量為：30 x 500 x 21,254,400 = 318,816,000,000 位元（約 318GB）。

STEP 4 | 接下來的步驟...

如果您決定 Panorama 需要更多日誌儲存容量：

- 擴展 Panorama 虛擬設備的日誌儲存容量。
- 增加 M-Series 設備的儲存容量。

© 2019 Palo Alto Networks, Inc.

設定 Panorama 虛擬設備

Panorama 虛擬設備可讓您利用現有的 VMware 虛擬基礎結構，以集中管理和監控 Palo Alto Networks 防火牆和專用日誌收集器。您可以在 ESXi 伺服器、Amazone Web Service（AWS）、AWS GovCloud、Microsoft Azure、Google Cloud Platform（GCP）、KVM、Hyper-V 上或 vCloud Air 中安裝虛擬設備。除了部署專用日誌收集器之外，您也可以將日誌直接轉送至 Panorama 虛擬設備。若要增加日誌儲存容量和更快產生報告，您可以選擇將虛擬設備從傳統模式切換至 Panorama 模式，並設定本機日誌收集器。如需 Panorama 虛擬設備及其模式的詳細資訊，請參閱 Panorama 型號。

這些主題假設您熟悉建立虛擬設備所需的公共和私密 *VMware* 產品，不涵蓋任何相關概念或術語。

- 設定 Panorama 虛擬設備的先決條件
- 安裝 Panorama 虛擬設備
- 執行 Panorama 虛擬設備的初始設定
- 設定 Panorama 虛擬設備作為日誌收集器
- 設定具備本機日誌收集器的 Panorama 虛擬設備
- 在 Panorama 模式下設定 Panorama 虛擬設備
- 在僅管理模式下設定 Panorama 虛擬設備
- 擴展 Panorama 虛擬設備的日誌儲存容量
- 在 Panorama 虛擬設備上增加 CPU 和記憶體
- 在 Panorama 虛擬設備上增加系統磁碟
- 完成 Panorama 虛擬設備設定

設定 Panorama 虛擬設備的先決條件

在設定 Panorama 虛擬設備前完成下列工作：

- 使用瀏覽器存取 Palo Alto Networks 客戶支援網站並註冊Panorama。您需要用到訂購完成電子郵件中的 Panorama 序號。註冊 Panorama 後，您可以存取 Panorama 軟體下載頁面。
- 檢閱 支援的 Panorama Hypervisor 以確認 Hypervisor 滿足部署 Panorama 的最低需求。
- 如果您要將 Panorama 安裝在 VMware ESXi 伺服器，請確認伺服器符合 Panorama 虛擬設備的系統需求中列出的最低需求。下列需求適用於 Panorama 5.1 與更新版本。需求根據您要以 Panorama 模式還是僅管理模式執行虛擬設備而異。如需模式的詳細資訊，請參閱 Panorama 型號。

  如果您將 *Panorama* 安裝在 *VMware vCloud Air*，則必須在安裝期間進行系統設定。

檢閱在 Amazon Web Services (AWS)、AWS GovCloud、Microsoft Azure、Google Cloud Platform (GCP)、Hyper-V、KVM 和 VMware ESXi 上部署 Panorama 虛擬設備的最低資源需求，以確保虛擬機器滿足所需模式（Panorama、僅管理或日誌收集器）的最低必要資源。Panorama 虛擬設備的最低資源需求是為了協助您在 Panorama 及日誌收集器模式收集日誌時，達成最大每秒日誌數 (LPS)。如果新增或移除虛擬日誌記錄磁碟導致組態不符合或超過所建議的虛擬日誌記錄磁碟數（參見下文），您的 LPS 將會降低。

如果 安裝 Panorama 虛擬設備 時未滿足 Panorama 的最低資源需求，Panorama 針對所有支援的公共（AWS、AWS GovCloud、Azure 和 GCP）和私人 Hypervisor（Hyper-V、KVM 和 VMware ESXi）預設為僅管理模式。如果不滿足僅管理模式的最低資源需求，Panorama 針對所有支援的公共 Hypervisor、Hyper-V 和 KVM 預設為維護模式。如果 在 VMware 上安裝 Panorama 時未滿足僅管理模式的最低資源需求，Panorama 預設為傳統模式。

© 2019 Palo Alto Networks, Inc.

建議在 *Panorama* 模式下部署 *Panorama* 管理伺服器，以實現裝置管理和日誌收集功能。雖然傳統模式仍受支援，但是建議不要在生產環境中使用。此外，無法再將 *Panorama* 切換至傳統模式。如需受支援模式的詳細資訊，請參閱 Panorama 型號。

表 1: **Panorama** 虛擬設備的系統需求

需求	僅管理模式下的 Panorama 虛擬設備	Panorama 模式的 Panorama 虛擬設備	日誌收集器模式下的 Panorama 虛擬設備
虛擬硬體版本	• **VMware ESXi** 及 **vCloud Air**—64 位元核心 VMware ESXi 5.5、6.0、6.5 或 6.7。ESXi 伺服器上支援的虛擬硬體系列類型版本（也被稱為 VMware 虛擬硬體版本）為 vmx-10。 • **Hyper-V**—Windows Server 2016 與 Hyper-V 角色或 Hyper-V 2016 • **KVM**—Ubuntu 版本 16.04 或 CentOS7 在 Panorama 模式中，任何 ESXi 版本上執行的虛擬設備最多支援 12 個虛擬日誌記錄磁碟，各有 2TB 的日誌儲存空間，合計容量最多為 24TB。 （僅限 VMware ESXi 及 vCloud Air）在傳統模式中，虛擬設備支援一個虛擬日誌記錄磁碟。ESXi 5.5 及更新版本支援一個最多 8TB 的磁碟。較早 ESXi 版本支援一個最多 2TB 的磁碟。		
（僅限 ESXi 及 vCloud Air） 用戶端電腦	若要安裝 Panorama 虛擬設備和管理其資源，您必須安裝與 ESXi 伺服器相容的 VMware vSphere 用戶端或 VMware 基礎結構用戶端。		
系統磁碟	• **Default**（預設值）—81GB • **Upgraded**（已升級）—224GB	• **Default**（預設值）—81GB • **Upgraded**（已升級）—224GB（SD-WAN 必備） 在日誌儲存方面，Panorama 使用虛擬日誌記錄磁碟，而非系統磁碟或 NFS 資料存放。	81GB 在日誌儲存方面，Panorama 使用虛擬日誌記錄磁碟，而非系統磁碟或 NFS 資料存放。

CPU、記憶體、虛擬日誌記錄磁碟	• 管理多至 500 個受管理的裝置
	  • 16 個 CPU
	  • 32GB 記憶體
	  • 不支援本機日誌儲存空間
	• 管理多至 1,000 個受管理的裝置
	  • 32 個 CPU
	  • 128GB 記憶體
	  • 不支援本機日誌儲存空間
	• 若要管理超過 1,000 個受管理的裝置，請參閱 增加的設備管理容量需求。
		• 多至 10,000 個日誌/秒：
		  • 16 個 CPU
		  • 32GB 記憶體
		  • 4 個 2TB 日誌記錄磁碟
		  • 管理多至 500 個受管理的裝置
		• 多至 20,000 個日誌/秒
		  • 32 個 CPU
		  • 128GB 記憶體
		  • 8 個 2TB 日誌記錄磁碟
		  • 管理多至 1,000 個受管理的裝置
			• 多至 15,000 個日誌/秒
			  • 16 個 CPU
			  • 32GB 記憶體
			  • 4 個 2TB 日誌記錄磁碟
			• 多至 25,000 個日誌/秒
			  • 32 個 CPU
			  • 128GB 記憶體
			  • 8 個 2TB 日誌記錄磁碟

© 2019 Palo Alto Networks, Inc.

需求	僅管理模式下的 Panorama 虛擬設備	Panorama 模式的 Panorama 虛擬設備	日誌收集器模式下的 Panorama 虛擬設備
日誌儲存容量	僅管理模式下的 Panorama 需要日誌轉送至專用日誌收集器。	2TB 至 24TB	2TB 至 24TB

支援的介面

介面可用於裝置管理、日誌收集、收集器群組通訊、授權和軟體更新。

功能	Amazon Web Services (AWS) 和 AWS GovCloud	Microsoft Azure	Google Cloud Platform (GCP)	KVM	Hyper-V	VMware (ESXi、vCloud Air)
裝置管理	任何支援的介面					
裝置日誌收集	任何支援的介面					
收集器群組通訊	任何支援的介面					
授權和軟體更新	僅限 MGT 介面	僅限 MGT 介面	僅限 MGT 介面	僅限 MGT 介面	任何支援的介面	任何支援的介面	任何支援的介面

安裝 Panorama 虛擬設備

在安裝之前，請決定是否要在 Panorama 模式、僅管理模式、日誌收集器模式或傳統模式（僅限 VMware）中執行虛擬設備。每個模式都有不同的資源需求，如設定 Panorama 虛擬設備的先決條件中所述。開始安裝之前，您必須完成先決條件。

最佳作法是以 *Panorama* 模式安裝虛擬設備，才會以最佳方式儲存日誌和產生報告。如需 *Panorama* 和傳統模式的詳細資訊，請參閱Panorama 型號。

- 在 VMware 上安裝 Panorama
- 在 AWS 上安裝 Panorama
- 在 AWS GovCloud 上安裝 Panorama
- 在 Azure 上安裝 Panorama
- 在 Google Cloud Platform 上安裝 Panorama
- KVM 上安裝 Panorama
- 在 Hyper-V 上安裝 Panorama

在 *VMware* 上安裝 *Panorama*

您可以在 ESXi 和 vCloud Air VMware 平台上安裝 Panorama 虛擬設備。

- 在 ESXi 伺服器上安裝 Panorama
- 在 vCloud Air 上安裝 Panorama
- Panorama 虛擬設備上的 VMware 工具支援

© 2019 Palo Alto Networks, Inc.

在 ESXi 伺服器上安裝 Panorama

使用這些指示在 VMware ESXi 伺服器上安裝新的 Panorama 虛擬設備。如果要升級現有 Panorama 虛擬設備，請跳至安裝 Panorama 的內容與軟體更新。

STEP 1 | 下載 Panorama 10.0 基本映像 Open Virtual Appliance (OVA) 檔案。

1. 前往 Palo Alto Networks 軟體下載網站。（如果無法登入，則前往 Palo Alto Networks 客戶支援網站尋求幫助。）
2. 在 Panorama 基本映像部分的下載欄中，下載 Panorama 最新版 OVA 檔案（`Panorama-ESX-10.0.0.ova`）。

STEP 2 | 安裝 Panorama。

1. 啟動 VMware vSphere Client 並連線至 VMware 伺服器。
2. 選取 **File**（檔案）> **Deploy OVF Template**（部署 **OVF** 範本）。
3. **Browse**（瀏覽）選取 Panorama OVA 檔案並按一下 **Next**（下一步）。
4. 確認產品名稱與描述符合下載的版本，然後按一下 **Next**（下一步）。
5. 輸入 Panorama 虛擬設備的描述性名稱，再按一下 **Next**（下一步）。
6. 選取資料存放位置（系統磁碟）來安裝 Panorama 映像。請參閱 設定 Panorama 虛擬設備的先決條件 瞭解受支援的系統磁碟大小。選取資料存放之後，按 **Next**（下一步）。
7. 選取 **Thick Provision Lazy Zeroed**（重量型佈建延遲歸零）做為磁碟格式，再按一下 **Next**（下一步）。
8. 指定清查中的哪些網路用於 Panorama 虛擬設備，然後按 **Next**（下一步）。
9. 確認選取的選項，按一下 **Finish**（完成）開始安裝程序，完成時按一下 **Close**（關閉）。還不要開啟 Panorama 虛擬設備的電源。

STEP 3 | 在 Panorama 虛擬設備上設定資源。

1. 右鍵按一下 Panorama 虛擬設備並 **Edit Settings**（編輯設定）。
2. 在 **Hardware**（硬體）設定中，依需要配置 CPU 和記憶體。

   如果您配置足夠的 *CPUs* 和 *Memory*（記憶體），並新增虛擬日誌記錄磁碟（此程序中稍後），虛擬設備會以 *Psnorama* 模式啟動。否則，設備會以「僅管理」模式啟動。如需模式的詳細資訊，請參閱 Panorama 型號。
3. 設定 **SCSI Controller**（**SCSI** 控制器）為 **LSI Logic Parallel**（**LSI Logic** 並行）。
4. 新增虛擬日誌記錄磁碟。

   下列狀況中需要此步驟：

   - 在 *Panorama* 模式下，將日誌儲存在專用日誌記錄磁碟上。
   - 在 *Management Only*（僅限管理）模式下管理您的 *SD-WAN* 部署。

   1. **Add**（新增）磁碟，選取 **Hard Disk**（硬碟）作為硬體類型，然後按 **Next**（下一步）。
   2. **Create a new virtual disk**（建立新虛擬磁碟），然後按一下 **Next**（下一步）。
   3. 將 **Disk Size**（磁碟大小）設定為剛好 2TB。

      在 *Panorama* 模式中，您稍後可以 add additional logging disks（新增額外日誌記錄磁碟）（共 *12* 個），儲存空間各為 *2TB*。不支援擴展已新增至 *Panorama* 的日誌記錄磁碟大小。
   4. 選取您偏好的 **Disk Provisioningg**（磁碟佈建）磁碟格式。

      選取磁碟佈建格式時，請考量您的業務需求。如需關於磁碟佈建效能考量的更多資訊，請參閱 VMware 重量型與輕量型磁碟及所有快閃陣列文件，或其他 VMware 文件。

© 2019 Palo Alto Networks, Inc.

新增多個日誌記錄磁碟時，最佳做法是對於所有磁碟皆選取相同的 *Disk Provisioning*（磁碟佈建）格式，以避免任何可能發生的非預期效能問題。

5. 選取 **Specify a datastore or datastore structure**（指定資料存放或資料存放結構）作為位置，**Browse**（瀏覽）至有足夠儲存空間的資料存放，按一下 **OK**（確定），然後按 **Next**（下一步）。
6. 選取 SCSI **Virtual Device Node**（虛擬設備節點）（您可以使用預設選項），然後按一下 **Next**（下一步）。

   如果您選取 *SCSI* 以外的格式，*Panorama* 無法啟動。

7. 確認設定正確，然後按一下 **Finish**（完成）。

5. 按一下 **OK**（確定）儲存您的變更。

STEP 4 | 開啟 Panorama 虛擬設備電源。

1. 在 vSphere 用戶端中，右鍵按一下 Panorama 虛擬設備並選取 **Power**（電源）> **Power On**（開啟電源）。等到 Panorama 啟動之後再繼續。
2. 確認虛擬設備以正確模式執行：
   1. 右鍵按一下 Panorama 虛擬設備並選取 **Open Console**（開啟主控台）。
   2. 輸入您的使用者名稱和密碼以登入（兩者都預設為 **admin**）。
   3. 執行下列命令來顯示模式：

```
> show system info
```

   在輸出中，`system-mode` 會指出 `panorama` 或 `management-only` 模式。

STEP 5 | 為 ESXi 伺服器上的 Panorama 增加系統磁碟 如果您意欲使用 Panorama 虛擬設備進行下列事項：

- 在 Panorama 模式下管理您的 SD-WAN 部署。
- 管理大規模防火牆部署時，需要額外儲存空間以用於動態更新。

您現在可以執行 Panorama 虛擬設備的初始設定。

在 vCloud Air 上安裝 Panorama

使用這些指示在 VMware vCloud Air 內安裝新的 Panorama 虛擬設備。如果您正在升級 vCloud Air 內部署的 Panorama 虛擬設備，跳至安裝 Panorama 的內容與軟體更新。

STEP 1 | 下載 Panorama 10.0 基本映像 Open Virtual Appliance (OVA) 檔案。

1. 前往 Palo Alto Networks 軟體下載網站。（如果無法登入，則前往 Palo Alto Networks 客戶支援網站尋求幫助。）
2. 在 Panorama 基本映像部分的下載欄中，下載 Panorama 10.0 版 OVA 檔案（`Panorama-ESX-10.0.0.ova`）。

STEP 2 | 匯入 Panorama 映像至 vCloud Air 目錄。

關於這些步驟的詳細資訊，請參參閱OVF 工具使用者指南。

1. 在您的用戶端系統上安裝 OVF 工具。
2. 存取用戶端系統 CLI。
3. 導覽至 OVF 工具的目錄（例如：C:\Program Files\VMware\VMware OVF Tool）。
4. 將 OVA 檔案轉換成 OVF 套件:

© 2019 Palo Alto Networks, Inc.

```
ovftool.exe <OVA-file-pathname> <OVF-file-pathname>
```

5. 使用瀏覽器存取 vCloud Air web 主控台，選取您的 **Virtual Private Cloud OnDemand**（虛擬私人雲 **OnDemand**），然後記錄瀏覽器上的 URL。您將使用該 URL 資訊完成下一步。The URL format is: **`https://<virtual-cloud-location>.vchs.vmware.com/compute/cloud/org/<vCloud-account-number>/#/catalogVAppTemplateList?catalog=<catalog-ID>`**.
6. 匯入 OVF 套件，使用 vCloud Air URL 資訊完成 <virtual-cloud-location>、<vCloud-account-number> 和 <catalog-ID> 變數。其他變數是您的 vCloud Air 使用者名稱和網域 <user>@<domain>、虛擬資料中心 <datacenter> 和vCloud Air 範本 <template>。

```
ovftool.exe -st="OVF" "<OVF-file-pathname>"
 "vcloud://<user>@<domain>:password@<virtual-cloud-
location>.vchs.vmware.com?vdc=<datacenter>&org=<vCloud-account-
number>&vappTemplate=<template>.ovf&catalog=default-catalog"
```

STEP 3 | 安裝 Panorama。

1. 存取 vCloud Air web 主控台並選取您的 **Virtual Private Cloud OnDemand**（虛擬私人雲 **OnDemand**）地區。
2. 建立 Panorama 虛擬機器。關於此步驟，請參閱在 vCloud Air 文件中心的範本內新增虛擬機器。設定 **CPU**、**Memory**（記憶體）和 **Storage**（儲存）如下：
   - 基於虛擬設備模式設定 **CPU** 和 **Memory**（記憶體）：請參閱 設定 Panorama 虛擬設備的先決條件。
   - 設定 **Storage**（儲存空間）以設定 Panorama 虛擬設備系統磁碟。有關基於 Panorama 虛擬設備模式支援的磁碟大小，請參閱 設定 Panorama 虛擬設備的先決條件。為了更好地記錄和報告效能，選取 **SSD-Accelerated**（**SSD** 加速）選項。

     若要增大日誌存儲容量，您必須新增虛擬磁碟至 vCloud Air 上的 Panorama。在 Panorama 模式中，虛擬設備不使用系統磁碟來儲存日誌；您必須新增虛擬日誌記錄磁碟。

STEP 4 | 在網關上建立 vCloud Air NAT 規則，允許 Panorama 虛擬設備的輸入輸出流量。

參考 vCloud Air 文件中心內的新增 NAT 規則，獲得詳細說明：

1. 新增 NAT 規則，允許 Panorama 接收來自防火牆的流量，並允許管理員存取 Panorama。
2. 新增 NAT 規則，允許 Panorama 從 Palo Alto Networks 更新伺服器擷取更新，並存取防火牆。

STEP 5 | 建立 vCloud Air 防火牆規則，允許 Panorama 虛擬設備上的輸入流量。

輸出流量預設為允許。

參考 vCloud Air 文件中心內的新增防火牆規則，獲得詳細說明。

STEP 6 | 如未啟動，開啟 Panorama 虛擬設備。

在 vCloud Air web 主控台內，選取 **Virtual Machines**（虛擬電腦）頁籤，選取 Panorama 虛擬機器，然後按一下 **Power On**（開啟電源）。

您現在可以執行 Panorama 虛擬設備的初始設定。

Panorama 虛擬設備上的 VMware 工具支援

VMware 工具與 Panorama 虛擬設備的軟體映像 (ovf) 一起搭售。對 VMware 工具的支援可讓您使用 vSphere 環境（vCloud Director 和 vCenter 伺服器）進行以下操作：

- 檢視指派給 Panorama 管理伺服器的 IP 位址。

© 2019 Palo Alto Networks, Inc.

- 檢視硬碟、記憶體及 CPU 的資源使用率標準。您還可以在 vCenter 伺服器或 vCloud Director 上使用這些指標來啟用警報或動作。
- 使用 vCenter 伺服器或 vCloud Director 上的電源關閉功能原則關閉或重新啟動 Panorama。
- 在 vCenter 伺服器和 Panorama 之間啟用活動訊號機制，以確認 Panorama 在原則運作或者確認防火牆/Panorama 是否在重新開機。如果防火牆進入維護模式，活動訊號將被停用，以便 vCenter 伺服器不會關閉防火牆。當防火牆處於維護模式時，無法向 vCenter 伺服器傳送活動訊號，而停用活動訊號可以讓防火牆保持運作。

在 *AWS* 上安裝 *Panorama*

您可以立即在 Amazon Web Services（AWS）部署 Panormama™ 和專用日誌收集器。Panorama 部署在 AWS 上的授權為自帶授權（BYOL），支援所有部署的模式（Panorama、日誌收集器和僅管理），且與 M-Series 硬體設備一樣共享相同的程序與功能。如需 Panorama 模式的詳細資訊，請參閱 Panorama 型號。

STEP 1 | 登入 AWS Web 服務主控台，然後選取 EC2 儀表板。

- Amazon Web 服務主控台
- AWS GovCloud Web 服務主控台

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 Panorama 虛擬設備，還是建立新的 VPC，Panorama 虛擬設備都必須能夠從 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。

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 Panorama 虛擬設備，則 VPC 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。Panorama 虛擬設備必須屬於公共子網路，才能設定它來存取網際網路。
   - 視需建立安全性群組，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，以確定路由流量可在 VPC 中整個子網路與安全性群組之間路由（若適當的話）。

STEP 3 | 在 Amazon Web Service 上部署 Panorama。

1. 在 EC2 儀表板中，按一下 **Instances**（實例）> **Launch Instance**（啟動實例）。
2. 選取 **AWS Marketplace**（**AWS** 市場），搜尋 **`Palo Alto Networks Panorama`**，並 **Select**（選取）Panorama AMI，然後 **Continue**（繼續）。
3. 選取 **EC2 instance type**（**EC2** 實例類型），以配置 Panorama 虛擬設備所需的資源，然後按 **Next**（下一步）：**Configure Instance Details**（設定實例詳細內容）。檢閱 設定 Panorama 虛擬設備的先決條件 瞭解最低資源需求。

   若您計劃使用 *Panorama* 虛擬設備作為專用日誌收集器，請確定將設備設定為在原始部署時擁有必要的資源。*Panorama* 虛擬設備若在您部署虛擬電腦後重新調整其大小，則不會仍舊維持日誌收集器模式，且會造成日誌資料的丟失。
4. Configure Instance Details（設定實例詳細內容）。
   1. 選取 **Next:Configure Instance Details**（設定實例詳細內容）。
   2. 選取您在上一步中建立的 **Network**（網路），或使用 AWS 所提供的預設 VPC。如果
   3. 選取您在上一步中建立的 **Subnet**（子網路），或使用 AWS 所提供的預設子網路。
   4. 若要 **Auto-assign Public IP**（自動指派公用 **IP**），請選取 **Enable**（啟用）。

© 2019 Palo Alto Networks, Inc.

您計劃使用 Panorama 管理的防火牆必須可以存取此 IP。這可讓您為 Panorama 虛擬設備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虛擬設備中斷關聯，彈性 IP 位址提供持續性，並可以將 IP 位址連線到 Panorama 虛擬設備的全新（或取代）實例，且無需在 Panorama 虛擬設備實例關閉時重新設定 IP 位址。

5. 視需要設定任何額外實例詳細內容。

5. 設定 Panorama 虛擬設備儲存空間。

   1. 選取 **Next:Add Storage**（下一步：新增儲存空間）。
   2. 檢閱 Root 系統磁碟大小並且確定您是否需要擴展至 224GB 系統磁碟。視需要將系統磁碟 **Size**（大小）增加至 224GB。

      為了支援大型資料集，管理大規模防火牆部署 需要 224GB 系統磁碟空間，以便有足夠的磁碟空間儲存用於動態更新等內容。

      （僅限 SD-WAN）如果您意欲使用處於 Panorama 模式的 Panorama 虛擬設備管理您的 SD-WAN 部署，224GB 系統磁碟將擴展儲存空間，以儲存受管理防火牆健康的管控和報告資料。

      如果您將 *Panorama* 虛擬設備實例部署為 *224GB* 系統磁碟，則未來將無法移轉至較小的系統磁碟。

   3. **Add New Volume**（新增新的磁碟區）以新增額外的日誌儲存空間。

      （僅限 SD-WAN）如果您計劃在 Management Only（僅限管理）模式中管理您的 SD-WAN 部署，您必須新增 2TB 日誌記錄磁碟。

      若您想要以 Panorama 模式或作為專用日誌收集器來使用 Panorama 虛擬設備，請在原始部署時新增虛擬日誌記錄磁碟。依預設，當符合 Panorama 模式資源需求並已新增至少一個虛擬日誌記錄磁碟，Panorama 虛擬設備在原始部署時為 Panorama 模式。否則，Panorama 虛擬設備預設為僅管理模式。若您只想要管理裝置與專用日誌收集器，且不要收集本機日誌，則變更 Panorama 虛擬設備為僅管理模式。

      AWS 上的 Panorama 虛擬設備僅支援 2TB 日誌記錄磁碟，並總計支援最高 24TB 的日誌儲存空間。您無法新增小於 2TB 的日誌記錄磁碟，或日誌記錄磁碟大小無法被 2TB 日誌記錄需求整除。Panorama 虛擬設備將大於 2TB 的日誌記錄磁碟分割在 2TB 分割區。

6. （選用）選取 **Next:Add Tags**（下一步：新增標籤），並新增一個或多個標籤作為中繼資料，以協助您識別並分組 Panorama 虛擬設備。舉例來說，新增一個 **Name**（名稱）標籤，其 **Value**（值）會協助您識別哪一個才是 Panorama 虛擬設備管理的防火牆。
7. 設定實例安全性群組。

   1. 選取 **Next:Configure Security Group**（下一步：設定安全性群組）。
   2. 建立新的 **Security Group**（安全性群組）或選取附有至少已啟動 HTTPS 和 SSH 的現有群組。此安全性群組適用於限制存取管理介面。

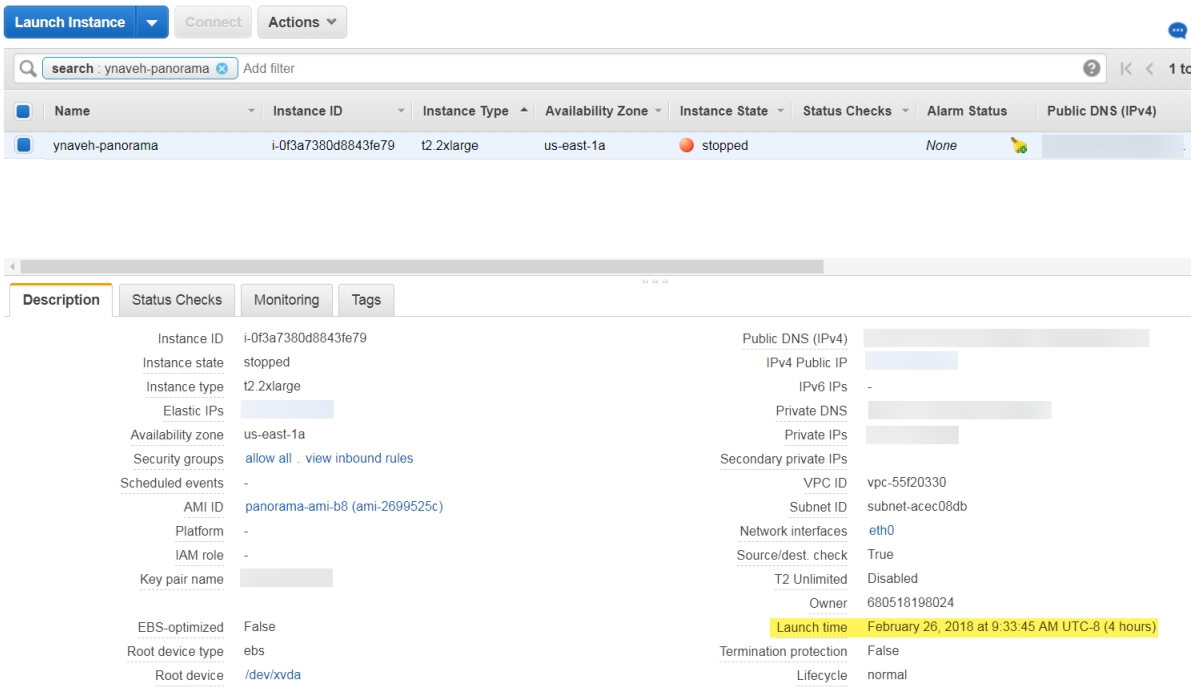
8. 選取 **Review and Launch**（複查並啟動）Panorama 虛擬設備實例，然後在 **Launch**（啟動）前確定您的選項正確。
9. 選取現有的金鑰配對或建立新的金鑰配對，並同意免責聲明。

   若您從 *AWS* 建立了一個新金鑰，請下載並儲存此金鑰到一個安全的地點。此檔案的副檔名為 *.pem*。您必須將公共金鑰載入至 PuTTYgen 並且以 *.ppk* 格式儲存。此金鑰如果遺失，您無法重新產生此金鑰。

在您在 AWS 上啟動 Panorama 虛擬設備後，部署需要約 30 分鐘。部署 Panorama 虛擬設備可能會花費較長的時間，依據連接至實例的磁碟數目與尺寸而定。透過選取 Panorama 虛擬設備實例（**Instances**）來檢視啟動時間。

© 2019 Palo Alto Networks, Inc.



若您計劃使用 *Panorama* 虛擬設備作為專用日誌收集器，則請確定您的設備擁有必要的資源。*Panorama* 虛擬設備若在您部署虛擬電腦後重新調整其大小，則不會仍舊維持日誌收集器模式，且會造成日誌資料的丟失。

STEP 4 | 關閉 Panorama 虛擬設備電源。

1. 在 EC2 儀表板中，選取 **Instances**（實例）。
2. 選取 Panorama 虛擬設備，然後按一下 **Actions**（動作）> **Instance State**（實例狀況）> **Stop**（停止）。

STEP 5 | 建立或指派彈性 IP（EIP）位址以管理介面。

1. 在 AWS 主控台中，選取 **Elastic IP**（彈性 IP）然後 **Allocate New Address**（配置新位址）。
2. 按一下 **Allocate**（配置）以生成新的 EIP 位址，按一下 **Actions**（行動）與 **Associate address**（相關位址）。
3. 選用 **Instance**（實例）選用指派給 EIP 位址的 Panorama 虛擬設備實例，並輸入與管理實例有關的 **Private IP address**（私人 **IP** 位址），然後按一下 **Associate**（關聯）。

STEP 6 | 開啟 Panorama 虛擬設備電源。

1. 在 EC2 儀表板中，選取 **Instance**（實例）。
2. 從清單上選取 Panorama 虛擬設備，然後按一下 **Actions**（動作）> **Instance State**（執行個體狀態）> **Start**（開啟）。

STEP 7 | 設定 Panorama 虛擬設備的新管理密碼。

您必須在存取 Panorama 虛擬設備的網頁介面前設定唯一管理密碼。要存取 CLI，則不可缺少用來啟動 Panorama 虛擬設備的金鑰。

- 若您在電腦安裝了 SSH 服務：

1. 輸入下列命令，以登入 Panorama 虛擬設備：

```
ssh -i <private_key.ppk> admin@<public-ip_address>
```


© 2019 Palo Alto Networks, Inc.

2. 使用下列命令設定新密碼，並依照畫面上的提示進行：

```
admin> configure
admin# set mgt-config users admin password
```

3. 如果需要啟動 BYOL，請設定 DNS 伺服器 IP 位址，以便 Panorama 虛擬設備可存取 Palo Alto Networks 授權伺服器。輸入下列命令設定 DNS 伺服器 IP 位址：

```
admin# set deviceconfig system dns-setting servers primary <ip_address>
```

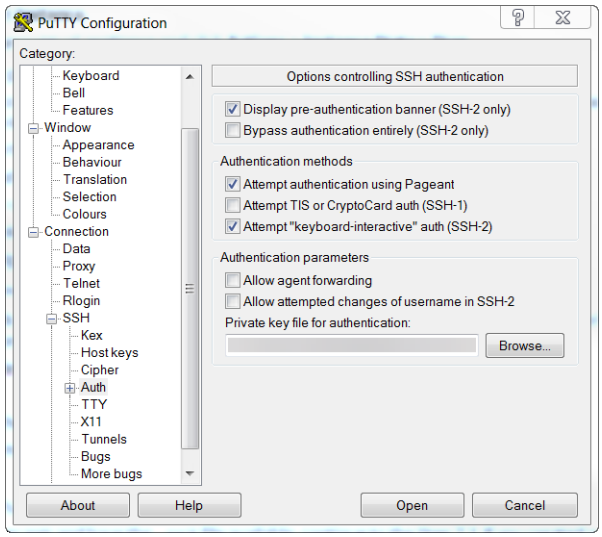
4. 使用下列命令提交變更：

```
admin# commit
```

5. 終止 SSH 工作階段。

- 若您使用 PuTTY 連至 Panorama 虛擬設備內的 SSH：

1. 若您使用現有金鑰配對且有可用的 `.ppk`檔，請繼續步驟 7.3。若您建立新的金鑰配對或在現有金鑰配對中僅有 `.pem` 檔，則請開啟 PuTTYgen 並 **Load**（載入） `.pem` 檔。
2. **Save the private key**（儲存私人金鑰）到本機可存取的目的地。
3. 開啟 PuTTY 並選取上一步儲存的 `.ppk` 檔的 **SSH** > **Auth**（驗證），然後進行 **Browse**（瀏覽）。



4. 選取 **Sessions**（工作階段）並輸入 Panorama 虛擬設備的公共 IP 位址。在安全提示出現時，按一下 **Open**（開啟）並按一下 **Yes**（是）。
5. 在提示時，以管理員登入。
6. 使用下列命令設定新密碼，並依照畫面上的提示進行：

```
admin> configure
admin# set mgt-config users admin password
```

7. 請設定 DNS 伺服器 IP 位址，以便 Panorama 虛擬設備可存取 Palo Alto Networks 授權伺服器。輸入下列命令設定 DNS 伺服器 IP 位址：

```
admin# set deviceconfig system dns-setting servers primary <ip_address>
```

8. 使用下列命令提交變更：

© 2019 Palo Alto Networks, Inc.

```
admin# commit
```

9. 終止 SSH 工作階段。

STEP 8 | 啟用裝置管理授權並支援在 Panorama 虛擬設備上的授權。

- 在 Panorama 虛擬設備與網際網路連線時，啟動/擷取防火牆管理授權
- 在 Panorama 虛擬設備並未與網際網路連線時，啟動/擷取防火牆管理授權
- 啟動 Panorama 支援授權

STEP 9 | 完成部署需要的 Panorama 虛擬設備設定。

- （僅管理模式）在僅管理模式下設定 Panorama 虛擬設備。
- （日誌收集器模式）在步驟 6 開始從 Panorama 模式切換為日誌收集器模式。

  在您將日誌收集器作為受管理的收集器新曾到 *Panorama* 管理伺服器時，輸入專用日誌收集器的公共 *IP* 位址。您無法指定 *IP* 位址、網路遮罩或 網閘。
- （僅限 Panorama 和管理模式）設定受管理收集器 以新增專用日誌收集器到 Panorama 虛擬設備。僅管理模式不支援本機日誌收集，且需要專用日誌收集器以儲存受管理的裝置日誌。

在 *AWS GovCloud* 上安裝 *Panorama*

您可以立即在 Amazon Web Services (AWS) GovCloud 上部署 Panormama™ 和專用日誌收集器。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。Panorama 部署在 AWS GovCloud 上為自帶授權 (BYOL)，支援所有部署模式（Panorama、日誌收集器和僅管理）。如需 Panorama 模式的詳細資訊，請參閱 Panorama 型號。

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，Panorama 虛擬設備在標準 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 Panorama 虛擬設備支援相同的特性與功能。

檢閱 設定 Panorama 虛擬設備的先決條件 查看支援的 EC2 實例類型。就緒後，參閱 在 AWS 上安裝 Panorama，在 AWS GovCloud 上安裝 Panorama 虛擬設備。

請參閱下列程序，以新增其他日誌紀錄儲存空間至 Panorama 虛擬設備，或增加配置的 CPU 核心與記憶體：

- 新增虛擬磁碟至 AWS 上的 Panorama
- 為 AWS 上的 Panorama 增加 CPU 和記憶體

在 *Azure* 上安裝 *Panorama*

您可以立即在 Microsoft Azure 部署 Panormama™ 和專用日誌收集器。Panorama 部署在 Azure 上的授權為自帶授權（BYOL），支援所有部署的模式（Panorama、日誌收集器和僅管理），且與 M-Series 硬體設備一樣共享相同的程序與功能。如需 Panorama 模式的詳細資訊，請參閱 Panorama 型號。

STEP 1 | 登入 Microsoft Azure 入口網站。

STEP 2 | 部署 Panorama 虛擬設備。

1. 在 Azure 儀表板中，選取 **Virtual machines**（虛擬電腦）並**Add**（新增）新的虛擬電腦。
2. 搜尋 Palo Alto Networks 並選取最新的 Panorama 虛擬設備映像。
3. **Create**（建立）Panorama 虛擬設備。

STEP 3 | 設定 Panorama 虛擬設備。

1. 選取 Azure **Subscription**（訂閱）。

© 2019 Palo Alto Networks, Inc.

2. 選取 Azure **Resource Group**（資源群組）以包含您的所有 Azure 實例資源。
3. 為 Panorama 虛擬設備輸入 **Virtual machine name**（虛擬機器名稱）。
4. 選取要部署 Panorama 虛擬設備的 **Region**（區域）。
5. （選用）選取 **Availability options**（可用性選項）。請參閱如何使用可用性設定組以瞭解詳細資料。
6. 選取用於部署 Panorama 管理伺服器的 **Image**（映像）。**Browse all public and private images**（瀏覽所有公用及私人映像）以從 Azure Marketplace 上的 Panorama 映像部署 Panorama 管理伺服器。
7. 重新設定 Panorama 虛擬設備的大小。檢閱 設定 Panorama 虛擬設備的先決條件 瞭解規模需求。

   若您計劃使用 *Panorama* 虛擬設備作為專用日誌收集器，請確定將設備設定為在原始部署時擁有必要的資源。*Panorama* 虛擬設備若在您部署虛擬電腦後重新調整其大小，則不會仍舊維持日誌收集器模式，且會造成日誌資料的丟失。
8. 輸入 Panorama 虛擬設備管理員的 **Username**（使用者名稱）。為確保您的使用者名稱的安全性，admin 並非有效輸入條目。
9. 輸入 **Password**（密碼）或複製並貼上 **SSH public key**（**SSH** 公共金鑰），保障 Panorama 虛擬設備的管理存取權。

   如果計劃在 *FIPS-CC* 操作模式中使用 *Panorama* 虛擬設備的此執行個體，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 *Panorama* 虛擬設備，但將操作模式變更為 *FIPS-CC* 之後，就無法以使用者名稱和密碼進行驗證。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 *Panorama Web* 介面。如需有關建立 *SSH* 金鑰的詳細資訊，請參閱 Azure 文件。
10. 設定 Panorama 虛擬設備實例 **Networking**（網路）
    1. 選取現有 **Virtual network**（虛擬網路）或建立新的虛擬網路。
    2. 設定 **Subnet**（子網路）。子網路依據您選取的或在之前步驟中所建立的虛擬網路。若您已選取現有的虛擬網路，則您可以為已選取的虛擬網路在此子網路中擇一使用。
    3. 選取現有的 **Public IP address**（公共 **IP** 位址）或建立新的位址。這會建立起用來存取 Panorama 虛擬設備的受管理的介面。
    4. 選取現有 **NIC network security group**（**NIC** 網路安全性群組）或建立新的安全性群組。網路安全性群組控制流向虛擬設備的流量。確定內送規則允許 HTTPS 和 SSH。
11. 設定實例 **Management**（管理）設定。
    1. 選取是否啟用 **Auto-shutdown**（自動關機）。自動關機讓您可以設定停用自動關閉功能虛擬設備每日自動關閉的時間，以避免新公共 IP 位址被指派給虛擬設備、日誌丟失、日誌並非所屬或您無法在 Panorama 虛擬設備關閉時管理防火牆的可能性。
    2. 選取是否啟用開啟 **Monitoring**（監控）。若啟用，則選取診斷儲存帳戶。自動監控傳送開機診斷日誌到您的診斷儲存帳戶。詳情請參閱 Microsoft Azure 監控概覽。
    3. 視需要設定其他設定。
12. 檢閱摘要，接受使用條款及隱私權原則，並 **Create**（建立）Panorama 虛擬設備。

STEP 4 | 確認已成功部署 Panorama 虛擬設備。

1. 選取 **Dashboard**（儀表板）> **Resource Groups**（資源群組），然後選取包含 Panorama 虛擬設備的資源群組。
2. 在設定下，選取虛擬電腦部署狀態的 **Deployments**（部置）。

   部署 *Panorama* 虛擬設備約需 *30* 分鐘。啟動 *Panorama* 虛擬設備可能需要較長的時間，依據虛擬設備設定的資源而定。*Microsoft Azure* 不允許 *ICMP* 協定測試其是否部署成功。

   若您計劃使用 *Panorama* 虛擬設備作為專用日誌收集器，則請確定您的設備已正確設定必要的資源。*Panorama* 虛擬設備若在您部署虛擬電腦後重新調整其大小，則不會仍舊維持日誌收集器模式，且會造成日誌資料的丟失。

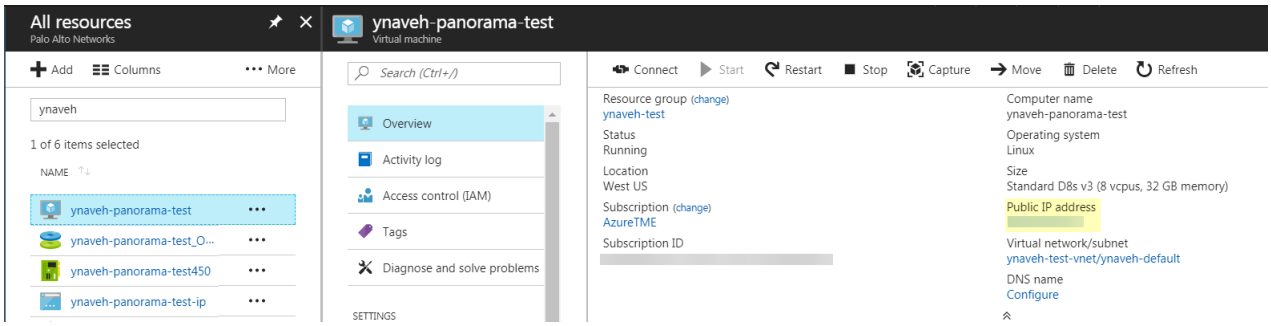
© 2019 Palo Alto Networks, Inc.

STEP 5 | 設定靜態公共 IP 位址。

1. 在 Azure 入口網站上，選取 **Virtual machines**（虛擬電腦），然後選取 Panorama 虛擬設備。
2. 選取 **Overview**（概覽）並按一下 **Public IP address**（公共 **IP** 位址）。
3. 在指派下，選取 **Static**（靜態） 並 **Save**（儲存）新的 IP 位址設定。

STEP 6 | 登入 Panorama 虛擬設備的 Web 介面。

1. 在 Azure 入口網站上，在 **All Resources**（所有資源）中，選取 Panorama 虛擬設備並檢視位於概覽部份的公共 IP 位址。



2. 從您的網路瀏覽器使用安全的（http）連線以使用公共 IP 位址登入 Panorama 虛擬設備。
3. 輸入 Panorama 虛擬設備的使用者名稱和密碼。您會接到一則憑證警告提示。接受憑證警告並設定網頁。

STEP 7 | 啟用裝置管理授權並支援在 Panorama 虛擬設備上的授權。

- 在 Panorama 虛擬設備與網際網路連線時，啟動/擷取防火牆管理授權
- 在 Panorama 虛擬設備並未與網際網路連線時，啟動/擷取防火牆管理授權
- 啟動 Panorama 支援授權

STEP 8 | 完成部署需要的 Panorama 虛擬設備設定。

（僅限 SD-WAN）如果您計劃在 Management Only（僅限管理）模式中管理您的 SD-WAN 部署，您必須新增 2TB 日誌記錄磁碟。

1. 新增虛擬磁碟至 Azure 上的 Panorama。依預設，81GB 系統磁碟會自動在原始部署期間建立。

   在您將 Panorama 虛擬設備變更為 Panorama 模式或日誌收集器模式時，必須新增虛擬日誌記錄磁碟。

   依預設，Azure 上的 Panorama 虛擬設備在原始部署時設定為僅管理模式。若您想要以 Panorama 模式或作為專用日誌收集器來使用 Panorama 虛擬設備，則在 Azure 上成功部署 Panorama 後新增虛擬日誌記錄磁碟。

   Azure 上的 Panorama 虛擬設備僅支援 2TB 日誌記錄磁碟，並總計支援最高 24TB 的日誌儲存空間。您無法新增小於 2TB 的日誌記錄磁碟，或日誌記錄磁碟大小無法被 2TB 日誌記錄需求整除。Panorama 虛擬設備將大於 2TB 的日誌記錄磁碟分割在 2TB 分割區。
2. 變更 Panorama 虛擬設備模式。

   依預設，Azure 上的 Panorama 虛擬設備設定為僅管理模式。若要變更至 Panorama 模式或日誌收集器模式，您必須在原始部署之後新增至少一個日誌記錄磁碟。若您只想要管理裝置與專用日誌收集器，且不要收集本機日誌，則變更 Panorama 虛擬設備為僅管理模式。

   - 在 Panorama 模式下設定 Panorama 虛擬設備。
   - （日誌收集器模式）在步驟 6 開始從 Panorama 模式切換為日誌收集器模式。

   在您將日誌收集器作為受管理的收集器新曾到 *Panorama* 管理伺服器時，輸入專用日誌收集器的公共 *IP* 位址。您無法指定 *IP* 位址、網路遮罩或 網閘。

© 2019 Palo Alto Networks, Inc.

3. （僅限 Panorama 和管理模式）設定受管理的收集器以新增專用日誌收集器到 Panorama 虛擬設備。僅管理模式不支援本機日誌收集，且需要專用日誌收集器以儲存受管理的裝置日誌。

在 Google Cloud Platform 上安裝 Panorama

您可以立即在 Google Cloud Platform (GCP) 部署 Panormama™ 和專用日誌收集器。Panorama 部署在 GCP 上的授權為自帶授權（BYOL），支援所有部署的模式（Panorama、日誌收集器和僅管理），且與 M-Series 硬體設備一樣共享相同的程序與功能。如需 Panorama 模式的詳細資訊，請參閱 Panorama 型號。

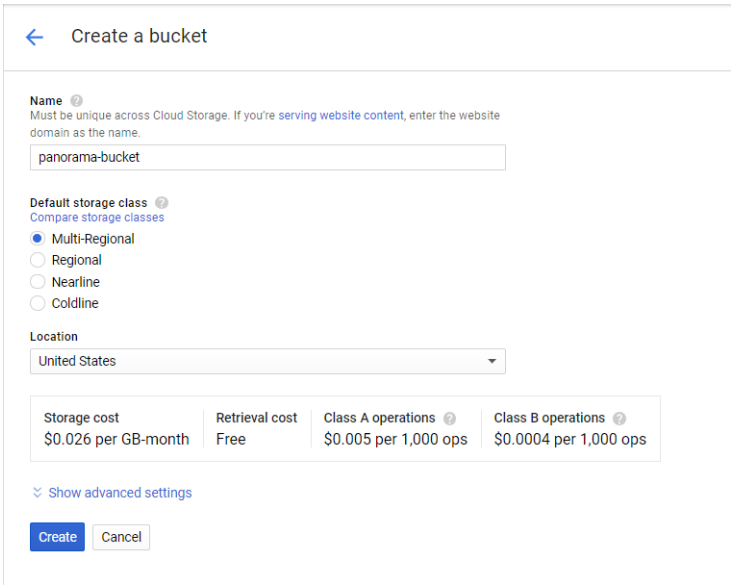
若要在 GCP 上部署 Panorama 虛擬設備，您需要建立自訂映像。若要開始此程序，您必須從 Palo Alto Networks 客戶支援入口網站下載 Panorama `tar.gz`，並將其上傳至 GCP 儲存空間。然後即可建立自訂映像，並使用映像在 GCP 上部署 Panorama 虛擬設備。

STEP 1 | 下載 Panorama 虛擬設備映像。

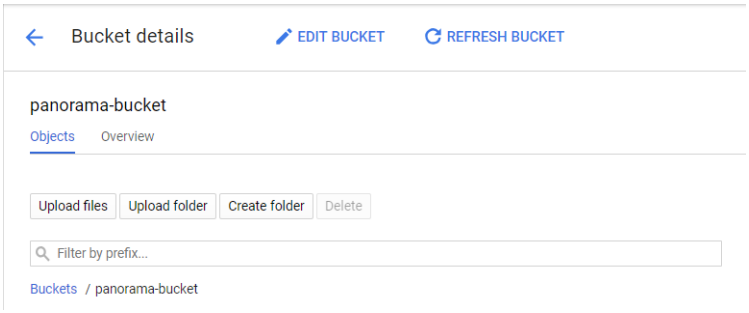
1. 登入 Palo Alto Networks Support 入口網站。
2. 選取 **Updates**（更新）> **Software Updates**（軟體更新），然後依 **Panorama Base Images**（**Panorama** 基本映像）篩選。
3. 在 GCP `tar.gz` 映像上下載最新版 Panorama。

STEP 2 | 上傳 Panorama 虛擬設備映像至 Google Cloud Platform。

1. 登入 Google Cloud 主控台。
2. 從 **Product and Service**（產品與服務）功能表中，選取 **Storage**（儲存空間）。
3. 按一下 **Create Bucket**（建立儲存空間），設定新的儲存空間，然後按一下 **Create**（建立）。

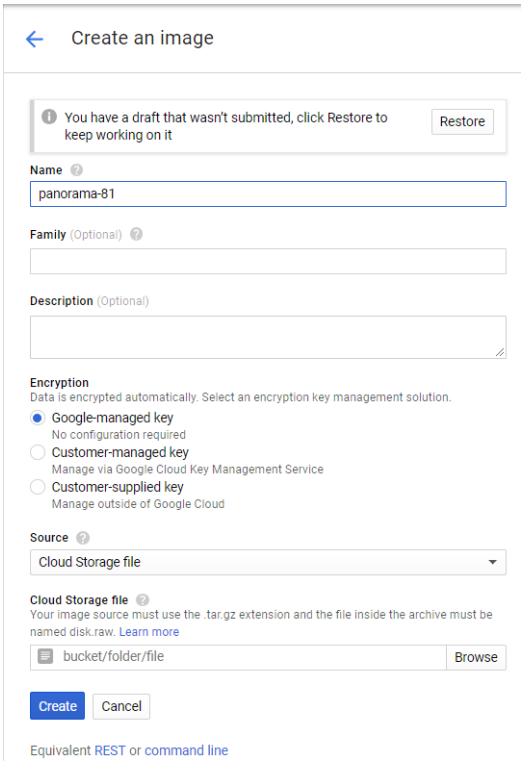


4. 選取您在上一步建立的儲存空間，按一下 **Upload files**（上傳檔案），然後選取您下載的 Panorama 虛擬設備。



© 2019 Palo Alto Networks, Inc.

5. 從 **Products and Services**（產品與服務）功能表中，選取 **Compute Engine**（計算引擎）> **Images**（映像）。
6. 按一下 **Create Image**（建立映像）並建立 Panorama 虛擬設備映像：
   1. **Name**（具名）Panorama 虛擬設備映像。
   2. 在 **Source**（來源）欄位，從下拉式選單中選取 **Cloud Storage file**（雲端儲存檔案）。
   3. 按一下 **Browse**（瀏覽）並導覽至您上傳 Panorama 虛擬設備映像的儲存空間，然後 **Select**（選取）上傳的映像。
   4. **Create**（建立）Panorama 虛擬設備映像。



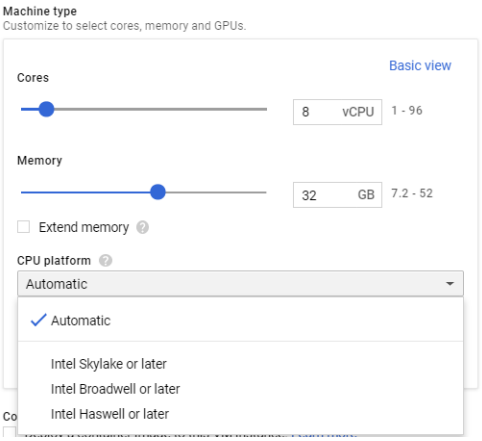
STEP 3 | 設定 Panorama 虛擬設備。

1. 從 **Products and Services**（產品與服務）功能表中，選取 **Compute Engine**（計算引擎）。
2. 按一下 **Create Instance**（建立實例），開始部署 Panorama 虛擬設備。
3. 新增說明性 **Name**（名稱）以輕鬆識別 Panorama 虛擬設備。
4. 選取您想要部署 Panorama 虛擬設備的 **Region**（地區）和 **Zone**（區域）。
5. 配置 **Machine Type**（機器類型）並 **Customize**（自訂）CPU 核心、記憶體和 CPU 平台。檢閱 設定 Panorama 虛擬設備的先決條件 瞭解最低資源需求。

若您計劃使用 *Panorama* 虛擬設備作為專用日誌收集器，請確定將設備設定為在原始部署時擁有必要的資源。*Panorama* 虛擬設備若在您部署虛擬電腦後重新調整其大小，則不會仍舊維持日誌收集器模式，且會造成日誌資料的丟失。

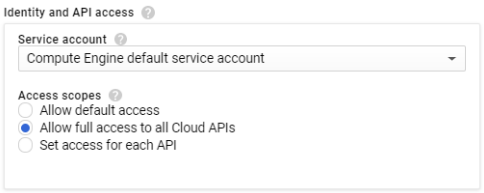
GCP 區域選取確定您可使用的 *CPU* 平台。如需更多資訊，請參閱 Regions and Zones（地區和區域）瞭解詳情。

© 2019 Palo Alto Networks, Inc.

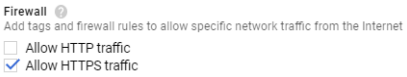


6. 設定 Panorama 啟動磁碟。
   1. 對於 **Boot Disk**（啟動磁碟），按一下 **Change**（變更）> **Custom image**（自訂映像），選取您在步驟 2 中上傳的 Panorama 映像檔案
   2. 設定啟動磁碟大小。依預設，系統磁碟為 81GB，但是您可以將系統磁碟大小增加至 224GB。

      （僅限 SD-WAN）如果您計劃使用處於 Panorama 模式的 Panorama 虛擬設備管理您的 SD-WAN 部署，您必須將系統磁碟大小增加至 224GB。如果您計劃在 Management Only（僅限管理）模式下管理您的 SD-WAN 部署，您必須新增 2TB 日誌記錄磁碟。
   3. 按一下 **Select**（選取）儲存設定。
7. 在 **Identity and API access**（識別和 **API** 存取）中，選取 **Allow full access to all Cloud APIs**（允許完整存取所有雲端 **API**）。



8. 在 **Firewall**（防火牆）下，選取 **Allow HTTPS traffic**（允許 **HTTPS** 流量）。

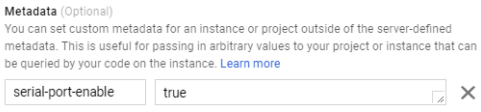


STEP 4 | 展開 **Management, security, disks, networking, sole tenancy**（管理、安全性、磁碟、網路、獨租租賃）Management, security, disks, networking, sole tenancy。

STEP 5 | 啟用存取序列連線埠以管理 Panorama 虛擬設備。

1. 選取 **Management**（管理）。
2. 輸入下列名稱-值配對作為中繼資料：

   ```
   serial-port-enable true
   ```



STEP 6 | 保留管理介面的 IP 位址。

若 Panorama 虛擬設備重新啟動，則保留靜態內部和外部 IP 位址，當重新指派 IP 位址時，您的受管理裝置不會與 Panorama 虛擬設備中斷連線。

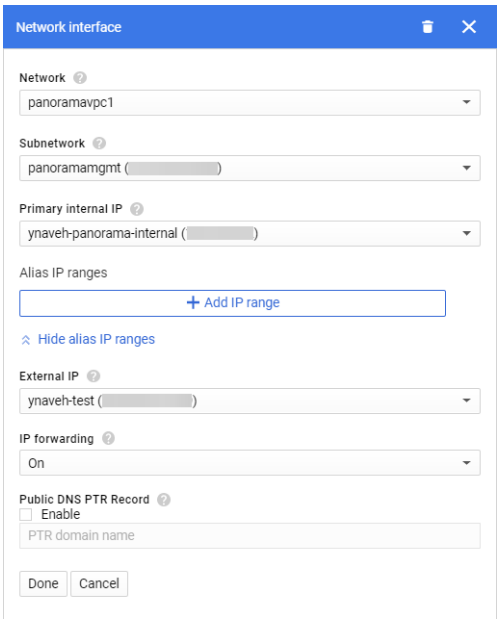
© 2019 Palo Alto Networks, Inc.

如需有關如何保留 IP 位址的詳細資料，請參考保留一個靜態內部 IP 位址和保留一個靜態外部 IP 位址。

1. 選取 **Networking**（網路）。
2. **Edit**（設定）網路介面。



3. 選取 Panorama 虛擬設備**Network**（網路）。
4. 選取 Panorama 虛擬設備**Subnetwork**（子網路）。在相同的子網路中的實例將使用其內部 IP 位址彼此通訊。
5. 設定 **Primary internal IP**（主要內部 **IP**）位址。
   - **Ephemeral (Automatic)**（暫時（自動））—自動指派主要內部 IP 位址。
   - **Ephemeral (Custom)**（暫時（自訂））—設定 GCP 用來指派主要內部 IP 位址的自訂 IP 範圍。
   - **Reserve a static internal IP address**（保留靜態內部 **IP** 位址）—手動設定靜態主要內部 IP 位址。
6. 設定 **External IP**（外部 **IP**）位址。
   - **Ephemeral**（暫時）—自動指派一個來自共享集區的外部 IP 位址。
   - 選取已有的保留外部 IP 位址。
   - **Create IP address**（建立 **IP** 位址）—保留外部 IP 位址。
7. 將 **IP forwarding**（**IP** 轉送）設定為 **On**（開啟）以允許 Panorama 虛擬設備接收來自非比對目的地或來源 IP 位址的封包。



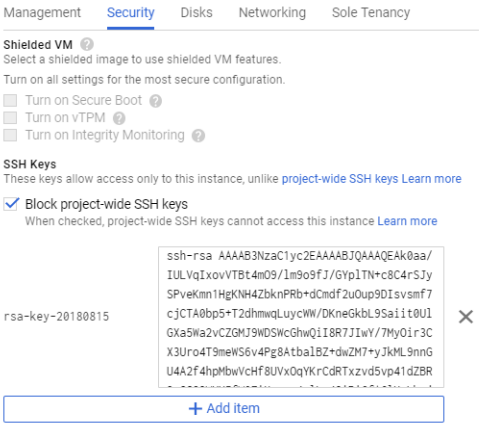
STEP 7 | 設定 SSH 金鑰。您需要 SSH 金鑰以存取 Panorama 虛擬設備 CLI，在原始部署後設定管理使用者的密碼。

1. 選取 **Security**（安全性）。
2. 選取 **Block project-wide SSH keys**（封鎖整個專案 **SSH** 金鑰）方塊。在原始部署之後，目前僅支援實例金鑰用於登入 Panorama 虛擬設備。
3. 在命令框中貼上 SSH 金鑰。有關正確 SSH 金鑰格式以及如何生成 GCP SSH 金鑰的資料，請參考在中繼資料中管理 SSH 金鑰。



當生成 *SSH* 金鑰時，以 *.ppk*格式儲存私人金鑰。在您設定管理密碼前，原始部署後，私人金鑰為登入 *Panorama* 虛擬設備的必要條件。

© 2019 Palo Alto Networks, Inc.

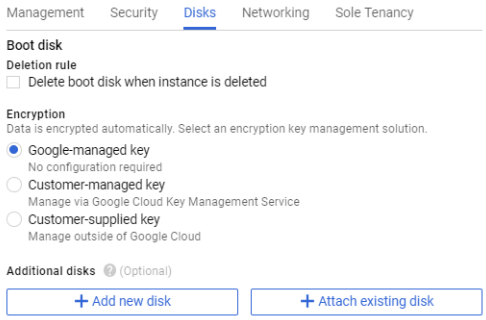


STEP 8 | （Panorama 和日誌收集器模式）新增日誌收集額外的儲存空間。視需重覆此步驟以新增額外的虛擬日誌記錄磁碟。

若您想要以 Panorama 模式或作為專用日誌收集器來使用 Panorama 虛擬設備，請在原始部署時新增虛擬日誌記錄磁碟。依預設，當符合 Panorama 模式資源需求並已新增至少一個虛擬日誌記錄磁碟，Panorama 虛擬設備在原始部署時為 Panorama 模式。否則，Panorama 虛擬設備預設為僅管理模式，在此模式下，您可以管理裝置與專用日誌收集器，但無法收集本機日誌。

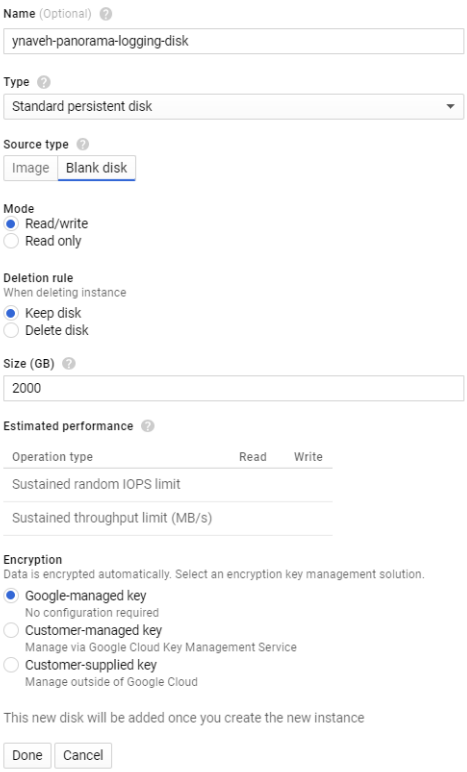
GCP 上的 Panorama 虛擬設備僅支援 2TB 日誌記錄磁碟，並總計支援最高 24TB 的日誌儲存空間。您無法新增小於 2TB 的日誌記錄磁碟，或日誌記錄磁碟大小無法被 2TB 日誌記錄需求整除。Panorama 虛擬設備將大於 2TB 的日誌記錄磁碟分割在 2TB 分割區。

1. 選取 **Disks**（磁碟）> **Add new disk**（新增磁碟）。



2. 輸入 **Name**（名稱）。
3. 展開 **Type**（類型）下拉式選單並選取想要的類型。
4. 對於 **Source type**（來源類型），選取 **Blank disk**（空白磁碟）。
5. 對於 **Mode**（模式），選取 **Read/write**（讀/寫）。
6. 選取 **Deletion rule**（刪除規則），以設定在刪除 Panorama 虛擬設備實例時是否刪除虛擬日誌記錄磁碟。至
7. 設定虛擬日誌記錄磁碟的**Size (GB)**（大小, **GB**）。
8. 為虛擬日誌記錄磁碟上的資料設定偏好的 **Encryption**（加密）解決方案。
9. 按一下 **Done**（完成）。

© 2019 Palo Alto Networks, Inc.



STEP 9 | **Create**（建立）Panorama 虛擬設備。Panorama 虛擬設備在原始部署後大約會花 10 分鐘啟動。

STEP 10 | 設定 Panorama 虛擬設備的新管理密碼。

您必須在存取 Panorama 虛擬設備的網頁介面前設定唯一管理密碼。使用私人金鑰存取 CLI 以啟動 Panorama 虛擬設備。

- 若您在電腦安裝了 SSH 服務：

1. 輸入下列命令，以登入 Panorama 虛擬設備：

```
ssh -i <private_key.ppk> admin@<public-ip_address>
```

2. 使用下列命令設定新密碼，並依照畫面上的提示進行：

```
admin> configure
admin# set mgt-config users admin password
```

3. 如果有需要的 BYOL，請設定 DNS 伺服器 IP 位址，以便 Panorama 虛擬設備可存取 Palo Alto Networks 授權伺服器。輸入下列命令設定 DNS 伺服器 IP 位址：

```
admin# set deviceconfig system dns-setting servers primary <ip_address>
```

4. 提交您的變更：

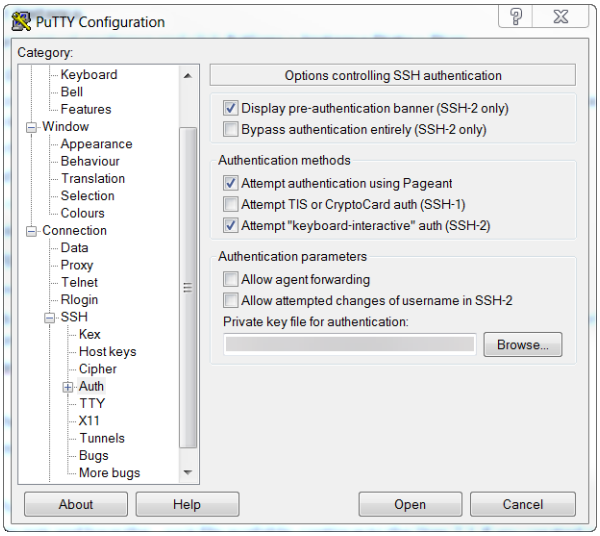
```
admin# commit
```

5. 終止 SSH 工作階段。

© 2019 Palo Alto Networks, Inc.

- 若您使用 PuTTY 連至 Panorama 虛擬設備內的 SSH：

1. 若您使用現有金鑰配對且有可用的 `.ppk`檔，請繼續步驟 11.3。若您建立新的金鑰配對或在現有金鑰配對中僅有 `.pem` 檔，則請開啟 PuTTYgen 並 **Load**（載入） `.pem` 檔。
2. **Save the private key**（儲存私人金鑰）到本機可存取的目的地。
3. 開啟 PuTTY 並選取上一步儲存的 `.ppk` 檔的**SSH** > **Auth**（驗證） 和 **Browse**（瀏覽）。



4. 選取 **Sessions**（工作階段）並輸入 Panorama 虛擬設備的公共 IP 位址。然後在出現安全提示時，**Open**（開啟）並按一下 **Yes**（是）。
5. 在提示時，以管理員登入。
6. 使用下列命令設定新密碼，並依照畫面上的提示進行：

```
admin> configure
admin# set mgt-config users admin password
```

7. 請設定 DNS 伺服器 IP 位址，以便 Panorama 虛擬設備可存取 Palo Alto Networks 授權伺服器。輸入下列命令設定 DNS 伺服器 IP 位址：

```
admin# set deviceconfig system dns-setting servers primary <ip_address>
```

8. 使用下列命令提交變更：

```
admin# commit
```

9. 終止 SSH 工作階段。

STEP 11 | 啟用裝置管理授權並支援在 Panorama 虛擬設備上的授權。

- 在 Panorama 虛擬設備與網際網路連線時，啟動/擷取防火牆管理授權
- 在 Panorama 虛擬設備並未與網際網路連線時，啟動/擷取防火牆管理授權
- 啟動 Panorama 支援授權

STEP 12 | 完成部署需要的 Panorama 虛擬設備設定。

- （僅管理模式）在僅管理模式下設定 Panorama 虛擬設備。
- （日誌收集器模式）在步驟 6 開始從 Panorama 模式切換為日誌收集器模式。

© 2019 Palo Alto Networks, Inc.

在您將日誌收集器作為受管理的收集器新曾到 *Panorama* 管理伺服器時，輸入專用日誌收集器的公共 *IP* 位址。您無法指定 *IP* 位址、網路遮罩或 網閘。

- （僅限 Panorama 和管理模式）設定受管理收集器 以新增專用日誌收集器到 Panorama 虛擬設備。僅管理模式不支援本機日誌收集，且需要專用日誌收集器以儲存受管理的裝置日誌。

KVM 上安裝 Panorama

您可以立即在 KVM 部署 Panormama™ 和專用日誌收集器。Panorama 部署在 KVM 上的授權為自帶授權（BYOL），支援所有部署的模式（Panorama、日誌收集器和僅管理），且與 M-Series 硬體設備一樣共享相同的程序與功能。如需 Panorama 模式的詳細資訊，請參閱 Panorama 型號。

STEP 1 | 下載 KVM 使用的 Panorama 虛擬設備映像。

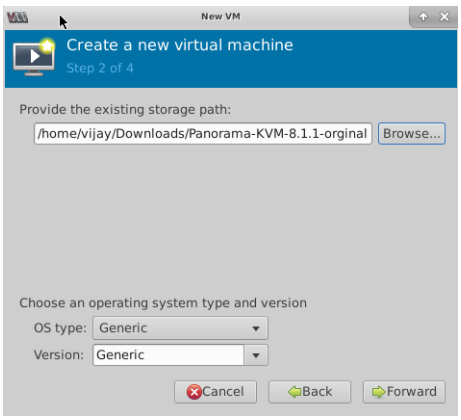
1. 登入 Palo Alto Networks Support 入口網站。
2. 選取 **Software Updates**（軟體更新）並找出 KVM 基本映像使用的 Panorama。
3. 下載最新可用的 Panorama .qcow2 檔案。

STEP 2 | 建立新的虛擬電腦映像並新增 KVM 用 Panorama 虛擬設備映像至虛擬電腦管理員。

1. 在虛擬電腦管理員上，選取 **Create a new virtual machine**（建立新虛擬電腦）。
2. 選取 **Import Existing disk image**（輸入現有磁碟映像）並按一下 **Forward**（轉送）。



3. **Browse**（瀏覽）並選取 Panorama 虛擬設備映像磁碟區，並 **Choose volume**（選取磁碟區）。
4. 按一下 **Forward**（轉送）。



STEP 3 | 設定記憶體和 CPU 設定。

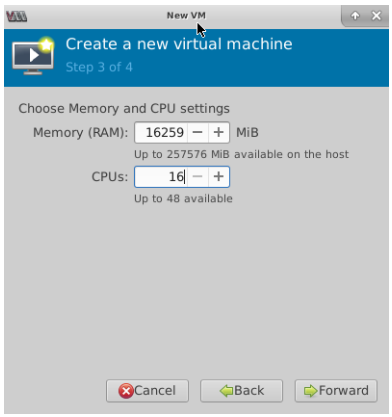
檢閱 設定 Panorama 虛擬設備的先決條件 瞭解最低資源需求。

© 2019 Palo Alto Networks, Inc.

若您計劃使用 *Panorama* 虛擬設備作為專用日誌收集器，請確定將設備設定為在原始部署時擁有必要的資源。*Panorama* 虛擬設備若在您部署虛擬電腦後重新調整其大小，則不會仍舊維持日誌收集器模式，且會造成日誌資料的丟失。

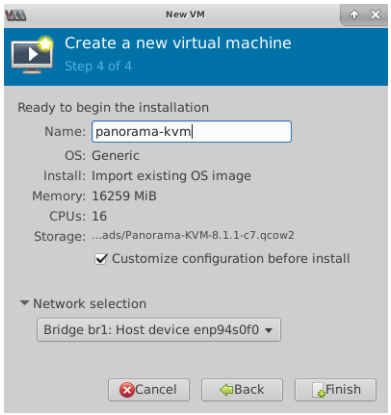
1. 根據所需作業模式的需求，設定 **Memory**（記憶體）。

   虛擬電腦管理員可使用 *MiB*（*mebibyte*）以依據執行的版本配置記憶體。若使用 *MiB*，則請確定正確轉換需要的記憶體配置，以避免低於 *Panorama* 虛擬設備佈建。
2. 根據所需作業模式的需求，設定 **CPU**。
3. 按一下 **Forward**（轉送）。



STEP 4 | 為 Panorama 虛擬設備命名、啟用設定自訂並選取管理介面橋接。

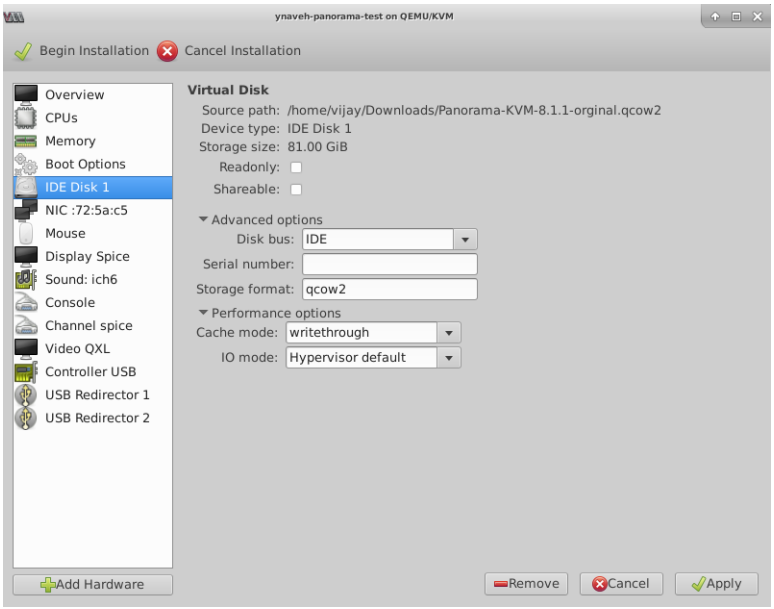
1. 為 Panorama 虛擬設備輸入具描述性的 **Name**（名稱）。
2. **Customize configuration before install**（安裝前自訂組態）。
3. 做出 **Network selection**（網路選取）—為管理介面選取橋接器，然後接受預設設定。
4. 按一下 **Finish**（完成）。



STEP 5 | 設定虛擬系統磁碟的設定。

1. 選取 **IDE Disk 1**（**IDE** 磁碟 **1**），前往 **Advanced options**（進階選項），然後選取以下選項：
   - **Disk Bus**（磁碟匯流排）—**VirtIO** 或 **IDE**，依您的設定而定。
   - **Storage format**（儲存格式）—**qcow2**
2. 前往 **Performance options**（效能選項），然後將 **Cache mode**（快取模式）設為 **writethrough**。此設定可改善 Panorama 虛擬設備的安裝時間與執行速度。
3. 按一下 **Apply**（套用）。

© 2019 Palo Alto Networks, Inc.

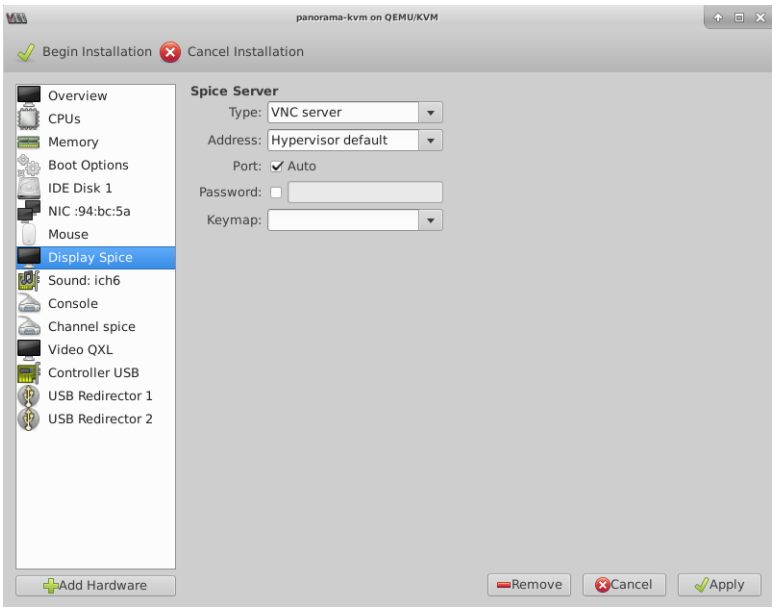


STEP 6 | 設定虛擬電腦主控台 顯示以使用與虛擬電腦互動的 VNC 伺服器。

1. 選取 **Display Spice**（顯示調味料）。

   若 *Display VNC*（顯示 *VNC*）因虛擬電腦已設定使用 *VNC* 伺服器顯示，而列於硬體清單中，則繼續下一個步驟。

2. 在 **Type**（類型）下拉式清單中選取 **VNC server**（**VNC** 伺服器）。
3. 按一下 **Apply**（套用）。



STEP 7 | （Panorama 和日誌收集器模式）新增日誌收集額外的儲存空間。視需重覆此步驟以新增額外的虛擬日誌記錄磁碟。

若您想要以 Panorama 模式或作為專用日誌收集器來使用 Panorama 虛擬設備，請在原始部署時新增虛擬日誌記錄磁碟。依預設，當符合 Panorama 模式資源需求並已新增至少一個虛擬日誌記錄磁碟，Panorama 虛擬設備在原始部署時為 Panorama 模式。否則，Panorama 虛擬設備預設為僅管理模

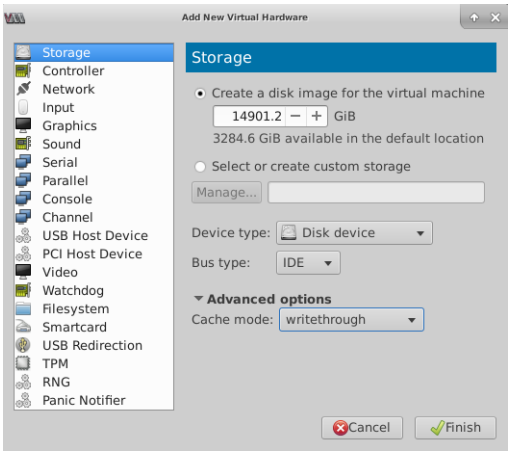
© 2019 Palo Alto Networks, Inc.

式。若您只想要管理裝置與專用日誌收集器，且不要收集本機日誌，則變更 Panorama 虛擬設備為僅管理模式。

KVM 上的 Panorama 虛擬設備僅支援 2TB 日誌記錄磁碟，並總計支援最高 24TB 的日誌儲存空間。您無法新增小於 2TB 的日誌記錄磁碟，或日誌記錄磁碟大小無法被 2TB 日誌記錄需求整除。Panorama 虛擬設備將大於 2TB 的日誌記錄磁碟分割在 2TB 分割區。

1. **Add Hardware**（新增硬體）。
2. 新增新的 **Storage**（儲存空間）磁碟：
   1. **Create a disk image for a virtual machine**（建立虛擬電腦的磁碟映像）並設定虛擬磁碟儲存容量為 14901.2 GiB（與 2TB 相等）。

      虛擬電腦管理員可使用 *GiB*（*gibibyte*）以依據執行的版本配置記憶體。若使用 *GiB*，請確定您正確轉換所需的儲存空間容量，以避免小於部建虛擬日誌記錄磁碟並傳送 *Panorama* 虛擬設備進入維護模式。
   2. 將 **Device type**（裝置類型）設定為 **Disk**（磁碟）裝置。
   3. 將 **Bus type**（匯流排類型）依據設定，設定為 **VirtIO** 或 **IDE**。
   4. 前往 **Advanced options**（進階選項），然後將 **Cache mode**（快取模式）設為 **writethrough**。
3. 按一下 **Finish**（完成）。



STEP 8 | **Begin Installation**（開始安裝）（Begin Installation）.Panorama 虛擬設備大約會花 10 分鐘啟動。

STEP 9 | 設定管理介面的網路存取設定。

1. 在主控台上開啟連線。
2. 使用預設使用者名稱與密碼：admin/admin 登入n防火牆。
3. 使用下列命令，進入組態模式：

```
admin> configure
```

4. 使用下列命令，設定並啟用管理介面存取：

```
admin# set deviceconfig system type static
admin# set deviceconfig system ip-address <Panorama-IP> netmask <netmask>
 default-gateway <gateway-IP> dns-setting servers primary <DNS-IP>
```

其中，*<Panorama-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。

© 2019 Palo Alto Networks, Inc.

```
admin# commit
```

STEP 10 | 啟用裝置管理授權並支援在 Panorama 虛擬設備上的授權。

- 在 Panorama 虛擬設備與網際網路連線時，啟動/擷取防火牆管理授權
- 在 Panorama 虛擬設備並未與網際網路連線時，啟動/擷取防火牆管理授權
- 啟動 Panorama 支援授權

STEP 11 | 完成部署需要的 Panorama 虛擬設備設定。

- （僅管理模式）在僅管理模式下設定 Panorama 虛擬設備。
- （日誌收集器模式）在步驟 6 開始從 Panorama 模式切換為日誌收集器模式。

  在您將日誌收集器作為受管理的收集器新曾到 *Panorama* 管理伺服器時，輸入專用日誌收集器的公共 *IP* 位址。您無法指定 *IP* 位址、網路遮罩或 網閘。
- （僅限 Panorama 和管理模式）設定受管理收集器 以新增專用日誌收集器到 Panorama 虛擬設備。僅管理模式不支援本機日誌收集，且需要專用日誌收集器以儲存受管理的裝置日誌。

在 *Hyper-V* 上安裝 *Panorama*

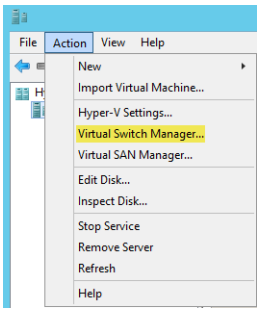
您可以立即在 Hyper-V 部署 Panormama™ 和專用日誌收集器。您現在可以在 Hyper-V 上部署 Panorama™ 和專用日誌收集器。Panorama 部署在 Hyper-V 上的授權為自帶授權 (BYOL)，支援所有部署的模式（Panorama、日誌收集器和僅管理），且與 M-Series 硬體設備一樣共享相同的程序與功能。如需 Panorama 模式的詳細資訊，請參閱 Panorama 型號。Hyper-V 上的 Panorama 虛擬設備和虛擬專用日誌收集器僅在 PAN-OS 8.1.3 和更新版本上可用。

STEP 1 | 下載 VHDX 檔案。

1. 登入 Palo Alto Networks Support 入口網站。
2. 選取 **Updates**（更新）> **Software Updates**（軟體更新），依 **Panorama Base Images**（**Panorama** 基本映像）篩選，然後下載 VHDX 檔案。

STEP 2 | 設定任何您需要的 vSwitch。如需更多資訊，檢閱 Virtual Switch Types（虛擬交換器類型）瞭解詳情。

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。

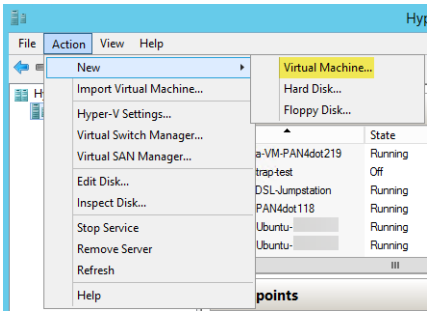


2. 在 **Create virtual switch**（建立虛擬交換器）項下，選取要建立的 vSwitch 的類型，然後按一下 **Create Virtual Switch**（建立虛擬交換器）。

STEP 3 | 安裝 Panorama 虛擬設備。

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：

© 2019 Palo Alto Networks, Inc.



1. 選取 Panorama 虛擬設備的 **Name**（名稱）和 **Location**（位置）。Panorama 虛擬設備在指定位置儲存 VHDX 檔案。
2. 選取 **Generation 1**。這是預設選項及唯一支援的版本。
3. 對於 **Startup Memory**（啟動記憶體），根據預期的系統模式指派記憶體。請參閱 設定 Panorama 虛擬設備的先決條件，瞭解每種模式的記憶體需求。

   請勿啟用動態記憶體；*Panorama* 虛擬設定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）。

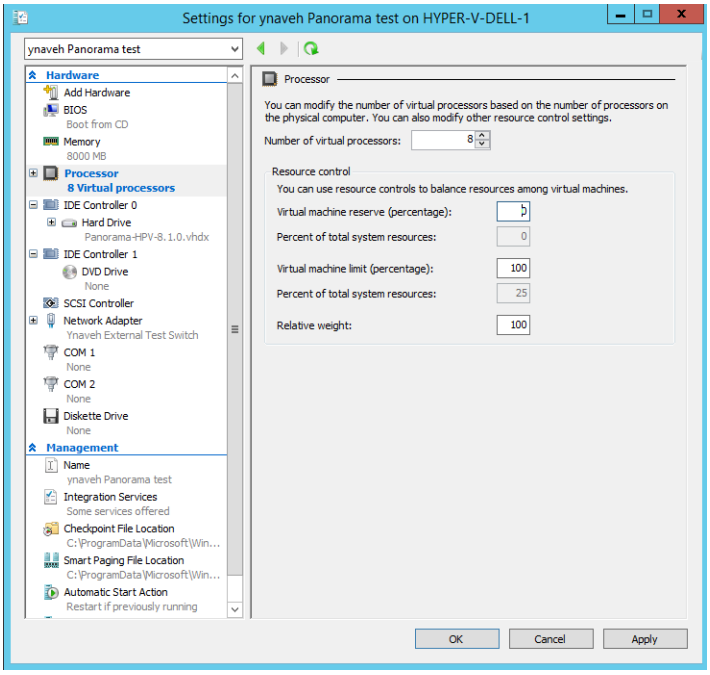
STEP 4 | 配置 Panorama 虛擬設備 CPU 核心。

檢閱 設定 Panorama 虛擬設備的先決條件 瞭解最低資源需求。

若您計劃使用 *Panorama* 虛擬設備作為專用日誌收集器，請確定將設備設定為在原始部署時擁有必要的資源。*Panorama* 虛擬設備若在您部署虛擬電腦後重新調整其大小，則不會仍舊維持日誌收集器模式，且會造成日誌資料的丟失。

1. 在 **Hardware**（硬體）清單中，選取 **Processor**（處理器）。
2. 編輯目前配置的 **Number of virtual processors**（虛擬處理器數目）。

© 2019 Palo Alto Networks, Inc.



STEP 5 | 請為防火牆上的資料平面介面連線至少一個網路介面卡。重複此動作，在 Panorama 虛擬設備上建立其他網路介面。

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 6 | （Panorama 和日誌收集器模式）新增日誌收集額外的儲存空間。視需重覆此步驟以新增額外的虛擬日誌記錄磁碟。若您想要以僅管理模式部署 Panorama 虛擬設備，則繼續至步驟 6。

若您想要以 Panorama 模式或作為專用日誌收集器來使用 Panorama 虛擬設備，請在原始部署時新增虛擬日誌記錄磁碟。依預設，當符合 Panorama 模式資源需求並已新增至少一個虛擬日誌記錄磁碟，Panorama 虛擬設備在原始部署時為 Panorama 模式。否則，Panorama 虛擬設備預設為僅管理模式。若您只想要管理裝置與專用日誌收集器，且不要收集本機日誌，則變更 Panorama 虛擬設備為僅管理模式。

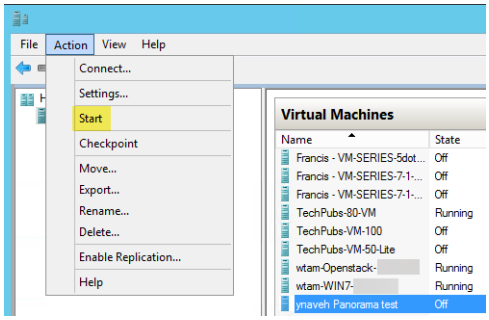
Hyper-V 上的 Panorama 虛擬設備僅支援 2TB 日誌記錄磁碟，並總計支援最高 24TB 的日誌儲存空間。您無法新增小於 2TB 的日誌記錄磁碟，或日誌記錄磁碟大小無法被 2TB 日誌記錄需求整除。Panorama 虛擬設備將大於 2TB 的日誌記錄磁碟分割在 2TB 分割區。

1. 在 Hyper-V 管理員上，選取主機並選取 **Action**（動作）> **New**（新增）> **Hard Disk**（硬碟）。
2. 如果您看到 Before You Begin（開始之前）提示，按一下 **Next**（下一步）以開始新增虛擬日誌紀錄磁碟。
3. 對於 Disk Format（磁碟格式），選取 **VHDX**。按一下 **Next**（下一步）繼續
4. 對於 Disk Type（磁碟類型），根據您的需求選取 **Fixed Size**（固定大小）或 **Dynamically Expanding**（動態擴充）。按一下 **Next**（下一步）繼續。
5. 指定虛擬日誌紀錄磁碟檔案的 **Name**（名稱）和 **Location**（位置）。按一下 **Next**（下一步）繼續。
6. 若要設定磁碟，選取 **Create a new virtual hard disk**（建立新虛擬磁碟），然後輸入磁碟大小。按一下 **Next**（下一步）繼續。
7. 檢閱 Summary（摘要）並 **Finish**（完成）擬擬日誌紀錄硬碟新增。

© 2019 Palo Alto Networks, Inc.

STEP 7 | 開啟 Panorama 虛擬設備電源。

1. 從 **Virtual Machines**（虛擬機器）清單中選取 Panorama 虛擬設備實例。
2. 選取 **Action**（動作）> **Start**（開啟）以開啟 Panorama 虛擬設備。



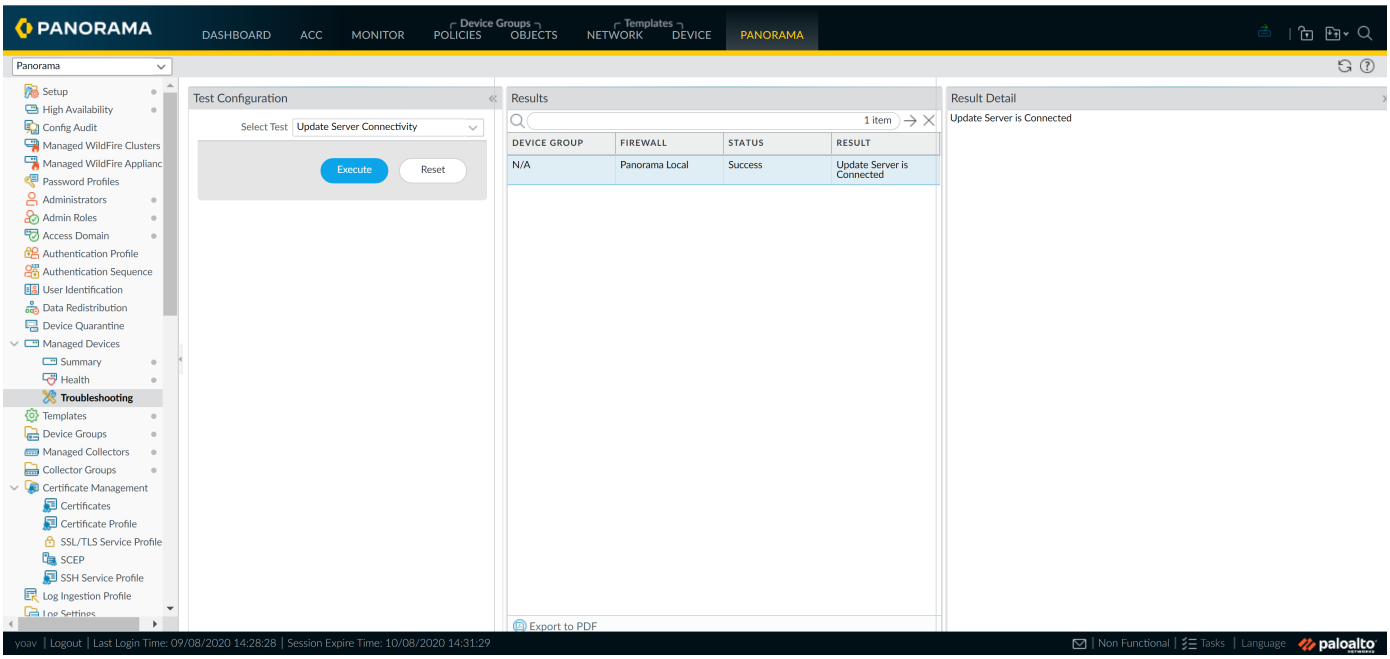
STEP 8 | 設定管理介面的 IP 位址。

若您在虛擬交換器網路上啟用了 DHCP 服務，則可跳過此步驟。

1. 在 **Virtual Machines**（虛擬機器）清單中，選取 Panorama 虛擬設備。
2. 選取 **Actions**（動作）> **Connect**（連線），然後輸入使用者名稱和密碼登入（兩者預設為 admin）。
3. 輸入下列命令，其中，*<Panorama-IP>* 是要指定給 Panorama 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：

```
admin> configure
admin# set deviceconfig system ip-address <Panorama-IP> netmask <netmask>
 default-gateway <gateway-IP> dns-setting servers primary <DNS-IP>
admin# commit
admin# exit
```

4. 疑難排解網路資源連線 確認防火牆管理所需的，對外部服務的網路存取，如預設網關、DNS 伺服器和 Palo Alto Networks 更新伺服器，如下例所示：



STEP 9 | 啟用裝置管理授權並支援在 Panorama 虛擬設備上的授權。

- 在 Panorama 虛擬設備與網際網路連線時，啟動/擷取防火牆管理授權

© 2019 Palo Alto Networks, Inc.

- 在 Panorama 虛擬設備並未與網際網路連線時，啟動/擷取防火牆管理授權
- 啟動 Panorama 支援授權

STEP 10 | 完成部署需要的 Panorama 虛擬設備設定。

- （僅管理模式）在僅管理模式下設定 Panorama 虛擬設備。
- （日誌收集器模式）在步驟 6 開始從 Panorama 模式切換為日誌收集器模式。

  在您將日誌收集器作為受管理的收集器新曾到 *Panorama* 管理伺服器時，輸入專用日誌收集器的公共 *IP* 位址。您無法指定 *IP* 位址、網路遮罩或 網閘。
- （僅限 Panorama 和管理模式）設定受管理收集器 以新增專用日誌收集器到 Panorama 虛擬設備。

僅管理模式不支援本機日誌收集，且需要專用日誌收集器以儲存受管理的裝置日誌。

執行 Panorama 虛擬設備的初始設定

依據您的 Panorama 型號，使用 AWS、Azure 或 GCP 網頁介面、KVM 虛擬電腦管理員、Hyper-V 管理員、VMware vSphere 用戶端或 vCloud Air 網頁主控台來設定對 Panorama 虛擬設備的網路存取。依預設，Panorama 虛擬設備設定在 Panorama 模式。對於統一報告，考慮使用格林威治標準時間 (GMT) 或世界標準時間 (UTC) 作為 Panorama 和所有受管理的防火牆和日誌收集器的統一時區。

STEP 1 | 從網路管理員收集必要資訊。

針對管理 (MGT) 介面收集下列資訊：

- ❑ 管理 (MGT) 介面的 IP 位址
- ❑ 網路遮罩
- ❑ 預設閘道
- ❑ DNS 伺服器 IP 位址

若要完成 *MGT* 介面的組態設定，必須指定 *IP* 位址、網路遮罩（適用於 *IPv4*）或首碼長度（適用於 *IPv6*）和預設閘道。如果您省略設定（例如預設閘道），則未來需要變更組態時，您只能透過主控台連接埠存取 *Panorama*。最佳作法是一律提交完整的 *MGT* 介面設定。

STEP 2 | 存取 Panorama 虛擬設備的主控台。

1. 存取主控台。

   在 ESXi 伺服器上：

   1. 啟動 VMware vSphere 用戶端。
   2. 選取 Panorama 虛擬設備的 **Console**（主控台）頁籤，並按下 Enter 存取登入畫面。

   在 vCloud Air 上：

   1. 存取 vCloud Air web 主控台並選取您的 **Virtual Private Cloud OnDemand**（虛擬私人雲 **OnDemand**）地區。
   2. 選取 **Virtual Machines**（虛擬機器）頁籤，右鍵按一下 Panorama 虛擬機器，然後選取 **Open In Console**（在主控台中打開）。
2. 輸入您的使用者名稱和密碼以登入（兩者都預設為 admin）。

   在 AWS、Azure、GCP、KVM 和 Hyper-V 上：

   - 登入 Panorama CLI。

STEP 3 | 變更預設的管理員密碼。

© 2019 Palo Alto Networks, Inc.

從 *PAN-OS 9.0.4* 開始，第一次登入裝置時必須變更預定義的預設密碼 *(admin/admin)*。新密碼至少必須包含八個字元，並且包含至少一個小寫字母與一個大寫字母，以及一個數字或特殊字元。

務必採用密碼強度最佳做法 以確保嚴格的密碼，並檢閱密碼複雜性設定。

若要確保管理介面的安全，設定最低密碼複雜度（*Panorama* > *Setup*（設定）> *Management*（管理））。

1. 按一下 web 介面頁尾左側的 **admin**（管理員）連結。
2. 輸入 **Old Password**（舊密碼）及 **New Password**（新密碼），並將新密碼存放在安全的位置。
3. 按一下 **OK**（確定）。

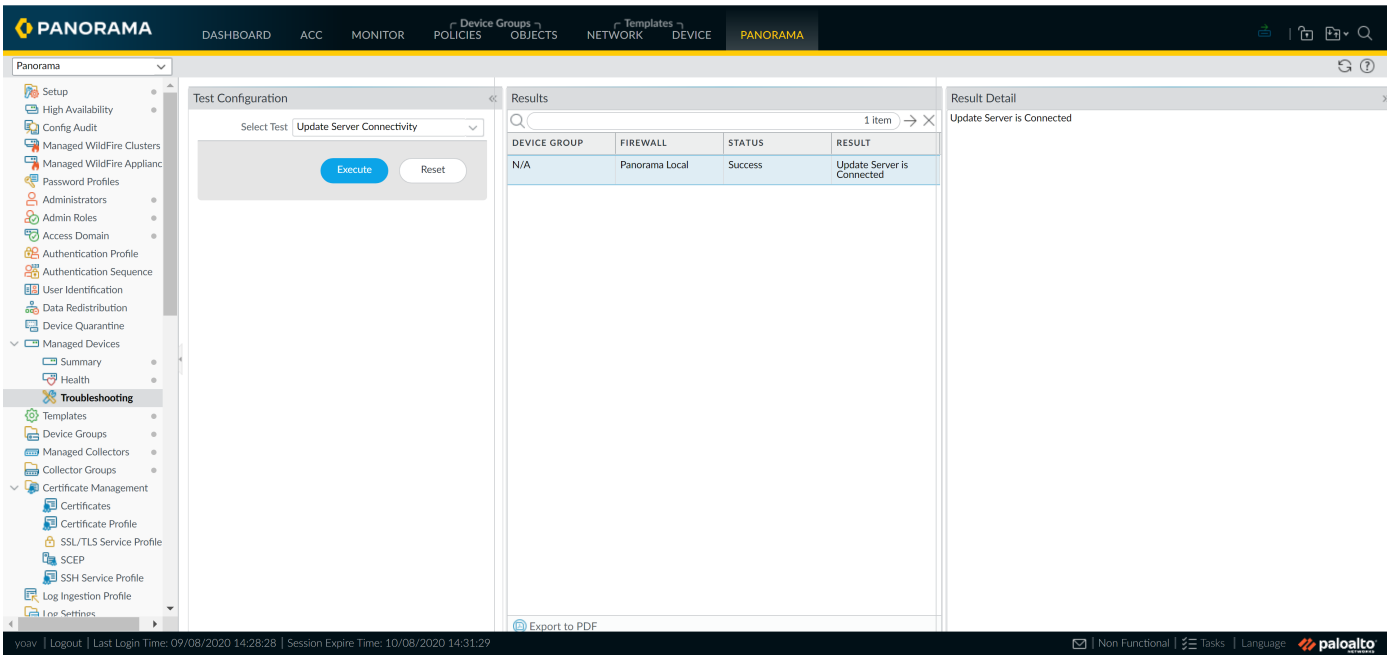
STEP 4 | 設定 MGT 介面的網路存取設定。

Panorama 將管理介面用於管理流量、高可用性同步、日誌收集，以及在收集器群組內進行通訊。

1. 輸入下列命令，其中，*<Panorama-IP>* 是要指定給 Panorama 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：

```
> configure
# set deviceconfig system ip-address <Panorama-IP> netmask <netmask>
 default-gateway <gateway-IP> dns-setting servers primary <DNS-IP>
# commit
# exit
```

2. 疑難排解網路資源連線 確認防火牆管理所需的，對外部服務的網路存取，如預設網關、DNS 伺服器和 Palo Alto Networks 更新伺服器，如下例所示：



STEP 5 | 設定一般設定。

1. 使用 Web 瀏覽器中的安全連線 (HTTPS)，使用您指定給管理介面的 IP 位址及密碼登入 Panorama web 介面（https://<IP 位址>）。
2. 選取 **Panorama** > **Setup**（設定）> **Management**（管理），再編輯 [一般設定]。

© 2019 Palo Alto Networks, Inc.

3. 輸入伺服器的 **Hostname**（主機名稱），並輸入網路 **Domain**（網域）名稱。網域名稱只是一種標籤；Panorama 加入網域時不會使用它。
4. 對準 Panorama 與受管理防火牆上的時鐘以使用相同的 **Time Zone**（時區），例如 GMT 或 UTC。如果打算使用 Cortex Data Lake（Cortex 資料湖），您必須設定 NTP，才能使 Panorama 與 Cortex Data Lake（Cortex 資料湖）保持同步。

   當 Panorama 接收日誌且受管理的防火牆產生日誌時，時間戳記被記錄。對準 Panorama 與防火牆上的時區，確保同步時間戳記，且在 Panorama 上查詢日誌與產生報告的程序並未產生衝突。
5. 輸入 **Latitude**（經度）與 **Longitude**（緯度），在世界地圖上精確定位 Panorama 管理伺服器。
6. 輸入您在訂購完成電子郵件中收到的 **Serial Number**（序號）。
7. 按一下 **OK**（確定）儲存您的變更。

STEP 6 | （選用）修改管理介面設定。

1. 選取 **Panorama** > **Setup**（設定）> **Interfaces**（介面），然後按一下 **Management**（管理）。
2. 若您的防火牆使用公共 IP 位址（轉譯為私密 IP 位址 (NAT)）連線至 Panorama 管理伺服器，請在 **Public IP Address**（公共 **IP** 位址）欄位輸入公共 IP，在 **IP Address**（**IP** 位址）欄位輸入私密 IP，以便推送兩者至您的防火牆。
3. 選取在介面上允許的網路連線服務（例如 **SSH** 存取）。

   請勿選取 *Telnet* 或 *HTTP*。這些服務使用純文字，安全性低於其他服務。
4. 按一下 **OK**（確定）以儲存對介面所做的變更。

STEP 7 | 提交組態變更。

選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

STEP 8 | 接下來的步驟...

1. 若有必要，擴展 Panorama 虛擬設備的日誌儲存容量。
2. （最佳作法）取代預設憑證，Panorama 使用此憑證來保護管理 (MGT) 介面上的 HTTPS 流量安全。
3. 啟動 Panorama 支援授權。
4. 在 Panorama 虛擬設備與網際網路連線時，啟動/擷取防火牆管理授權。
5. 安裝 Panorama 的內容與軟體更新。
6. 設定對 Panorama 的管理存取權

設定 Panorama 虛擬設備作為日誌收集器

如果您想要一個專為日誌收集用的虛擬設備，則在日誌收集器模式下，在 ESXi、AWS、AWS GovCloud、Azure、Google Cloud Platform、KVM 或 Hyper-V 上設定 Panorama 虛擬設備。為此，首先在 Panorama 模式下執行虛擬設備的初始設定，包括授權、安裝軟體和內容更新以及設定管理 (MGT) 介面。然後您可以將 Panorama 虛擬設備切換至日誌收集器模式，並完成日誌收集器設定。此外，如果您要使用專用 M-Series 設備介面（建議）（而非 MGT 介面）進行日誌收集和收集器群組通訊，您必須先為 Panorama 管理伺服器設定介面，再為日誌收集器設定介面，然後執行 Panorama 提交，接著再執行收集器群組提交。

執行下列步驟，將新的虛擬設備設定為日誌收集器，或者轉換現有的虛擬設備（之前部署為 Panorama 管理伺服器）。

如果將虛擬設備從 *Panorama* 模式切換至日誌收集器模式時，將會重新啟動設備、刪除本機日誌收集器、刪除任何現有日誌資料，以及刪除所有組態（但管理存取設定除外）。切換模式不會刪除授權、軟體更新或內容更新。

STEP 1 | 如果還未設定將用於管理日誌收集器的 Panorama 虛擬設備管理伺服器，請先進行設定。

執行下列其中一個工作：

© 2019 Palo Alto Networks, Inc.

- 設定 Panorama 虛擬設備
- 設定 M-Series 設備

STEP 2 | 記錄 Panorama 管理伺服器的管理 IP 位址。

如果您已採用高可用性 (HA) 設定部署 Panorama，則需要每個 HA 端點的 IP 位址。

1. 登入 Panorama 管理伺服器的 Web 介面。
2. 選取 **Panorama** > **Setup**（設定） > **Management**（管理） 並查看管理介面設定，記錄單獨（非 HA）或主動 (HA) Panorama 的 **IP Address**（**IP** 位址）。
3. 對於 HA 部署，選取 **Panorama** > **High Availability**（高可用性） 並查看設定部分，記錄被動 Panorama 的 **Peer HA IP Address**（端點 **HA IP** 位址）。

STEP 3 | 設定將作為專用日誌收集器的 Panorama 虛擬設備。

如果您之前已將該設備部署為 Panorama 管理伺服器，則可以跳過此步驟，因為已經設定了 MGT 介面並且已經安裝了授權和更新。

日誌收集器模式下的 Panorama 虛擬設備沒有用於設定工作的 Web 介面，只有 CLI。因此，在 Panorama 虛擬設備上變更模式之前，先在 Panorama 模式中使用 Web 介面：

1. 設定在以下一個支援的管理程式中的 Panorama 虛擬設備：
   - 在 ESXi 伺服器上安裝 Panorama
   - 在 AWS 上安裝 Panorama。
   - 在 AWS GovCloud 上安裝 Panorama
   - 在 Azure 上安裝 Panorama。
   - 在 Google Cloud Platform 上安裝 Panorama。
   - 在 Hyper-V 上安裝 Panorama
2. 執行 Panorama 虛擬設備的初始設定。
3. 註冊 Panorama 並安裝授權。
4. 安裝 Panorama 的內容與軟體更新。

STEP 4 | （僅對 Azure 上的 Panorama）修改管理員密碼。

專用日誌收集器僅支援管理的管理員用戶，以便能改變為日誌收集器模式。修改管理員密碼以讓您可以使用管理的管理員用戶登入。

1. 登入 Panorama 網頁介面。
2. 選取 **Panorama** > **Administrators**（管理員），然後選取 **admin**。
3. 輸入 **Password**（密碼）、**Confirm Password**（確認密碼），然後按一下 **OK**（確認）。
4. 選取 **Commit**（提交） > **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交） 您的變更。

STEP 5 | （僅 AWS 和 Azure 上的 Panorama）刪除所有用戶，特別是對管理用戶來說。

1. 作為管理員登入 Panorama 網頁介面。
2. 選取 **Panorama** > **Administrators**（管理員）。
3. 選取除 admin 外的現有管理員，並**Delete**（刪除）。
4. 選取 **Commit**（提交） > **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交） 您的變更。

STEP 6 | 登入 Panorama CLI。

STEP 7 | 從 Panorama 模式切換至日誌收集器模式。

1. 輸入下列命令，切換至日誌收集器模式：

© 2019 Palo Alto Networks, Inc.

```
> request system system-mode logger
```

2. 輸入 **Y** 以確認模式變更。虛擬設備重新啟動。重新啟動會終止終端機模擬軟體的工作階段並重新連線至虛擬設備以顯示 Panorama 登入提示。

   如果您看到 ***CMS Login***（*CMS* 登入）提示，則表示日誌收集器未完成重新啟動。在提示框中按 *Enter*，而不輸入使用者名稱或密碼。
3. 重新登入 CLI。
4. 確認已成功切換至日誌收集器模式：

```
> show system info | match system-mode
```

如果模式變更成功，則輸出顯示為：

```
system-mode: logger
```

STEP 8 | 啟用日誌收集器和 Panorama 管理伺服器之間的連線。

在日誌收集器 CLI 上輸入以下命令，其中 *<IPaddress1>* 單獨（非 Ha）或主動 (HA) Panorama 的 MGT 介面，*<IPaddress2>* 是被動 (HA) Panorama 的 MGT 介面（如果適用）。

```
> configure
# set deviceconfig system panorama-server <IPaddress1> panorama-server-2
 <IPaddress2>
# commit
# exit
```

STEP 9 | 記錄日誌收集器的序號。

您需要這些序號以便在 Panorama 管理伺服器上將日誌收集器新增為受管理的收集器。

1. 在日誌收集器 CLI 中輸入下列命令可顯示序號。

```
> show system info | match serial
```

2. 記錄序號。

STEP 10 | 將日誌收集器作為受管理的收集器新增至 Panorama 管理伺服器。

1. 選取 **Panorama** > **Managed Collectors**（受管理的收集器），再 **Add**（新增）受管理的收集器。
2. 在 **General**（一般）設定中，輸入您記錄的收集器序號（**Collector S/N**（收集器序號））。
3. 在 **Panorama Server IP**（**Panorama** 伺服器 **IP**）欄位中，輸入 IP 位址或單獨（非 HA）或主動 (HA) Panorama 的 FQDN。對於 HA 部署，在 **Panorama Server IP 2**（**Panorama** 伺服器 **IP 2**）欄位中輸入 IP 位址或被動端點的 FQDN。

   這些 IP 位址必須指定已啟用 **Device Management and Device Log Collection**（裝置管理和裝置日誌收集）服務的 Panorama 介面。依預設，只能在 MGT 介面上啟用這些服務則。不過，當您設定 M-Series 設備而設備是 Panorama 管理伺服器時，您可能已在其他介面上啟用這些服務。
4. 選取 **Interfaces**（介面），按一下 **Management**（管理），然後輸入專用日誌收集器的 **Public IP Address**（公共 **IP** 位址）。
5. 按一下 **OK**（確定）兩次，以儲存對日誌收集器所做的變更。
6. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後將您的變更 **Commit**（提交）至 Panorama 組態。

© 2019 Palo Alto Networks, Inc.

7. 確認 **Panorama** > **Managed Collectors**（受管理的收集器）列出您已新增的日誌收集器。Connected（已連線）欄中會顯示核取標記，表示日誌收集器已連線至 Panorama。您可能需要等待幾分鐘，然後頁面才會顯示更新後的連線狀態。

   此時，*Configuration Status*（組態狀態）欄會顯示 *Out of Sync*（不同步），*Run Time Status*（執行階段狀態）欄會顯示 *disconnected*（已中斷連線）。設定收集器群組之後，狀態將變更為 *In Sync*（同步）和 *connected*（已連線）。

STEP 11 | 啟用日誌記錄磁碟。

1. 選取 **Panorama** > **Managed Collectors**（受管理的收集器），再編輯日誌收集器。
2. 選取 **Disks**（磁碟），然後 **Add**（新增）每一個磁碟。
3. 按一下 **OK**（確定）儲存您的變更。
4. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後將您的變更 **Commit**（提交）至 Panorama 組態。

STEP 12 | （建議）如果 Panorama 管理伺服器和日誌收集器會將 **Ethernet1**、**Ethernet2**、**Ethernet3**、**Ethernet4** 和 **Ethernet5** 介面用於裝置日誌收集（從防火牆接收日誌）和 **Collector Group Communication**（收集器群組通訊），請設定這些介面。

如果您先前已將日誌收集器部署為 Panorama 管理伺服器，並配置這些介面，則必須重新設定，因為切換至日誌收集器模式已刪除所有組態（管理存取設定除外）。

1. 在 Panorama 管理伺服器上設定每個介面（但不是 MGT 介面）（若尚未設定）：
   1. 選取 **Panorama** > **Setup**（設定）> **Interfaces**（介面），然後按一下 Interface Name（介面名稱）。
   2. 選取 *<interface-name>* 以啟用介面。
   3. 視您網路的 IP 通訊協定而定，完成下列其中一個或兩個欄位集：
      - 對 ESXi
        - IPv4—**Public IP Address**（公共 **IP** 位址）、**IP Address**, **Netmask**, and **Default Gateway**

          IPv6—**IPv6 Address/Prefix Length**（**IPv6** 位址/首碼長度）及 **Default IPv6 Gateway**（預設的 **IPv6** 閘道）
      - 對 AWS、Azure 和 Google™ Cloud Platform
        - 公共 **IP** 位址
   4. 選取介面支援的裝置管理服務：

      Device Management and Device Log Collection（裝置管理和裝置日誌收集）—您可以指派一個或多個介面。

      Collector Group Communication（收集器群組通訊）—您只能指派一個介面。

      Device Deployment（裝置部署）（軟體和內容更新）—您只能指派一個介面。
   5. 按一下 **OK**（確定）儲存您的變更。
2. 在日誌收集器上設定每個介面（但不是 MGT 介面）：
   1. 選取 **Panorama** > **Managed Collectors**（受管理的收集器），再編輯日誌收集器。
   2. 選取 **Interfaces**（介面），然後按一下介面的名稱。
   3. 選取 *<interface-name>* 以啟用介面。
   4. 視您網路的 IP 通訊協定而定，完成下列其中一個或兩個欄位集：
      - 對 ESXi
        - IPv4—**Public IP Address**（公共 **IP** 位址）、**IP Address**, **Netmask**, and **Default Gateway**

© 2019 Palo Alto Networks, Inc.

IPv6—**IPv6 Address/Prefix Length**（**IPv6** 位址/首碼長度）及 **Default IPv6 Gateway**（預設的 **IPv6** 閘道）

- 對 AWS 和 Azure
  - 公共 **IP** 位址

5. 選取介面支援的裝置管理服務：

   Device Log Collection（裝置日誌收集）—您可以指派一個或多個介面。

   Collector Group Communication（收集器群組通訊）—您只能指派一個介面。
6. 按一下 **OK**（確定）以儲存對介面所做的變更。

3. 按一下 **OK**（確定），以儲存對日誌收集器所做的變更。
4. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後將您的變更 **Commit**（提交）至 Panorama 組態。

STEP 13 | （選用）如果您的部署使用自訂憑證在 Panorama 和受管理的裝置之間驗證，請部署自訂用戶端裝置憑證。如需詳細資訊，請參閱設定使用自訂憑證進行驗證。

1. 選取 **Panorama** > **Certificate Management**（憑證管理）> **Certificate Profile**（憑證設定檔），然後從下拉式清單中選擇憑證設定檔，或按一下 **New Certificate Profile**（新憑證設定檔）以建立憑證設定檔。
2. 針對日誌收集器，選取 **Panorama** > **Managed Collectors**（受管理的收集器）> **Add**（新增）> **Communication**（通訊）。
3. 選取 **Secure Client Communication**（安全用戶端通訊）核取方塊。
4. 從 Type（類型）下拉式清單中，選取裝置憑證的類型。
   - 如果您使用本機裝置憑證，請從 **Certificate**（憑證）和 **Certificate Profile**（憑證設定檔）各自的下拉式清單中選取。
   - 如果您使用 SCEP 作為裝置憑證，請從 **SCEPC Profile**（**SCEP** 設定檔）和 **Certificate Profile**（憑證設定檔）各自的下拉式清單中選取。
5. 按一下 **OK**（確定）。

STEP 14 | （選用）在日誌收集器上設定 安全伺服器通訊。如需詳細資訊，請參閱設定使用自訂憑證進行驗證。

1. 選取 **Panorama** > **Managed Collectors**（受管理的收集器）> **Add**（新增）> **Communication**（通訊）。
2. 確認未選取 **Custom Certificate Only**（僅限自訂憑證）核取方塊。這樣可讓您在移轉至自訂憑證期間繼續管理所有裝置。

   選取 *Custom Certificate Only*（僅限自訂憑證）核取方塊時，日誌收集器不會使用預先定義的憑證來驗證裝置，也無法使用這種憑證從裝置接收日誌。
3. 從 **SSL/TLS Service Profile**（**SSL/TLS** 服務設定檔）下拉式清單中，選取 SSL/TLS 服務設定檔。此 SSL/TLS 服務設定檔會套用至日誌收集器和送來日誌的裝置之間的所有 SSL 連線。
4. 從 **Certificate Profile**（憑證設定檔）下拉式清單中，選取憑證設定檔。
5. 選取 **Authorize Client Based on Serial Number**（根據序號來授權用戶端），讓伺服器根據受管理裝置的序號來檢查用戶端。用戶端憑證必須以特殊關鍵字 $UDID 來設定 CN，才能根據序號來驗證。
6. 在 **Disconnect Wait Time (min)**（中斷連線等候時間（分鐘））中，輸入 Panorama 在中斷並重新建立與受管理裝置間的連線之前應該等候的時間量。依預設，此欄位是空白，範圍是 0 至 44,640 分鐘。

   直到您提交新設定，中斷連線等候時間才會開始倒數計時。
7. （選用）設定授權清單。
   1. 按一下 Authorization List（授權清單）下的 **Add**（新增）。

© 2019 Palo Alto Networks, Inc.

2. 選取 **Subject**（主體）或 **Subject Alt Name**（主體別名）作為識別項類型。
3. 輸入所選類型的識別項。
4. 按一下 **OK**（確定）。
5. 選取 **Check Authorization List**（檢查授權清單）以強制執行授權清單。

8. 按一下 **OK**（確定）。
9. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**）。

STEP 15 | 將日誌收集器指派給收集器群組。

1. 設定收集器群組。您必須先執行 Panorama 提交再執行收集器群組提交，以將日誌收集器群組與 Panorama 同步，並在日誌收集器上使 Eth1、Eth2、Eth3、Eth4 和 Eth5 介面（如果您已設定）進入運作狀態。

   在任何單一收集器群組中，所有日誌收集器都必須在相同 *Panorama* 型號上執行：全部是 *M-600* 設備、全部都是 *M-500* 設備、全部都是 *M-200*，或全部是 *Panorama* 虛擬設備。

   如果您將多個日誌收集器新增至單一收集器群組，則最佳作法是 *Enable log redundancy across collectors*（啟用跨收集器的日誌備援）。使用此選項時，每個日誌收集器必須有相同數目的日誌記錄磁碟。

2. 選取 **Panorama** > **Managed Collectors**（受管理的收集器），確認日誌收集器設定已與 Panorama 同步。

   Configuration Status（組態狀態）欄應該顯示 In Sync（同步），Run Time Status（執行階段狀態）欄應該顯示 connected（已連線）。

3. 存取日誌收集器的 CLI，輸入以下命令以確認其介面是否運作：

   ```
   > show interface all
   ```

   對於正在運作的介面，輸出將顯示 `state`（狀態）為 `up`（正常）。

4. 如果收集器群組內有多個日誌收集器，請對日誌收集器使用的每個介面執行以下命令，疑難排解網路資源連線 以確認日誌收集器能夠相互通訊。對於 `source`（來源）IP 位址，則指定您要執行命令的日誌收集器介面。對於 `host`（主機）IP 位址，則指定同一收集器群組內另一個日誌收集器的相符介面。

STEP 16 | 接下來的步驟...

啟用日誌收集器以接收防火牆日誌：

1. 設定日誌轉送至 Panorama。
2. 確認日誌轉送至 Panorama。

設定具備本機日誌收集器的 Panorama 虛擬設備

如果 Panorama 虛擬設備在您從 Panorama 8.0 或更舊版本升級為 Panorama 8.1（或更新）版本時為傳統模式，則切換為 Panorama 模式以建立本機日誌收集器、在不丟失已有日誌下新增多個日誌記錄磁碟、增加日誌儲存上限至 24TB 以及啟用較快的記錄生成。

從傳統模式變更為 *Panorama* 模式後，傳統模式不再可用。

升級至 Panorama 8.1 之後，首先要將虛擬設備上的系統資源增加到 Panorama 模式所需的最低數量。增加資源時，Panorama 會重新啟動，所以請在維護時段內執行此程序。您必須安裝較大的系統磁碟 (81GB)、根據日誌儲存容量來增加 CPU 和記憶體，以及新增虛擬日誌記錄磁碟。新日誌記錄磁碟的容量，至少必須為

© 2019 Palo Alto Networks, Inc.

設備目前在傳統模式中使用的容量，而且不能小於 2TB。新增虛擬磁碟可讓您將現有日誌移轉至日誌收集器，還可讓日誌收集器儲存新的日誌。

如果 Panorama 部署在 HA 設定中，請先在次要對等上執行下列步驟，再於主要對等上執行。

STEP 1 | 決定您需要增加哪些系統資源，才能讓虛擬設備以 Panorama 模式運作。

即使您認為 *Panorama* 已有足夠的資源，也必須執行此步驟所指定的命令。

1. 存取 Panorama CLI：
   1. 使用終端機模擬軟體（例如 PuTTY），針對您指定給 Panorama MGT 介面的 IP 位址開啟 SSH 工作階段。
   2. 按照提示登入 CLI。
2. 執行下列命令以檢查您必須增加的資源：

```
> request system system-mode panorama
```

出現提示時，輸入 **y** 以繼續。輸出會指明您必須增加的資源。例如：

```
Panorama mode not supported on current system disk of size 52.0 GB.
Please attach a disk of size 81.0 GB, then use 'request system clone-
system-disk' to migrate the current system disk
Please add a new virtual logging disk with more than 50.00 GB of storage
 capacity.
Not enough CPU cores: Found 4 cores, need 8 cores
```

STEP 2 | 增加 CPU 和記憶體，並將系統磁碟更換為更大的磁碟。

1. 存取 VMware ESXi vSphere 用戶端，選取 **Virtual Machines**（虛擬機器），右鍵按一下 Panorama 虛擬設備並選取 **Power**（電源）> **Power Off**（關閉電源）。
2. 右鍵按一下 Panorama 虛擬設備並 **Edit Settings**（編輯設定）。
3. 選取 **Memory**（記憶體），並輸入新的 **Memory Size**（記憶體大小）。
4. 選取 **CPUs**，並指定 CPU 的數目（**Number of virtual sockets**（虛擬插槽數目）乘以 **Number of cores per socket**（每個插槽的核心數目））。
5. 新增虛擬磁碟。

   您將使用此磁碟來更換現有系統磁碟。

   1. 在 **Hardware**（硬體）設定中，**Add**（新增）磁碟、選取 **Hard Disk**（硬碟）作為硬體類型，然後按 **Next**（下一步）。
   2. **Create a new virtual disk**（建立新虛擬磁碟），然後按一下 **Next**（下一步）。
   3. 將 **Disk Size**（磁碟大小）設為剛好 81GB，並選取 **Thick Provision Lazy Zeroed**（重量型佈建延遲歸零）磁碟格式。
   4. 選取 **Specify a datastore or datastore structure**（指定資料存放或資料存放結構）作為位置，**Browse**（瀏覽）到至少有 81GB 的資料存放，按一下 **OK**（確定），然後按 **Next**（下一步）。
   5. 選取 SCSI **Virtual Device Node**（虛擬設備節點）（您可以使用預設選項），然後按一下 **Next**（下一步）。

      如果您選取 *SCSI* 以外的格式，*Panorama* 無法啟動。

   6. 確認設定正確，然後按一下 **Finish**（完成）和 **OK**（確定）。

© 2019 Palo Alto Networks, Inc.

6. 右鍵按一下 Panorama 虛擬設備並選取 **Power**（電源）> **Power On**（開啟電源）。等到 Panorama 重新啟動之後再繼續。
7. 返回 Panorama CLI，將資料從原始系統磁碟複製到新的系統磁碟：

```
> request system clone-system-disk target sdb
```

出現提示時，輸入 **y** 以繼續。

複製程序大約需要 20 至 25 分鐘，在此期間，Panorama 會重新啟動。程序完成時，輸出會指示您關閉 Panorama。

8. 返回 vSphere 用戶端主控台，右鍵按一下 Panorama 虛擬設備並選取 **Power**（電源）> **Power Off**（關閉電源）。
9. 右鍵按一下 Panorama 虛擬設備並 **Edit Settings**（編輯設定）。
10. 選取原始系統磁碟，按一下 **Remove**（移除），選取 **Remove from virtual machine**（從虛擬機器中移除），然後按一下 **OK**（確定）。
11. 右鍵按一下 Panorama 虛擬設備並 **Edit Settings**（編輯設定）。
12. 選取新的系統磁碟，將 **Virtual Device Node**（虛擬裝置節點）設為 **SCSI (0:0)**，然後按一下 **OK**（確定）。
13. 右鍵按一下 Panorama 虛擬設備並選取 **Power**（電源）> **Power On**（開啟電源）。繼續之前，等待 Panorama 以新的系統磁碟重新啟動（大約 15 分鐘）。

STEP 3 | 新增虛擬日誌記錄磁碟。

現有日誌將移轉到此磁碟。

1. 在 VMware ESXi vSphere 用戶端中，右鍵按一下 Panorama 虛擬設備並選取 **Power**（電源）> **Power Off**（關閉電源）。
2. 右鍵按一下 Panorama 虛擬設備並 **Edit Settings**（編輯設定）。
3. 重複步驟來新增虛擬磁碟。根據您需要的日誌儲存數量，將 **Disk Size**（磁碟大小）設為 2TB 的倍數。容量至少必須等於 Panorama 目前用於日誌的現有虛擬磁碟或 NFS 儲存空間大小。磁碟容量必須為 2TB 的倍數，最多為 24TB。例如，如果現有磁碟有 5TB 的日誌儲存空間，則您新增的磁碟至少必須有 6TB。

   切換至 Panorama 模式之後，Panorama 會自動將新磁碟分割成 2TB 分割區，各成為獨立的虛擬磁碟。
4. 右鍵按一下 Panorama 虛擬設備並選取 **Power**（電源）> **Power On**（開啟電源）。等到 Panorama 重新啟動之後再繼續。

STEP 4 | 從傳統模式切換至 Panorama 模式。

切換模式之後，設備會再次重新啟動，然後自動建立本機日誌收集器和收集器群組。在您稍後於此程序中移轉現有日誌之前，現有日誌無法供查詢或產生報告。

1. 返回 Panorama CLI 並執行下列命令。

```
> request system system-mode panorama
```

出現提示時，輸入 **y** 以繼續。重新啟動之後，Panorama 會自動建立本機日誌收集器（名為 Panorama），並建立收集器群組（名為 default）來包含此收集器。Panorama 也會設定您新增的虛擬日誌記錄磁碟，並分割成獨立的 2TB 磁碟。等待程序完成和 Panorama 重新啟動之後（大約五分鐘）再繼續。

2. 登入 Panorama 網頁介面。
3. 在 **Dashboard**（儀表板）的 **General Information**（一般資訊）設定中，確認 **Mode**（模式）現在為 **panorama**。

© 2019 Palo Alto Networks, Inc.

在 HA 部署中，次要對等此時處於暫停狀態，因為其模式 (Panorama) 不符合主要對等的模式（傳統）。稍後在此程序中將主要對等切換至 Panorama 模式之後，您將取消暫停次要對等。

4. 選取 **Panorama** > **Collector Groups**（收集器群組），以確認已建立 **default**（預設）收集器群組，且本機日誌收集器是預設收集器群組的一部分。
5. 將設定推送至受管理防火牆。
   - 若沒有擱置變更：
     1. 選取 **Commit**（提交）> **Push to Devices**（推送至裝置）和 **Edit Selections**（編輯選擇）。
     2. 選取 **Collector Group**（收集器群組）並確定已選取 **default**（預設）收集器群組。
     3. 按一下 **OK**（確定）與 **Commit**（提交）。
   - 若有擱置變更：
     1. 選取 **Commit**（提交）> **Commit and Push**（提交並推送），然後 **Edit Selections**（編輯選擇）。
     2. 確認包含 **Device Group**（裝置群組）裝置和 **Templates**（範本）。
     3. 選取 **Collector Group**（收集器群組）並確定已選取 **default**（預設）收集器群組。
     4. 按一下 **OK**（確定）以及 **Commit and Push**（提交並推送）。
6. 選取 **Panorama** > **Managed Collectors**（受管理的收集器），並確認本機日誌收集器的各欄顯示下列資訊：
   - Collector Name（收集器名稱）—預設為 Panorama 主機名稱。應該會列在 **default**（預設）收集器群組下方。
   - Connected（已連線）—核取標記
   - Configuration Status（組態狀態）—In sync（同步）
   - Run Time Status（執行階段狀態）—connected（已連線）

STEP 5 | （僅限 HA）將主要 Panorama 從傳統模式切換至 Panorama 模式。



此步驟會觸發容錯移轉。

1. 在主要 Panorama 上重複步驟 1 至步驟 4。

   等待主要 Panorama 重新啟動並返回主動 HA 狀態。如果未啟用先佔，您必須手動容錯回復：選取 **Panorama** > **High Availability**（高可用性），在 Operational Commands（操作命令）部分中，選取 **Make local Panorama functional**（讓本機 **Panorama** 運作）。
2. 在主要 Panorama 上，選取 **Dashboard**（儀表板），在 High Availability（高可用性）部分中，選取 **Sync to peer**（同步至對等），按一下 **Yes**（是），然後等待 **Running Config**（執行中設定）顯示 **Synchronized**（已同步）狀態。
3. 在次要 Panorama 上，選取 **Panorama** > **High Availability**（高可用性），在 Operational Commands（操作命令）部分中，選取 **Make local Panorama functional**（讓本機 **Panorama** 運作）。

   需要此步驟才能讓次要 Panorama 結束已暫停的 HA 狀態。

STEP 6 | 將現有日誌移轉至新的虛擬日誌記錄磁碟。

如果已將 Panorama 部署在 HA 設定中，請只在主要對等上執行此步驟。

1. 返回 Panorama CLI。
2. 啟動日誌移轉：

```
> request logdb migrate vm start
```

程序持續時間隨您移轉的日誌資料量而異。若要檢查移轉的狀態，請執行下列命令：

© 2019 Palo Alto Networks, Inc.

```
> request logdb migrate vm status
```

移轉完成時，輸出會顯示：`migration has been done`。

3. 確認現有日誌可用。
   1. 登入 Panorama 網頁介面。
   2. 選取 **Panorama** > **Monitor**（監控），選取您知道與某些現有日誌相符的日誌類型（例如，**Panorama** > **Monitor**（監控）> **System**（系統）），並確認日誌出現。

STEP 7 | 接下來的步驟...

設定將日誌轉送至 Panorama，讓日誌收集器從防火牆接收新的日誌。

在 Panorama 模式下設定 Panorama 虛擬設備

Panorama 模式把 Panorama™ 虛擬設備當作附本機日誌收集容量的 Panorama 管理伺服器操作。依預設，當原始部署上至少一個虛擬日誌記錄磁碟連接至 Amazon Web Services (AWS)、AWS、Google Cloud Platform、KVM、Hyper-V、ESXi 或 vCloud Air 時，Panorama 虛擬設備以 Panorama 模式部署。



雖然仍受支援，但不建議在生產環境中將具有 *50GB* 日誌記錄磁碟的傳統模式切換到 *Panorama* 模式。如果您切換到具有 *50GB* 日誌記錄磁碟的 *Panorama* 模式，將無法新增額外日誌記錄磁碟。

STEP 1 | 登入 Panorama CLI。

STEP 2 | 切換為 Panorama 模式。

1. 變更為 Panorama 模式：

```
> request system system-mode panorama
```

2. 輸入 **Y** 以確認模式變更。Panorama 虛擬設備重新啟動。重新啟動會終止終端機模擬軟體的工作階段並重新連線至 Panorama 虛擬設備以顯示 Panorama 登入提示。

   如果您看到 `CMS` 登入提示，則表示 Panorama 虛擬設備未完成重新啟動。在提示框中按 Enter，而不輸入使用者名稱或密碼。

STEP 3 | 確認已成功切換至 Panorama 模式。

1. 重新登入 CLI。
2. 確認已成功切換至 Panorama 模式：

```
> show system info | match system-mode
```

如果模式變更成功，則輸出顯示為：

```
> system mode:panorama
```

在僅管理模式下設定 Panorama 虛擬設備

僅管理模式模式把 Panorama 虛擬設備當作不附本機日誌收集容量的 Panorama 管理伺服器嚴格操作。依預設，Panorama 虛擬設備在原始部署時為 Panorama 模式。建議在原始部署之後將 Panorama 虛擬設備立即變更為僅管理模式，因為變更為僅管理模式必須在沒有將日誌轉送到 Panorama 管理伺服器時才可進行，因

© 2019 Palo Alto Networks, Inc.

為僅管理模式下的 Panorama 虛擬設備不支援日誌收集。在您變更為僅管理模式後，任何儲存於 Panorama 虛擬設備上的日誌資料會變為無法存取，且 ACC 和回報功能無法查詢儲存在 Panorama 設備上的日誌。

STEP 1 | 登入 Panorama CLI。

STEP 2 | 切換至僅管理模式。

1. 變更至僅管理模式：

```
> request system system-mode management-only
```

2. 輸入 **y** 以確認模式變更。Panorama 虛擬設備重新啟動。重新啟動會終止終端機模擬軟體的工作階段並重新連線至 Panorama 虛擬設備以顯示 Panorama 登入提示。

   如果您看到 `CMS` 登入提示，則表示 Panorama 虛擬設備未完成重新啟動。在提示框中按 Enter，而不輸入使用者名稱或密碼。

STEP 3 | 確認已成功切換至僅管理模式。

1. 重新登入 CLI。
2. 確認已成功切換至僅管理模式：

```
> show system info | match system-mode
```

如果模式變更成功，則輸出顯示為：

```
> system mode:management-only
```

擴展 Panorama 虛擬設備的日誌儲存容量

在執行 Panorama 虛擬設備的原始設定後，可用日誌儲存容量和擴展容量的選項需依據虛擬平台（VMware ESXi、vCloud Air、AWS、AWS GovCloud、Azure、Google Cloud Platform、KVM 或 Hyper-V）與模式（傳統、Panorama 或日誌收集器模式）：請參閱（Panorama 型號）以瞭解詳細資訊。

若要擴充 Panorama 虛擬設備上的日誌儲存容量，您必須新增額外日誌記錄磁碟。不支援擴充現有日誌記錄磁碟的日誌儲存容量，並且 Panorama 無法辨識額外儲存容量。例如，如果您已新增一個 2TB 日誌記錄磁碟，然後將現有日誌記錄磁碟擴充至 4TB，Panorama 會繼續將日誌記錄磁碟辨識為具有 2TB 儲存容量，並且忽略額外 2TB 儲存容量。



如需額外的日誌儲存空間，您還可以將防火牆日誌轉送至專用日誌收集器（請參閱設定受管理收集器）或設定日誌從 Panorama 轉送至外部目的地。

在擴展 Panorama 上的日誌儲存容量之前，先確定 Panorama 日誌儲存要求。

- 在傳統模式的 Panorama 虛擬設備上新增儲存空間時保留現有日誌
- 新增虛擬磁碟至 ESXi 伺服器上的 Panorama
- 新增虛擬磁碟至 vCloud Air 上的 Panorama
- 新增虛擬磁碟至 AWS 上的 Panorama
- 新增虛擬磁碟至 Azure 上的 Panorama
- 新增虛擬磁碟至 Google Cloud Platform 上的 Panorama
- 新增虛擬磁碟至 KVM 上的 Panorama
- 新增虛擬磁碟至 Hyper-V 上的 Panorama
- 將 Panorama ESXi 伺服器掛載到 NFS 資料存放

© 2019 Palo Alto Networks, Inc.

在傳統模式的 *Panorama* 虛擬設備上新增儲存空間時保留現有日誌

依預設，傳統模式的 Panorama 虛擬設備只能使用一個虛擬磁碟來記錄日誌。因此，如果您新增一個專用於記錄日誌的虛擬磁碟，Panorama 會停止使用系統磁碟上預設的 11GB 日誌儲存空間，而且會自動將任何現有日誌複製到新的日誌記錄磁碟。（Panorama 會繼續將系統磁碟用於儲存日誌以外的其他資料。）

如果您將現有的專用日誌記錄磁碟（最多 2TB 儲存容量）更換為 8TB 的磁碟，現有磁碟上的日誌將遺失。若要保留這些日誌，您可以：

- 在更換虛擬磁碟之前，設定日誌轉送至外部目的地。
- 為新的 8TB 磁碟設定新的 Panorama 虛擬設備並保留對包含舊磁碟的 Panorama 的存取權限，知道您不需要這些日誌為止。若要將防火牆日誌轉送至新的 Panorama 虛擬設備，您可以選擇重新設定防火牆，以連線至新的 Panorama IP 位址（選取 **Device**（裝置）> **Setup**（設定）> **Management**（管理），然後編輯 Panorama 設定），新增防火牆 至新的 Panorama 成為受管理的設備，以及 設定日誌轉送至 Panorama。若要在新的 Panorama 上重複使用舊的 Panorama IP 位址，還可以匯出設定（舊 Panorama），然後在新 Panorama 上匯入並載入設定。
- 將日誌從舊磁碟複製到新磁碟。視乎磁碟上目前儲存的日誌數目，複製過程可能需要數小時，在此期間，Panorama 將無法收集日誌。如需相關說明，請聯絡 Palo Alto Networks 客戶支援。

新增虛擬磁碟至 *ESXi* 伺服器上的 *Panorama*

若要擴充 Panorama 虛擬設備上的日誌儲存容量，您可以新增虛擬日誌記錄磁碟。如果設備處於 Panorama 模式，您可以新增 1 至 12 個虛擬日誌記錄磁碟（每個 2TB），或 1 個 24TB 的日誌記錄磁碟 ，合計最多 24TB。如果設備是傳統模式，則在 ESXi 5.5 和更新版本上，您可以新增一個最多 8TB 的虛擬日誌記錄磁碟，而在更舊的 ESXi 版本上，可以新增一個最多 2TB 的磁碟。此外，建議新增磁碟佈建格式相同的日誌記錄磁碟，避免因使用多個佈建格式不同的磁碟而帶來任何非預期的效能。

如果 *Panorama* 失去與新虛擬磁碟的連線，*Panorama* 可能會在失敗間隔期間遺失日誌。

若要允許備援，請使用 *RAID* 設定中的虛擬磁碟。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。

如有必要，您可以更換 ESXi 伺服器上的虛擬磁碟。

STEP 1 | 將額外磁碟新增至 Panorama

在所有模式下，*Panorama VM* 上的第一個日誌記錄磁碟至少必須為 *2TB*，才能新增額外的磁碟。如果第一個日誌記錄磁碟小於 *2TB*，則無法新增額外的磁碟空間。

1. 存取 VMware vSphere 用戶端並選取 **Virtual Machines**（虛擬機器）。
2. 右鍵按一下 Panorama 虛擬設備並選取 **Power**（電源）> **Power Off**（關閉電源）。
3. 右鍵按一下 Panorama 虛擬設備並選取 **Edit Settings**（編輯設定）。
4. 按一下 **Hardware**（硬體）頁籤中的 **Add**（新增），啟動 Add Hardware（新增硬體）精靈。
5. 從硬體類型中選取 **Hard Disk**（硬碟），然後按一下 **Next**（下一步）。
6. **Create a new virtual disk**（建立新虛擬磁碟），然後按一下 **Next**（下一步）。
7. 設定 **Disk Size**（磁碟大小）。如果 Panorama 虛擬設備是 Panorama 模式，大小至少要設為 2TB。如果設備是傳統模式，大小最多可以設為 8TB。

在 *Panorama* 模式下，您可以新增大於 *2TB* 的磁碟大小，*Panorama* 會自動建立最多的 *2TB* 分割區。例如，如果磁碟 *sdc* 是 *24TB*，則會建立 *12* 個 *2TB* 分割區。這些磁碟將命名為 *sdc1-12*。

© 2019 Palo Alto Networks, Inc.

8. 請選取 **Disk Provisioning**（磁碟佈建）格式，然後按一下 **Next**（下一步）。
9. **Specify a datastore or datastore structure**（指定資料存放或資料存放結構），**Browse**（瀏覽）至有足夠空間容納指定之 **Disk Size**（磁碟大小）的資料存放，按一下 **OK**（確定），然後按 **Next**（下一步）。
10. 選取 SCSI **Virtual Device Node**（虛擬設備節點）（您可以使用預設選項），然後按一下 **Next**（下一步）。

    所選取的節點必須為 *SCSI* 格式；如果選取其他格式，*Panorama* 將無法啟動。

11. 確認設定正確，然後按一下 **Finish**（完成）和 **OK**（確定）。

    隨即會將新磁碟顯示在虛擬設備的設備清單中。
12. 如有必要，請重複 步驟 4 至 步驟 11，將額外的磁碟新增至 Panorama 虛擬設備。
13. 右鍵按一下 Panorama 虛擬設備並選取 **Power**（電源）> **Power On**（開啟電源）。虛擬磁碟在第一次使用時會初始化。新磁碟大小決定了初始化所需的時長。

STEP 2 | 設定每個磁碟。

下列範例使用 sdc 虛擬磁碟。

1. 登入 Panorama CLI。
2. 輸入下列命令，以檢視 Panorama 虛擬設備上的磁碟：

   `show system disk details`

   使用者會看到下列回應：

```
 Name
: sdb
 State : Present
 Size : 2048 MB
 Status : Available
 Reason : Admin enabled
 Name : sdc
 State : Present
 Size : 2048 MB
 Status : Available
 Reason : Admin disabled
```

3. 針對所有出現下列回應的磁碟，輸入下列命令並於提示時確認要求：`Reason：Admindisabled` 回應：

   `request system disk add sdc`

   `requestsystem disk add` 命令不適用於僅管理模式下的 *Panorama* 管理伺服器，因為該模式不支援日誌紀錄。如果您沒有看到該命令，在 Panorama 模式下設定 Panorama 虛擬設備 可啟用日誌記錄磁碟。進入 *Panorama* 模式後，登入 Panorama CLI 並繼續前往步驟 4 以確認磁碟新增。
4. 輸入 **`show system disk details`** 命令，以確認磁碟新增狀態。當新增的磁碟全都顯示下列回應時，繼續 步驟 3：`Reason：Adminenabled`。

STEP 3 | 使磁碟可用於記錄日誌。

1. 登入 Panorama 網頁介面。
2. 選取 **Panorama** > **Managed Collectors**（受管理的收集器），再編輯日誌收集器。
3. 選取 **Disks**（磁碟），然後 Add（新增）每個新增的磁碟。
4. 按一下 **OK**（確定）。

© 2019 Palo Alto Networks, Inc.

5. 選取 **Commit**（提交）> **Commit and Push**（提交並推送），然後 **Commit and Push**（提交並推送）您的變更。

STEP 4 | 設定 Panorama 接收日誌。

此步驟適用於 Panorama 模式下新的 Panorama 部署。如果您要將日誌記錄磁碟新增至現有 Panorama 虛擬設備，請繼續 步驟 5。

1. 設定受管理的收集器。
2. 設定收集器群組。
3. 設定日誌轉送至 Panorama。

STEP 5 | 確認 Panorama 日誌儲存容量已增加。

1. 登入 Panorama 網頁介面。
2. 選取 **Panorama** > **Collector Groups**（收集器群組），然後選取 Panorama 虛擬設備所屬的收集器群組。
3. 確認 **Log Storage**（日誌儲存）容量正確地顯示磁碟容量。

新增虛擬磁碟至 *vCloud Air* 上的 *Panorama*

您可以新增虛擬日誌記錄磁碟以擴充在 Panorama™ 虛擬設備上的日誌儲存容量。如果設備處於 Panorama 模式，您可以新增 1 至 12 個虛擬日誌記錄磁碟（每個 2TB），或 1 個 24TB 的日誌記錄磁碟 ，合計最多 24TB。如果設備是傳統模式，您只能新增一個最多 8 TB 的虛擬日誌記錄磁碟。

如果 *Panorama* 失去與新虛擬磁碟的連線，*Panorama* 可能會在失敗期間丟失日誌。

如有必要，您可以更換 vCloud Air 上的虛擬磁碟。

STEP 1 | 將額外磁碟新增至 Panorama。

在所有模式下，*Panorama VM* 上的第一個日誌記錄磁碟至少必須為 *2TB* 以新增額外的磁碟。如果第一個日誌記錄磁碟小於 *2TB*，則無法新增額外的磁碟空間。

1. 存取 vCloud Air web 主控台，選取您的 **Virtual Private Cloud On Demand**（隨需的虛擬私人雲端）地區。
2. 在 **Virtual Machines**（虛擬機器）頁籤內，選取 Panorama 虛擬設備。
3. **Add another disk**（新增另一個磁碟）（動作 > 編輯資源 ）。
4. 設定 **Storage**（儲存空間）大小。如果 Panorama 虛擬設備是 Panorama 模式，大小至少要設為 2TB。如果設備是傳統模式，大小最多可以設為 8TB。

   在 *Panorama* 模式下，您可以新增大於 *2TB* 的磁碟大小，*Panorama* 會自動建立最多的 *2TB* 分割區。例如，如果磁碟 *sdc* 是 *24TB*，則 *Panorama* 將建立 *12* 個 *2TB* 分割區。這些磁碟將命名為 *sdc1* 到 *sdc12*。
5. 將儲存層設為 **Standard**（標準）或 **SSD-Accelerated**（**SSD** 加速）。
6. 如有必要，請重複之前步驟，將額外的磁碟新增至 Panorama 虛擬設備。
7. **Save**（儲存）變更。

STEP 2 | 設定每個磁碟。

下列範例使用 sdc 虛擬磁碟。

1. 登入 Panorama CLI。
2. 輸入下列命令，以檢視 Panorama 虛擬設備上的磁碟：

```
show system disk details
```


© 2019 Palo Alto Networks, Inc.

使用者會看到下列回應：

```
 Name
: sdb
 State : Present
 Size : 2048 MB
 Status : Available
 Reason : Admin enabled
 Name : sdc
 State : Present
 Size : 2048 MB
 Status : Available
 Reason : Admin disabled
```

3. 針對所有出現下列回應的磁碟，輸入下列命令並於提示時確認要求：`Reason：Admindisabled` 回應：

   `request system disk add sdc`

   `requestsystem disk add` 命令不適用於僅管理模式下的 *Panorama* 管理伺服器，因為該模式不支援日誌紀錄。如果您沒有看到該命令，在 Panorama 模式下設定 Panorama 虛擬設備 可啟用日誌記錄磁碟。進入 *Panorama* 模式後，登入 Panorama CLI 並繼續前往步驟 4 以確認磁碟新增。

4. 輸入 **`show system disk details`** 命令，以確認磁碟新增狀態。當新增的磁碟全都顯示下列回應時，繼續下一步：`Reason：Adminenabled`。

STEP 3 | 使磁碟可用於記錄日誌。

1. 登入 Panorama 網頁介面。
2. 選取 **Panorama** > **Managed Collectors**（受管理的收集器），再編輯日誌收集器。
3. 選取 **Disks**（磁碟），然後 **Add**（新增）每一個新磁碟。
4. 按一下 **OK**（確定）。
5. 選取 **Commit**（提交）> **Commit and Push**（提交並推送），然後 **Commit and Push**（提交並推送）您的變更。

STEP 4 | 設定 Panorama 接收日誌。

此步驟適用於 Panorama 模式下新的 Panorama 部署。如果您要將日誌記錄磁碟新增至現有虛擬 Panorama 設備，請繼續下一步。

1. 設定受管理的收集器。
2. 設定收集器群組。
3. 設定日誌轉送至 Panorama。

STEP 5 | 確認 Panorama 日誌儲存容量已增加。

1. 登入 Panorama 網頁介面。
2. 選取 **Panorama** > **Collector Groups**（收集器群組），然後選取虛擬 Panorama 設備所屬的收集器群組。
3. 確認 **Log Storage**（日誌儲存）容量正確地顯示新的磁碟容量。

新增虛擬磁碟至 *AWS* 上的 *Panorama*

在 AWS 上安裝 Panorama 或 在 AWS GovCloud 上安裝 Panorama後，新增虛擬日誌記錄磁碟至 Panorama™ 虛擬設備實例以提供受管理的防火牆所生成日誌的儲存空間。您可以針對 Panorama 模式下的 Panorama 虛擬設備或專用日誌收集器，將虛擬磁碟新增至本機日誌收集器。若要新增虛擬磁碟，則必須存取 Amazon Web Service 主控台、Panorama 命令行介面（CLI）和 Panorama 網頁介面。

© 2019 Palo Alto Networks, Inc.

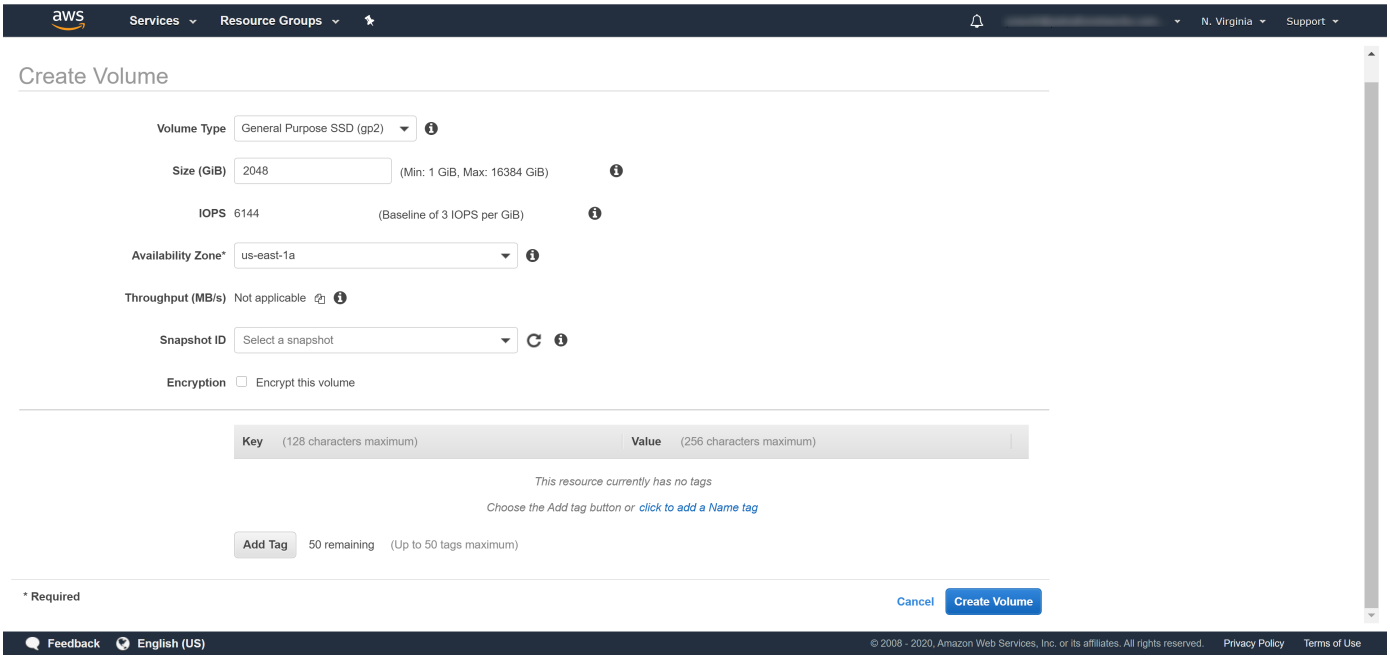
AWS 上的 Panorama 虛擬設備僅支援 2TB 日誌記錄磁碟，並總計支援最高 24TB 的日誌儲存空間。您無法新增少於 2TB 的日誌記錄磁碟，或無法被 2TB 整除的磁碟空間大小，因為 Panorama 虛擬設備分割區日誌記錄磁碟位於 2TB 分割區。例如，如果附加 4TB 日誌記錄磁碟，則 Panorama 將建立 2 個 2TB 分割區。但是您不能新增一個 5TB 日誌記錄磁碟，因為系統將不會視剩餘的 1TB 為分割區加以支援。

STEP 1 | 登入 AWS Web 服務主控台，然後選取 EC2 儀表板。

- Amazon Web 服務主控台
- AWS GovCloud Web 服務主控台

STEP 2 | 新增 Panorama 虛擬日誌記錄磁碟。

1. 在 EC2 儀表板上，選取 **Volumes**（磁碟區）並 **Create Volume**（建立磁碟區）：
   - 選取您想要的磁碟區類型。針對一般目的使用，選取 **General Purpose SSD (GP2)**（通用型 **SSD**）。
   - 將磁碟區的 **Size**（大小）設定為 2048 GiB。
   - 選取與您 Panorama 虛擬設備實例所在相同位置的可用區域。
   - （選用）加密磁碟區。
   - （選用）新增標籤至磁碟區。
2. 按一下 **Create Volume**（建立磁碟區）。



3. 在磁碟區網頁，選取磁碟區，然後選取 **Actions**（動作）> **Attach Volume**（連接磁碟區）。
4. 連接 Panorama 虛擬設備實例。

STEP 3 | 設定每個磁碟。

下列範例使用 sdc 虛擬磁碟。

1. 登入 Panorama CLI。
2. 輸入下列命令，以檢視 Panorama 虛擬設備上的磁碟：

   `show system disk details`

   使用者會看到下列回應：

```
 Name
: sdb
```


© 2019 Palo Alto Networks, Inc.

```
State : Present
Size : 2048 MB
Status : Available
Reason : Admin enabled
Name : sdc
State : Present
Size : 2048 MB
Status : Available
Reason : Admin disabled
```

3. 針對所有出現下列回應的磁碟，輸入下列命令並於提示時確認要求：`Reason：Admindisabled` 回應：

   `request system disk add sdc`

   `requestsystem disk add` 命令不適用於僅管理模式下的 *Panorama* 管理伺服器，因為該模式不支援日誌紀錄。如果您沒有看到該命令，在 Panorama 模式下設定 Panorama 虛擬設備 可啟用日誌記錄磁碟。進入 *Panorama* 模式後，登入 Panorama CLI 並繼續前往步驟 4 以確認磁碟新增。

4. 輸入 **`show system disk details`** 命令，以確認磁碟新增狀態。當新增的磁碟全都顯示下列回應時，繼續下一步：`Reason：Adminenabled`。

STEP 4 | 使磁碟可用於記錄日誌。

1. 登入 Panorama 網頁介面。
2. 編輯日誌收集器（**Panorama** > **Managed Collectors**（受管理的收集器））。
3. 選取 **Disks**（磁碟），然後**Add**（新增）每個新增的磁碟。
4. 按一下 **OK**（確定）。
5. 選取 **Commit**（提交）> **Commit and Push**（提交並推送），然後 **Commit and Push**（提交並推送）您的變更。

STEP 5 | （僅限在 Panorama 模式下的新 Panorama 部署）設定接收日誌的 Panorama。

如果您要將日誌記錄磁碟新增至現有 Panorama 虛擬設備，請跳至步驟 6。

1. 設定收集器群組。
2. 設定日誌轉送至 Panorama。

STEP 6 | 確認 Panorama 日誌儲存容量已增加。

1. 登入 Panorama 網頁介面。
2. 選取 Panorama 虛擬設備所屬收集器群組（**Panorama** > **Collector Groups**（收集器群組））。
3. 確認 **Log Storage**（日誌儲存）容量正確地顯示磁碟容量。

新增虛擬磁碟至 *Azure* 上的 *Panorama*

在 Azure 上安裝 Panorama 後，新增虛擬日誌記錄磁碟至 Panorama™ 虛擬設備實例以提供受管理的防火牆所生成日誌的儲存空間。您可以針對 Panorama 模式下的 Panorama 虛擬設備或專用日誌收集器，將虛擬磁碟新增至本機日誌收集器。若要新增虛擬磁碟，則必須存取 Microsoft Azure 入口網站、Panorama 命令行介面（CLI）和 Panorama 網頁介面。

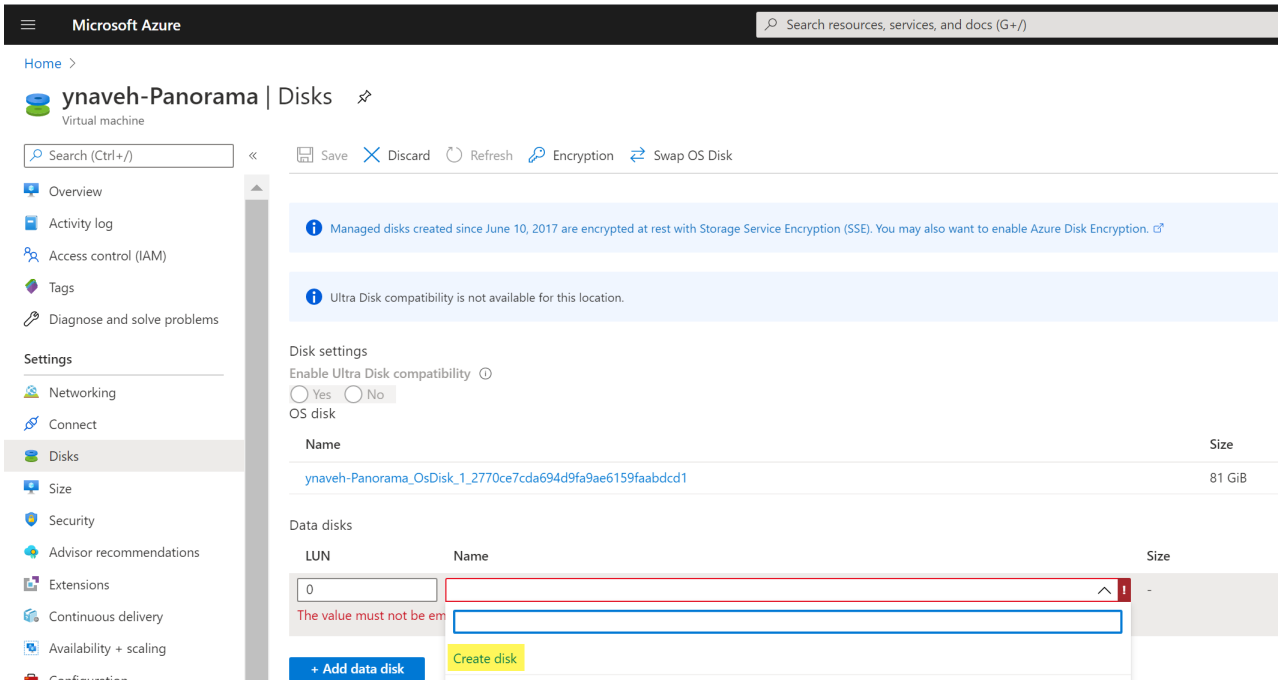
Azure 上的 Panorama 虛擬設備僅支援 2TB 日誌記錄磁碟，並總計支援最高 24TB 的日誌儲存空間。您無法新增少於 2TB 的日誌記錄磁碟，或無法被 2TB 整除的磁碟空間大小，因為 Panorama 虛擬設備分割區日誌記錄磁碟位於 2TB 分割區。例如，如果附加 4TB 日誌記錄磁碟，則 Panorama 將建立 2 個 2TB 分割區。但是您不能新增一個 5TB 日誌記錄磁碟，因為系統將不會視剩餘的 1TB 為分割區加以支援。

STEP 1 | 登入 Microsoft Azure 入口網站。

STEP 2 | 新增 Panorama 虛擬日誌記錄磁碟。

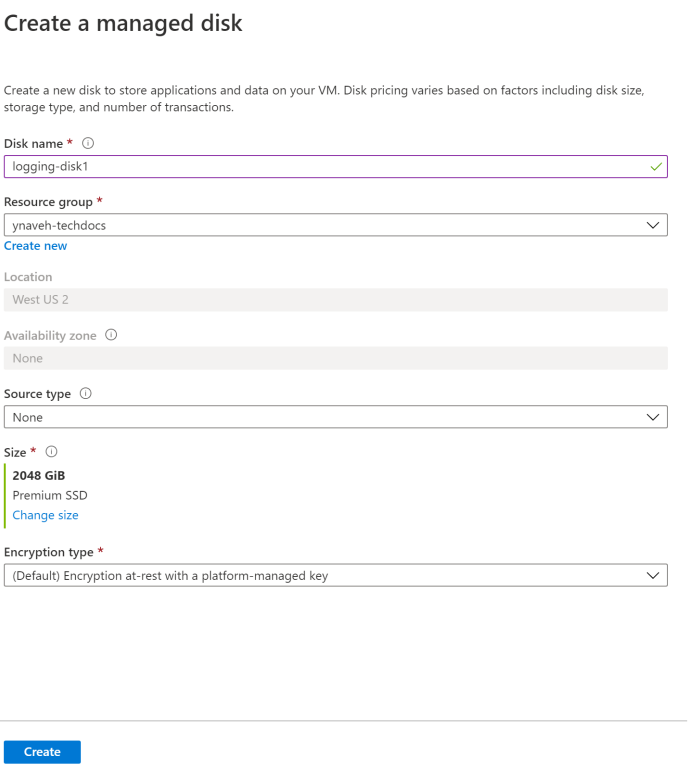
© 2019 Palo Alto Networks, Inc.

1. 在Azure 儀表板中，選取您想要新增日誌磁碟的 Panorama **Virtual Machines**（虛擬電腦）。
2. 選取 **Disks**（磁碟）。
3. **+Add data disk**（+新增資料磁碟）。
4. 在新磁碟的下拉式選單 **Create disk**（建立磁碟）。

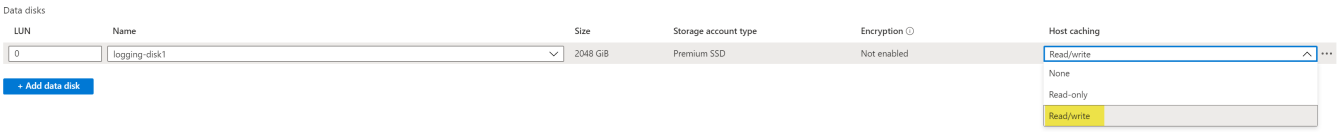


5. 設定日誌記錄磁碟。
    1. 輸入磁碟**Name**（名稱）。
    2. 選取資源群組。若您 **Create new**（建立新的）資源群組，則請輸入群組名稱。
    3. 確定 **Account type**（帳號類型）（此欄位為自動填充）。
    4. 在 **Source type**（來源類型）下拉式選單中，選取 **None**（無）。
    5. 選取 **Change Size**（變更大小），然後選取 2048 GiB 記錄磁碟。
    6. **Create**（建立）新記錄磁碟。

© 2019 Palo Alto Networks, Inc.



7. 對於 **Host caching**（主機快取），選取 **Read/write**（讀取/寫入）。



STEP 3 | 啟用每個磁碟。

下列範例使用 sdc 虛擬磁碟。

1. 登入 Panorama CLI。
2. 輸入下列命令，以檢視 Panorama 虛擬設備上的磁碟：

   `show system disk details`

   使用者會看到下列回應：

```
 Name
: sdb
 State : Present
 Size : 2048 MB
 Status : Available
 Reason : Admin enabled
 Name : sdc
 State : Present
 Size : 2048 MB
 Status : Available
 Reason : Admin disabled
```

3. 針對所有出現下列回應的磁碟，輸入下列命令並於提示時確認要求：`Reason：Admindisabled` 回應：

© 2019 Palo Alto Networks, Inc.

```
request system disk add sdc
```

> ***requestsystem disk add*** 命令不適用於僅管理模式下的 *Panorama* 管理伺服器，因為該模式不支援日誌紀錄。如果您沒有看到該命令，在 Panorama 模式下設定 Panorama 虛擬設備 可啟用日誌記錄磁碟。進入 *Panorama* 模式後，登入 Panorama CLI 並繼續前往步驟 4 以確認磁碟新增。

4. 輸入 **show system disk details** 命令，以確認磁碟新增狀態。當新增的磁碟全都顯示下列回應時，繼續下一步：`Reason：Adminenabled`。

STEP 4 | 使磁碟可用於記錄日誌。

1. 登入 Panorama 網頁介面。
2. 編輯日誌收集器（**Panorama** > **Managed Collectors**（受管理的收集器））
3. 選取 **Disks**（磁碟），然後**Add**（新增）每個新增的磁碟。
4. 按一下 **OK**（確定）。
5. 選取 **Commit**（提交）> **Commit and Push**（提交並推送），然後 **Commit and Push**（提交並推送）您的變更。

STEP 5 | （僅限在 Panorama 模式下的新 Panorama 部署）設定接收日誌的 Panorama。

如果您要將日誌記錄磁碟新增至現有 Panorama 虛擬設備，請跳至步驟 6。

1. 設定收集器群組。
2. 設定日誌轉送至 Panorama。

STEP 6 | 確認 Panorama 日誌儲存容量已增加。

1. 登入 Panorama 網頁介面。
2. 選取 Panorama 虛擬設備所屬收集器群組（**Panorama** > **Collector Groups**（收集器群組））。
3. 確認 **Log Storage**（日誌儲存）容量正確地顯示磁碟容量。

新增虛擬磁碟至 *Google Cloud Platform* 上的 *Panorama*

在 Google Cloud Platform 上安裝 Panorama 後，新增虛擬日誌記錄磁碟至 Panorama™ 虛擬設備實例，以提供受管理的防火牆所生成日誌的儲存空間。您可以針對 Panorama 模式下的 Panorama 虛擬設備或專用日誌收集器，將虛擬磁碟新增至本機日誌收集器。Google Cloud Platform 上的 Panorama 虛擬設備僅支援 2TB 日誌記錄磁碟，並總計支援最高 24TB 的日誌儲存空間。您無法新增少於 2TB 的日誌記錄磁碟，或無法被 2TB 整除的磁碟空間大小，因為 Panorama 虛擬設備分割區日誌記錄磁碟位於 2TB 分割區。例如，如果附加 4TB 日誌記錄磁碟，則 Panorama 將建立 2 個 2TB 分割區。但是您不能新增一個 5TB 日誌記錄磁碟，因為系統將不會視剩餘的 1TB 為分割區加以支援。

STEP 1 | 登入 Google Cloud 主控台。

STEP 2 | 新增虛擬日誌記錄磁碟。

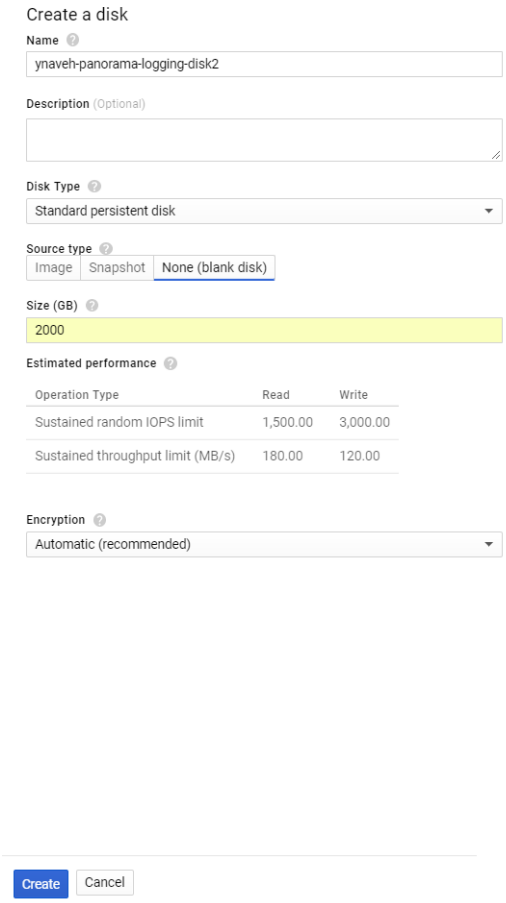
1. 在產品與服務功能表中，選取並 **Edit**（編輯）Panorama 虛擬設備實例（**Compute Engine**（計算引擎）> **VM Instances**（**VM** 實例））。
2. 在額外的磁碟部分內 **Add Item**（新增項目）。
3. **Create disk**（建立磁碟）（**Name**（命名）下拉式選單）。

STEP 3 | 設定虛擬日誌記錄磁碟。

1. 輸入 **Name**（名稱）。
2. 展開 **Disk Type**（磁碟類型）下拉式選單並選取想要的類型。
3. 對於 **Source type**（來源類型），選取 **None (blank disk)**（無，空白磁碟）。
4. 設定虛擬日誌記錄磁碟的**Size (GB)**（大小, **GB**）。

© 2019 Palo Alto Networks, Inc.

5. 按一下 **Create**（建立）。



6. **Save**（儲存）變更以更新 Panorama 虛擬設備實例。

STEP 4 | 設定每個磁碟。

下列範例使用 sdc 虛擬磁碟。

1. 登入 Panorama CLI。
2. 輸入下列命令，以檢視 Panorama 虛擬設備上的磁碟：

   `show system disk details`

   使用者會看到下列回應：

```
 Name
: sdb
 State : Present
 Size : 2048 MB
 Status : Available
 Reason : Admin enabled
 Name : sdc
 State : Present
 Size : 2048 MB
 Status : Available
 Reason : Admin disabled
```

3. 針對所有出現下列回應的磁碟，輸入下列命令並於提示時確認要求：`Reason：Admin disabled` 回應：

© 2019 Palo Alto Networks, Inc.

```
request system disk add sdc
```

> ***request system disk add*** 命令不適用於僅管理模式下的 *Panorama* 管理伺服器，因為該模式不支援日誌紀錄。如果您沒有看到該命令，在 Panorama 模式下設定 Panorama 虛擬設備 可啟用日誌記錄磁碟。進入 *Panorama* 模式後，登入 Panorama CLI 並繼續前往步驟 4 以確認磁碟新增。

4. 輸入 **show system disk details** 命令，以確認磁碟新增狀態。當新增的磁碟全都顯示下列回應時，繼續下一步：`Reason：Admin enabled`。

STEP 5 | 使磁碟可用於記錄日誌。

1. 登入 Panorama 網頁介面。
2. 編輯日誌收集器（**Panorama** > **Managed Collectors**（受管理的收集器））。
3. 選取 **Disks**（磁碟），然後**Add**（新增）每個新增的磁碟。
4. 按一下 **OK**（確定）。
5. 選取 **Commit**（提交）> **Commit and Push**（提交並推送），然後 **Commit and Push**（提交並推送）您的變更。

STEP 6 | （僅限在 Panorama 模式下的新 Panorama 部署）設定接收日誌的 Panorama。

如果您要將日誌記錄磁碟新增至現有 Panorama 虛擬設備，請跳至步驟 7。

1. 設定收集器群組。
2. 設定日誌轉送至 Panorama。

STEP 7 | 確認 Panorama 日誌儲存容量已增加。

1. 登入 Panorama 網頁介面。
2. 選取 Panorama 虛擬設備所屬收集器群組（**Panorama** > **Collector Groups**（收集器群組））。
3. 確認 **Log Storage**（日誌儲存）容量正確地顯示磁碟容量。

新增虛擬磁碟至 *KVM* 上的 *Panorama*

在 KVM 上安裝 Panorama 後，新增虛擬日誌記錄磁碟至 Panorama™ 虛擬設備實例以提供受管理的防火牆所生成日誌的儲存空間。您可以針對 Panorama 模式下的 Panorama 虛擬設備或專用日誌收集器，將虛擬磁碟新增至本機日誌收集器。KVM 上的 Panorama 虛擬設備僅支援 2TB 日誌記錄磁碟，並總計支援最高 24TB 的日誌儲存空間。您無法新增少於 2TB 的日誌記錄磁碟，或無法被 2TB 整除的磁碟空間大小，因為 Panorama 虛擬設備分割區日誌記錄磁碟位於 2TB 分割區。例如，如果附加 4TB 日誌記錄磁碟，則 Panorama 將建立 2 個 2TB 分割區。但是您不能新增一個 5TB 日誌記錄磁碟，因為系統將不會視剩餘的 1TB 為分割區加以支援。

STEP 1 | **Shutdown**（關閉）在虛擬電腦管理員上的 Panorama 虛擬設備實例。

STEP 2 | 在虛擬電腦管理員上的 Panorama 虛擬設備實例按兩下，並**Show virtual hardware details**（顯示虛擬硬體詳細內容）。

STEP 3 | 新增虛擬日誌記錄磁碟。視需重覆此步驟。

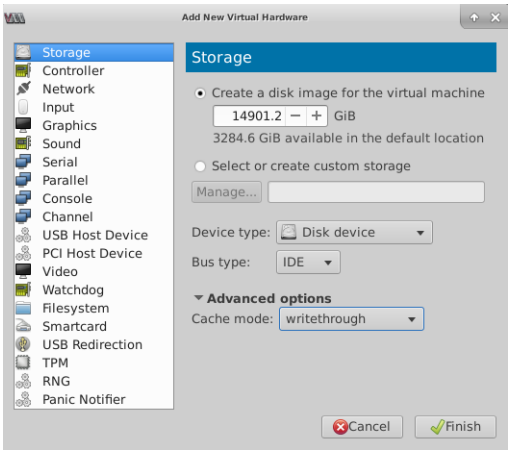
1. **Create a disk image for a virtual image**（建立虛擬映像磁碟映像）（**Add Hardware** > **Storage**（新增硬體儲存空間））並設定虛擬磁碟量到適當的 2TB value:2000GB 或 14901.2GiB，視虛擬電腦管理員而定。

   > 依據版本，有些虛擬電腦管理員使用 *GiB*（*gibibyte*）來配置記憶體。請確定您正確轉換所需的儲存空間容量，以避免小於部建虛擬日誌記錄磁碟並傳送 *Panorama* 虛擬設備進入維護模式。

2. 在 **Device type**（裝置類型）下拉式選單中，選取 **Disk device**（磁碟裝置）。

© 2019 Palo Alto Networks, Inc.

3. 在 **Bus type**（匯流排類型）下拉式清單中，依您的設定來選取 **VirtIO** 或 **IDE**。
4. 展開 **Advanced options**（進階選項），然後在 **Cache mode**（快取模式）下拉式清單中，選取 **writethrough**。
5. 按一下 **Finish**（完成）。



STEP 4 | 將 Panorama 虛擬設備實例 **Power on**（開啟電源）。

STEP 5 | 設定每個磁碟。

下列範例使用 sdc 虛擬磁碟。

1. 登入 Panorama CLI。
2. 輸入下列命令，以檢視 Panorama 虛擬設備上的磁碟：

   `show system disk details`

   使用者會看到下列回應：

```
 Name
: sdb
 State : Present
 Size : 2048 MB
 Status : Available
 Reason : Admin enabled
 Name : sdc
 State : Present
 Size : 2048 MB
 Status : Available
 Reason : Admin disabled
```

3. 針對所有出現下列回應的磁碟，輸入下列命令並於提示時確認要求：`Reason：Admin disabled` 回應：

   `request system disk add sdc`

   `request system disk add` 命令不適用於僅管理模式下的 *Panorama* 管理伺服器，因為該模式不支援日誌紀錄。如果您沒有看到該命令，在 Panorama 模式下設定 Panorama 虛擬設備 可啟用日誌記錄磁碟。進入 *Panorama* 模式後，登入 Panorama CLI 並繼續前往步驟 4 以確認磁碟新增。

4. 輸入 **`show system disk details`** 命令，以確認磁碟新增狀態。當新增的磁碟全都顯示下列回應時，繼續下一步：`Reason：Admin enabled`。

STEP 6 | 使磁碟可用於記錄日誌。

© 2019 Palo Alto Networks, Inc.

1. 登入 Panorama 網頁介面。
2. 編輯日誌收集器（**Panorama** > **Managed Collectors**（受管理的收集器））。
3. 選取 **Disks**（磁碟），然後**Add**（新增）每個新增的磁碟。
4. 按一下 **OK**（確定）。
5. 選取 **Commit**（提交）> **Commit and Push**（提交並推送），然後 **Commit and Push**（提交並推送）您的變更。

STEP 7 | （僅限在 Panorama 模式下的新 Panorama 部署）設定接收日誌的 Panorama。

如果您要將日誌記錄磁碟新增至現有 Panorama 虛擬設備，請跳至步驟 8。

1. 設定收集器群組。
2. 設定日誌轉送至 Panorama。

STEP 8 | 確認 Panorama 日誌儲存容量已增加。

1. 登入 Panorama 網頁介面。
2. 選取 Panorama 虛擬設備所屬收集器群組（**Panorama** > **Collector Groups**（收集器群組））。
3. 確認 **Log Storage**（日誌儲存）容量正確地顯示磁碟容量。

新增虛擬磁碟至 *Hyper-V* 上的 *Panorama*

在 在 Hyper-V 上安裝 Panorama 後，新增虛擬日誌記錄磁碟至 Panorama™ 虛擬設備實例以提供受管理的防火牆所生成日誌的儲存空間。您可以針對 Panorama 模式下的 Panorama 虛擬設備或專用日誌收集器，將虛擬磁碟新增至本機日誌收集器。Hyper-V 上的 Panorama 虛擬設備僅支援 2TB 日誌記錄磁碟，並總計支援最高 24TB 的日誌儲存空間。您無法新增少於 2TB 的日誌記錄磁碟，或無法被 2TB 整除的磁碟空間大小，因為 Panorama 虛擬設備分割區日誌記錄磁碟位於 2TB 分割區。例如，如果附加 4TB 日誌記錄磁碟，則 Panorama 將建立 2 個 2TB 分割區。但是您不能新增一個 5TB 日誌記錄磁碟，因為系統將不會視剩餘的 1TB 為分割區加以支援。

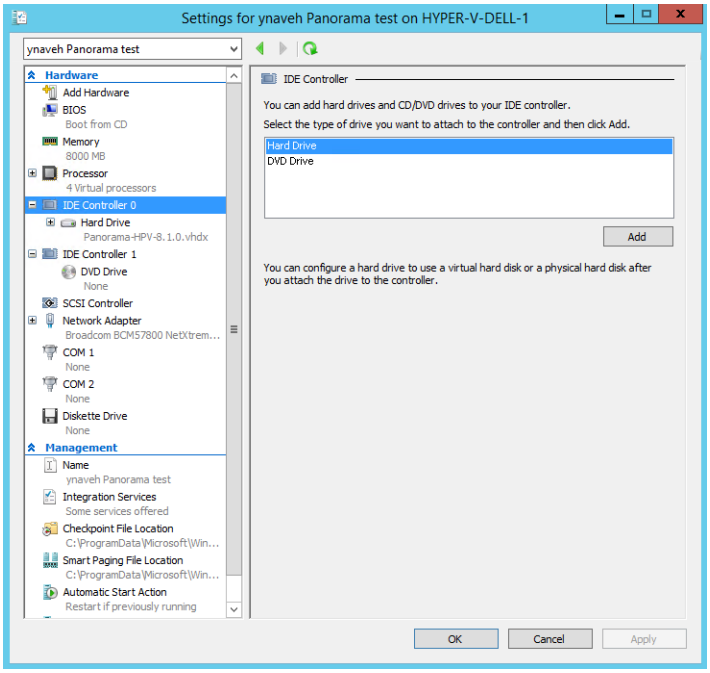
STEP 1 | 關閉 Panorama 虛擬設備電源。

1. 在 Hyper-V 管理員上，從 **Virtual Machines**（虛擬機器）清單中選取 Panorama 虛擬設備實例。
2. 選取 **Action**（動作）> **Turn Off**（關閉）以關閉 Panorama 虛擬設備。

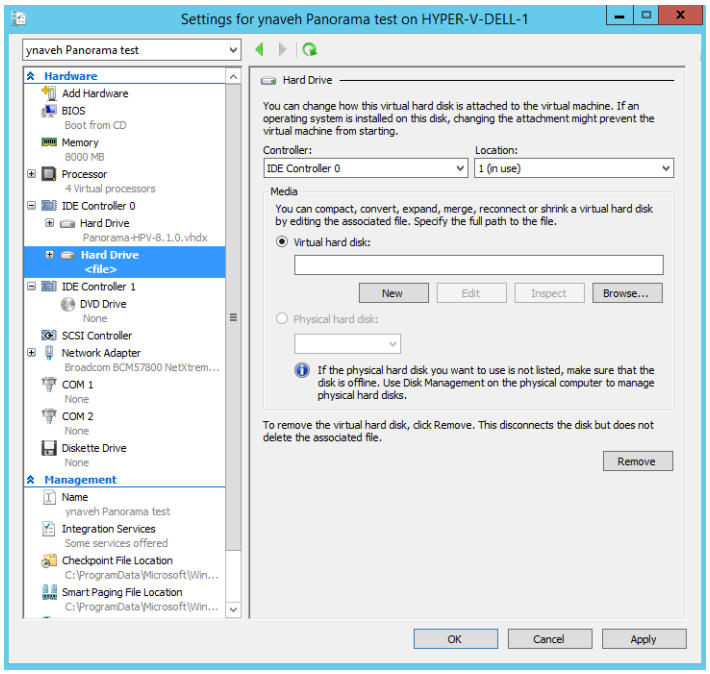
STEP 2 | 新增虛擬日誌記錄磁碟。視需重覆此步驟。

1. 從 **Virtual Machines**（虛擬機器）清單中，選取 Panorama 虛擬設備，然後選取 **Action**（動作）> **Settings**（設定）。
2. 在 **Hardware**（硬體）清單中，選取 **IDE Controller 0**（**IDE** 控制器 **0**）。
3. 從 **IDE Controller**（**IDE** 控制器）磁碟機清單中，選取 **Hard Drive**（硬碟），然後 **Add**（新增）新的虛擬日誌紀錄磁碟。

© 2019 Palo Alto Networks, Inc.



4. 選取 **IDE Controller 0**（**IDE** 控制器 **0**）下建立的新 **Hard Drive**（硬碟）。
5. 在 **Media**（媒體）下，新增一個 **New**（新）硬碟。

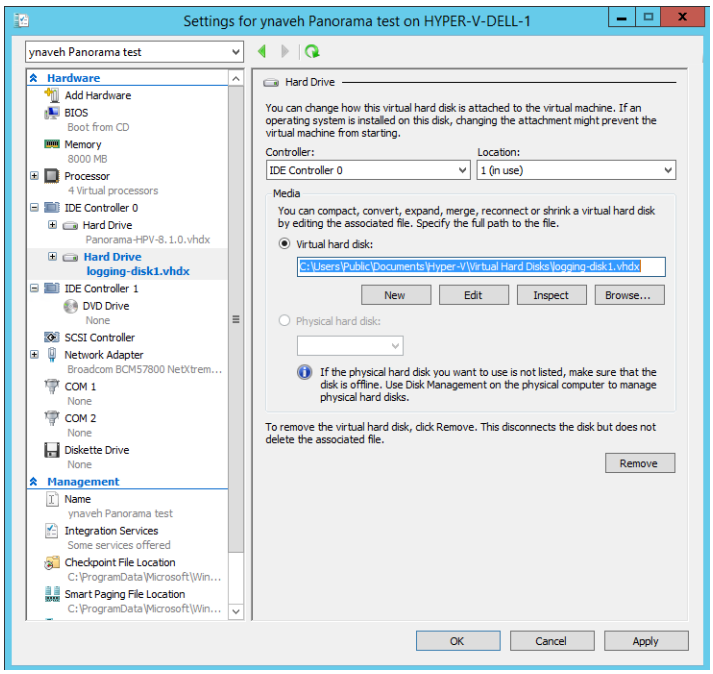


STEP 3 | 設定新的虛擬日誌記錄磁碟。

1. 如果您看到 Before You Begin（開始之前）提示，按一下 **Next**（下一步）以開始新增虛擬日誌紀錄磁碟。
2. 對於 Disk Format（磁碟格式），選取 **VHDX**。按一下 **Next**（下一步）繼續。
3. 對於 Disk Type（磁碟類型），根據您的需求選取 **Fixed Size**（固定大小）或 **Dynamically Expanding**（動態擴充）。按一下 **Next**（下一步）繼續。
4. 指定虛擬日誌紀錄磁碟檔案的 **Name**（名稱）和 **Location**（位置）。按一下 **Next**（下一步）繼續。

© 2019 Palo Alto Networks, Inc.

5. 若要設定磁碟，選取 **Create a new virtual hard disk**（建立新虛擬磁碟），然後輸入磁碟大小。按一下 **Next**（下一步）繼續。
6. 檢閱 Summary（摘要）並 **Finish**（完成）擬擬日誌紀錄硬碟新增。
7. **Apply**（套用）新硬碟新增。



STEP 4 | 開啟 Panorama 虛擬設備電源。

1. 從 **Virtual Machines**（虛擬機器）清單中選取 Panorama 虛擬設備實例。
2. 選取 **Action**（動作）> **Start**（開啟）以開啟 Panorama 虛擬設備。

STEP 5 | 設定每個磁碟。

下列範例使用 sdc 虛擬磁碟。

1. 登入 Panorama CLI。
2. 輸入下列命令，以檢視 Panorama 虛擬設備上的磁碟：

   `show system disk details`

   使用者會看到下列回應：

```
 Name
: sdb
 State : Present
 Size : 2048 MB
 Status : Available
 Reason : Admin enabled
 Name : sdc
 State : Present
 Size : 2048 MB
 Status : Available
 Reason : Admin disabled
```

3. 針對所有出現下列回應的磁碟，輸入下列命令並於提示時確認要求：`Reason：Admin disabled` 回應：

   `request system disk add sdc`

© 2019 Palo Alto Networks, Inc.



request system disk add 命令不適用於僅管理模式下的 *Panorama* 管理伺服器，因為該模式不支援日誌紀錄。如果您沒有看到該命令，在 Panorama 模式下設定 Panorama 虛擬設備 可啟用日誌記錄磁碟。進入 *Panorama* 模式後，登入 Panorama CLI 並繼續前往步驟 4 以確認磁碟新增。

4. 輸入 **show system disk details** 命令，以確認磁碟新增狀態。當新增的磁碟全都顯示下列回應時，繼續下一步：`Reason：Admin enabled`。

STEP 6 | 使磁碟可用於記錄日誌。

1. 登入 Panorama 網頁介面。
2. 編輯日誌收集器（**Panorama** > **Managed Collectors**（受管理的收集器））。
3. 選取 **Disks**（磁碟），然後**Add**（新增）每個新增的磁碟。
4. 按一下 **OK**（確定）。
5. 選取 **Commit**（提交）> **Commit and Push**（提交並推送），然後 **Commit and Push**（提交並推送）您的變更。

STEP 7 | （僅限在 Panorama 模式下的新 Panorama 部署）設定接收日誌的 Panorama。

如果您要將日誌記錄磁碟新增至現有 Panorama 虛擬設備，請跳至步驟 8。

1. 設定收集器群組。
2. 設定日誌轉送至 Panorama。

STEP 8 | 確認 Panorama 日誌儲存容量已增加。

1. 登入 Panorama 網頁介面。
2. 選取 Panorama 虛擬設備所屬收集器群組（**Panorama** > **Collector Groups**（收集器群組））。
3. 確認 **Log Storage**（日誌儲存）容量正確地顯示磁碟容量。

將 *Panorama ESXi* 伺服器掛載到 *NFS* 資料存放

當傳統模式的 Panorama 虛擬設備在 ESXi 伺服器上執行時，掛載 Network File System（網路檔案系統 - NFS）資料存放允許將日誌記錄到中央位置，並將日誌儲存容量擴展至超出虛擬磁碟支援的上限。（在 ESXi 5.5 及更新版本支援多達 8TB 的虛擬磁碟。較早 ESXi 版本支援最多 2TB 的虛擬磁碟。）在 Panorama 高可用性 (HA) 設定中設定 NFS 資料存放之前，請參閱 Panorama HA 中的日誌記錄注意事項。



Panorama 模式的 *Panorama* 虛擬設備不支援 *NFS*。

STEP 1 | 選取 **Panorama** > **Setup**（設定）> **Operations**（操作），然後在 [雜項] 部分中，按一下 **Storage Partition Setup**（儲存分割區設定）。

STEP 2 | 將 **Storage Partition**（儲存分割區）類型設為 **NFS V3**。

STEP 3 | 輸入 NFS **Server**（伺服器）的 IP 位址。

STEP 4 | 輸入儲存日誌檔案的 **Log Directory**（日誌目錄）路徑。例如，export/panorama。

STEP 5 | 對於 **Protocol**（協定），選取 **TCP** 或 **UDP**，再輸入用來存取 NFS 伺服器的 **Port**（連接埠）。



若要在 *TCP* 上使用 *NFS*，則 *NFS* 伺服器必須支援它。一般的 *NFS* 連接埠是 *UDP/TCP 111*（適用於 *RPC*）和 *UDP/TCP 2049*（適用於 *NFS*）。

© 2019 Palo Alto Networks, Inc.

STEP 6 | 為了獲得理想的 NFS 效能，請在 **Read Size**（讀取大小）和 **Write Size**（寫入大小）欄位中，指定用戶端與伺服器彼此往來傳送的資料區塊大小上限。定義讀取/寫入大小，最佳化在 Panorama 與 NFS 資料存放之間傳輸資料的資料量和速度。

STEP 7 | （選用）選取 **Copy On Setup**（安裝時複製）將 Panorama 上儲存的現有日誌複製到 NFS 磁碟區。如果 Panorama 有大量的現有日誌，則啟用此選項可能會啟動傳輸大量資料。

STEP 8 | 按一下 **Test Logging Partition**（測試日誌記錄分割區）以確認 Panorama 可存取 NFS **Server**（伺服器）和 **Log Directory**（日誌目錄）。

STEP 9 | 按一下 **OK**（確定）儲存您的變更。

STEP 10 | 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。重新開機時，Panorama 虛擬設備將日誌寫入本機儲存磁碟。

STEP 11 | 選取 **Panorama** > **Setup**（設定）> **Operations**（操作），然後在 Device Operations（裝置操作）部分中選取 **Reboot Panorama**（重新啟動 **Panorama**）。重新啟動後，Panorama 開始寫入日誌至 NFS 資料存放。

在 Panorama 虛擬設備上增加 CPU 和記憶體

當您執行 Panorama 虛擬設備的原始設定時，您需要根據設備是 Panorama 模式或僅管理模式，並根據日誌儲存容量或受管理防火牆數目，以指定記憶體和 CPU 數目。如果您後來增加儲存容量或受管理的防火牆，您也必須增加記憶體和 CPU。在日誌收集器模式下的 Panorama 虛擬設備必須符合系統需求，並不需要擁有超出最低需求的 CPU 和記憶體。檢閱 設定 Panorama 虛擬設備的先決條件 以瞭解各 Panorama 模式的 CPU 及記憶體需求。

- 為 ESXi 伺服器上的 Panorama 增加 CPU 和記憶體
- 為 vCloud Air 伺服器上的 Panorama 增加 CPU 和記憶體
- 為 AWS 上的 Panorama 增加 CPU 和記憶體
- 為 Azure 上的 Panorama 增加 CPU 和記憶體
- 為 Google Cloud Platform 的 Panorama 增加 CPU 和記憶體
- 為 KVM 上的 Panorama 增加 CPU 和記憶體
- 為 Hyper-V 上的 Panorama 增加 CPU 和記憶體

為 *ESXi* 伺服器上的 *Panorama* 增加 *CPU* 和記憶體

關於 Panorama 需要的最少 CPU 和記憶體，請參閱 在 Panorama 虛擬設備上增加 CPU 和記憶體。

STEP 1 | 存取 VMware vSphere 用戶端並選取 **Virtual Machines**（虛擬機器）。

STEP 2 | 右鍵按一下 Panorama 虛擬設備並選取 **Power**（電源）> **Power Off**（關閉電源）。

STEP 3 | 右鍵按一下 Panorama 虛擬設備並選取 **Edit Settings**（編輯設定）。

STEP 4 | 選取 **Memory**（記憶體），並輸入新的 **Memory Size**（記憶體大小）。

STEP 5 | 選取 **CPUs**，並指定 CPU 的數目（**Number of virtual sockets**（虛擬插槽數目）乘以 **Number of cores per socket**（每個插槽的核心數目））。

STEP 6 | 按一下 **OK**（確定）儲存您的變更。

STEP 7 | 右鍵按一下 Panorama 虛擬設備並選取 **Power**（電源）> **Power On**（開啟電源）。

© 2019 Palo Alto Networks, Inc.

為 *vCloud Air* 伺服器上的 *Panorama* 增加 *CPU* 和記憶體

關於 Panorama 需要的最少 CPU 和記憶體，請參閱 在 Panorama 虛擬設備上增加 CPU 和記憶體。

STEP 1 | 存取 vCloud Air web 主控台並選取您的 **Virtual Private Cloud OnDemand**（虛擬私人雲 **OnDemand**）地區。

STEP 2 | 在 **Virtual Machines**（虛擬機器）頁籤中，選取 Panorama 虛擬機器，然後 **Power Off**（關閉電源）。

STEP 3 | 選取 **Actions**（動作）> **Edit Resources**（編輯資源）。

STEP 4 | 設定 **CPU** 和 **Memory**（記憶體）。

STEP 5 | **Save**（儲存）變更。

STEP 6 | 選取 Panorama 虛擬機器，然後 **Power On**（開啟電源）。

為 *AWS* 上的 *Panorama* 增加 *CPU* 和記憶體

有關 Panorama™ 所需最低 CPU 與記憶體，請參閱在 Panorama 虛擬設備上增加 CPU 和記憶體。

日誌收集器模式內的 *Panorama* 虛擬設備若在您部署虛擬電腦後重新調整其大小，則不會仍舊維持日誌收集器模式，且會造成日誌資料的丟失。

STEP 1 | 登入 AWS Web 服務主控台，然後選取 EC2 儀表板。

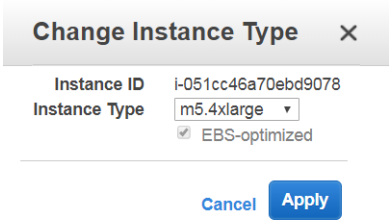
- Amazon Web 服務主控台
- AWS GovCloud Web 服務主控台

STEP 2 | 在 EC2 儀表板上，選取 **Instances**（實例），然後選取 Panorama 虛擬設備實例。

STEP 3 | 選取 **Actions**（動作）> **Instance State**（實例狀態）> **Stop**（停止）以關閉 Panorama 虛擬設備實例。

STEP 4 | 選取 **Actions**（動作）> **Instance Settings**（實例設定）> **Change Instance Type**（變更實例類型）以變更 Panorama 虛擬設備實例類型。

STEP 5 | 選取您想要升級的 **Instance Type**（實例類型）並 **Apply**（套用）它。



STEP 6 | 選取 **Actions**（動作）> **Instance State**（實例狀態）> **Start**（啟動）以啟動 Panorama 虛擬設備實例。

為 *Azure* 上的 *Panorama* 增加 *CPU* 和記憶體

有關 Panorama™ 所需最低 CPU 與記憶體，請參閱在 Panorama 虛擬設備上增加 CPU 和記憶體。

© 2019 Palo Alto Networks, Inc.

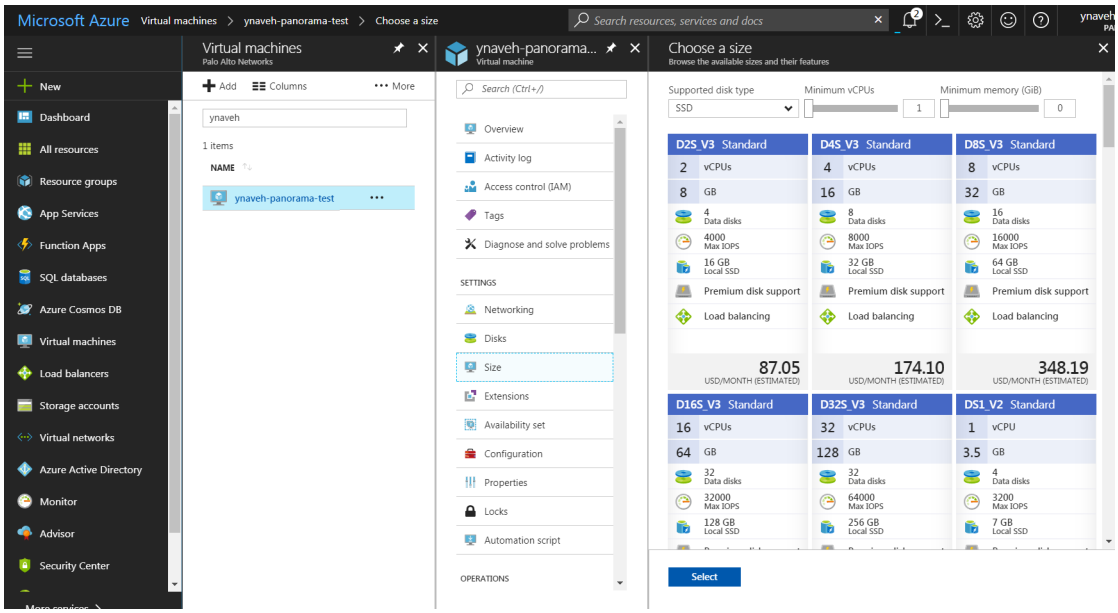
日誌收集器模式內的 *Panorama* 虛擬設備若在您部署虛擬電腦後重新調整其大小，則不會仍舊維持日誌收集器模式，且會造成日誌資料的丟失。

STEP 1 | 登入 Microsoft Azure 入口網站。

STEP 2 | 在 Azure 儀錶板上的 **Virtual machines**（虛擬電腦）下，選取 Panorama 虛擬設備。

STEP 3 | 選取 **Overview**（概觀）和 **Stop**（停止）Panorama 虛擬設備。

STEP 4 | 選取新虛擬電腦 **Size**（大小），然後 **Select**（選取）它。



STEP 5 | 選取 **Overview**（概觀）和 **Start**（啟動）Panorama 虛擬設備。

為 *Google Cloud Platform* 的 *Panorama* 增加 *CPU* 和記憶體

有關 Panorama™ 所需最低 CPU 與記憶體，請參閱在 Panorama 虛擬設備上增加 CPU 和記憶體。

日誌收集器模式內的 *Panorama* 虛擬設備若在您部署虛擬電腦後重新調整其大小，則不會仍舊維持日誌收集器模式，且會造成日誌資料的丟失。

STEP 1 | 登入 Google Cloud 主控台。

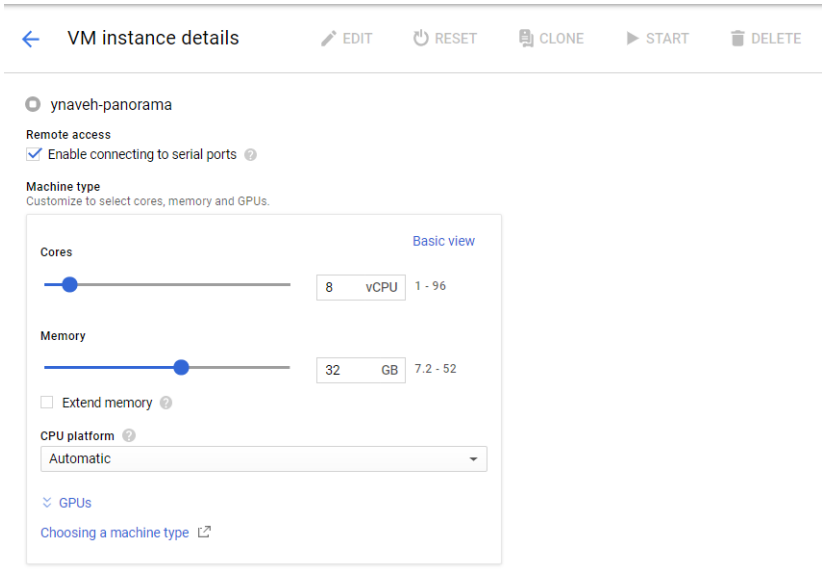
STEP 2 | 停止 Panorama 虛擬設備實例。

1. 在產品與服務功能表中，選取 Panorama 虛擬設備實例（**Compute Engine**（計算引擎）> **VM Instances**（VM 實例））。
2. **Stop**（停止）Panorama 虛擬設備實例。Panorma 虛擬設備將花費 2 到 3 分鐘才能完成關機。

STEP 3 | 重新設定 Panorama 虛擬設備資源。

1. 編輯（**Edit**）Panorama 虛擬設備實例詳細內容。
2. 在電腦類型下，**Customize**（自訂）Panorama 虛擬設備 CPU 核心和記憶體。

© 2019 Palo Alto Networks, Inc.



STEP 4 | **Save**（儲存）變更以更新 Panorama 虛擬設備實例。

STEP 5 | **Start**（啟動）Panorama 虛擬設備。

為 *KVM* 上的 *Panorama* 增加 *CPU* 和記憶體

有關 Panorama™ 所需最低 CPU 與記憶體，請參閱在 Panorama 虛擬設備上增加 CPU 和記憶體。

日誌收集器模式內的 *Panorama* 虛擬設備若在您部署虛擬電腦後重新調整其大小，則不會仍舊維持日誌收集器模式，且會造成日誌資料的丟失。

STEP 1 | **Shutdown**（關閉）在虛擬電腦管理員上的 Panorama 虛擬設備實例。

STEP 2 | 在虛擬電腦管理員上的 Panorama 虛擬設備實例按兩下，並**Show virtual hardware details**（顯示虛擬硬體詳細內容）。

STEP 3 | 編輯配置的 Panorama 虛擬設備 CPU 核心。

1. 編輯目前配置的 **CPU**。
2. **Apply**（套用）重新設定的 CPU 核心配置。

STEP 4 | 編輯配置的 Panorama 虛擬設備記憶體。

1. 編輯目前配置的 記憶體。
2. **Apply**（套用）重新設定的記憶體配置。

STEP 5 | 將 Panorama 虛擬設備實例 **Power on**（開啟電源）。

為 *Hyper-V* 上的 *Panorama* 增加 *CPU* 和記憶體

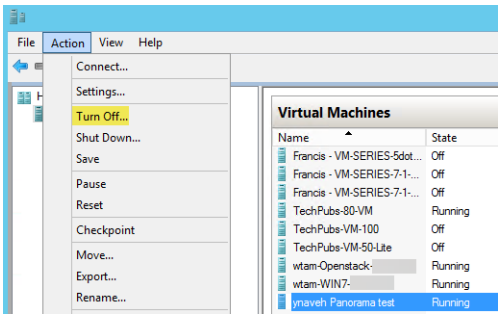
有關 Panorama™ 所需最低 CPU 與記憶體，請參閱在 Panorama 虛擬設備上增加 CPU 和記憶體。

日誌收集器模式內的 *Panorama* 虛擬設備若在您部署虛擬電腦後重新調整其大小，則不會仍舊維持日誌收集器模式，且會造成日誌資料的丟失。

STEP 1 | 關閉 Panorama 虛擬設備電源。

© 2019 Palo Alto Networks, Inc.

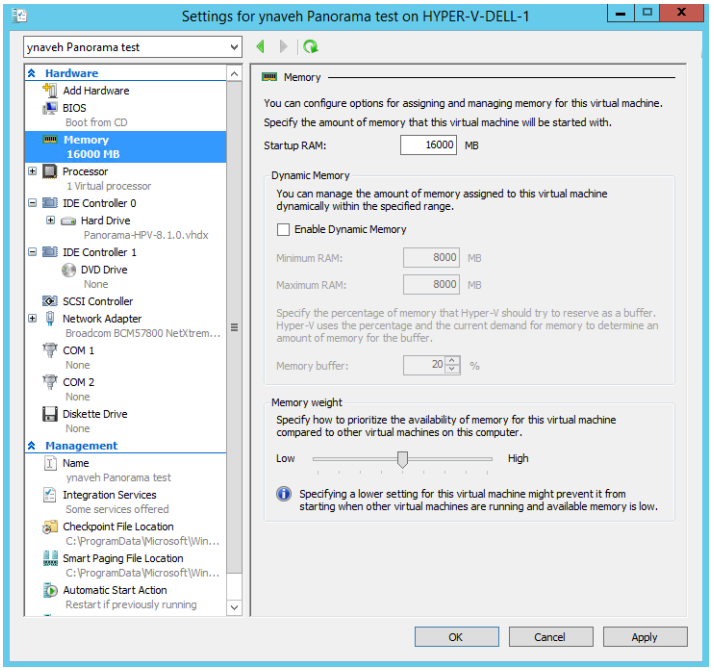
1. 在 Hyper-V 管理員上，從 **Virtual Machines**（虛擬機器）清單中選取 Panorama 虛擬設備實例。
2. 選取 **Action**（動作）> **Turn Off**（關閉）以關閉 Panorama 虛擬設備。



STEP 2 | 在 Hyper-V 管理員上，從 **Virtual Machines**（虛擬機器）清單中選取 Panorama 虛擬設備實例，然後選取 **Action**（動作）> **Settings**（設定）以編輯 Panorama 虛擬設備資源。

STEP 3 | 編輯配置的 Panorama 虛擬設備記憶體。

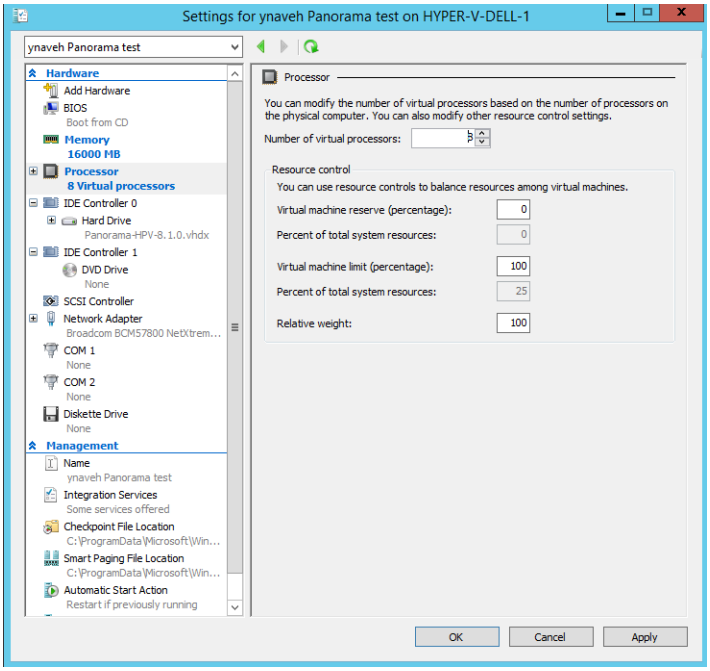
1. 在 **Hardware**（硬體）清單中，選取 **Memory**（記憶體）。
2. 編輯目前配置的 **Startup RAM**（啟動 RAM）。



STEP 4 | 編輯配置的 Panorama 虛擬設備 CPU 核心。

1. 在 **Hardware**（硬體）清單中，選取 **Processor**（處理器）。
2. 編輯目前配置的 **Number of virtual processors**（虛擬處理器數目）。

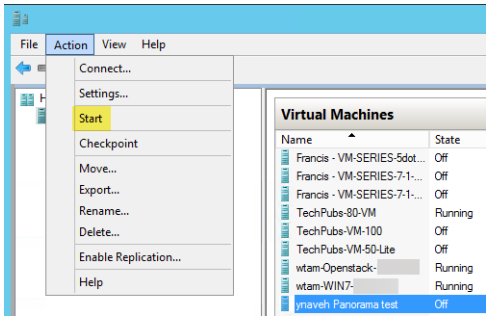
© 2019 Palo Alto Networks, Inc.



STEP 5 | **Apply**（套用）重新配置的記憶體和 CPU 核心。

STEP 6 | 開啟 Panorama 虛擬設備電源。

1. 從 **Virtual Machines**（虛擬機器）清單中選取 Panorama 虛擬設備實例。
2. 選取 **Action**（動作）> **Start**（開啟）以開啟 Panorama 虛擬設備。



在 Panorama 虛擬設備上增加系統磁碟

將 Panorama 虛擬設備的系統磁碟容量擴展至 224GB 以支援大型資料集，以在您 管理大規模防火牆部署 時，有足夠的磁碟空間用於動態更新等內容。此外，如果您意欲使用處於 Panorama 模式的 Panorama 虛擬設備管理您的 SD-WAN 部署，224GB 系統磁碟將擴展儲存空間，以儲存受管理防火牆健康的監控和報告資料

- 為 ESXi 伺服器上的 Panorama 增加系統磁碟
- 為 Google Cloud Platform 上的 Panorama 增加系統磁碟

為 *ESXi* 伺服器上的 *Panorama* 增加系統磁碟

新增 224GB 系統磁碟以取代預設的 81GB 系統磁碟。有關 Panorama 虛擬設備的最低資源需求，請參閱 設定 Panorama 虛擬設備的先決條件。

© 2019 Palo Alto Networks, Inc.

不支援將 *Panorama* 虛擬設備系統磁碟減少至 *81GB*。

STEP 1 | （最佳做法）儲存及匯出 Panorama 和防火牆組態。

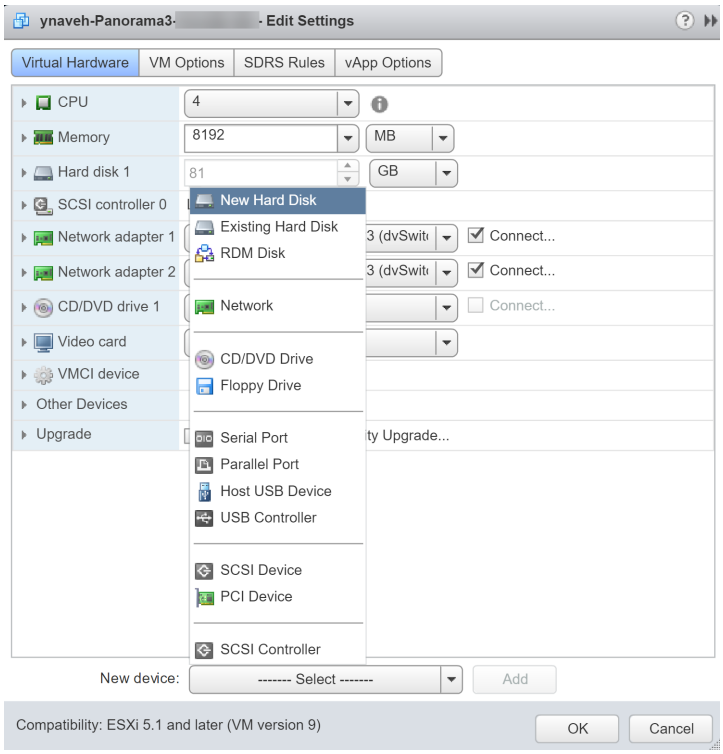
儲存并匯出 Panorama 及防火牆組態，以確保您在遇到任何問題時可以復原 Panorama。

STEP 2 | 存取 VMware vSphere 用戶端並導覽至您的 Panorama 虛擬設備。

STEP 3 | 右鍵按一下 Panorama 虛擬設備並選取 **Power**（電源）> **Power Off**（關閉電源）。

STEP 4 | 新增新的 224GB 系統磁碟。

1. 右鍵按一下 Panorama 虛擬設備並 **Edit Settings**（編輯設定）。
2. 選取 **New Hard Disk**（新硬碟）作為 **New Device**（新裝置）並 **Add**（新增）新裝置。
3. 將新硬碟設定為 224GB，然後按一下 **OK**（確定）。



STEP 5 | 右鍵按一下 Panorama 虛擬設備並選取 **Power**（電源）> **Power On**（開啟電源）。

Panorama 初始化新的系統磁碟可能需要最多 *30* 分鐘。在此期間，將無法使用 *Panorama* 網頁介面及 *CLI*。

STEP 6 | 將磁碟資料從舊系統磁碟移轉至新系統磁碟。

在此範例中，我們將移轉至標示為 sdb 的新增系統磁碟。

1. 登入 Panorama CLI。
2. 輸入下列命令以檢視可供移轉的系統磁碟：

```
admin> request system clone-system-disk target ?
```

3. 使用下列命令將磁碟資料移轉至新系統磁碟：

© 2019 Palo Alto Networks, Inc.

```
admin> request system clone-system-disk target sdb
```

出現提示時，請輸入 **y** 以開始移轉磁碟。

為了開始移轉，*Panorama* 將重新啟動，完成磁碟移轉需要至少 *20* 分鐘。在此期間，將無法使用 *Panorama* 網頁介面及 *CLI*。

4. 從 Web 主控台監控磁碟移轉。只有在 Panorama 顯示下列指示磁碟移轉完成的訊息後才繼續下一步驟。

```
==================================
Disk Cloning Utility (Version 1.0)
==================================
SOURCE - Disk sda (82944 MB)
TARGET - Disk sdb (229376 MB)

Gathering disks info
Finished gathering disks info

Preparing disks
Finished preparing disks

Copying data
Finished copying data

Making disk bootable
Finished making disk bootable

Disk cloning procedure completed. Please shutdown the sytem and switch disks..._
```

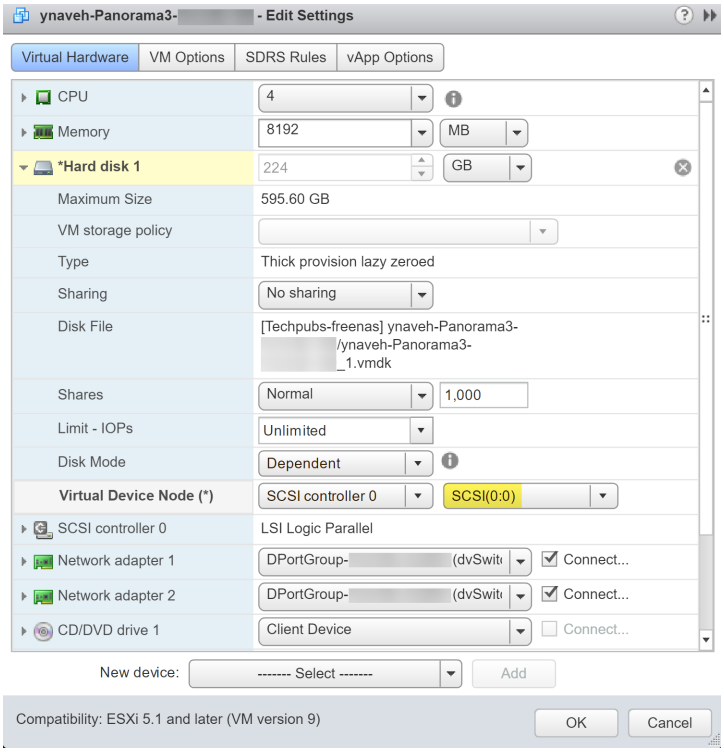
STEP 7 | 刪除舊的系統磁碟。

1. 存取 VMware vSphere 用戶端並導覽至您的 Panorama 虛擬設備。
2. 右鍵按一下 Panorama 虛擬設備並選取 **Power**（電源）> **Power Off**（關閉電源）。
3. 右鍵按一下 Panorama 虛擬設備並 **Edit Settings**（編輯設定）。
4. 刪除舊的 81GB 系統磁碟，然後按一下 **OK**（確定）。

STEP 8 | 修改新系統磁碟的 Virtual Device Node（虛擬裝置節點）。

1. 展開新系統磁碟的設定選項。
2. 選取 **SCSI(0:0)** 作為 **Virtual Device Node**（虛擬裝置節點）。
3. 按一下 **OK**（確定）儲存組態變更。

© 2019 Palo Alto Networks, Inc.



STEP 9 | 右鍵按一下 Panorama 虛擬設備並選取 **Power**（電源）> **Power On**（開啟電源）。

STEP 10 | 確認已成功移轉至新系統磁碟。

1. 登入 Panorama CLI。
2. 輸入下列命令以檢視系統磁碟分割區。

   您必須新增 `/dev/root`、`/dev/sda5`、`/dev/sda6` 及 `/dev/sda8` 分割區，以確認磁碟大小已增加。

```
admin> show system disk-space
```

```
admin@Panorama-Ynaveh> show system disk-space

Filesystem      Size  Used Avail Use% Mounted on
/dev/root        16G  3.4G   12G  23% /
none            4.0G   60K  4.0G   1% /dev
/dev/sda5        76G  1.8G   71G   3% /opt/pancfg
/dev/sda6        23G  5.0G   17G  24% /opt/panrepo
tmpfs           4.0G  110M  3.8G   3% /dev/shm
cgroup_root     4.0G     0  4.0G   0% /cgroup
/dev/sda8        92G   52G   35G  60% /opt/panlogs
/dev/loop0       50G  7.4G   40G  16% /opt/mongobuffer
tmpfs            12M     0   12M   0% /opt/pancfg/mgmt/ssl/private
```

為 *Google Cloud Platform* 上的 *Panorama* 增加系統磁碟

新增 224GB 系統磁碟以取代預設的 81GB 系統磁碟。有關 Panorama 虛擬設備的最低資源需求，請參閱 設定 Panorama 虛擬設備的先決條件。

STEP 1 | （最佳做法）儲存及匯出 Panorama 和防火牆組態。

儲存并匯出 Panorama 及防火牆組態，以確保您在遇到任何問題時可以復原 Panorama。

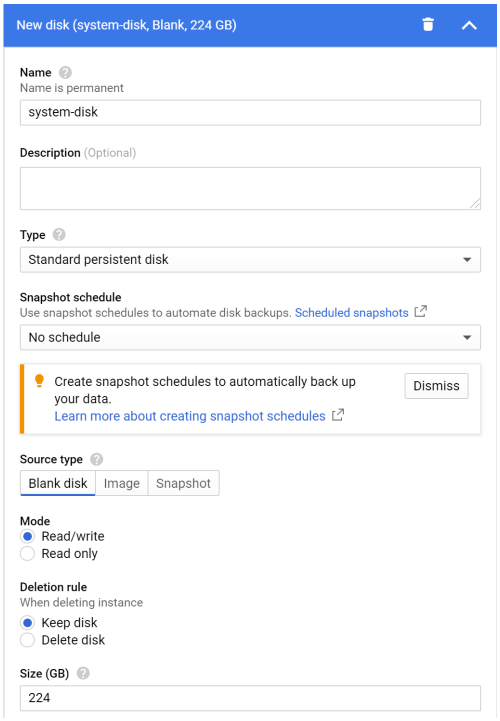
© 2019 Palo Alto Networks, Inc.

STEP 2 | 登入 Google Cloud 主控台。

STEP 3 | 在 **VM Instances**（**VM** 實例）中，**Stop**（停止）Panorama VM 實例。

STEP 4 | 新增新的 224GB 系統磁碟。

1. 選取 Panorama VM 實例並且選取 **Edit**（編輯）。
2. 在 **Additional disks**（額外的磁碟）區段 **Add new disk**（新增新的磁碟）。
3. 將新磁碟設為 224GB，然後按一下 **OK**（確定）。



STEP 5 | 在 **VM Instances**（**VM** 實例）中，**Start**（啟動）Panorama VM 實例。

STEP 6 | 將磁碟資料從舊系統磁碟移轉至新系統磁碟。

在此範例中，我們將移轉至標示為 sdb 的新增系統磁碟。

1. 登入 Panorama CLI。
2. 輸入下列命令以檢視可供移轉的系統磁碟：

```
admin> request system clone-system-disk target ?
```

3. 使用下列命令將磁碟資料移轉至新系統磁碟：

```
admin> request system clone-system-disk target sdb
```

出現提示時，請輸入 **y** 以開始移轉磁碟。

為了開始移轉，*Panorama* 將重新啟動，完成磁碟移轉需要至少 *20* 分鐘。在此期間，將無法使用 *Panorama* 網頁介面及 *CLI*。

4. 嘗試登入 Panorama CLI，以監控磁碟移轉。系統磁碟移轉完成後，Panorama 管理伺服器將處於維護模式，並允許您在維護模式中登入 Panorama CLI。

© 2019 Palo Alto Networks, Inc.

STEP 7 | 連接新的 224GB 系統磁碟。

1. 在 **VM Instances**（**VM** 實例）中，**Stop**（停止）Panorama VM 實例。
2. 選取 Panorama VM 實例並且選取 **Edit**（編輯）。
3. 在 **Additional disks**（額外磁碟）部份中，卸除新的 224GB 系統磁碟。
4. 在 **Boot Disk**（開機磁碟）部份中，卸除舊的 81GB 系統磁碟。
5. 在 **Boot Disk**（開機磁碟）部份中，**Add item**（新增項目）並且選取新的 224GB 系統磁碟。。
6. **Save**（儲存）您的組態變更。

STEP 8 | 在 **VM Instances**（**VM** 實例）中，**Start**（啟動）Panorama VM 實例。

STEP 9 | 確認已成功移轉至新系統磁碟。

1. 登入 Panorama CLI。
2. 輸入下列命令以檢視系統磁碟分割區。

   您必須新增 `/dev/root`、`/dev/sda5`、`/dev/sda6` 及 `/dev/sda8` 分割區，以確認磁碟大小已增加。

```
admin> show system disk-space
```

```
admin@Panorama-Ynaveh> show system disk-space

Filesystem      Size  Used Avail Use% Mounted on
/dev/root        16G  3.4G   12G  23% /
none            4.0G   60K  4.0G   1% /dev
/dev/sda5        76G  1.8G   71G   3% /opt/pancfg
/dev/sda6        23G  5.0G   17G  24% /opt/panrepo
tmpfs           4.0G  110M  3.8G   3% /dev/shm
cgroup_root     4.0G     0  4.0G   0% /cgroup
/dev/sda8        92G   52G   35G  60% /opt/panlogs
/dev/loop0       50G  7.4G   40G  16% /opt/mongobuffer
tmpfs            12M     0   12M   0% /opt/pancfg/mgmt/ssl/private
```

完成 Panorama 虛擬設備設定

當您 執行 Panorama 虛擬設備的初始設定 之後，請繼續下列工作來進行其他設定：

- 啟動 Panorama 支援授權
- 在 Panorama 虛擬設備與網際網路連線時，啟動/擷取防火牆管理授權
- 安裝 Panorama 的內容與軟體更新
- 存取並導覽 Panorama 管理介面
- 設定對 Panorama 的管理存取權
- 管理防火牆

© 2019 Palo Alto Networks, Inc.

設定 M-Series 設備

M-600、M-500、M-200 設備為您可以在僅管理模式（作為未附本機日誌收集的 Panorama 管理伺服器）、Panorama 模式（作為附本機日誌收集的 Panorama 管理伺服器）或日誌收集器模式（作為專用日誌收集器）部署的高性能硬體設備。這種設備提供多個介面，供您指派給各種 Panorama 服務，例如防火牆管理和日誌收集。在設定設備之前，請考量如何設定介面以達到最佳安全性、啟用網路分段（在大規模部署中），以及平衡 Panorama 服務流量的負載。

- M-Series 設備介面
- 執行 M-Series 設備的初始設定
- M-Series 設定概觀
- 將 M-Series 設備設定為日誌收集器
- 增加 M-Series 設備的儲存容量
- 設定 Panorama 來使用多個介面

M-Series 設備介面

Panorama M-600、M-500、M-200 和 M-100 設備有數個介面可以與其他系統通訊，例如受管理的防火牆，以及 Panorama 管理員的用戶端系統。Panorama 會與這些系統通訊以執行各種服務，包括管理裝置（防火牆、日誌收集器及 WildFire 設備和設備叢集）、收集日誌、與收集器群組通訊、將軟體和內容更新部署至裝置，以及支援對 Panorama 的管理存取。依預設，Panorama 會使用管理 (MGT) 介面執行所有這些服務。不過，您可以將 MGT 介面保留給管理存取，並以不同的介面專用於其他服務，以改善安全性。在具有多個子網路和日誌流量很大的大型網路中，使用多個介面來管理裝置和收集日誌也有助於網路分段和負載平衡（請參閱設定 Panorama 來使用多個介面）。

將 Panorama 服務指派給各個介面時，記住，只有 MGT 介面允許對 Panorama 進行管理存取以執行設定和監控工作。當執行 M-Series 設備的初始設定時，您可以指派任何介面到其他服務。M-Series 設備硬體參考指南解釋介面的纜線連接位置。M-100 設備的所有介面支援 1Gbps 輸送量：MGT、Eth1、Eth2 和 Eth3。除了這些介面，M-500 設備的 Eth4 和 Eth5 介面還支援 10Gbps 輸送量。

M-Series 設備不支援以 *Link Aggregation Control Protocol*（連結彙總控制協定 - *LACP*）來彙總介面。

支援的介面

介面可用於裝置管理、日誌收集、收集器群組通訊、授權和軟體更新。請參閱 設定 Panorama 來使用多個介面 瞭解更多有關網路區段的資訊。

介面	速度上限	M-600 設備	M-500 設備	M-200 設備
管理 (MGT)	1Gbps	✓	✓	✓
乙太網路 1 (Eth1)	1Gbps	✓	✓	✓
乙太網路 2 (eth2)	1Gbps	✓	✓	✓
乙太網路 3 (eth3)	1Gbps	✓	✓	✓
乙太網路 4 (eth4)	10Gbps	✓	✓	—
乙太網路 5 (eth5)	10Gbps	✓	✓	—

© 2019 Palo Alto Networks, Inc.

日誌記錄速率

檢閱所有 M-Series 設備機型的日誌記錄速率。若要達成下列日誌記錄速率，M-Series 設備必須是收集器群組中的單一日誌收集器，並且您必須安裝您的 M-Series 型號的所有日誌記錄磁碟。例如，為了使 M-500 設備達成 30,000 個日誌/秒的速率，您必須安裝所有 12 個日誌記錄磁碟（1TB 或 2TB）。

型號容量與功能	M-600 設備	M-500 設備	M-200 設備
處於僅管理模式的 Panorama 的最大日誌記錄速率	不支援本機日誌儲存空間		
處於 Panorama 模式的 Panorama 的最大日誌記錄速率	25,000 個日誌/秒	20,000 個日誌/秒	10,000 個日誌/秒
處於日誌收集器模式的 Panorama 的最大日誌記錄速率	50,000 個日誌/秒	30,000 個日誌/秒	28,000 個日誌/秒
設備上的最大日誌儲存容量	48TB（12 個 8TB RAID 磁碟）	• 24TB（24 個 2TB RAID 磁碟） • 12TB（24 個 1TB RAID 磁碟）	16TB（4 個 8TB RAID 磁碟）
設備上的預設日誌儲存容量	16TB（4 個 8TB RAID 磁碟）	4TB（4 個 2TB RAID 磁碟）	16TB（4 個 8TB RAID 磁碟）
設備上的 SSD 儲存容量（用於 M-Series 設備產生的日誌）	240GB	240GB	240GB
NFS 附加日誌儲存	不可用		

執行 M-Series 設備的初始設定

依預設，Panorama 的 IP 位址為 192.168.1.1，且使用者名稱/密碼為 admin/admin。基於安全因素，您必須在繼續其他設定工作前變更這些設定。您必須從管理 (MGT) 介面，或使用直接序列連接埠來連接 M-600、M-500 或 M-200 設備上的主控台連接埠，從而執行這些初始設定工作。

如果您在日誌收集器模式中使用 *10GB* 介面設定 *M-Series* 設備，則必須完成整個設定程序，才能使 *10GB* 介面顯示為 `Up`（啟動）。

STEP 1 | 向網路管理員收集必要的介面與伺服器資訊。

- 針對您打算設定的每個介面（MGT、Eth1、Eth2、Eth3、Eth4、Eth5），收集的 IP 位址、網路遮罩 (IPv4) 或首碼長度 (IPv6)，以及預設閘道。僅 MGT 介面為必要。

Palo Alto Networks 建議您為 *MGT* 介面指定所有這些設定。如果您省略其中某些設定的值（例如預設閘道），則未來需要變更組態時，您只能透過主控台連接埠存取 *Panorama*。除非您指定所有這些設定，否則無法為其他介面提交設定。

© 2019 Palo Alto Networks, Inc.

如果您打算將設備作為 Panorama 管理伺服器，Palo Alto Networks 建議將 MGT 介面專用於管理 Panorama，而將其他介面用於管理裝置、收集日誌、與收集器群組通訊，以及將更新部署至裝置（請參閱 M-Series 設備介面）。
- 收集 DNS 伺服器的 IP 位址。

STEP 2 | 從電腦存取 M-Series 設備。

1. 以下列其中一種方式連接至 M-Series 設備：
   - 從電腦中將序列纜線連接至 M-Series 設備上的主控台連接埠，然後使用終端機模擬軟體連線 (9600-8-N-1)。
   - 將 RJ-45 乙太網路纜線從電腦連接至 M-Series 設備的 MGT 連接埠。在瀏覽器中前往 https://192.168.1.1。若要允許存取此 URL，可能需要將電腦上的 IP 位址變更為 192.168.1.0 網路中的位址（例如 192.168.1.2）。
2. 當收到提示時，使用預設使用者名稱與密碼 (admin/admin) 登入設備。設備將開始初始化。

STEP 3 | 變更預設的管理員密碼。

從 *PAN-OS 9.0.4* 開始，第一次登入裝置時必須變更預定義的預設密碼 *(admin/admin)*。新密碼至少必須包含八個字元，並且包含至少一個小寫字母與一個大寫字母，以及一個數字或特殊字元。

務必採用密碼強度最佳做法 以確保嚴格的密碼，並檢閱密碼複雜性設定。

1. 按一下網頁介面左下角的 **admin**（管理員）連結。
2. 輸入 **Old Password**（舊密碼）、**New Password**（新密碼），**Confirm New Password**（確認新密碼），然後按一下 **OK**（確定）。將新密碼存放在安全位置。

為了確保維持安全的 *MGT* 介面，請設定最小密碼複雜性（選取 *Panorama* > *Setup*（設定）> *Management*（管理）），並指定管理員必須變更其密碼的間隔。

STEP 4 | 針對您要用於管理 Panorama、管理裝置、收集日誌、與收集器群組通訊，以及將更新部署至裝置的每個介面，進行網路存取設定。

1. 選取 **Panorama** > **Setup**（設定）> **Interfaces**（介面），然後按一下 Interface Name（介面名稱）。
2. （僅限非 MGT 介面）**Enable**（啟用）介面。
3. 編輯 Panorama 將使用的每個介面的網路存取設定。僅 MGT 介面為必要。Eth1、Eth2、Eth3、Eth4 和 Eth5 介面為選用，只有當您打算將 M-Series 設備作為 Panorama 管理伺服器時才適用。
   1. 視您網路的 IP 通訊協定而定，完成下列其中一個或兩個欄位集：

      IPv4—**Public IP Address**（公共 **IP** 位址）、**IP Address**, **Netmask**, and **Default Gateway**

      若您的防火牆使用公共 *IP* 位址（轉譯為私密 *IP* 位址 *(NAT)*）連線至 *Panorama* 管理伺服器，請在 *Public IP Address*（公共 *IP* 位址）欄位輸入公共 *IP*，在 *IP Address*（*IP* 位址）欄位輸入私密 *IP*，以便推送兩者至您的防火牆。

      IPv6—**IPv6 Address/Prefix Length**（**IPv6** 位址/首碼長度）及 **Default IPv6 Gateway**（預設的 **IPv6** 閘道）
   2. 選取介面支援的裝置管理服務：

      Device Management and Device Log Collection（裝置管理和裝置日誌收集）—您可以指派一個或多個介面。

      Collector Group Communication（收集器群組通訊）—您只能指派一個介面。

      Device Deployment（裝置部署）（軟體和內容更新）—您只能指派一個介面。

© 2019 Palo Alto Networks, Inc.

3. （選用）選取介面支援的網路連線服務。



（僅限 *MGT* 介面）停用 *Telnet* 和 *HTTP*；這些服務使用純文字，比其他服務更不安全。

4. 按一下 **OK**（確定）儲存您的變更。

STEP 5 | 設定主機名稱、時區和一般設定。

1. 選取 **Panorama** > **Setup**（設定）> **Management**（管理），再編輯 [一般設定]。
2. 對準 Panorama 與受管理防火牆上的時鐘以使用相同的 **Time Zone**（時區），例如 GMT 或 UTC。如果打算使用 Cortex Data Lake（Cortex 資料湖），您必須設定 NTP，才能使 Panorama 與 Cortex Data Lake（Cortex 資料湖）保持同步。

   防火牆將記錄其產生日誌時的，而 Panorama 將記錄接收日誌時的時間戳記。符合時區以確保時間戳記會同步，且在 Panorama 上查詢日誌與產生報告的程序並未產生衝突。
3. 輸入伺服器的 **Hostname**（主機名稱）。Panorama 使用此名稱做為設備的顯示名稱/標籤。例如，這是在 CLI 提示時顯示的名稱。如果您在 **Panorama** > **Managed Collectors**（受管理的收集器）頁面上將設備新增成受管理收集器時，此名稱也會出現在 [收集器名稱] 欄位中。
4. （選用）輸入 **Latitude**（經度）與 **Longitude**（緯度），在世界地圖上精確定位 M-Series 設備。**App Scope** > **Traffic Maps**（流量地圖）及 **App Scope** > **Threat Maps**（威脅地圖）將使用這些值。
5. 按一下 **OK**（確定）儲存您的項目。

STEP 6 | 設定 DNS 伺服器和 Palo Alto Networks 更新伺服器。

1. 選取 **Panorama** > **Setup**（設定）> **Services**（服務），再編輯設定。
2. 輸入 **Primary DNS Server**（主要 **DNS** 伺服器）的 IP 位址，並選擇性地輸入 **Secondary DNS Server**（次要 **DNS** 伺服器）的 IP 位址。
3. 輸入 **Update Server**（更新伺服器）的 URL 或靜態位址（預設為 updates.paloaltonetworks.com）。



如果您想要 *Panorama* 確認其下載軟體或內容套件的更新伺服器有信任的授權單位簽署的 *SSL* 憑證，請選取 *Verify Update Server Identity*（驗證更新伺服器識別碼）。此選項會在 *Panorama* 伺服器與更新伺服器之間的通訊，增加額外的安全性層級。

4. 按一下 **OK**（確定）儲存您的項目。

STEP 7 | 提交組態變更。

選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。



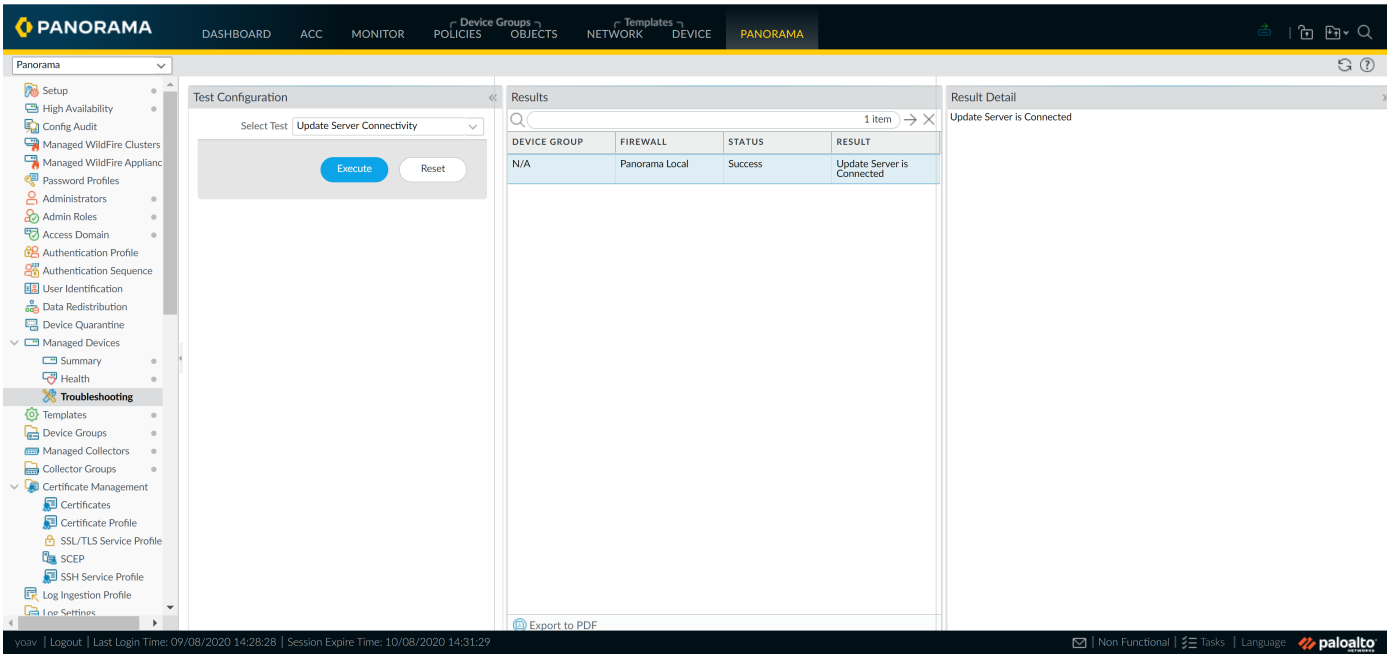
如果您打算將 *M-Series* 設備作為 *Panorama* 管理伺服器，並且已設定 *MGT* 以外的介面，當您設定受管理的收集器時，您必須將這些介面指派給 *Device Log Collection*（設備日誌收集）或 *Collector Group Communication*（收集器群組通訊）功能。若要使介面運作，您還必須為受管理的收集器設定收集器群組，並執行收集器群組認可。

STEP 8 | 驗證執行 Panorama 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. 以下列其中一種方式連接至 M-Series 設備：
   - 將序列纜線從電腦連接至 M-Series 設備的主控台連接埠。然後使用終端機模擬軟體 (9600-8-N-1) 進行連線。
   - 使用終端機模擬軟體（例如 PuTTY），針對在初始設定期間指定給 M-Series 設備 MGT 介面的 IP 位址開啟 SSH 工作階段。
2. 按照提示登入 CLI。使用預設的管理員帳戶，及在初始設定期間指定的密碼。
3. 使用更新伺服器連線測試來確認與 Palo Alto Networks 更新伺服器的網路連線，如下列範例所示。
   1. 選取 **Panorama** > **Managed Devices**（受管理的裝置）> **Troubleshooting**（疑難排解），然後從選取測試下拉式清單中選取 **Update Server Connectivity**（更新伺服器連線）。

© 2019 Palo Alto Networks, Inc.

2. **Execute**（執行）更新伺服器連線測試。



4. 使用以下 CLI 命令從更新伺服器擷取 Panorama 支援權利的資訊：

```
admin> request support check
```

如果您可以連線，更新伺服器將回應 Panorama 的支援狀態。由於 Panorama 未註冊，更新伺服器將返回以下訊息：

```
Contact Us
https://www.paloaltonetworks.com/company/contact-us.html
Support Home
https://www.paloaltonetworks.com/support/tabs/overview.html
Device not found on this update server
```

STEP 9 | 接下來的步驟...

1. 註冊 Panorama 並安裝授權。
2. 安裝 Panorama 的內容與軟體更新。



最佳作法是取代預設證書（*Panorama* 用於保證 *MGT* 介面上 *HTTPS* 流量的安全）。

M-Series 設定概觀

請使用下列程序來設定 M-Series 設備：

- 在僅管理模式下設定 M-Series 設備
- 在 Panorama 模式下設定 M-Series 設備
- 在日誌收集器模式下設定 M-Series 設備

© 2019 Palo Alto Networks, Inc.

在僅管理模式下設定 *M-Series* 設備

STEP 1 | 在機架中安裝 M-Series 設備。請參閱 M-Series 設備硬體參考指南的指示。

STEP 2 | 執行 M-Series 設備的初始設定

STEP 3 | 註冊 Panorama 與安裝授權

STEP 4 | 安裝 Panorama 的內容與軟體更新

STEP 5 | 變更至已僅管理模式。

1. 登入 Panorama CLI。
2. 從 Panorama 模式切換至僅管理模式：

   `request system system-mode management-only`
3. 輸入 **`y`** 以確認模式變更。Panorama 管理伺服器重新啟動。重新啟動會終止終端機模擬軟體的工作階段並重新連線至 Panorama 管理伺服器以顯示 Panorama 登入提示。

   如果您看到 `CMS` 登入提示，則表示 Panorama 管理伺服器未完成重新啟動。在提示框中按 Enter，而不輸入使用者名稱或密碼。
4. 重新登入 CLI。
5. 確認已成功切換至僅管理模式：

   `show system info | match system-mode`

   如果模式變更成功，則輸出顯示為：

   ```
   system mode:management-only
   ```

STEP 6 | 設定對 Panorama 的管理存取權

STEP 7 | 管理防火牆

STEP 8 | 管理日誌收集

在 *Panorama* 模式下設定 *M-Series* 設備

STEP 1 | 在機架中安裝 M-Series 設備。請參閱 M-Series 設備硬體參考指南的指示。

STEP 2 | 執行 M-Series 設備的初始設定。

STEP 3 | 註冊 Panorama 並安裝授權。

STEP 4 | 安裝 Panorama 的內容與軟體更新。

STEP 5 | 設定每個陣列。為了使 RAID 磁碟可用於記錄日誌，需要完成此工作。您也可以選擇新增磁碟以增加 M-Series 設備的儲存容量。

STEP 6 | 設定對 Panorama 的管理存取。

STEP 7 | 管理防火牆。

STEP 8 | 管理日誌收集。

在日誌收集器模式下設定 *M-Series* 設備

© 2019 Palo Alto Networks, Inc.

STEP 1 | 在機架中安裝 M-Series 設備。請參閱 M-Series 設備硬體參考指南的指示。

STEP 2 | 執行 M-Series 設備的初始設定

STEP 3 | 註冊 Panorama 與安裝授權

STEP 4 | 安裝 Panorama 的內容與軟體更新

STEP 5 | 請參閱步驟設定每個陣列.。為了使 RAID 磁碟可用於記錄日誌，需要完成此工作。您也可以選擇新增磁碟以增加 M-Series 設備的儲存容量。

STEP 6 | 將 M-Series 設備設定為日誌收集器

STEP 7 | 管理日誌收集

將 M-Series 設備設定為日誌收集器

如果您想使用專用設備進行日誌收集，可以將 M-200、M-500 或 M-600 設備設定為日誌收集器模式。為此，首先在 Panorama 模式下執行設備的初始設定，包括授權、安裝軟體和內容更新以及設定管理 (MGT) 介面。然後您可以將 M-Series 設備切換至日誌收集器模式，並完成日誌收集器設定。此外，如果您要使用專用 M-Series 設備介面（建議）（而非 MGT 介面）進行日誌收集和收集器群組通訊，您必須先為 Panorama 管理伺服器設定介面，再為日誌收集器設定介面，然後執行 Panorama 提交，接著再執行收集器群組提交。

執行下列步驟，將新的 M-Series 設備設定為日誌收集器，或者轉換現有的 M-Series 設備（之前部署為 Panorama 管理伺服器）。

如果您在日誌收集器模式中使用 *10GB* 介面設定 *M-Series* 設備，則必須完成整個設定程序，才能使 *10GB* 介面顯示為 `Up`（啟動）。

如果將 *M-Series* 設備從 *Panorama* 模式切換至日誌收集器模式時，將會重新啟動設備、刪除本機日誌收集器、刪除任何現有日誌資料，以及刪除所有組態（但管理存取設定除外）。切換模式不會刪除授權、軟體更新或內容更新。

STEP 1 | 如果還未設定將用於管理日誌收集器的 Panorama 管理伺服器，請先進行設定。

執行下列其中一個工作：

- 設定 Panorama 虛擬設備
- 設定 M-Series 設備

STEP 2 | 記錄 Panorama 管理伺服器的管理 IP 位址。

如果您已採用高可用性 (HA) 設定部署 Panorama，則需要每個 HA 端點的 IP 位址。

1. 登入 Panorama 管理伺服器的 Web 介面。
2. 選取 **Panorama** > **Setup**（設定）> **Management**（管理）並查看管理介面設定，記錄單獨（非 HA）或主動 (HA) Panorama 的 **IP Address**（**IP** 位址）。
3. 對於 HA 部署，選取 **Panorama** > **High Availability**（高可用性）並查看設定部分，記錄被動 Panorama 的 **Peer HA IP Address**（端點 **HA IP** 位址）。

STEP 3 | 設定將作為專用日誌收集器的 M-Series 設備。

如果您之前已將該設備部署為 Panorama 管理伺服器，則可以跳過此步驟，因為已經設定了 MGT 介面並且已經安裝了授權和更新。

日誌收集器模式下的 M-Series 設備沒有用於設定工作的 Web 介面，只有 CLI。因此，在 M-Series 設備上變更模式之前，先在 Panorama 模式中使用 Web 介面：

© 2019 Palo Alto Networks, Inc.

1. 執行 M-Series 設備的初始設定。
2. 註冊 Panorama 並安裝授權。
3. 安裝 Panorama 的內容與軟體更新。

STEP 4 | 存取 M-Series 設備的 CLI。

1. 以下列其中一種方式連接至 M-Series 設備：
   - 將序列纜線從電腦連接至 M-Series 設備的主控台連接埠。然後使用終端機模擬軟體 (9600-8-N-1) 進行連線。
   - 使用終端機模擬軟體（例如 PuTTY），針對在初始設定期間指定給 M-Series 設備 MGT 介面的 IP 位址開啟 SSH 工作階段。
2. 按照提示登入 CLI。使用預設的管理員帳戶，及在初始設定期間指定的密碼。

STEP 5 | 從 Panorama 模式切換至日誌收集器模式。

1. 輸入下列命令，切換至日誌收集器模式：

```
> request system system-mode logger
```

2. 輸入 **y** 以確認模式變更。M-Series 設備重新啟動。重新啟動會終止終端機模擬軟體的工作階段並重新連線至 M-Series 設備以顯示 Panorama 登入提示。

   如果您看到 ***CMS Login***（*CMS* 登入）提示，則表示日誌收集器未完成重新啟動。在提示框中按 *Enter*，而不輸入使用者名稱或密碼。

3. 重新登入 CLI。
4. 確認已成功切換至日誌收集器模式：

```
> show system info | match system-mode
```

如果模式變更成功，則輸出顯示為：

```
system-mode: logger
```

STEP 6 | 將日誌記錄磁碟設定為 RAID1 配對。

如果您之前已將該設備部署為 Panorama 管理伺服器，則可以跳過此步驟，因為磁碟配對已經設定好並且可用。

視磁碟機上的資料數量而定，設定磁碟機所需要的時間可能會從幾分鐘到幾小時不等。

1. 確定在 M-Series 設備上有哪些磁碟配對可設定為 RAID 配對：

```
> show system raid detail
```

執行剩餘步驟，以設定所有擁有 `present`（存在）磁碟的磁碟配對。此範例中使用 A1/A2 磁碟配對。

2. 若要新增此配對中的第一個磁碟，可輸入以下命令，並在提示時輸入**y** 以確認請求：

```
> request system raid add A1
```

等候此過程完成，然後再新增此配對中的第二個磁碟。若要監控 RAID 設定的進度，請再次輸入：

© 2019 Palo Alto Networks, Inc.

```
> show system raid detail
```

新增第一個磁碟之後，輸出顯示磁碟配對狀態為 `Available`（可用），但是 `degraded`（已降級）。

3. 新增配對中的第二個磁碟：

```
> request system raid add A2
```

4. 確認磁碟設定是否已完成：

```
> show system raid detail
```

新增第二個磁碟之後，輸出顯示磁碟配對狀態為 `Available`（可用）和 `clean`（乾淨）。

```
Disk Pair A      Available
Status         clean
```

STEP 7 | 啟用日誌收集器和 Panorama 管理伺服器之間的連線。

在日誌收集器 CLI 上輸入以下命令，其中 *<IPaddress1>* 單獨（非 Ha）或主動 (HA) Panorama 的 MGT 介面，*<IPaddress2>* 是被動 (HA) Panorama 的 MGT 介面（如果適用）。

```
> configure
# set deviceconfig system panorama-server <IPaddress1> panorama-server-2
 <IPaddress2>
# commit
# exit
```

STEP 8 | 記錄日誌收集器的序號。

您需要這些序號以便在 Panorama 管理伺服器上將日誌收集器新增為受管理的收集器。

1. 在日誌收集器 CLI 中輸入下列命令可顯示序號。

```
> show system info | match serial
```

2. 記錄序號。

STEP 9 | 將日誌收集器作為受管理的收集器新增至 Panorama 管理伺服器。

1. 選取 **Panorama** > **Managed Collectors**（受管理的收集器），再 **Add**（新增）受管理的收集器。
2. 在 **General**（一般）設定中，輸入您記錄的收集器序號（**Collector S/N**（收集器序號））。
3. 在 **Panorama Server IP**（**Panorama** 伺服器 **IP**）欄位中，輸入 IP 位址或單獨（非 HA）或主動 (HA) Panorama 的 FQDN。對於 HA 部署，在 **Panorama Server IP 2**（**Panorama** 伺服器 **IP 2**）欄位中輸入 IP 位址或被動端點的 FQDN。

   這些 IP 位址必須指定已啟用 **Device Management and Device Log Collection**（裝置管理和裝置日誌收集）服務的 Panorama 介面。依預設，只能在 MGT 介面上啟用這些服務則。不過，當您設定 M-Series 設備而設備是 Panorama 管理伺服器時，您可能已在其他介面上啟用這些服務。
4. 選取**Interfaces**（介面），按一下**Management**（管理），然後根據網路的 IP 通訊協定而定，為 MGT 介面設定下列其中一個或兩個欄位集。
   - IPv4—**IP Address**（**IP** 位址）、**Netmask**（網路遮罩）及 **Default Gateway**（預設閘道）

© 2019 Palo Alto Networks, Inc.

- IPv6—**IPv6 Address/Prefix Length**（**IPv6** 位址/首碼長度）及 **Default IPv6 Gateway**（預設的 **IPv6** 閘道）

5. 按一下 **OK**（確定）兩次，以儲存對日誌收集器所做的變更。
6. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後將您的變更 **Commit**（提交）至 Panorama 組態。

   需要先完成此步驟，才能啟用日誌記錄磁碟。
7. 確認 **Panorama** > **Managed Collectors**（受管理的收集器）列出您已新增的日誌收集器。Connected（已連線）欄中會顯示核取標記，表示日誌收集器已連線至 Panorama。您可能需要等待幾分鐘，然後頁面才會顯示更新後的連線狀態。



此時，*Configuration Status*（組態狀態）欄會顯示 *Out of Sync*（不同步），*Run Time Status*（執行階段狀態）欄會顯示 *disconnected*（已中斷連線）。設定收集器群組之後（步驟將日誌收集器指派給收集器群組），狀態將變更為 *In Sync*（同步）和 *connected*（已連線）。

STEP 10 | 啟用日誌記錄磁碟。

1. 選取 **Panorama** > **Managed Collectors**（受管理的收集器），再編輯日誌收集器。
2. 選取 **Disks**（磁碟），然後 **Add**（新增）每一個 RAID 磁碟配對。
3. 按一下 **OK**（確定）儲存您的變更。
4. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後將您的變更 **Commit**（提交）至 Panorama 組態。

STEP 11 | （建議）如果 Panorama 管理伺服器和日誌收集器會將 **Ethernet1**、**Ethernet2**、**Ethernet3**、**Ethernet4** 和 **Ethernet5** 介面用於裝置日誌收集（從防火牆接收日誌）和 **Collector Group Communication**（收集器群組通訊），請設定這些介面。

如果您先前已將日誌收集器部署為 Panorama 管理伺服器，並配置這些介面，則必須重新設定，因為切換至日誌收集器模式（從 Panorama 模式切換至日誌收集器模式）已刪除所有組態（管理存取設定除外）。

1. 在 Panorama 管理伺服器上設定每個介面（但不是 MGT 介面）（若尚未設定）：
   1. 選取 **Panorama** > **Setup**（設定）> **Interfaces**（介面），然後按一下 Interface Name（介面名稱）。
   2. 選取 *<interface-name>* 以啟用介面。
   3. 視您網路的 IP 通訊協定而定，完成下列其中一個或兩個欄位集：

      IPv4—**IP Address**（**IP** 位址）、**Netmask**（網路遮罩）及 **Default Gateway**（預設閘道）

      IPv6—**IPv6 Address/Prefix Length**（**IPv6** 位址/首碼長度）及 **Default IPv6 Gateway**（預設的 **IPv6** 閘道）
   4. 選取介面支援的裝置管理服務：

      Device Management and Device Log Collection（裝置管理和裝置日誌收集）—您可以指派一個或多個介面。

      Collector Group Communication（收集器群組通訊）—您只能指派一個介面。

      Device Deployment（裝置部署）（軟體和內容更新）—您只能指派一個介面。
   5. 按一下 **OK**（確定）儲存您的變更。
2. 在日誌收集器上設定每個介面（但不是 MGT 介面）：
   1. 選取 **Panorama** > **Managed Collectors**（受管理的收集器），再編輯日誌收集器。
   2. 選取 **Interfaces**（介面），然後按一下介面的名稱。
   3. 選取 *<interface-name>* 以啟用介面。
   4. 視您網路的 IP 通訊協定而定，完成下列其中一個或兩個欄位集：

      IPv4—**IP Address**（**IP** 位址）、**Netmask**（網路遮罩）及 **Default Gateway**（預設閘道）

© 2019 Palo Alto Networks, Inc.

IPv6—**IPv6 Address/Prefix Length**（**IPv6** 位址/首碼長度）及 **Default IPv6 Gateway**（預設的 **IPv6** 閘道）

5. 選取介面支援的裝置管理服務：

   Device Log Collection（裝置日誌收集）—您可以指派一個或多個介面。

   Collector Group Communication（收集器群組通訊）—您只能指派一個介面。

6. 按一下 **OK**（確定）以儲存對介面所做的變更。

3. 按一下 **OK**（確定），以儲存對日誌收集器所做的變更。
4. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後將您的變更 **Commit**（提交）至 Panorama 組態。

STEP 12 | （選用）如果您的部署使用自訂憑證在 Panorama 和受管理的裝置之間驗證，請部署自訂用戶端裝置憑證。如需詳細資訊，請參閱設定使用自訂憑證進行驗證。

1. 選取 **Panorama** > **Certificate Management**（憑證管理）> **Certificate Profile**（憑證設定檔），然後從下拉式清單中選擇憑證設定檔，或按一下 **New Certificate Profile**（新憑證設定檔）以建立憑證設定檔。
2. 針對日誌收集器，選取 **Panorama** > **Managed Collectors**（受管理的收集器）> **Add**（新增）> **Communication**（通訊）。
3. 選取 **Secure Client Communication**（安全用戶端通訊）核取方塊。
4. 從 Type（類型）下拉式清單中，選取裝置憑證的類型。
   - 如果您使用本機裝置憑證，請從 **Certificate**（憑證）和 **Certificate Profile**（憑證設定檔）各自的下拉式清單中選取。
   - 如果您使用 SCEP 作為裝置憑證，請從 **SCEPC Profile**（**SCEP** 設定檔）和 **Certificate Profile**（憑證設定檔）各自的下拉式清單中選取。
5. 按一下 **OK**（確定）。

STEP 13 | （選用）在日誌收集器上設定 Secure Server Communication（安全伺服器通訊）。如需詳細資訊，請參閱設定使用自訂憑證進行驗證。

1. 選取 **Panorama** > **Managed Collectors**（受管理的收集器）> **Add**（新增）> **Communication**（通訊）。
2. 確認未選取 **Custom Certificate Only**（僅限自訂憑證）核取方塊。這樣可讓您在移轉至自訂憑證期間繼續管理所有裝置。

   選取 *Custom Certificate Only*（僅限自訂憑證）核取方塊時，日誌收集器不會使用預先定義的憑證來驗證裝置，也無法使用這種憑證從裝置接收日誌。

3. 從 **SSL/TLS Service Profile**（**SSL/TLS** 服務設定檔）下拉式清單中，選取 SSL/TLS 服務設定檔。此 SSL/TLS 服務設定檔會套用至日誌收集器和送來日誌的裝置之間的所有 SSL 連線。
4. 從 **Certificate Profile**（憑證設定檔）下拉式清單中，選取憑證設定檔。
5. 選取 **Authorize Client Based on Serial Number**（根據序號來授權用戶端），讓伺服器根據受管理裝置的序號來檢查用戶端。用戶端憑證必須以特殊關鍵字 $UDID 來設定 CN，才能根據序號來驗證。
6. 在 **Disconnect Wait Time (min)**（中斷連線等候時間（分鐘））中，輸入 Panorama 在中斷並重新建立與受管理裝置間的連線之前應該等候的時間量。依預設，此欄位是空白，範圍是 0 至 44,640 分鐘。

   直到您提交新設定，中斷連線等候時間才會開始倒數計時。

7. （選用）設定授權清單。
   1. 按一下 Authorization List（授權清單）下的 **Add**（新增）。
   2. 選取 **Subject**（主體）或 **Subject Alt Name**（主體別名）作為識別項類型。
   3. 輸入所選類型的識別項。

© 2019 Palo Alto Networks, Inc.

4. 按一下 **OK**（確定）。
5. 選取 **Check Authorization List**（檢查授權清單）以強制執行授權清單。

8. 按一下 **OK**（確定）。
9. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**）。

STEP 14 | 將日誌收集器指派給收集器群組。

1. 設定收集器群組。您必須先執行 Panorama 提交再執行收集器群組提交，以將日誌收集器群組與 Panorama 同步，並在日誌收集器上使 Eth1、Eth2、Eth3、Eth4 和 Eth5 介面（如果您已設定）進入運作狀態。

   在任何單一收集器群組中，所有日誌收集器都必須在相同 *Panorama* 型號上執行：全部是 *M-600* 設備、全部都是 *M-500* 設備、全部都是 *M-200*，或全部是 *Panorama* 虛擬設備。

   如果您將多個日誌收集器新增至單一收集器群組，則最佳作法是 *Enable log redundancy across collectors*（啟用跨收集器的日誌備援）。使用此選項時，每個日誌收集器必須有相同數目的日誌記錄磁碟。
2. 選取 **Panorama** > **Managed Collectors**（受管理的收集器），確認日誌收集器設定已與 Panorama 同步。

   Configuration Status（組態狀態）欄應該顯示 In Sync（同步），Run Time Status（執行階段狀態）欄應該顯示 connected（已連線）。
3. 存取日誌收集器的 CLI，輸入以下命令以確認其介面是否運作：

   ```
   > show interface all
   ```

   對於正在運作的介面，輸出將顯示 `state`（狀態）為 `up`（正常）。
4. 如果收集器群組內有多個日誌收集器，請對日誌收集器使用的每個介面執行以下命令，疑難排解網路資源連線 以確認日誌收集器能夠相互通訊。對於 `source`（來源）IP 位址，則指定您要執行命令的日誌收集器介面。對於 `host`（主機）IP 位址，則指定同一收集器群組內另一個日誌收集器的相符介面。

STEP 15 | 接下來的步驟...

啟用日誌收集器以接收防火牆日誌：

1. 設定日誌轉送至 Panorama。
2. 確認日誌轉送至 Panorama。

增加 M-Series 設備的儲存容量

當您執行 M-Series 設備的初始設定之後，您可以透過以下方式增大設備的日誌存儲容量：將現有磁碟機配對升級為更大容量的磁碟機，或在空磁碟機擴充插槽內安裝更多磁碟機配對。例如，在 M-500 設備上，您可以選擇將現有的 1TB 磁碟機升級至 2TB，或在空磁碟機擴充插槽（B1 到 D2）內新增 2TB 磁碟機。

M-Series 設備採用 *RAID 1*，在磁碟故障時可發揮資料備援。因此，*RAID 1* 陣列中的磁碟機配對必須相同。不過，您可以跨不同 *RAID 1* 陣列來混合磁碟機容量。例如，*A1/A2 RAID 1* 陣列中的磁碟機可以是 *1TB* 磁碟機，而 *B1/B2 RAID 1* 陣列中的磁碟機可以是 *2TB* 磁碟機。

下表列出 M-Series 設備上支援的磁碟機擴充插槽數目上限及可用的磁碟機容量。

因為每個磁碟機配對（例如 *A1/A2*）都位於 *RAID 1* 陣列，總儲存容量是已安裝的磁碟機總數的一半。例如，如果 *M-500* 設備在磁碟機擴充插槽 *A1/A2* 和 *B1/B2* 中安裝 *2TB* 磁碟機，則 *A1/A2* 陣列提供 *2TB* 總儲存容量，而 *B1/B2* 陣列提供另一個 *2TB*，合計為 *4TB*。

© 2019 Palo Alto Networks, Inc.

裝置	支援的磁碟機擴充插槽數目	支援的磁碟機容量
M-200 設備	4	8TB
M-500 設備	24	1TB 或 2TB
M-600 設備	12	8TB

在擴展日誌儲存容量之前，先確定 Panorama 日誌儲存要求。如果您需要比單一 M-Series 設備所支援的儲存容量更大的日誌儲存容量，可以新增專用日誌收集器（請參閱設定受管理收集器，或者也可以設定日誌從 Panorama 轉送至外部目的地。



在為已部署的 *M-Series* 設備新增磁碟機時，您不需要使 *M-Series* 設備離線即可擴展儲存容量。如果新增的磁碟機可設定並且可用，*M-Series* 設備會在所有磁碟機之間重新分配日誌。此日誌重新分配程序是在背景中執行，並且不會影響 *M-Series* 設備的執行時間或可用性。但是，此程序確實會減慢最大日誌記錄速率。*Redistribution State*（重新分配狀態）欄（*Panorama* > *Collector Groups*（收集器群組））會以百分比表示完成狀態。

- 為 M-Series 設備新增磁碟機
- 在執行 Panorama 7.0.8 或更新版本的 M-Series 設備上升級磁碟機
- 在執行 Panorama 7.0.7 或更舊版本的 M-Series 設備上升級磁碟機

為 *M-Series* 設備新增磁碟機

STEP 1 | 在適當的磁碟機擴充插槽中安裝新磁碟機。

務必依序在接下來開啟的磁碟擴充插槽中新增磁碟機。例如，先將磁碟機新增至 B1 和 B2，再將磁碟機新增至 C1 和 C2。

STEP 2 | 在 M-Series 設備上存取命令行介面 (CLI)。

以下列兩種方式之一連接至 M-Series 設備：

- 從電腦中將序列纜線連接至主控台連接埠，然後使用終端機模擬軟體連線至 M-Series 設備 (9600-8-N-1)。
- 使用終端機模擬軟體（例如 PuTTY），針對 M-Series 設備的 IP 位址開啟 Secure Shell (SSH) 工作階段。

STEP 3 | 出現提示時，登入裝置。

使用預設的管理員帳戶及指定的密碼。

STEP 4 | 設定每個陣列。



視磁碟機上的資料數量而定，在磁碟機上鏡像資料所需要的時間可能會從幾分鐘到幾小時不等。

下列範例使用擴充插槽 B1 和 B2 中的磁碟機。

1. 輸入下列命令，並在出現提示時確認要求：

```
> request system raid add B1
> request system raid add B2
```

2. 若要監控 RAID 設定的進度，請輸入下列命令：

© 2019 Palo Alto Networks, Inc.

```
> show system raid detail
```

完成 RAID 設定時會顯示下列回應：

```
Disk Pair A       Available
   Status         clean
   Disk id A1     Present
       model        : ST91000640NS
       size         : 953869 MB
       status       : active sync
   Disk id A2     Present
       model        : ST91000640NS
       size         : 953869 MB
       status       : active sync
Disk Pair B        Available
   Status          clean
   Disk id B1      Present
       model        : ST91000640NS
       size         : 953869 MB
       status       : active sync
   Disk id B2     Present
       model        : ST91000640NS
       size         : 953869 MB
       status       : active sync
```

STEP 5 | 使陣列可用於記錄日誌。

若要使陣列可用於記錄日誌，您必須將設備新增為 Panorama 上的受管理收集器。如果未新增，請參閱設定一個受管理的收集器。

1. 登入 Panorama 管理伺服器（負責管理此日誌收集器）的網頁介面。
2. 選取 **Panorama** > **Managed Collectors**（受管理的收集器），再編輯日誌收集器。
3. 選取 **Disks**（磁碟），然後 **Add**（新增）每一個陣列。
4. 按一下 **OK**（確定）儲存您的變更。
5. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。
6. 選取 **Commit**（提交）> **Push to Devices**（推送至裝置），然後選取 Collector Group（控制器群組）並 **Push**（推送）您的變更。

在執行 *Panorama 7.0.8* 或更新版本的 *M-Series* 設備上升級磁碟機

STEP 1 | 在 M-Series 設備上存取命令行介面 (CLI)。

以下列兩種方式之一連接至 M-Series 設備：

- 從電腦中將序列纜線連接至主控台連接埠，然後使用終端機模擬軟體連線至 M-Series 設備 (9600-8-N-1)。
- 使用終端機模擬軟體（例如 PuTTY），針對 M-Series 設備的 IP 位址開啟 Secure Shell (SSH) 工作階段。

STEP 2 | 出現提示時，登入裝置。

使用預設的管理員帳戶及指定的密碼。

© 2019 Palo Alto Networks, Inc.

STEP 3 | 驗證所安裝磁碟機的 RAID 1 狀態是否顯示至少有兩個正在運作的 RAID 1 陣列。在升級期間，您將一次升級一個 RAID 1 陣列，而且必須至少有另一個 RAID 1 陣列供設備使用。如果您上是從設定中移除唯一在運作的陣列，設備將顯示中止錯誤。

輸入下列命令以檢視 RAID 狀態：

```
> show system raid detail
```

例如，以下資訊顯示具有兩個可用陣列（磁碟配對 A 和磁碟配對 B）的 M-500 設備的輸出。如果只有一個可用陣列，在升級磁碟機之前，您必須新增第二個陣列，如為 M-Series 設備新增磁碟機所述。

```
Disk Pair A                              Available
   Status                                    clean
   Disk id A1                              Present
       model         : ST91000640NS
       size          : 953869 MB
       status        : active sync
   Disk id A2                              Present
       model         : ST91000640NS
       size          : 953869 MB
       status        : active sync
Disk Pair B                              Available
   Status                                    clean
   Disk id B1                              Present
       model         : ST91000640NS
       size          : 953869 MB
       status        : active sync
   Disk id B2                              Present
       model         : ST91000640NS
       size          : 953869 MB
       status        : active sync
```

STEP 4 | 移除第一個 1TB 磁碟機，換上 2TB 磁碟機。

1. 若要從 RAID 1 陣列設定中移除第一個磁碟機（本範例中的 A1），輸入以下命令，並在提示時輸入 **y** 以確認請求：

   ```
   > request system raid remove A1
   ```

2. 從磁碟機擴充插槽中拆下第一個磁碟機。按下磁碟機擴充插槽 A1 中磁碟機托架上的彈出按鈕，釋放拉手。然後朝向自己拉動拉手，使磁碟機從設備中滑出。
3. 將 2TB 磁碟機從包裝內取出，和您剛剛拆下的磁碟機並排放在桌面上。留意將磁碟機安裝到托架中的方法，因為要將 2TB 磁碟機安裝到相同的托架內。
4. 拆下將 1TB 磁碟機固定到托架內的四顆螺釘，然後將磁碟機從托架內取出。
5. 使用從 1TB 磁碟機上拆下的螺釘將 2TB 磁碟機安裝到托架上，然後將裝有 2TB 磁碟機的托架重新插入磁碟機擴充插槽 A1。
6. 輸入下列命令，確認已辨識 2TB 磁碟機：

   ```
   show system raid detail
   ```

   確認 A1 磁碟顯示正確的型號和大小（大約 2TB）。如果型號和大小不正確，請再執行一次上述命令，直到出現正確型號和大小為止。

   如果一直出現錯誤的型號和大小，請輸入下列命令：

© 2019 Palo Alto Networks, Inc.

```
request system raid remove A1
```

執行上述命令之後等待 30 秒，然後移除磁碟再重新插入，並重複 **show system raid detail** 命令來驗證大小和型號。

STEP 5 | 將資料從 RAID 1 陣列中剩餘的 1TB 磁碟機上複製到該陣列中新安裝的 2TB 磁碟機上。

視磁碟機上的資料數量而定，複製資料所需要的時間可能會從幾分鐘到幾小時不等。

1. 若要將資料從磁碟機擴充插槽 A2 中的 1TB 磁碟機上複製到磁碟機擴充插槽 A1 中新安裝的 2TB 磁碟機上，請輸入以下命令，並在提示時輸入 **y**：

```
> request system raid copy from A2 to A1
```

2. 若要檢視複製過程的狀態，請執行下列命令：

```
> show system raid detail
```

繼續執行此命令，以檢視 RAID 的詳細輸出，直到您看到陣列（本範例中的 A1/A2）顯示 `Available`。

此時，磁碟機 *A2* 將顯示 *not in use*（未使用），因為磁碟機大小不相符。

STEP 6 | 將 RAID 1 陣列中的第二個磁碟機升級為 2TB 磁碟機。

1. 移除 RAID 1 陣列設定中的第二個 1TB 磁碟機（在目前範例中是從磁碟機擴充插槽 A2 中移除）：

```
> request system raid remove A2
```

2. 將剛安裝 2TB 磁碟機的托架插入磁碟機擴充插槽 A2 中，並新增至 RAID 1 陣列設定：

```
> request system raid add A2
```

系統會將資料從 A2 複製到 A1，以鏡像磁碟機。

3. 若要檢視複製過程的狀態，請執行下列命令：

```
> show system raid detail
```

繼續檢視 RAID 的詳細輸出，直到您看到陣列（本範例中的 A1/A2）顯示 `Available` 且兩個磁碟都顯示 `active sync`。

```
Disk Pair A       Available
   Status         clean
   Disk id A1     Present
       model        : ST2000NX0253
       size         : 1907138 MB
       status       : active sync
Disk id A2     Present
       model        : ST2000NX0253
       size         : 1907138 MB
```


© 2019 Palo Alto Networks, Inc.

```
        status       : active sync
```

STEP 7 | 依需要升級額外 RAID 1 陣列的磁碟機。

若要將額外的 RAID 1 陣列升級至 2TB 磁碟機，請重複此程序，並視情況更換磁碟機代號。例如，用 B1 取代 A1，用 B2 取代 A2，以升級 B1/B2 RAID 1 陣列中的磁碟機。

在執行 *Panorama 7.0.7* 或更舊版本的 *M-Series* 設備上升級磁碟機

在運行 *Panorama 7.0.7* 或更早版本的 *M-Series* 設備上升級磁碟機機之後，*1TB* 磁碟機上的日誌將不可用。即使可以接受這種情況，我們還是建議您在維護時段執行此升級操作。

如果保留日誌對您非常重要，您必須先升級至 *Panorama 7.0.8* 或更新版本，然後使用 在執行 Panorama 7.0.8 或更新版本的 M-Series 設備上升級磁碟機 程序。

STEP 1 | 在 M-Series 設備上存取命令行介面 (CLI)。

以下列兩種方式之一連接至 M-Series 設備：

- 從電腦中將序列纜線連接至主控台連接埠，然後使用終端機模擬軟體連線至 M-Series 設備 (9600-8-N-1)。
- 使用終端機模擬軟體（例如 PuTTY），針對 M-Series 設備的 IP 位址開啟 Secure Shell (SSH) 工作階段。

STEP 2 | 出現提示時，登入裝置。

使用預設的管理員帳戶及指定的密碼。

STEP 3 | 驗證所安裝磁碟機的 RAID 1 狀態是否顯示至少有兩個正在運作的 RAID 1 陣列。在升級期間，您將一次升級一個 RAID 1 陣列，而且必須至少有另一個 RAID 1 陣列供設備使用。如果您上是從設定中移除唯一在運作的陣列，設備將顯示中止錯誤。

輸入下列命令以檢視 RAID 狀態：

```
> show system raid detail
```

例如，以下資訊顯示具有兩個可用陣列（磁碟配對 A 和磁碟配對 B）的 M-500 設備的輸出。如果只有一個可用陣列，在升級磁碟機之前，您必須新增第二個陣列，如 為 M-Series 設備新增磁碟機 所述。

```
Disk Pair A                              Available
   Status                                    clean
   Disk id A1                              Present
       model          : ST91000640NS
       size           : 953869 MB
       status         : active sync
   Disk id A2                              Present
       model          : ST91000640NS
       size           : 953869 MB
       status         : active sync
Disk Pair B                              Available
   Status                                    clean
   Disk id B1                              Present
       model          : ST91000640NS
       size           : 953869 MB
       status         : active sync
   Disk id B2                              Present
       model          : ST91000640NS
```


© 2019 Palo Alto Networks, Inc.

```
        size          : 953869 MB
        status        : active sync
```

STEP 4 | 從第一個 RAID 1 陣列設定中移除前兩個 1TB 磁碟機，然後實際移除磁碟機。

1. 若要從 RAID 1 陣列設定中移除磁碟機（本範例中的 A1 和 A2），請輸入以下命令，並在提示時輸入 **y** 以確認每個要求：

```
> request system raid remove A1
> request system raid remove A2
```

2. 從磁碟機擴充插槽中拆下磁碟機。按下磁碟機托架上的彈出按鈕，釋放拉手。然後朝向自己拉動拉手，使磁碟機從設備中滑出。
3. 將兩個 2TB 磁碟機從包裝內取出，和您剛剛拆下的磁碟機並排放在桌面上。留意將磁碟機安裝到托架中的方法，因為要將 2TB 磁碟機安裝到相同的托架內。
4. 拆下將磁碟機固定到托架內的四顆螺釘，然後將磁碟機從托架內取出。
5. 使用剛剛拆下的螺釘將 2TB 磁碟機安裝到托架上，然後將裝有 2TB 磁碟機的托架插入磁碟機擴充插槽（本範例中的 A1 和 A2）。

STEP 5 | 為新安裝的 2TB 磁碟機建立新的 RAID 1 陣列，確保兩個磁碟機都位於新陣列中。

1. 若要建立包含磁碟機擴充插槽 A1 中磁碟機的新陣列，請輸入以下命令：

```
> request system raid add A1
```

2. 若要檢視並確認新 RAID 1 陣列設定的狀態，請輸入下列命令：

```
> show system raid detail
```

以下輸出顯示 `Disk Pair A`（磁碟配對 `A`）陣列為 `Available`（可用）。

此時，磁碟機 *A2* 將顯示 *`not in use`*（未使用）。

```
Disk Pair A       Available
   Status         clean, degraded
   Disk id A1     Present
       model        : ST91000640NS
       size         : 953869 MB
       status       : active sync
   Disk id A2       Present
       model        : ST91000640NS
       size         : 953869 MB
       status       : not in use
```

3. 將第二個磁碟新增到新陣列中。在此範例中，新增 A2：

```
> request system raid add A2
```

4. 繼續執行 **`show system raid detail`** 命令以檢視 RAID 輸出，直至磁碟配對狀態顯示 `clean`，並且兩個磁碟均顯示 `active sync`。

STEP 6 | 依需要升級額外 RAID 1 陣列的磁碟機。

若要將額外的 RAID 1 陣列升級至 2TB 磁碟機，請重複此程序，並視情況更換磁碟機代號。例如，用 B1 取代 A1，用 B2 取代 A2，以升級 B1/B2 RAID 1 陣列中的磁碟機。

© 2019 Palo Alto Networks, Inc.

設定 Panorama 來使用多個介面

在大型網路中，您可以實作網路分割，以改善安全性和降低壅塞，這需要根據資源使用方式、使用者角色和安全性需求來隔開子網路。Panorama 支援網路分割，可讓您使用多個 M-Series 設備介面 來管理裝置（防火牆、日誌收集器及 WildFire 設備和設備叢集）和收集日誌；您可以將個別介面指派給個別子網路上的裝置。

使用多個介面來收集日誌也有利於負載平衡，這在防火牆高速將日誌轉送至日誌收集器的環境下特別有用。如果您在收集器群組日誌轉送偏好設定清單中啟用轉送到所有日誌收集器設定，日誌會在所有已設定介面上進行傳送。否則，日誌將在單個介面上轉送，如果該介面關閉，則繼續在下一個設定的介面上進行日誌轉送。例如，您設定 Eth1/1、Eth1/2 和 Eth1/3 用於日誌轉送。如果 Eth1/1 介面關閉，則會透過 Eth1/2 繼續進行日誌轉送。

因為管理員是透過 MGT 介面來存取和管理 Panorama，保護該介面的安全性尤其重要。改善 MGT 介面安全性的方法之一是將 Panorama 服務卸載到其他介面。除了管理裝置和收集日誌，您還可以將收集器群組通訊及軟體和內容更新的部署，卸載到防火牆、日誌收集器，以及 WildFire 設備和設備叢集。藉由卸載這些服務，您可以將 MGT 介面保留給管理流量，並指派給安全的子網路，而這個子網路與防火牆、日誌收集器及 WildFire 設備和設備叢集所在的子網路隔開。

- 多個介面支援網路分割的範例
- 設定 Panorama 來支援網路分割

多個介面支援網路分割的範例

圖 10: 多個 Panorama 介面 說明在 Panorama 模式和日誌收集器模式的 M-500 設備上使用多個介面的部署。在此範例中，介面支援網路分段，如下所示：

- **Panorama** 管理網路—為了保護 Panorama 網頁介面、CLI 和 XML API 免受未經授權的存取，Panorama 上的 MGT 介面會連接至只有管理員才能存取的子網路。
- 網際網路—Panorama 使用 MGT 介面來與外部服務通訊，例如 Palo Alto Networks 更新伺服器。
- 周邊閘道和資料中心—Panorama 使用個別一對介面來管理每個子網路中的防火牆和日誌收集器。管理防火牆所產生的流量，通常比查詢日誌收集器以取得報告資訊所產生的流量更少。因此，Panorama 使用 1Gbps 介面（Eth1 和 Eth2）來管理防火牆，並使用 10Gbps 介面（Eth4 和 Eth5）來查詢和管理日誌收集器。每個日誌收集器使用 MGT 介面來回應查詢，但使用 Eth4 和 Eth5 介面，以應付從防火牆收集日誌時所產生的較大流量。
- 軟體和內容更新—兩個子網路中的防火牆和日誌收集器，都透過 Panorama 上的 Eth3 介面來擷取軟體和內容更新。

© 2019 Palo Alto Networks, Inc.

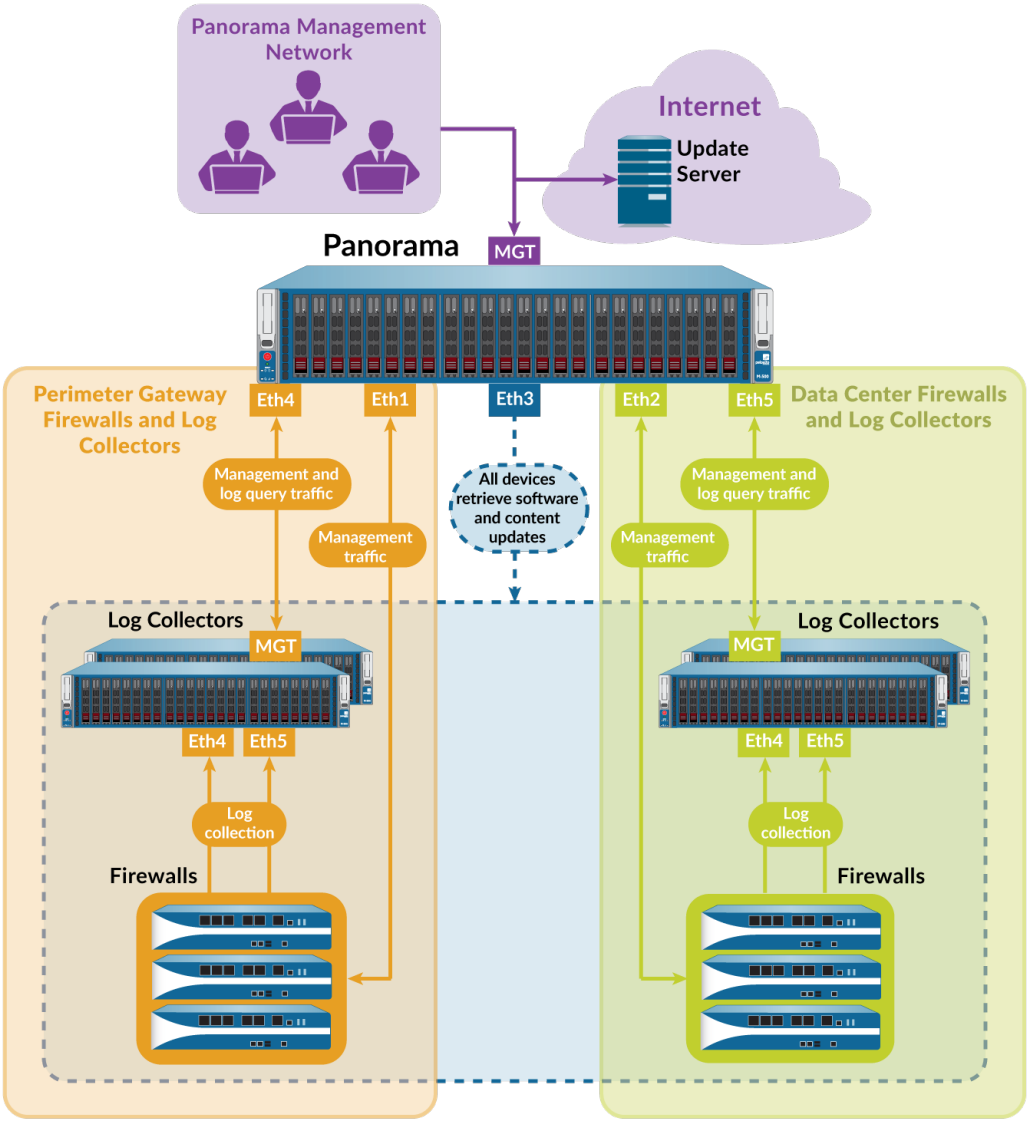


圖 10: 多個 **Panorama** 介面

設定 *Panorama* 來支援網路分割

若要將 Panorama 服務從 MGT 介面卸載到其他介面，首先，請在 Panorama 管理伺服器上設定介面。如果網路的日誌流量很大，請記住，M-500 和 M-600 設備的 Eth4 和 Eth5 介面支援的輸送量 (10Gbps) 高於其他介面 (1Gbps)。然後，在每個子網路上，設定日誌收集器來連接 Panorama 上特定的介面。對於每個日誌收集器，您還需要選取收集器群組通訊所用的介面，以及一個或多個介面來收集防火牆的日誌。最後，在每個子網路上，設定防火牆來連接 Panorama 上的介面。

如果您在日誌收集器模式中使用 *10GB* 介面設定 *M-Series* 設備，則必須完成整個設定程序，才能使 *10GB* 介面顯示為 *Up*（啟動）。

Palo Alto Networks 建議您指定 *MGT* 介面的 *IP* 位址、網路遮罩（適用於 *IPv4*）或首碼長度（適用於 *IPv6*），以及預設閘道。如果您省略其中一項設定（例如預設閘道），則未來需要變更組態時，您只能透過主控台連接埠存取 *M-Series* 設備。

請執行下列步驟，設定 Panorama 和專用日誌收集器來使用多個介面：

© 2019 Palo Alto Networks, Inc.

STEP 1 | 確認 Panorama 設備和防火牆支援多個介面，且有必要的軟體版本和設定。

- M-Series 設備必須執行 Panorama 8.0 或更新版本，才能使用個別介面來部署更新，也才能使用多個介面來管理裝置和收集日誌。M-200 和 M-600 設備必須執行 Panorama 8.1 或更新版本。部署於 ESXi、vCloud、Air、Hyper-V 和 KVM 上的 Panorama 設備必須執行 Panorama 8.1 或更新版本。
- 如果您已將 Panorama 或日誌收集器部署為虛擬設備，請確認 Panorama 虛擬設備支援的介面。
- M-Series 設備必須執行 Panorama 6.1 或更新版本，才能使用個別介面來收集日誌或進行收集器群組通訊。
- 每個 Panorama 管理伺服器的初始設定已完成。其中包括設定 MGT 介面。
- 日誌收集器和收集器群組已設定。其中包括在日誌收集器上設定 MGT 介面。
- 防火牆的初始設定已完成、您已將防火牆新增至 Panorama 成為受管理的裝置，以及每個子網路中的防火牆都指派給個別範本。
- WildFire 設備的初始設定已完成，而且您已將 WildFire 設備新增至 Panorama 成為受管理的裝置。

STEP 2 | 在單獨（非 HA）或主動 (HA) Panorama 管理伺服器上設定介面。



因為已在 *Panorama* 初始設定期間設定 *MGT* 介面，不必再次設定。

對每個介面執行下列步驟：

1. 登入 Panorama 網頁介面 存取單獨（非 HA）或主動 (HA) Panorama 管理伺服器的網頁介面。
2. 選取 **Panorama** > **Setup**（設定） > **Interfaces**（介面）。
3. 按一下介面名稱以編輯介面。
4. 選取 *<interface-name>* 以啟用介面。
5. 視網路的 IP 通訊協定而定，設定下列其中一個或兩個欄位集：
   - IPv4—**IP Address**（**IP** 位址）、**Netmask**（網路遮罩）及 **Default Gateway**（預設閘道）
   - IPv6—**IPv6 Address/Prefix Length**（**IPv6** 位址/首碼長度）及 **Default IPv6 Gateway**（預設的 **IPv6** 閘道）
6. 選取介面支援的服務：
   - **Device Management and Device Log Collection**（裝置管理和裝置日誌收集）—管理防火牆、日誌收集器及 WildFire 設備和設備叢集、收集日誌收集器所產生的日誌，以及查詢日誌收集器來取得報告資訊。若要支援分段網路，您可以在多個介面上啟用這些服務。
   - **Collector Group Communication**（收集器群組通訊）—與 Panorama 在所有子網路上管理的收集器群組進行通訊。
   - **Device Deployment**（裝置部署）—將軟體和內容更新部署至所有子網路上的防火牆、日誌收集器，以及 WildFire 設備和設備叢集。
7. 按一下 **OK**（確定）以儲存對介面所做的變更。
8. 按一下 **Commit**（提交） > **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交） 您的變更。
9. 按一下 **Commit**（提交） > **Push to Devices**（推送至裝置） 並將變更推送至含有您修改了日誌收集器的收集器群組。

STEP 3 | （僅限 HA）在被動 Panorama 管理伺服器上設定介面。

1. 登入 Panorama 網頁介面 存取主動 Panorama 管理伺服器的網頁介面。
2. 選取 **Panorama** > **Managed Collectors**（受管理的收集器），再選取被動 HA 對等。
3. 選取 **Interfaces**（介面），然後按一下要編輯的介面。
4. 按一下 **Enable Interface**（啟用介面）核取方塊以啟用介面。
5. 視網路的 IP 通訊協定而定，設定下列其中一個或兩個欄位集：
   - IPv4—**IP Address**（**IP** 位址）、**Netmask**（網路遮罩）及 **Default Gateway**（預設閘道）

© 2019 Palo Alto Networks, Inc.

- IPv6—**IPv6 Address/Prefix Length**（**IPv6** 位址/首碼長度）及 **Default IPv6 Gateway**（預設的 **IPv6** 閘道）

6. 選取介面支援的服務：
   - **Device Management and Device Log Collection**（裝置管理和裝置日誌收集）—管理防火牆、日誌收集器及 WildFire 設備和設備叢集、收集日誌收集器所產生的日誌，以及查詢日誌收集器來取得報告資訊。若要支援分段網路，您可以在多個介面上啟用這些服務。
   - **Collector Group Communication**（收集器群組通訊）—與 Panorama 在所有子網路上管理的收集器群組進行通訊。
   - **Device Deployment**（裝置部署）—將軟體和內容更新部署至所有子網路上的防火牆、日誌收集器，以及 WildFire 設備和設備叢集。
7. 按一下 **OK**（確定）以儲存對介面所做的變更。
8. 選取 **Commit**（提交）> **Commit and Push**（提交並推送），將您的變更提交至 Panorama，並將變更推送至收集器群組，其中包含您已修改的 HA 對等。

STEP 4 | 設定每個日誌收集器來連接 Panorama 介面。

若要支援分段網路，您可以將每個子網路中的日誌收集器連接至個別的 Panorama 介面。這些介面必須啟用 **Device Management and Device Log Collection**（裝置管理和裝置日誌收集），如上一步所述。

1. 登入 Panorama 網頁介面 存取單獨（非 HA）或主動 (HA) Panorama 管理伺服器的網頁介面。
2. 選取 **Panorama** > **Managed Collectors**（受管理的收集器），再編輯日誌收集器。
3. 在 **Panorama Server IP**（**Panorama** 伺服器 **IP**）欄位中，輸入單獨（非 HA）或主動 (HA) Panorama 上的一個介面的 IP 位址。
4. （僅限 HA）在 **Panorama Server IP 2**（**Panorama** 伺服器 **IP 2**）欄位中，輸入被動 Panorama 上的一個介面的 IP 位址，如果主動 Panorama 發生容錯移轉，此介面將支援 **Device Management and Device Log Collection**（裝置管理和裝置日誌收集）。
5. 按一下 **OK**（確定）儲存您的變更。
6. 選取 **Commit**（提交）> **Commit and Push**（提交並推送），將您的變更提交至 Panorama，並將變更推送至收集器群組，其中包含您已修改的日誌收集器。
7. 在每個專用日誌收集器上執行下列步驟：
   1. 使用模擬軟體（例如 PuTTY）來存取日誌收集器 CLI，以利用 MGT 介面 IP 位址對日誌收集器開啟 SSH 工作階段。出現提示時，使用 Panorama 管理員認證登入。
   2. 執行下列命令，其中 *<IPaddress1>* 用於單獨（非 HA）或主動 (HA) Panorama，*<IPaddress2>* 用於被動 Panorama（如適用）。

```
> configure
# set deviceconfig system panorama-server <IPaddress1> panorama-
server-2 <IPaddress2>
# commit
```

STEP 5 | （僅限 HA）在被動 Panorama 管理伺服器上設定介面，以便在主動 Panorama 容錯移轉時部署更新。

1. 登入 Panorama 網頁介面 存取被動 Panorama 管理伺服器的網頁介面。
2. 選取 **Panorama** > **Setup**（設定）> **Interfaces**（介面）。
3. 按一下介面名稱以編輯介面。
4. 選取 *<interface-name>* 以啟用介面。
5. 視網路的 IP 通訊協定而定，設定下列其中一個或兩個欄位集：
   - IPv4—**IP Address**（**IP** 位址）、**Netmask**（網路遮罩）及 **Default Gateway**（預設閘道）
   - IPv6—**IPv6 Address/Prefix Length**（**IPv6** 位址/首碼長度）及 **Default IPv6 Gateway**（預設的 **IPv6** 閘道）

© 2019 Palo Alto Networks, Inc.

6. 選取 **Device Deployment**（裝置部署）。
7. 按一下 **OK**（確定）儲存您的變更。
8. 按一下 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

STEP 6 | 設定介面供日誌收集器用來收集防火牆的日誌，以及與其他日誌收集器進行通訊。



因為已在日誌收集器的初始設定期間設定 *MGT* 介面，不必再次設定。

1. 登入 Panorama 網頁介面 存取單獨（非 HA）或主動 (HA) Panorama 管理伺服器的網頁介面。
2. 選取 **Panorama** > **Managed Collectors**（受管理的收集器），再編輯日誌收集器。
3. 選取 **Interfaces**（介面），對每個介面執行下列步驟：
   1. 按一下介面名稱以編輯該介面。
   2. 選取 *<interface-name>* 以啟用介面。
   3. 視網路的 IP 通訊協定而定，設定下列其中一個或兩個欄位集。

      IPv4—IP Address（**IP** 位址）、**Netmask**（網路遮罩）及 **Default Gateway**（預設閘道）

      IPv6—IPv6 Address/Prefix Length（**IPv6** 位址/首碼長度）及 **Default IPv6 Gateway**（預設的 **IPv6** 閘道）
   4. 選取介面支援的功能：

      Device Log Collection（裝置日誌收集）—從防火牆收集日誌。您可以啟用多個介面來執行此功能，以平衡日誌記錄流量的負載。

      Collector Group Communication（收集器群組通訊）—與收集器群組中的其他日誌收集器進行通訊。
   5. 按一下 **OK**（確定）以儲存對介面所做的變更。
4. 按一下 **OK**（確定），以儲存對日誌收集器所做的變更。
5. 選取 **Commit**（提交）> **Commit and Push**（提交並推送），將您的變更提交至 Panorama，並將變更推送至收集器群組，其中包含您已修改的日誌收集器。
6. 選取 **Panorama** > **Managed Collectors**（受管理的收集器），確認日誌收集器已同步和連接至 Panorama。

   Configuration Status（組態狀態）欄應該顯示 `In Sync`（同步），Run Time Status（執行階段狀態）欄應該顯示 `connected`（已連線）。

STEP 7 | 設定防火牆來連接 Panorama 介面。

若要支援分段網路，您可以將每個子網路中的防火牆連接至個別的 Panorama 介面。這些介面必須啟用 **Device Management and Device Log Collection**（裝置管理和裝置日誌收集）。此步驟假設您使用個別範本來設定個別子網路中的防火牆。



在此範例部署中，*Panorama* 使用這些介面來管理防火牆，但不收集防火牆日誌。當您設定收集器群組時，您會指定哪些專用日誌收集器將收集防火牆日誌。

1. 登入 Panorama 網頁介面 存取單獨（非 HA）或主動 (HA) Panorama 管理伺服器的網頁介面。
2. 在 Panorama 上，選取 **Device**（裝置）> **Setup**（設定）> **Management**（管理），並選取 **Template**（範本），然後編輯 Panorama Settings（Panorama 設定）。
3. 在第一個 **Panorama Servers**（**Panorama** 伺服器）欄位中，輸入單獨（非 HA）或主動 (HA) Panorama 上的一個介面的 IP 位址。
4. （僅限 HA）在第二個 **Panorama Servers**（**Panorama** 伺服器）欄位中，輸入被動 Panorama 上的一個介面的 IP 位址，如果發生容錯移轉，此介面將支援裝置管理。
5. 按一下 **OK**（確定）儲存您的變更。

© 2019 Palo Alto Networks, Inc.

6. 選取 **Commit**（提交）> **Commit and Push**（提交並推送），將您的變更提交至 Panorama，並將範本變更推送至防火牆。
7. 選取 **Panorama** > **Managed Devices**（受管理的裝置），確認防火牆已同步和連接至 Panorama。

   Device State（裝置狀態）欄應該顯示 `Connected`（已連線）。Shared Policy（共用原則）和 Template（範本）欄應該顯示 `In Sync`（同步）。

© 2019 Palo Alto Networks, Inc.

註冊 Panorama 與安裝授權

您必須先註冊、啟動及擷取 Panorama 裝置管理與支援的授權，才能開始使用 Panorama 進行集中管理、日誌記錄和報告。Panorama 的每個實例都需要有效的授權，才能讓您管理防火牆與取得支援。防火牆裝置管理授權強制規定 Panorama 可管理的防火牆數目上限。此授權基於防火牆序號，而非各防火牆上的虛擬系統數量。支援授權啟用 Panorama 軟體更新和動態內容更新（例如，針對最新的應用程式和威脅簽章）。此外，在 AWS 和 Azure 上的 Panorama 虛擬設備必須自 Palo Alto Networks 購買，且無法在 AWS 或 Azure 市場上購買。

在升級 Panorama 虛擬設備至 PAN-OS 8.1 後，您會收到提示，詢問是否未成功安裝容量授權，或是否 Panorama 管理的防火牆總數超出裝置管理授權數。如果未安裝授權，則您從升級到安裝有效裝置管理授權有180 天的時間。如果受管理的防火牆數量超出裝置的管理授權，則您有 180 天的時間刪除防火牆，以符合裝置管理授權需求，或升級您的裝置管理授權。如果在 180 天內未安裝有效裝置管理授權或現有裝置管理授權數量不符，則所有提交都會失敗。若要購買裝置管理授權，請聯絡您的 Palo Alto Networks 銷售人員或授權的經銷商。

如果您要使用雲端式 Cortex Data Lake（Cortex 資料湖），則除了防火牆管理授權和進階支援授權，您還需要 Cortex Data Lake（Cortex 資料湖）授權。若要購買授權，請聯絡您的 Palo Alto Networks 系統工程師或零售商。



如果您正在 *Panorama* 虛擬設備上執行防火牆管理的試用授權，並想要套用已購買的 *Panorama* 授權，請執行註冊 Panorama 與在 Panorama 虛擬設備已連線網際網路時，啟動/擷取防火牆管理授權工作。

- 註冊 Panorama
- 啟動 Panorama 支援授權
- 在 Panorama 虛擬設備與網際網路連線時，啟動/擷取防火牆管理授權
- 在 Panorama 虛擬設備並未與網際網路連線時，啟動/擷取防火牆管理授權
- 在 M-Series 設備上啟動/擷取防火牆管理授權

註冊 Panorama

STEP 1 | 記下 Panorama 序號或授權碼，並記下您的銷售訂單號碼或客戶 ID。

若要知道授權碼、銷售訂單號碼或客戶 ID，請見您在向 Panorama 下單時 Palo Alto Networks 客戶服務寄給您的訂購完成電子郵件。

序號所在位置視型號而定：

- M-Series 設備——登入 Panorama網頁介面並記錄一般資訊部分 **Dashboard**（儀表板）頁籤內的 **Serial #**（序號）值。
- Panorama 虛擬設備—請參閱訂購完成電子郵件。

STEP 2 | 註冊 Panorama。步驟視您是否已登入支援網站而定。

- 如果這是您註冊的第一台 Palo Alto Networks 裝置且您尚未登入：
  1. 前往 Palo Alto Networks 客戶支援網站。
  2. 按一下頁面底部的 **Register**（註冊）（**Overview**（概觀）> **Get Help**（獲取幫助）> **Register**（註冊）），輸入您的 **Email Address**（電子郵件地址），輸入頁面上顯示的代碼，然後按一下 **Submit**（提交）。
  3. 完成 **Create Contact Details**（建立聯絡詳細資料）部分的欄位。
  4. 輸入 **Display Name**（顯示名稱）、**Confirm Email Address**（確認電子郵件地址）及**Password/Confirm Password**（密碼/確認密碼）。

© 2019 Palo Alto Networks, Inc.

5. 輸入 Panorama **Device Serial Number**（裝置序號）或 **Auth Code**（驗證碼）。
6. 輸入 **Sales Order Number**（銷售訂單號碼）或 **Customer ID**（客戶 ID）。
7. 按一下 **Submit**（提交）。

- 如果您已具有支援帳戶：

1. 登入 Palo Alto Networks 客戶支援網站。
2. 按一下 **Assets**（資產）> **Devices**（裝置）> **Register New Device**（註冊新裝置）。
3. 選取 **Register device using Serial Number or Authorization Code**（使用序號或授權碼註冊裝置），然後按一下 **Submit**（提交）。
4. 若 Panorama 管理伺服器無法與網際網路連線，則請查看 **Device will be used offline**（離線時將使用的裝置）並選取 **OS Release**（OS 發佈）版本。
5. 輸入 Panorama **Serial Number**（序號）。
6. 若您已購買 4 小時的 RMA，則輸入必要的地點資訊（如星號所標示）。
7. **Agree and Submit**（同意並提交）EULA。

   看到註冊完成訊息之後，關閉 Device Registration（裝置註冊）對話。

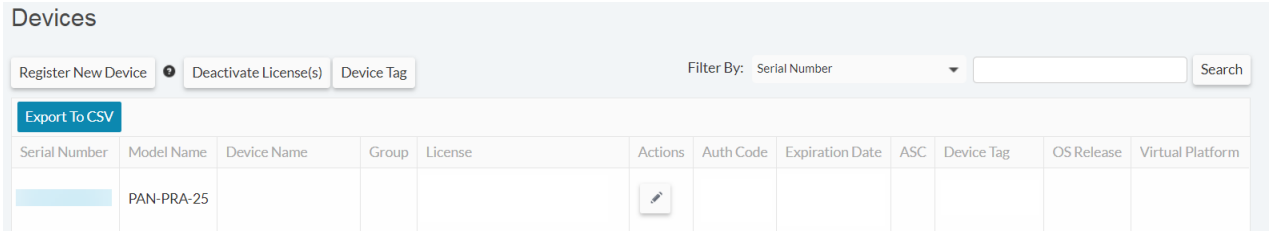
啟動 Panorama 支援授權

在 Panorama M-Series 設備或 Panorama 虛擬設備上啟動 Panorama 支援授權前，您必須註冊 Panorama。

如果支援授權到期，*Panorama* 仍可管理防火牆和收集日誌，但軟體和內容更新將不可用。*Panorama* 上的軟體和內容更新版本必須與受管理的防火牆版本一致或更新，否則將發生錯誤。請參閱 Panorama、日誌收集器、防火牆和 WildFire 版本相容性。

STEP 1 | 登入 Palo Alto Networks 客戶支援入口網站以啟動驗證碼。

1. 選取 **Assets**（資產）> **Devices**（裝置）並輸入 Panorama 序號，以按照 **Serial Number**（序號）篩選。



2. 選取 Action（動作）欄中的鉛筆圖示，選取 **Activate Auth-Code**（啟動驗證碼），輸入支援授權 **Authorization Code**（授權碼），然後按一下 **Agree and Submit**（同意並提交）。

STEP 2 | 登入 Panorama 網頁介面，選取 **Panorama** > **Support**（支援）> **Activate feature using authorization code**（使用授權碼啟動功能）。

STEP 3 | 輸入**Authorization Code**（授權碼），然後按一下**OK**（確定）。

STEP 4 | 確認使用授權已啟動。在頁面的 Support（支援）部分中，檢查其中的詳細資訊（例如 **Expiry Date**（到期日期）、支援 **Level**（層級）和 **Description**（說明））。

© 2019 Palo Alto Networks, Inc.

在 Panorama 虛擬設備與網際網路連線時，啟動/擷取防火牆管理授權

為了在 Panorama 上管理裝置，您需要啟動 PAN-OS 產生的防火牆管理授權。您啟動的裝置管理授權，將決定 Panorama 所能管理的裝置數目。日誌收集器和 WildFire 設備不視為受管理的裝置，不會計入裝置管理授權所分配的裝置數目內。

在 Panorama 虛擬設備上啟動與擷取防火牆管理授權之前，您必須註冊 Panorama。如果您正在執行試用授權，而且想要套用您購買的授權，您仍必須註冊與啟動/擷取購買的授權。此外，您必須將 Panorama 序號從評估序號變更為生產序號。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 選取 **Panorama** > **Setup**（設定）> **Management**（管理），再編輯 [一般設定]。

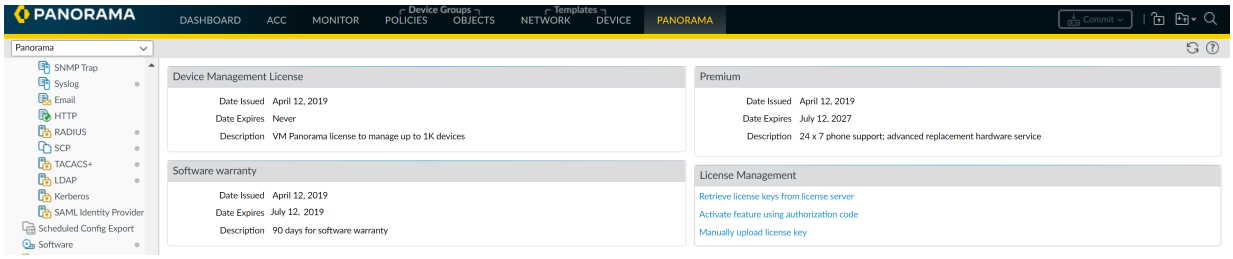
STEP 3 | 輸入 Panorama **Serial Number**（序號）（包含在訂單完成電子郵件中），然後按一下 **OK**（確定）。

STEP 4 | 選擇 **Panorama** > **Licenses**（授權）以啟動或擷取防火牆管理授權：

- **Retrieve license keys from license server**（從授權伺服器擷取授權金鑰）—Panorama 自動從 Panorama 更新伺服器擷取並啟動防火牆管理授權。
- **Activate feature using authorization code**（透過驗證碼啟動功能）—輸入防火牆管理授權驗證碼，並按一下 **OK**（確定）以啟動授權。驗證碼可從訂單履行電子郵件中獲得，或透過登入 Palo Alto 網路客戶支援網站 找到 Panorama 管理伺服器獲得。
- **Manually upload license key**（手動上傳授權金鑰）—登入 Palo Alto 網路客戶支援網站 ，找到您的 Panorama 管理伺服器，然後下載防火牆管理授權金鑰至您的本機裝置。在下載授權金鑰後，按一下 **Choose File**（選擇檔案）以選擇授權金鑰並按一下 **OK**（確定）。

STEP 5 | 驗證防火牆管理授權是否啟動。

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



在 Panorama 虛擬設備並未與網際網路連線時，啟動/擷取防火牆管理授權

在 Panorama 虛擬設備上啟動與擷取防火牆管理授權之前，您必須註冊 Panorama。為了在 Panorama 上管理裝置，您需要啟動裝置管理授權。您啟動的裝置管理授權，將決定 Panorama 所能管理的裝置數目。日誌收集器和 WildFire 設備不視為受管理的裝置，不會計入裝置管理授權所分配的裝置數目內。如果您正在執行試用授權，而且想要套用您購買的授權，您仍必須註冊與啟動/擷取購買的授權。

在升級到 PAN-OS 8.1 後，在 Panorama 結束重新啟動，您第一次登入 Panorama 網頁介面時，您將收到提示，要求您取得有效的 Panorama 管理授權。若要在 Panorama 虛擬設備離線或無法聯絡 Palo Alto Networks 更新伺服器的情況下啟動或取得有效的管理授權，您必須獲得 Panorama 虛擬設備的相關設備資料，並將其上傳至自訂支援網站。

© 2019 Palo Alto Networks, Inc.

STEP 1 | 登入 Panorama 網頁介面。

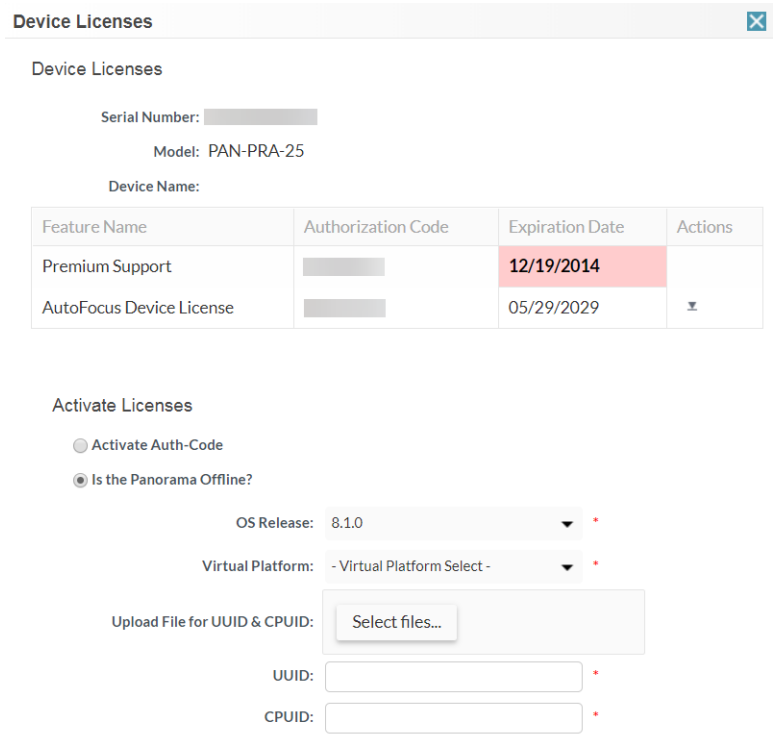
STEP 2 | （僅限原始部署）輸入 Panorama **Serial Number**（序號）。

1. 選取 **Panorama** > **Setup**（設定）> **Management**（管理），再編輯 [一般設定]。
2. 輸入 Panorama **Serial Number**（序號）（包含在訂單完成電子郵件中），然後按一下 **OK**（確定）。
3. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

STEP 3 | 上傳 Panorama 虛擬設備資料到自訂支援網站。

1. 在取得管理授權對話中，按一下 **here**（此處）連結以收集 UUID、CPUID、Panorama 版本與虛擬平台資料。按一下 **Download Link**（下載連結）以下載可以上傳至自訂支援入口網站的必要 Panorama 資料的 XML 檔案。

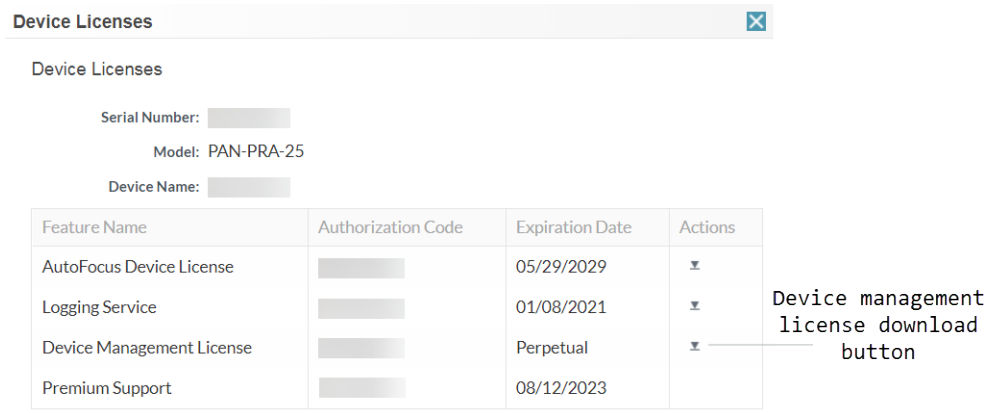
   在原始部署中，也許需要登入然後再登入到網頁介面才能看到對話。
2. 登入 Palo Alto Networks 客戶支援網站。
3. 按一下右上角的 **Get Support**（獲得支援）。
4. 選取 **Assets**（資產）> **Devices**（裝置），尋找您的 Panorama 虛擬設備，然後按一下 Action（動作）欄中的編輯圖示 ()。
5. 選取 **Is the Panorama Offline?**（**Panorama** 是否離線？）並輸入步驟 2 中收集的 Panorama 資料，或按一下 **Select files...**（選取檔案...）以上傳下載的 XML 檔案。
6. **Agree and Submit**（同意並提交）EULA。



STEP 4 | 安裝設備管理授權。

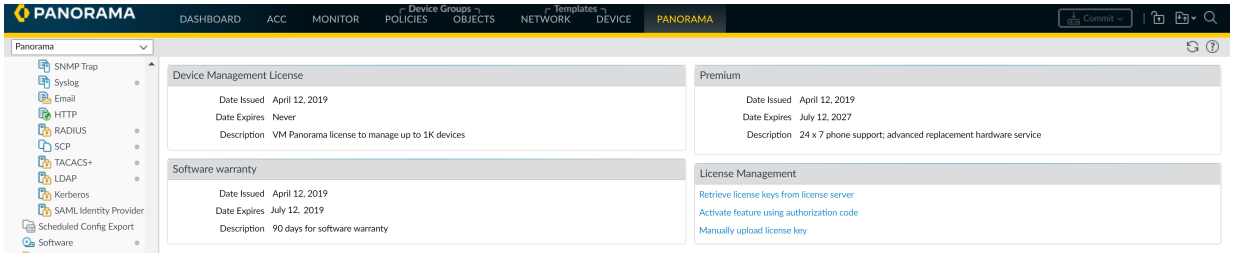
1. 在動作欄中下載裝置管理授權。

© 2019 Palo Alto Networks, Inc.



2. 在 Panorama Web 介面中，按一下 **Panorama** > **Licenses**（授權），以及 **Manually upload license key**（手動上傳授權金鑰）。
3. 按一下 **Chose file**（選取檔案）以找出下載的裝置管理授權金鑰並按一下 **OK**（確定）。

STEP 5 | 確認裝置管理授權顯示授權資料，即可確定裝置管理授權已成功上傳。



在 M-Series 設備上啟動/擷取防火牆管理授權

為了在 Panorama 上管理裝置，您需要啟動容量授權。容量授權決定了 Panorama 所能管理的裝置數目。日誌收集器和 WildFire 設備不視為受管理的裝置，不會計入容量授權所分配的裝置數目內。

在 M-Series 設備上啟動與擷取 Panorama 防火牆管理授權：

- 註冊 Panorama。
- 找到購買的產品/使用授權的授權碼。當您下訂單後，Palo Alto Networks 客戶服務會寄給您一封電子郵件，其中列出所購買產品的授權碼。如果您找不到此封電子郵件，請先與 Palo Alto Networks 客戶支援聯絡以取得授權碼，再繼續進行。

在您啟動與擷取授權後，**Panorama** > **Licenses**（授權）頁面會顯示相關的發行日期、到期日，以及授權允許 Panorama 管理的防火牆數目。

若要啟動與擷取授權，則選項有：

- 使用 Web 介面啟動與擷取授權。

  如果 Panorama 準備好連線至 Palo Alto Networks 更新伺服器（您已完成執行 M-Series 設備的初始設定工作），且您尚未在Palo Alto Networks 客戶支援網站上啟動授權時，請選取此選項。

  1. 選取 **Panorama** > **Licenses**（授權），然後按一下**Activate feature using authorization code**（使用授權碼啟動功能）。
  2. 輸入**Authorization Code**（授權碼），然後按一下**OK**（確定）。Panorama 隨即擷取與啟動授權。

- 從授權伺服器擷取授權金鑰。

© 2019 Palo Alto Networks, Inc.

如果 Panorama 尚未準備好連線至更新伺服器（例如，您尚未完成初始 M-Series 設備設定），您可以在支援網站上啟動授權，如此一來當 Panorama 準備好連線時，您可以使用 Web 介面擷取啟動的授權。處理擷取已啟動授權的速度，比同時處理擷取與啟動的速度快。

1. 請在 Palo Alto Networks 客戶支援網站上啟動授權。
    1. 在可存取網際網路的主機上，使用 Web 瀏覽器存取Palo Alto Networks 客戶支援網站，然後登入。
    2. 選取 **Assets**（資產）> **Devices**（裝置），尋找您的 M-Series 設備，然後按一下 Action（動作）欄中的編輯圖示 ()。
    3. 選取 **Activate Auth-Code**，輸入 **Authorization Code**（授權碼），然後按一下 **Agree and Submit**（同意並提交）以啟動授權。
2. 設定 Panorama 連線至更新伺服器：請參閱執行 M-Series 設備的初始設定。
3. 選取 **Panorama** > **Licenses**（授權），然後按一下**Retrieve license keys from the license server**（從授權伺服器擷取授權金鑰）。Panorama 隨即擷取已啟動的授權。

- 手動將授權從主機上傳至 Panorama。Panorama 必須具有該主機的存取權。

如果 Panorama 已設定（您已完成執行 M-Series 設備的初始設定工作），但沒有與更新伺服器連線，請啟動支援網站上的授權，先將授權下載至與更新伺服器連線的主機，然後上傳至 Panorama。

1. 請在 Palo Alto Networks 客戶支援網站上啟動並下載授權。
    1. 在可存取網際網路的主機上，使用 Web 瀏覽器存取Palo Alto Networks 客戶支援網站，然後登入。
    2. 選取 **Assets**（資產）> **Devices**（裝置），尋找您的 M-Series 設備，然後按一下 Action（動作）欄中的編輯圖示 ()。
    3. 選取 **Activate Auth-Code**，輸入 **Authorization Code**（授權碼），然後按一下 **Agree and Submit**（同意並提交）以啟動授權。
    4. 在 Action（動作）欄中，按一下下載圖示，然後將授權金鑰儲存至主機。
2. 在 Panorama Web 介面中，選取 **Panorama** > **Licenses**（授權），按一下 **Manually upload license key**（手動上傳授權金鑰），然後按一下 **Browse**（瀏覽）。
3. 選取您下載至主機的金鑰檔案，然後按一下 **Open**（開啟）。
4. 按一下 **OK**（確定）以上傳啟動的授權金鑰。

© 2019 Palo Alto Networks, Inc.

安裝 Panorama 裝置憑證

在 PAN-OS 9.1.3 及更新版本中，您必須在 Panorama™ 管理伺服器上安裝裝置憑證，才能向 Palo Alto Networks 客戶支援入口網站 (CSP) 成功驗證 Panorama，及利用零接觸佈建 (ZTP)、裝置遙測、IoT 和企業資料遺失防護 (DLP) 等雲端服務。Panorama 必須具有網際網路存取權才能成功安裝裝置憑證。

如果您正在使用雲端服務外掛程式，則必須安裝雲端服務外掛程式 1.5 或更高版本才能成功安裝 *Panorama* 裝置憑證。

STEP 1 | 註冊 Panorama 使用 Palo Alto Networks 客戶支援入口網站 (CSP)。

STEP 2 | 設定網路時間協定 (NTP) 伺服器。

需要 NTP 伺服器驗證裝置憑證到期日，確定裝置憑證未提前到期或失效。

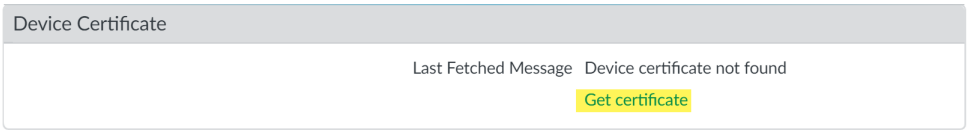
1. 登入 Panorama 網頁介面。
2. 選取 **Panorama** > **Setup**（設定）> **Services**（服務）。
3. 選取 **NTP** 並輸入主機名稱 `pool.ntp.org` 作為 **Primary NTP Server**（主要 **NTP** 伺服器）或輸入主要 NTP 伺服器的 IP 位址。
4. （選用）輸入 **Secondary NTP Server**（次要 **NTP** 伺服器）位址。
5. （選用）若要驗證 NTP 伺服器的時間更新，為每個伺服器選取下列的 **Authentication Type**（驗證類型）。
   - 無—（預設）停用 NTP 驗證。
   - 對稱金鑰—防火牆使用對稱金鑰交換 (共用密碼）來驗證時間更新。
     - 金鑰 **ID**—輸入金鑰 ID (1-65534)
     - 演算法—選取在 NTP 驗證中要使用的演算法（**MDS** 或 **SHA1**）
6. 按一下 **OK**（確定）儲存組態變更。
7. 按一下 **Commit**（提交）和 **Commit to Panorama**（提交至 **Panorama**）。

STEP 3 | 產生一次性密碼 (OTP)。

1. 登入客戶支援入口網站。
2. 選取 **Assets**（資產）> **Device Certificates**（裝置憑證）及 **Generate OTP**（產生 **OTP**）。
3. 對於 **Device Type**（裝置類型），選取 **Generate OTP for Panorama**（產生 **Panorama** 的 **OTP**）及 **Generate OTP**（產生 **OTP**）。
4. 輸入 **Panorama Device**（**Panorama** 裝置）序號。
5. **Generate OTP**（產生 **OTP**）且複製 OTP。

STEP 4 | 登入 Panorama 網頁介面 以管理員使用者身份。

STEP 5 | 選取 **Panorama** > **Setup**（設定）> **Management**（管理）> **Device Certificate Settings**（裝置憑證設定）及 **Get certificate**（取得憑證）。



STEP 6 | 輸入您產生的 **One-time Password**（一次性密碼）並按一下 **OK**（確定）。

STEP 7 | Panorama 成功擷取並安裝憑證。

© 2019 Palo Alto Networks, Inc.

Device Certificate	
Current Device Certificate Status	Valid
Not Valid Before	2020/04/01 21:52:28 PDT
Not Valid After	2020/06/30 21:52:28 PDT
Last Fetched Message	Successfully fetched device certificate
Last Fetched Status	success
Last Fetched Timestamp	2020/04/01 22:02:28 PDT

© 2019 Palo Alto Networks, Inc.

安裝 Panorama 的內容與軟體更新

有效的支援使用授權允許存取 Panorama 軟體影像與版本資訊。為了享有最新修正與安全性強化，請升級至轉售商或 Palo Alto Networks 系統工程師針對您的部署所建議的最新軟體與內容更新。安裝軟體與內容更新的程序，視 Panorama 是否直接與網際網路連線和是否有高可用性 (HA) 設定而定。

- Panorama、日誌收集器、防火牆和 WildFire 版本相容性
- 在 HA 組態中為 Panorama 安裝更新
- 為有網際網路連線的 Panorama 安裝更新
- 為沒有網際網路連線的 Panorama 安裝更新
- 為沒有網際網路連線的 Panorama 自動安裝更新
- 將 Panorama 日誌移轉為新的日誌格式

Panorama、日誌收集器、防火牆和 WildFire 版本相容性

為了得到最佳結果，請遵守下列 Panorama™ 相容性方針：

- 在 Panorama 管理伺服器和專用日誌收集器上安裝相同的 Panorama 版本。
- Panorama 必須執行與其管理的防火牆相同或更新的 PAN-OS 版本。在升級防火牆到 PAN-OS 10.0 前，您必須先升級 Panorama 至 10.0。

  Panorama 6.1 和更新版本無法將設定推送至執行 *PAN-OS 6.0.0* 至 *PAN-OS 6.0.3* 的防火牆。
- 執行 PAN-OS 10.0 的 Panorama 可以管理執行相同或更舊 PAN-OS 10.0 版本的 WildFire® 設備和 WildFire 設備叢集。建議 Panorama 管理伺服器、Wildfire 設備和 Wildfire 設備叢集執行相同的 PAN-OS 版本。
- Panorama 管理伺服器上的內容發行版本，與任何專用日誌收集器和受管理防火牆上的內容發行版本相比，必須是相同（或更舊）版本。

  Palo Alto Networks® 建議在 *Panorama* 上安裝與專用日誌收集器和防火牆上相同的「應用程式」資料庫版本。

  無論您的訂閱包含「應用程式」資料庫還是「應用程式與威脅」資料庫，Panorama 都只會安裝「應用程式」資料庫。Panorama 和專用日誌收集器不會執行原則規則，因此不需要「威脅」資料庫中的威脅特徵碼。「應用程式」資料庫中包含了當您在定義原則規則以推送至受管理防火牆以及在判讀日誌和報告中的威脅資訊時，可以在 Panorama 和專用日誌收集器上使用的威脅中繼資料（例如威脅 ID 和名稱）。不過，防火牆需要完整的「應用程式與威脅」資料庫，才能將日誌中記錄的識別碼，與對應的威脅、URL 或應用程式名稱進行比對。請參閱版本資訊，瞭解 Panorama 版本所需的最低內容發行版本。

在 HA 組態中為 Panorama 安裝更新

在高可用性 (HA) 設定中更新 Panorama 軟體時，為了確保容錯移轉順暢，主動和被動 Panorama 對等必須執行相同的 Panorama 版本及相同的應用程式資料庫版本。下列範例說明如何升級 HA 配對（主動對等為 Primary_A，被動對等為 Secondary_B）。

更新 Panorama 之前，請參閱版本資訊，瞭解 PAN-OS 10.0 所需的最低內容發行版本。

STEP 1 | 在 Secondary_B（被動）對等上升級 Panorama 軟體。

在 Secondary_B 對等上執行下列其中一項工作：

- 為有網際網路連線的 Panorama 安裝更新
- 為沒有連線至網際網路的 Panorama 安裝更新

© 2019 Palo Alto Networks, Inc.

升級後，此 Panorama 會轉變為非運作狀態，因為對等執行的軟體版本已不相同。

STEP 2 | 暫停 Primary_A 對等以強制容錯移轉。

在 Primary_A 對等上：

1. 在 **Operational Commands**（操作命令）部分中（**Panorama** > **High Availability**（高可用性）），**Suspend local Panorama**（暫停本機 **Panorama**）。
2. 確認狀態為 `suspended`（暫停）（顯示在網頁介面的右下角）。

   容錯移轉結果應該會使 Secondary_B 對等轉變為 `active`（主動）狀態。

STEP 3 | 在 Primary_A（主動）對等上升級 Panorama 軟體。

在 Primary_A 對等上執行下列其中一項工作：

- 為有網際網路連線的 Panorama 安裝更新
- 為沒有連線至網際網路的 Panorama 安裝更新

重新啟動後，Primary_A 對等最初仍然為被動狀態。接著，如果啟用先佔（預設值），Primary_A 對等會自動轉變為主動狀態，Secondary_B 對等會還原為被動狀態。

如果您已停用先佔，則手動將主要 Panorama 還原至主動狀態。

STEP 4 | 確認兩個對等現在都執行任何新安裝的內容發行版本，以及新安裝的 Panorama 版本。

在每個 Panorama 對等的 **Dashboard**（儀表板），檢查 Panorama 軟體版本和應用程式版本，並確認這些版本在兩個對等上都相同，且執行中的設定已同步。

STEP 5 | （僅在一個收集器群組內的本機日誌收集器）在收集器群組內升級剩餘日誌收集器。

- 當 Panorama 連線至網際網路時升級日誌收集器
- 當 Panorama 未連線至網際網路時升級日誌收集器

為有網際網路連線的 Panorama 安裝更新

如果 Panorama™ 直接與網際網路連線，請依需要，執行下列步驟來安裝 Panorama 軟體和內容更新。如果 Panorama 在高可用性 (HA) 設定中執行，請升級每個對等上的 Panorama 軟體（請參閱在 HA 組態中為 Panorama 安裝更新）。

在 Panorama 虛擬設備上升級軟體不會變更系統模式；切換至 Panorama 模式或僅管理模式是手動工作，需要額外的設定，如設定具備本機日誌收集器的 Panorama 虛擬設備所述。

PAN-OS® 9.0 為本機和專用日誌收集器引入了新的日誌資料格式。在升級到 PAN-OS 10.0 的路徑上，當您升級至 PAN-OS 10.0 時，已有日誌資料自動移轉至新的格式。重新格式化過程中，日誌資料在 **ACC** 或 **Monitor**（監控器）頁籤中不可見。此外，重新格式化完成之前，新日誌資料不會被轉送至日誌收集器。在重新格式化時，新日誌被寫入防火牆系統磁碟，並在程序順利完成後，新日誌將被轉送至相應的日誌收集器。

您必須同時在收集器群組內升級所有日誌收集器，以避免丟失日誌資料。如果收集器群組內的日誌收集器並非執行相同的 PAN-OS 版本，則無法進行日誌轉送或日誌收集。此外，除非所有日誌收集器執行相同的 PAN-OS 版本，否則收集器群組內的日誌收集器日誌資料在 **ACC** 或 **Monitor**（監控器）頁籤內不可見。例如，如果您在收集器群組內有三個日誌收集器，且您升級了其中兩個，則不會有日誌被轉送至收集器群組內的任何日誌收集器。

更新 Panorama 之前，請參閱版本資訊，瞭解 PAN-OS 10.0 所需的最低內容發行版本。

對於 Azure 上的 Panorama，在您可以成功升級軟體版本之前，必須執行額外的步驟。若要升級，您需要匯出 Panorama 組態，升級內容和軟體版本，並在升級成功後匯入設定至 Panorama 管理伺服器。

© 2019 Palo Alto Networks, Inc.

STEP 1 | 確認您計劃安裝的更新適合您的 Panorama 部署。

- ❑ 請參閱版本資訊，瞭解 Panorama 軟體版本所需的最低內容發行版本。如果您要升級日誌收集器和防火牆至特定版本，必須先將 Panorama 升級至該版本（或更新版本）。
- ❑ 對於 Hypervisor 上執行的 Panorama 虛擬設備，確保實例符合 設定 Panorama 虛擬設備的先決條件。

STEP 2 | 儲存目前 Panorama 組態檔案的備份，如果升級發生問題，此檔案可用來還原設定。



雖然 *Panorama* 會自動建立設定的備份，但最好在升級前建立備份並儲存在外部。

1. **Save named Panorama configuration snapshot**（儲存具名 **Panorama** 組態快照）（**Panorama** > **Setup**（設定）> **Operations**（操作）），輸入設定的 **Name**（名稱），然後按一下 **OK**（確定）。
2. **Export named Panorama configuration snapshot**（匯出具名 **Panorama** 組態快照），選取您剛儲存的設定 **Name**（名稱），按一下 **OK**（確定），並將匯出的檔案儲存至 Panorama 外部的位置。

STEP 3 | （依需要）安裝內容更新。



如果 *Panorama* 執行的內容版本，不是您要升級到的 *Panorama* 版本所需的最低內容版本，您必須先將內容版本更新至最低（或更新）版本，然後才安裝軟體更新。請參閱版本資訊，瞭解 *Panorama* 版本的最低內容發行版本。



Palo Alto Networks® 高度建議 *Panorama*、日誌收集器和所有受管理的防火牆執行相同的內容發行版本。此外，建議您排定自動的週期性更新，以一律執行最新內容版本（請參考 9）。

1. **Check Now**（立即檢查）（**Panorama** > **Dynamic Updates**（動態更新））有無最新更新。如果在 Action（動作）欄中的值為 **Download**（下載），則表示可進行該項更新。

   請確定 *Panorama* 執行的內容發行版本，與受管理的防火牆和日誌收集器相同，但並不是更新的版本。
2. （依需要）在 Panorama 上更新內容發行版本之前，務必升級受管理的防火牆和日誌收集器（請參閱當 Panorama 連線至網際網路時升級日誌收集器）至相同（或更新）的內容發行版本。

   如果您此時不需要安裝內容更新，請直接跳至下個步驟。
3. 依需要安裝其餘的內容更新。安裝後，Currently Installed（目前已安裝）欄會顯示核取標記。
   1. **Download**（下載）並 **Install**（安裝）應用程式和威脅更新。無論您的訂閱如何，Panorama 都只安裝和需要應用程式內容更新，而不是威脅內容。請參閱 Panorama、日誌收集器、防火牆和 WildFire 版本相容性。
   2. 依需要、一次一個、以任意順序 **Download**（下載）並 **Install**（安裝）其他更新（防毒、WildFire® 或 URL 篩選）。

STEP 4 | 決定升級到 PAN-OS 10.0 的路徑。

您無法略過路徑中任何功能發佈版本的安裝，從目前執行的 PAN-OS 版本到 PAN-OS 10.0 版本皆是如此。針對您在升級路徑中會經過的每個版本，檢閱版本資訊中的已知問題和預設行為變更，以及新功能指南中的升級/降級注意事項。

（如果您從 7.1 或更舊版本升級，則必須）PAN-OS 8.0 引用新的日誌儲存格式。升級至 PAN-OS 8.0 後，您必須在繼續升級路徑之前，將 Panorama 日誌移轉至新日誌格式。日誌移轉為一次性工作；如果您已在升級至 PAN-OS 8.0 時移轉了日誌收集器上的日誌，則不需要再移轉一次。

© 2019 Palo Alto Networks, Inc.

如果是升級多個日誌收集器，在您開始下載映之前，請決定您想升級的所有日誌收集器的升級路徑，讓過程順暢進行。

STEP 5 | 安裝 Panorama 10.0。

1. **Check Now**（立即檢查）（**Panorama** > **Software**（軟體））有無最新版本。如果有可用的軟體版本，Action（動作）欄會顯示 **Download**（下載）。
2. 根據您要升級到的發行版本，尋找並 **Download**（下載）適合的型號特定檔案。例如，若要將 M-Series 設備升級至 Panorama 10.0.0，請下載 `Panorama_m-10.0.0` 映像；若要將 Panorama 虛擬設備升級至 Panorama 10.0.0，請下載 `Panorama_pc-10.0.0` 映像。成功下載之後，已下載的映像的 Action（動作）欄會從 **Download**（下載）變更為 **Install**（安裝）。
3. （您無法略過路徑中任何功能發佈版本的安裝，從目前執行的 PAN-OS 版本到 PAN-OS 10.0.0 版本皆是如此。）安裝下載映像並重新啟動。
   1. 安裝映像。
   2. 安裝成功完成後，使用下列其中一種方法重新啟動：
      - 如果提示重新啟動，請按一下 **Yes**（是）。如果您看到 CMS Login（CMS 登入）提示，請按下 Enter，無須鍵入使用者名稱或密碼。當 Panorama 登入提示出現時，請輸入您在初始設定期間指定的使用者名稱與密碼。
      - 如果未提示您重新啟動，請從 Device Operations（裝置操作）部分 **Reboot Panorama**（重新啟動 **Panorama**）（**Panorama** > **Setup**（設定）> **Operations**（操作））。
4. （只有在升級至 PAN-OS 9.1.1 或更新版本時需要）針對 PAN-OS 10.0 基本映像完成上述步驟之後，請重複步驟 1 至 3，以升級至目標維護版本。

STEP 6 | 成功升級至 PAN-OS 10.0 後，檢查日誌格式移轉的狀態。

1. 登入 Panorama CLI 日誌收集器。
2. 執行下列命令，檢查日誌格式轉移的狀態：

```
admin> debug logdb show-es-upgrade-time
```

當日誌格式轉移仍在進行中的回應示例：

```
Response
from logger 23456212: 50.98% of indices upgraded complete. Approximately
less than a minute remaining until migration is complete. Once the
log migration is complete, please run the 'show log-collector-es-cluster
health' command to check the ElasticSearch cluster status to verify
logging and reporting functionality is restored.
```

當日誌格式轉移完成時的回應：

```
Response
from logger 23456212: 100% of indices complete. Please run the 'show
log-collector-es-cluster health' command to check the ElasticSearch
cluster status to verify logging and reporting functionality is
restored.
```

3. 日誌格式轉移完成後，在繼續下一步之前，請執行下列命令以檢查 ElasticSearch 叢集的狀態：

```
admin> show log-collector-es-cluster health
```


© 2019 Palo Alto Networks, Inc.

當 ElasticSearch 叢集健康「狀態」顯示「綠色」時，繼續下一步驟：

```
admin@Panorama(primary-active)> show log-collector-es-cluster health

{
  "cluster_name" : "__pan_cluster__",
  "status" : "green",
  "timed_out" : false,
  "number_of_nodes" : 2,
  "number_of_data_nodes" : 2,
  "active_primary_shards" : 21,
  "active_shards" : 26,
  "relocating_shards" : 0,
  "initializing_shards" : 0,
  "unassigned_shards" : 0,
  "delayed_unassigned_shards" : 0,
  "number_of_pending_tasks" : 0,
  "number_of_in_flight_fetch" : 0,
  "task_max_waiting_in_queue_millis" : 0,
  "active_shards_percent_as_number" : 100.0
}
```

STEP 7 | （僅對 Azure 上的 Panorama）載入步驟 2 中匯出的 Panorama 組態。

1. **Import named Panorama configuration snapshot**（匯入具名 **Panorama** 組態快照）（**Panorama** > **Setup**（設定）> **Operations**（作業））**Browse**（瀏覽）並選取 Panorama 組態檔案，然後按一下 **OK**（確定）。
2. **Load named Panorama configuration snapshot**（載入具名 **Panorama** 組態快照），選取您剛匯入的設定 **Name**（名稱），如有需要則輸入 **Decryption Key**（解密金鑰），然後按一下 **OK**（確定）。
3. 登入 Panorama CLI。
4. 輸入下列命令提交 Panorama 組態：

```
admin> configure
```

```
admin> commit force
```

STEP 8 | （如果本機日誌收集器位於收集器群組內）在收集器群組內升級剩餘日誌收集器。

- 當 Panorama 連線至網際網路時升級日誌收集器
- 當 Panorama 未連線至網際網路時升級日誌收集器

STEP 9 | （最佳作法）排程自動週期性內容更新。

Panorama 不會在 *HA* 端點之間同步內容更新排程。您必須在主動和被動 *Panorama* 上執行此工作。

在每種更新類型的標題列中（**Panorama** > **Dynamic Updates**（動態更新））**Schedule**（排程）最初設定為 **None**（無）。針對每種更新類型執行下列步驟。

1. 按一下 **None**（無），然後選取更新頻率（**Recurrence**（週期性））。頻率選項取決於更新類型。
2. 選取排程動作：
   - **Download And Install**（下載並安裝）（最佳作法）—Panorama 下載更新後會自動安裝更新。
   - **Download Only**（僅下載）—您必須在 Panorama 下載完成後手動安裝更新。
3. 根據組織的安全性狀態的最佳作法，設定有可用的更新之後到 Panorama 下載更新之前的延遲（**Threshold**（閾值））。
4. 按一下 **OK**（確定）儲存您的變更。
5. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

© 2019 Palo Alto Networks, Inc.

為沒有連線至網際網路的 Panorama 安裝更新

如果 Panorama™ 未直接與網際網路連線，請依需要，執行下列步驟來安裝 Panorama 軟體和內容更新。如果 Panorama 部署在高可用性 (HA) 設定中，您必須升級每個對等（請參閱在 HA 組態中為 Panorama 安裝更新）。

在 Panorama 虛擬設備上升級軟體不會變更系統模式；切換至 Panorama 模式或僅管理模式是手動工作，需要額外的設定，如設定具備本機日誌收集器的 Panorama 虛擬設備所述。

PAN-OS® 9.0 為本機和專用日誌收集器引入了新的日誌資料格式。在升級到 PAN-OS 10.0 的路徑上，當您升級至 PAN-OS 10.0 時，已有日誌資料自動移轉至新的格式。重新格式化過程中，日誌資料在 **ACC** 或 **Monitor**（監控器）頁籤中不可見。此外，重新格式化完成之前，新日誌資料不會被轉送至日誌收集器。在重新格式化時，新日誌被寫入防火牆系統磁碟，並在程序順利完成後，新日誌將被轉送至相應的日誌收集器。

您必須同時在收集器群組內升級所有日誌收集器，以避免丟失日誌資料。如果收集器群組內的日誌收集器並非執行相同的 PAN-OS 版本，則無法進行日誌轉送或日誌收集。此外，除非所有日誌收集器執行相同的 PAN-OS 版本，否則收集器群組內的日誌收集器日誌資料在 **ACC** 或 **Monitor**（監控器）頁籤內不可見。例如，如果您在收集器群組內有三個日誌收集器，且您升級了其中兩個，則不會有日誌被轉送至收集器群組內的任何日誌收集器。

升級 Panorama 之前，請參閱版本資訊，瞭解 PAN-OS® 10.0 所需的最低內容發行版本。

對於 Azure 上的 Panorama，在您可以成功升級軟體版本之前，必須執行額外的步驟。若要升級，您需要匯出 Panorama 組態，升級內容和軟體版本，並在升級成功後匯入設定至 Panorama 管理伺服器。

STEP 1 | 確認您計劃安裝的更新適合您的 Panorama 部署。

- ☐ 參考版本資訊，瞭解您必須為 Panorama 軟體版本安裝的最低內容版本。如果您要升級日誌收集器和防火牆至特定版本，必須先將 Panorama 升級至該版本（或更新版本）。
- ☐ 對於 Panorama 虛擬設備，確保實例符合 設定 Panorama 虛擬設備的先決條件 。

STEP 2 | 儲存目前 Panorama 組態檔案的備份，如果升級發生問題，此檔案可用來還原設定。

雖然 *Panorama* 會自動建立設定的備份，但最好在升級前建立備份並儲存在外部。

1. **Save named Panorama configuration snapshot**（儲存具名 **Panorama** 組態快照）（**Panorama** > **Setup**（設定）> **Operations**（操作）），輸入設定的 **Name**（名稱），然後按一下 **OK**（確定）。
2. **Export named Panorama configuration snapshot**（匯出具名 **Panorama** 組態快照），選取您剛儲存的設定 **Name**（名稱），按一下 **OK**（確定），並將匯出的檔案儲存至 Panorama 外部的位置。

STEP 3 | 決定您需要安裝的內容更新。

Palo Alto Networks 高度建議 *Panorama*、日誌收集器和所有受管理的防火牆執行相同的內容發行版本。

1. 針對每個內容更新，決定是否需要更新，以及您需要下載下列步驟中的哪些內容更新。

   請確定 *Panorama* 執行的內容發行版本，與受管理的防火牆和日誌收集器相同，但並不是更新的版本。

2. （依需要）在 Panorama 上更新內容發行版本之前，務必升級受管理的防火牆和日誌收集器（請參閱當 Panorama 連線至網際網路時升級日誌收集器）至相同（或更新）的內容發行版本。

STEP 4 | 決定升級到 PAN-OS 10.0 的路徑。

© 2019 Palo Alto Networks, Inc.

您無法略過路徑中任何功能發佈版本的安裝，從目前執行的 PAN-OS 版本到 PAN-OS 10.0 版本皆是如此。針對您在升級路徑中會經過的每個版本，檢閱版本資訊中的已知問題和預設行為變更，以及新功能指南中的升級/降級注意事項。

（ 如果您從 7.1 或更舊版本升級，則必須 ）PAN-OS 8.0 引用新的日誌儲存格式。升級至 PAN-OS 8.0 後，您必須在繼續升級路徑之前，將 Panorama 日誌移轉至新日誌格式。日誌移轉為一次性工作；如果您已在升級至 PAN-OS 8.0 時移轉了日誌收集器上的日誌，則不需要再移轉一次。



如果是升級多個日誌收集器，在您開始下載映之前，請決定您想升級的所有日誌收集器的升級路徑，讓過程順暢進行。

STEP 5 | （ 依需要 ）將內容更新下載到可透過 SCP 或 HTTPS 連線至 Panorama 來上傳內容的主機。

如果您此時不需要安裝內容更新，請直接跳至步驟 6。

1. 使用可存取網際網路的主機登入 Palo Alto Networks 客戶支援網站。
2. 依需要下載內容更新：
   1. 在 Resources（資源）區段按一下 **Updates**（更新）> **Dynamic Updates**（動態更新）。
   2. **Download**（下載）適當的內容更新，然後將檔案儲存至主機。針對您需要更新的各內容類型執行此步驟。

STEP 6 | 依需要安裝內容更新。



您必須在軟體升級前安裝內容升級，且必須在 *Panaroma* 管理伺服器安裝防火牆和日誌收集器前，先升級防火牆後，再升級日誌收集器。

先安裝「應用程式」或「應用程式和威脅」更新，再一次一個、以任意順序安裝其他任何更新（防毒、WildFire® 和 URL 篩選）。



無論您的訂閱是否同時包含應用程式和威脅內容，*Panorama* 都只需要並且只會安裝應用程式內容。請參閱 Panorama、日誌收集器、防火牆和 WildFire 版本相容性。

在 Panorama 中（**Panorama** > **Dynamic Updates**（動態更新））， 針對各內容類型執行下列步驟：

1. 按一下 **Upload**（上傳），選取內容 **Type**（類型），**Browse**（瀏覽）至您已將更新下載至主機上的那個位置，選取更新，然後按一下 **OK**（確定）。
2. **Install From File**（從檔案安裝），選取 **Package Type**（套件類型），並按一下 **OK**（確定）。

STEP 7 | 將軟體更新下載到可透過 SCP 或 HTTPS 連線至 Panorama 來上傳內容的主機。

1. 使用可存取網際網路的主機登入 Palo Alto Networks 客戶支援網站。
2. 下載軟體更新：
   1. 在 Palo Alto Networks 客戶支援網站的主頁面，按一下 **Updates**（更新）> **Software Updates**（軟體更新）。
   2. 針對升級路徑中的第一個（或下一個）Panorama 版本，找出型號特定檔案。例如，若要將 M-Series 設備升級至 Panorama 10.0.0，請下載 `Panorama_m-10.0.0` 映像；若要將 Panorama 虛擬設備升級至 Panorama 10.0.0，請下載 `Panorama_pc-10.0.0` 映像。

      您可以從 *Filter By*（篩選依據）下拉式清單中，選取 *Panorama M Images*（*Panorama M* 映像）（*M-Series* 設備）或 *Panorama Updates*（*Panorama* 更新）（虛擬設備），快速找到 *Panorama* 映像。
   3. 按一下檔名，並將檔案儲存至主機。
   4. 針對步驟 4 中決定升級路徑中的其他任何發行版本，重複步驟 2。

© 2019 Palo Alto Networks, Inc.

STEP 8 | 安裝 Panorama 10.0。

針對升級路徑中的每個版本（從最舊版本開始），執行下列步驟：

1. 按一下 Upload（上傳）（**Panorama** > **Software**（軟體））。
2. **Browse**（瀏覽）至您已將更新下載至主機上的那個位置，如果 Panorama 在 HA 設定中，請選取 **Sync To Peer**（同步至對等）核取方塊（將軟體映像推送至次要對等），然後按一下 **OK**（確定）。
3. 安裝軟體映像並重新啟動。

   若為 HA 設定，請在 HA 組態中為 Panorama 安裝更新；否則：

   1. 安裝已下載的映像。
   2. 成功完成安裝後，使用下列其中一種方法重新啟動：
      - 如果提示重新啟動，請按一下 **Yes**（是）。如果您看到 CMS Login（CMS 登入）提示，請按下 Enter，無須鍵入使用者名稱或密碼。當 Panorama 登入提示出現時，請輸入您在初始設定期間指定的使用者名稱與密碼。
      - 如果未提示您重新啟動，請從 Device Operations（裝置操作）部分 **Reboot Panorama**（重新啟動 **Panorama**）（**Panorama** > **Setup**（設定）> **Operations**（操作））。
4. 針對路徑中的每個版本，根據需要重複子步驟 1 至 3。

STEP 9 | 成功升級至 PAN-OS 10.0 後，檢查日誌格式移轉的狀態。

1. 登入 Panorama CLI 日誌收集器。
2. 執行下列命令，檢查日誌格式轉移的狀態：

```
admin> debug logdb show-es-upgrade-time
```

當日誌格式轉移仍在進行中的回應示例：

```
Response from logger 23456212: 50.98% of indices upgraded complete.
 Approximately less than a minute remaining until migration is complete.
 Once the log migration is complete, please run the 'show log-collector-
es-cluster health' command to check the ElasticSearch cluster status to
 verify logging and reporting functionality is restored.
```

當日誌格式轉移完成時的回應：

```
Response from logger 23456212: 100% of indices complete. Please
 run the 'show log-collector-es-cluster health' command to check
 the ElasticSearch cluster status to verify logging and reporting
 functionality is restored.
```

3. 日誌格式轉移完成後，在繼續下一步之前，請執行下列命令以檢查 ElasticSearch 叢集的狀態：

```
admin> show log-collector-es-cluster health
```

當 ElasticSearch 叢集健康 「狀態」 顯示 「綠色」 時，繼續下一步驟：

© 2019 Palo Alto Networks, Inc.

```
admin@Panorama(primary-active)> show log-collector-es-cluster health

{
  "cluster_name" : "__pan_cluster__",
  "status" : "green",
  "timed_out" : false,
  "number_of_nodes" : 2,
  "number_of_data_nodes" : 2,
  "active_primary_shards" : 21,
  "active_shards" : 26,
  "relocating_shards" : 0,
  "initializing_shards" : 0,
  "unassigned_shards" : 0,
  "delayed_unassigned_shards" : 0,
  "number_of_pending_tasks" : 0,
  "number_of_in_flight_fetch" : 0,
  "task_max_waiting_in_queue_millis" : 0,
  "active_shards_percent_as_number" : 100.0
}
```

STEP 10 | （僅對 Azure 上的 Panorama）載入步驟 2 中匯出的 Panorama 組態。

1. **Import named Panorama configuration snapshot**（匯入具名 **Panorama** 組態快照）（**Panorama** > **Setup**（設定）> **Operations**（作業））**Browse**（瀏覽）並選取 Panorama 組態檔案，然後按一下 **OK**（確定）。
2. **Load named Panorama configuration snapshot**（載入具名 **Panorama** 組態快照），選取您剛匯入的設定 **Name**（名稱），如有需要則輸入 **Decryption Key**（解密金鑰），然後按一下 **OK**（確定）。
3. 登入 Panorama CLI。
4. 輸入下列命令提交 Panorama 組態：

```
admin> configure
```

```
admin> commit force
```

STEP 11 | （如果本機日誌收集器位於收集器群組內）在收集器群組內升級剩餘日誌收集器。

- 當 Panorama 連線至網際網路時升級日誌收集器
- 當 Panorama 未連線至網際網路時升級日誌收集器

為沒有網際網路連線的 Panorama 自動安裝更新

自動下載動態更新到氣隙網路中的防火牆、日誌收集器和 WildFire® 設備，在該網路中，Panorama™ 管理伺服器、受管理防火牆、日誌收集器和 WildFire 設備均未連線至網際網路。要實現這一點，您必須部署一個能夠存取網際網路的額外 Panorama 和一個 SCP 伺服器。在部署能夠存取網際網路的 Panorama 後，請設定連線網際網路的 Panorama 以自動下載動態更新到 SCP 伺服器。氣隙 Panorama 設定為根據動態更新排程從該 SCP 伺服器自動下載並安裝動態更新。當能夠存取網際網路的 Panorama 下載動態更新到 SCP 伺服器或當氣隙 Panorama 從 SCP 伺服器下載並安裝動態更新時，Panorama 會產生系統日誌。

僅支援從具有網際網路連線的 Panorama 到無網際網路連線的 Panorama 的以下動態更新排程：

在將動態更新檔案成功下載到 *SCP* 伺服器後，不要操縱或變更其名稱。*Panorama* 不能下載和安裝檔案名稱已修改的動態更新。此外，為成功完成自動動態更新，您必須確保 *SCP* 伺服器上有足夠的磁碟空間、準備開始下載時 *SCP* 伺服器正在執行，以及兩個 *Panorama* 均已開啟且不在重新啟動的過程中。

本範例顯示如何為應用程式和威脅動態更新設定自動內容更新。

STEP 1 | 部署 SCP 伺服器。

© 2019 Palo Alto Networks, Inc.

從連線到網際網路的 Panorama 下載受管理防火牆、日誌收集器和 WildFire 設備的動態更新。氣隙 Panorama 從 SCP 伺服器下載動態更新，然後將更新安裝在受管理防火牆、WildFire 設備和日誌收集器上。



為動態更新建立資料夾目錄時，最佳做法是為每種類型的動態更新各建一個資料夾。這是管理大量動態更新的負擔，減少了刪除不應從 *SCP* 伺服器刪除的動態更新的可能性。

STEP 2 | 部署連線到網際網路的 Panorama。

此 Panorama 與 Palo Alto Networks 更新伺服器進行通訊，並將動態更新下載到 SCP 伺服器。

1. 設定 Panorama 管理伺服器。
   - 設定 M-Series 設備
   - 設定 Panorama 虛擬設備
2. 執行初始 Panorama 設定。
   - 執行 M-Series 設備的初始設定
   - 執行 Panorama 虛擬設備的初始設定

STEP 3 | 部署沒有網際網路連線的 Panorama。

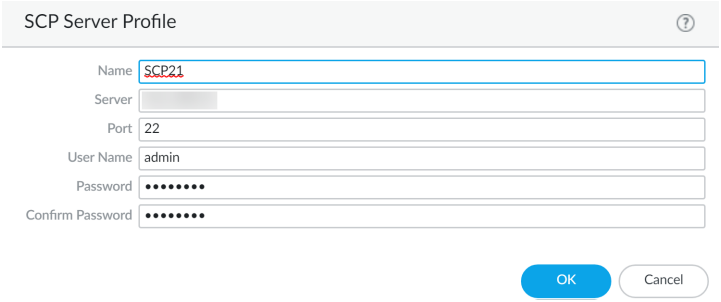
此 Panorama 與 SCP 伺服器進行通訊，以在受管理防火牆、日誌收集器和 WildFire 設備上下載並安裝動態更新。

1. 設定 Panorama 管理伺服器。
   - 設定 M-Series 設備
   - 設定 Panorama 虛擬設備
2. 執行初始 Panorama 設定。
   - 執行 M-Series 設備的初始設定
   - 執行 Panorama 虛擬設備的初始設定
3. 新增受管理防火牆、日誌收集器和 WildFire 設備。
   - 將防火牆新增為受管理的裝置
   - 設定受管理收集器
   - 新增獨立 WildFire 設備給 Panorama 管理

STEP 4 | 設定連線到網際網路的 Panorama 以下載動態更新到 SCP 伺服器。

1. 登入 Panorama 網頁介面。
2. 建立 SCP 伺服器設定檔。
   1. 選取 **Panorama** > **Server Profiles**（伺服器設定檔）> **SCP**，並 **Add**（新增）新的 SCP 伺服器設定檔。
   2. 輸入 SCP 伺服器設定檔的描述性 **Name**（名稱）。
   3. 輸入 SCP **Server**（伺服器）IP 位址。
   4. 輸入 **Port**（連接埠）。
   5. 輸入 SCP 伺服器 **User Name**（使用者名稱）。
   6. 輸入 SCP 伺服器 **Password**（密碼）與 **Confirm Password**（確認密碼）。
   7. 按一下 **OK**（確定）儲存您的變更。

© 2019 Palo Alto Networks, Inc.



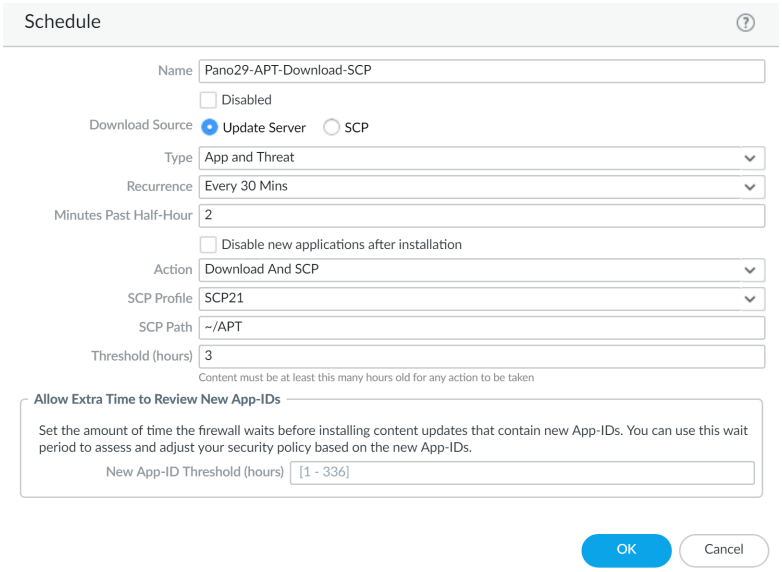
3. 建立動態更新排程，以定期將動態更新下載到 SCP 伺服器。

   您必須為打算自動下載並安裝在受管理防火牆、日誌收集器和 WildFire 設備上的每種類型的動態更新建立排程。

   1. 選取 **Panorama** > **Device Deployment**（裝置部署）> **Dynamic Updates**（動態更新），選取 **Schedules**（排程），然後 **Add**（新增）動態更新排程。
   2. 為動態更新排程輸入描述性 **Name**（名稱）。
   3. 對於 **Download Source**（下載來源），選取 **Update Server**（更新伺服器）。
   4. 選取動態更新 **Type**（類型）。
   5. 選取 **Recurrence**（週期性）設定 Panorama 在 Palo Alto Networks 更新伺服器上查看新動態更新的間隔。

      要設定更精確的週期性排程，請輸入所選週期性間隔之後的分鐘數。如果您排程使用相同的週期性間隔下載多個動態更新，請交錯安排以免 *Panorama* 和 *SCP* 伺服器過載。

   6. 對於 **Action**（動作），選取 **Download And SCP**（下載和 **SCP**）。
   7. 選取您在上一步中設定的 **SCP Profile**（**SCP** 設定檔）。
   8. 輸入動態更新類型的 **SCP Path**（**SCP** 路徑）。
   9. （選用）輸入動態更新的 **Threshold**（閾值）（以小時為單位）。Panorama 僅下載達到此存在小時數（或更久）的動態更新
   10. 按一下 **OK**（確定）儲存您的變更。

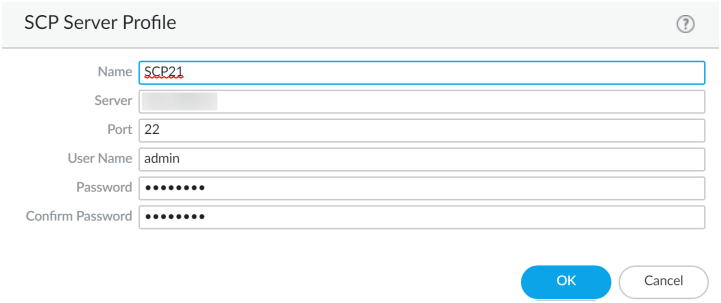


4. **Commit**（提交）您的變更。

© 2019 Palo Alto Networks, Inc.

STEP 5 | 設定氣隙 Panorama 從 SCP 伺服器下載動態更新，然後將更新安裝在受管理防火牆、日誌收集器和 WildFire 設備上。

1. 登入 Panorama 網頁介面。
2. 建立 SCP 伺服器設定檔。
   1. 選取 **Panorama** > **Server Profiles**（伺服器設定檔）> **SCP**，並 **Add**（新增）新的 SCP 伺服器設定檔。
   2. 輸入 SCP 伺服器設定檔的描述性 **Name**（名稱）。
   3. 輸入 SCP **Server**（伺服器）IP 位址。
   4. 輸入 **Port**（連接埠）。
   5. 輸入 SCP 伺服器 **User Name**（使用者名稱）。
   6. 輸入 SCP 伺服器 **Password**（密碼）與 **Confirm Password**（確認密碼）。
   7. 按一下 **OK**（確定）儲存您的變更。



3. 建立動態更新排程，以定期從 SCP 伺服器下載並安裝動態更新。

   您必須為打算自動下載並安裝在受管理防火牆、日誌收集器和 WildFire 設備上的每種類型的動態更新建立排程。

   1. 選取 **Panorama** > **Device Deployment**（裝置部署）> **Dynamic Updates**（動態更新），選取 **Schedules**（排程），然後 **Add**（新增）動態更新排程。
   2. 為動態更新排程輸入描述性 **Name**（名稱）。
   3. 對於 **Download Source**（下載來源），選取 **SCP**。
   4. 選取您在上一步中設定的 **SCP Profile**（**SCP** 設定檔）。
   5. 輸入動態更新類型的 **SCP Path**（**SCP** 路徑）。
   6. 選取動態更新 **Type**（類型）。
   7. 選取 **Recurrence**（週期性）設定 Panorama 在 Palo Alto Networks 更新伺服器上查看新動態更新的間隔。

      要設定更精確的週期性排程，請輸入所選週期性間隔之後的分鐘數。如果您排程使用相同的週期性間隔下載多個動態更新，請交錯安排以免 *Panorama* 和 *SCP* 伺服器過載。
   8. 對於 **Action**（動作），選取 **Download**（下載）或 **Download And Install**（下載並安裝）。

      當 *Download Source*（下載來源）為 *SCP* 時，僅支援 *Download*（下載）和*Download and Install*（下載並安裝）。

      如果您選取 *Download*（下載），則必須手動在受管理防火牆上開始進行動態更新安裝。
   9. 選取要安裝動態更新的 **Devices**（裝置）。
   10. （選用）輸入動態更新的 **Threshold**（閾值）（以小時為單位）。Panorama 僅下載達到此存在小時數（或更久）的動態更新
   11. 按一下 **OK**（確定）儲存您的變更。

© 2019 Palo Alto Networks, Inc.



4. **Commit**（提交）您的變更。

將 Panorama 日誌移轉為新的日誌格式

升級至 Panorama 8.0（或更新）版本之後，Panorama 日誌收集器會使用新的日誌儲存格式。因為 Panorama 在升級之後無法從 8.0 版以前日誌格式的日誌產生報告或 ACC 資料，當您將 Panorama 及其日誌收集器從 PAN-OS® 7.1 或更舊版本升級至 PAN-OS 8.0 或更新版本時，您必須盡快移轉現有的日誌，而且必須在升級受管理的防火牆之前這樣做。Panorama 在日誌移轉期間會繼續從受管理的裝置收集日誌，但在您升級至 PAN-OS 8.0 或更新版本之後，將會以新的日誌格式儲存傳入的日誌。因此，在 Panorama 完成日誌移轉程序之前，您在 ACC 和報告中只會看到局部資料。

將日誌移轉至新格式是一次性工作，必須在升級至 *PAN-OS 8.0* 或更新版本（或當您升級至 *PAN-OS 8.0* 作為升級路徑的一部分）時執行；在升級至更新的 *PAN-OS* 版本時不需要再一次執行此移轉。

Panorama 完成日誌移轉程序所需的時間，取決於寫入 Panorama 的新日誌數量，以及您要移轉的日誌資料庫大小。因為日誌移轉是很耗用 CPU 的程序，請在日誌記錄速率較低的期間才開始移轉。如果在尖峰期間發現 CPU 使用率很高，您一律可以停止移轉，等到傳入日誌速率較低時再繼續移轉。

在安裝 Panorama 內容和軟體更新 和升級日誌收集器之後，請如下移轉日誌：

- 檢視進入日誌記錄速率。

  最佳作法是在傳入日誌速率較低時開始日誌移轉。若要檢查速率，請從日誌收集器 CLI 執行下列命令：

```
admin@FC-M500-1> debug log-collector log-collection-stats show incoming-logs
```


© 2019 Palo Alto Networks, Inc.

在日誌移轉期間，*CPU* 使用率通常很高（接近 *100%*），操作會繼續正常運作。在資源競用的情況下，日誌移轉會調節以利於傳入日誌和其他程序。

- 開始將每個日誌收集器上的日誌移轉為新格式。

  若要開始移轉，請從每個日誌收集器的 CLI 輸入下列命令：

```
admin@FC-M500-1> request logdb migrate lc serial-number <ser_num> 開始
```

- 檢視日誌移轉狀態，以估計將所有現有日誌移轉為新格式所需的時間。

```
admin@FC-M500-1> request logdb migrate lc serial-number <ser_num> 狀態 Slot:
 all
Migration State: In Progress
Percent Complete: 0.04
Estimated Time Remaining: 451 hour(s) 47 min(s)
```

- 停止日誌移轉程序。

  若要暫時停止日誌移轉程序，請從日誌收集器 CLI 輸入下列命令：

```
admin@FC-M500-1 request logdb migrate lc serial-number <ser_num> 停止
```


© 2019 Palo Alto Networks, Inc.

轉移至不同的 Panorama 型號

當您的網路要求變更時（例如，日誌記錄速率增加），您可以轉移 Panorama 管理伺服器和專用日誌收集器至可以更好支援這些要求的 Panorama 型號。

- 從 Panorama 虛擬設備移轉至 M-Series 設備
- 將 Panorama 虛擬設備移轉至不同的 Hypervisor
- 從 M-Series 設備移轉至 Panorama 虛擬設備
- 從 M-100 設備移轉至 M-500 設備

從 Panorama 虛擬設備移轉至 M-Series 設備

在 Panorama 模式下，您可以從 Panorama 虛擬設備轉移 Panorama 組態至 M-Series 設備。但是，您無法轉移日誌因為 Panorama 虛擬設備上的日誌格式與 M-Series 設備上的不相容。由此，如果您想要保持對 Panorama 虛擬設備上儲存的舊日誌的存取，必須在轉移後繼續運行 Panorama 虛擬設備。M-Series 設備將收集轉移後防火牆轉送的新日誌。預先轉移日誌過期或由於老化變得不相關後，可以關閉 Panorama 虛擬設備。

Legacy Mode（傳統模式）在 PAN-OS 8.1 或更新版本中不再受支援。如果舊 Panorama 虛擬設備處於 Legacy Mode（傳統模式）下，您必須變更 Panorama 為 Panorama 模式，然後在轉移至新 Hypervisor，以保留日誌設置和日誌收集器轉送設定。在 Legacy Mode（傳統模式）中，將舊 Panorama 的設定匯入 Panorama 模式下的新 Panorama 中，會導致所有日誌和日誌轉送設置被移除。

您無法在 Hypervisor 之間轉移日誌。由此，如果您想要保持對 Panorama 虛擬設備上儲存的舊日誌的存取，必須在轉移後繼續運行舊 Panorama 虛擬設備，並將其作為受管理的日誌收集器新增至新 Panorama 虛擬設備上。這允許新 Panorama 虛擬設備收集轉移之後防火牆轉送的新日誌，同時保留對舊日誌資料的存取。預先轉移日誌過期或由於老化變得不相關後，可以關閉 Panorama 虛擬設備。



如果您將防火牆日誌儲存在專用日誌收集器（日誌收集器模式的 *M-Series* 設備），而非儲存在 *Panorama* 虛擬設備，您可以移轉專用日誌收集器至 *Panorama* 模式的 *M-Series* 設備，就能繼續存取日誌。

STEP 1 | 規劃轉移。

- 如果 M -Series 設備需要更新的軟體版本（M-500 設備需要 Panaroma 7.0 或更新版本。M-600 和 M-200 設備需要 Panorama 8.1 或更新版本），則在轉移之前，請先在 Panorama 虛擬設備上的更新軟體。如需瞭解軟體版本的重要詳細資訊，請參閱 Panorama、日誌收集器、防火牆和 WildFire 版本相容性。
- 為轉移排程維護時段。雖然防火牆可以在 Panorama 虛擬設備離線後緩衝日誌，並在 M-Series 設備上線後轉送日誌，但最好在維護時段完成轉移，以盡量避免日誌在 Panorama 型號之間轉移時超出緩衝容量並遺失。
- 考慮在移轉至存取現有日誌後是否保留對 Panorama 虛擬設備的存取權。最有效的方法是指派新 IP 位址至 Panorama 虛擬設備並將其舊 IP 位址供 M-Series 設備重複使用。這確保了 Panorama 虛擬設備仍保留存取權，且防火牆可以對應至 M-Series 設備而無需在各防火牆上重新設定 Panorama IP 位址。

STEP 2 | 購買新 M-Series 設備，轉移您的訂閱至新設備。

1. 購買新 M-Series 設備。
2. 購買新支援授權和轉移授權。
3. 在您購買新的 M-Series 虛擬設備時，向銷售代表提供您逐漸淘汰的 Panorama 虛擬設備序號和裝置管理驗證碼，以及您選擇的授權轉移日期。在收到您的 M-Series 設備後，透過 Palo Alto Networks 提供的轉移和支援驗證碼，註冊設備並啟動轉至管理和支援授權。在轉移時，Panorama 虛擬設備上的裝置管理授權被解除委任，您無法再透過 Panorama 虛擬設備管理裝置或收集日誌。但是，支援

© 2019 Palo Alto Networks, Inc.

授權將被保留，Panorama 設備仍受支援。您可以在生效日期之後完成轉移，但無法在已解除委任的 Panorama 虛擬設備上提交任何組態變更。

STEP 3 | （Legacy Mode（傳統模式））在舊 Panorama 虛擬設備上，變更至 Panorama 模式。

必須透過此步驟保留 *Panorama* 虛擬設備的日誌資料、設置和日誌轉送設定。如果您在 *Legacy Mode*（傳統模式）下匯出 *Panorama* 組態，這些設置將丟失。如果您在繼續前沒有變更 *Panorama* 至 *Panorama* 模式，您必須完成第 9 步。

如果 *Panorama* 虛擬設備已處於 *Panorama* 或 *Management Only*（僅管理模式），繼續下一步。

1. 在 Panorama 模式下設定 Panorama 虛擬設備。
2. 將 Panorama 日誌移轉為新的日誌格式 如果您想在舊 Panorama 虛擬設備上保留現有日誌資料。

STEP 4 | 從 Panorama 虛擬設備匯出 Panorama 組態。

1. 登入 Panorama 虛擬設備，然後選取 **Panorama** > **Setup**（設定）> **Operations**（操作）。
2. 按一下 **Save named Panorama configuration snapshot**（儲存具名 **Panorama** 組態快照），輸入 **Name**（名稱）以識別設定，然後按一下 **OK**（確定）。
3. 按一下 **Export named Panorama configuration snapshot**（匯出具名 **Panorama** 組態快照），選取您剛儲存的設定 **Name**（名稱），然後按一下 **OK**（確定）。Panorama 以 XML 檔案格式匯出設定至您的用戶端系統。

STEP 5 | 如果轉移後無需存取，可關閉 Panorama 虛擬設備，或如果您需要存取，可指派新 IP 位址至其管理 (MGT) 介面。

若要關閉 Panorama 虛擬設備的電源，請參閱 VMware 產品的文件。

若要變更在 Panorama 虛擬設備上的 IP 位址：

1. 選取 **Panorama** > **Setup**（設定）> **Management**（管理），然後編輯 [管理介面設定]。
2. 輸入新 **IP Address**（**IP** 位址），然後按一下 **OK**（確定）。
3. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

STEP 6 | 執行 M-Series 設備的初始設定。

1. 在機架中安裝 M-Series 設備。請參閱 M-Series 設備硬體參考指南的指示。
2. 執行 M-Series 設備的初始設定以定義啟動授權和安裝更新所需的網路連線。
3. 註冊 Panorama。
4. 啟動 Panorama 支援授權。
5. 在 M-Series 設備上啟動/擷取防火牆管理授權。使用轉移授權相關的授權碼。
6. 安裝 Panorama 的內容與軟體更新。安裝 Panorama 虛擬設備上所執行的相同版本。

STEP 7 | 將從 Panorama 虛擬設備匯出的 Panorama 組態快照載入 M-Series 設備。

1. 在 M-Series 設備上，選取 **Panorama** > **Setup**（設定）> **Operations**（操作）。
2. 按一下 **Import named Panorama configuration snapshot**（匯入具名 **Panorama** 組態快照），**Browse**（瀏覽）至您從 Panorama 虛擬設備匯出的 Panorama 組態檔案，並按一下 **OK**（確定）。
3. 按一下 **Load named Panorama configuration snapshot**（載入具名 **Panorama** 組態快照），選取您剛匯入的設定 **Name**（名稱），選取 **Decryption Key**（解密金鑰）（Panorama 主要金鑰），然後按一下 **OK**（確定）。Panorama 透過載入的設定覆寫其當前應徵者設定。Panorama 顯示載入設定檔時所發生的任何錯誤。
4. 如果發生錯誤，請將錯誤儲存至本機檔案。解決各錯誤，確保轉移設定有效。

© 2019 Palo Alto Networks, Inc.

STEP 8 | 修改 M-Series 設備上的設定。

如果 M-Series 設備會使用 Panorama 虛擬設備不同的值，則必須執行此步。如果您要保留對 Panorama 虛擬設備的存取權，以存取其日誌，為 M-Series 設備使用不同的主機名稱和 IP 位址。

1. 選取 **Panorama** > **Setup**（設定）> **Management**（管理）。
2. 編輯一般設定，修改 **Hostname**（主機名稱），然後按一下 **OK**（確定）。
3. 編輯管理介面設定，根據需要修改值，並按一下 **OK**（確定）。

STEP 9 | 新增預設受管理的收集器和收集器群組至 M-Series 設備。

從 Panorama 虛擬設備載入設定（第 7 步），將移除各 M-Series 設備上預定義的，預設受管理收集器和受管理群組。

1. 設定受管理收集器（M-Series 設備的本機收集器）
2. 為預設的受管理收集器設定收集器群組。
3. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後將您的變更 **Commit**（提交）至 Panorama 組態。

STEP 10 | 將 M-Series 設備與防火牆同步，以恢復防火牆管理。

請在維護時段內完成此步驟，將網路斷線的情況降到最低。

1. 在 M-Series 設備上，選取 **Panorama** > **Managed Devices**（受管理的裝置）並確認裝置狀態欄顯示防火牆 **Connected**（已連線）。

   此時，共用原則（裝置群組）和範本欄顯示防火牆 **Out of sync**（不同步）。
2. 將您的變更推送至裝置群組和範本：
   1. 選取 **Commit**（提交）> **Push to Devices**（推送至裝置）和 **Edit Selections**（編輯選擇）。
   2. 選取 **Device Groups**（裝置群組），選取每個裝置群組，以及 **Include Device and Network Templates**（包括裝置和網路範本），然後按一下 **OK**（確定）。
   3. **Push**（推送）您的變更。
3. 在 **Panorama** > **Managed Devices**（受管理的設備）頁面中，確認共用原則和範本欄顯示防火牆 **In sync**（同步）。

將 Panorama 虛擬設備移轉至不同的 Hypervisor

在 Management Only mode（僅管理模式）或 Panorama 模式下，從一個支援的 Hypervisor 轉移 Panorama 虛擬設備的 Panorama 設定至另一個支援的 Hypervisor。在轉移 Panorama 虛擬設備至新的 Hypervisor 之前，檢閱 Panorama 型號 以確保您轉移至的新 Hypervisor 受支援。此外，如果您的 Panorama 設定有多個裝置管理的介面設定，包括日誌收集、收集器群組通訊、授權和軟體更新，檢閱 設定 Panorama 虛擬設備的先決條件 以確認您轉移至的 Hypervisor 支援多個介面。

Legacy Mode（傳統模式）在 PAN-OS 8.1 或更新版本中不再受支援。如果舊 Panorama 虛擬設備處於 Legacy Mode（傳統模式）下，您必須變更 Panorama 為 Panorama 模式，然後在轉移至新 Hypervisor，以保留日誌設置和日誌收集器轉送設定。在 Legacy Mode（傳統模式）中，將舊 Panorama 的設定匯入 Panorama 模式下的新 Panorama 中，會導致所有日誌和日誌轉送設置被移除。

您不能從 Panorama 虛擬設備移轉日誌。因此，如果您想要繼續存取舊 Panorama 虛擬設備上儲存的日誌，則必須在轉移後以日誌收集器模式繼續執行舊 Panorama 虛擬設備，並將其作為受管理的日誌收集器新增至新 Panorama 虛擬設備。這允許新 Panorama 虛擬設備收集轉移之後防火牆轉送的新日誌，同時保留對舊日誌資料的存取。預先轉移日誌過期或由於老化變得不相關後，可以關閉 Panorama 虛擬設備。

© 2019 Palo Alto Networks, Inc.

如果您將防火牆日誌儲存在專用日誌收集器（日誌收集器模式的 *Panorama* 虛擬設備），而非儲存在 *Panorama* 虛擬設備，您可以 移轉專用日誌收集器 至 *Panorama* 模式的新 *Panorama* 虛擬設備，就能繼續存取日誌。

STEP 1 | 規劃轉移。

- 如果新 Panoprama 虛擬設備需要當前軟體的更新版本，轉移前，在 Panorama 虛擬設備上 升級軟體。AWS 和 Microsoft Azure 上的 Panorama 需要 8.1 或更新版本，Google Cloud Platform (GCP) 需要 8.1.1 或更新版本，KVM 和 AWS GovCloud 需要 8.1.2 或更新版本，Hyper-V 需要 8.1.3 或更新版本。關於軟體版本的重要詳細資料，請參閱 Panorama、日誌收集器、防火牆和 WildFire 版本相容性。
- 為轉移排程維護時段。雖然防火牆可以在 Panorama 虛擬設備離線後緩衝日誌，並在新 Panorama 虛擬設備上線後轉送日誌，但最好在維護時段完成轉移，以盡量避免日誌在 Hypervisor 之間轉移時超出緩衝容量並遺失。
- 考慮在移轉至存取現有日誌後是否保留對舊 Panorama 虛擬設備的存取權。最有效的方法是指派新 IP 位址至舊 Panorama 虛擬設備並將其舊 IP 位址供 Panorama 虛擬設備重複使用。這確保了舊 Panorama 虛擬設備仍保留存取權，且防火牆可以對應至新 Panorama 虛擬設備而無需在各防火牆上重新設定 Panorama IP 位址。

STEP 2 | 購買新 Panorama 虛擬設備授權，轉移您的訂閱至虛擬設備。

1. 購買新 Panorama 虛擬設備授權。
2. 購買新支援授權和轉移授權。
3. 在您購買新的 Panorama 虛擬設備授權時，向銷售代表提供您逐漸淘汰的 Panorama 虛擬設備序號和裝置管理驗證碼，以及您選擇的授權轉移日期。在部署新 Panorama 虛擬設備後，透過 Palo Alto Networks 提供的轉移和支援驗證碼，註冊設備並啟動轉至管理和支援授權。在轉移時，Panorama 虛擬設備上的裝置管理授權被解除委任，您無法再透過 Panorama 虛擬設備管理裝置或收集日誌。但是，支援授權將被保留，Panorama 設備仍受支援。您可以在生效日期之後完成轉移，但無法在已解除委任的 Panorama 虛擬設備上提交任何組態變更。

STEP 3 | （Legacy Mode（傳統模式））在舊 Panorama 虛擬設備上，變更至 Panorama 模式。

必須透過此步驟保留 *Panorama* 虛擬設備的日誌資料、設置和日誌轉送設定。如果您在 *Legacy Mode*（傳統模式）下匯出 *Panorama* 組態，這些設置將丟失。如果您在繼續前沒有變更 *Panorama* 至 *Panorama* 模式，您必須完成第 10 步。

如果 *Panorama* 虛擬設備已處於 *Panorama* 或 *Management Only*（僅管理模式），繼續下一步。

1. 在 Panorama 模式下設定 Panorama 虛擬設備。
2. 將 Panorama 日誌移轉為新的日誌格式 如果您想在舊 Panorama 虛擬設備上保留現有日誌資料。

STEP 4 | 從舊 Panorama 虛擬設備匯出 Panorama 組態。

1. 登入 Panorama 網頁介面。
2. 選取 **Panorama** > **Setup**（設定）> **Operations**（操作）。
3. 按一下 **Save named Panorama configuration snapshot**（儲存具名 **Panorama** 組態快照），輸入 **Name**（名稱）以識別設定，然後按一下 **OK**（確定）。
4. 按一下 **Export named Panorama configuration snapshot**（匯出具名 **Panorama** 組態快照），選取您剛儲存的設定 **Name**（名稱），然後按一下 **OK**（確定）。Panorama 以 XML 檔案格式匯出設定至您的用戶端系統。

STEP 5 | 如果轉移後無需存取，可關閉舊 Panorama 虛擬設備，或如果您需要存取，可指派新 IP 位址至其管理 (MGT) 介面。

要關閉 Panorama 虛擬設備，請參閱部署了舊 Panorama 虛擬設備的 Hypervisor 支援文檔。

© 2019 Palo Alto Networks, Inc.

若要變更在 Panorama 虛擬設備上的 IP 位址：

1. 在舊 Panorama 虛擬設備 Web 介面上，選取 **Panorama** > **Setup**（設定）> **Management**（管理），然後編輯 [管理介面設定]。
2. 輸入新 **IP Address**（IP 位址），然後按一下 **OK**（確定）。
3. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

STEP 6 | 執行新 Panorama 虛擬設備的初始組態。

1. 設定 Panorama 虛擬設備。
2. 執行 Panorama 虛擬設備的初始設定 定義啟動授權和安裝更新所需的網路連線。
3. 註冊 Panorama。
4. 啟動 Panorama 支援授權。
5. 在 Panorama 虛擬設備與網際網路連線時，啟動/擷取防火牆管理授權。使用轉移授權相關的授權碼。
6. 安裝 Panorama 的內容與軟體更新。安裝舊 Panorama 虛擬設備上所執行的相同版本。

STEP 7 | 將從舊 Panorama 虛擬設備匯出的 Panorama 組態快照載入新 Panorama 虛擬設備。

1. 登入 Panorama 網頁介面 新 Panorama 虛擬設備。
2. 選取 **Panorama** > **Setup**（設定）> **Operations**（操作）。
3. 按一下 **Import named Panorama configuration snapshot**（匯入具名 **Panorama** 組態快照），**Browse**（瀏覽）至您從 Panorama 虛擬設備匯出的 Panorama 組態檔案，並按一下 **OK**（確定）。
4. 按一下 **Load named Panorama configuration snapshot**（載入具名 **Panorama** 組態快照），選取您剛匯入的設定 **Name**（名稱），將 **Decryption Key**（解密金鑰）留空，然後按一下 **OK**（確定）。Panorama 透過載入的設定覆寫其當前應徵者設定。Panorama 顯示載入設定檔時所發生的任何錯誤。
5. 如果發生錯誤，請將錯誤儲存至本機檔案。解決各錯誤，確保轉移設定有效。

STEP 8 | 修改新 Panorama 虛擬設備上的設定。

如果新 Panorama 虛擬設備會使用舊 Panorama 虛擬設備不同的值，則必須執行此步。如果您要保留對舊 Panorama 虛擬設備的存取權，以存取其日誌，為新 Panorama 虛擬設備使用不同的主機名稱和 IP 位址。

AWS、*AWS GovCloud*、*Microsoft Azure* 和 *GCP* 上部署的 *Panorama* 不支援多介面設定。您必須重新設定裝置管理、日誌收集、收集器群組通訊、授權和軟體更新以操作 *MGT* 介面（當轉移至這些 *Hypervisor* 之一時）。

1. 選取 **Panorama** > **Setup**（設定）> **Management**（管理）。
2. 編輯一般設定，修改 **Hostname**（主機名稱），然後按一下 **OK**（確定）。
3. 編輯管理介面設定，根據需要修改值，並按一下 **OK**（確定）。

STEP 9 | 新增 預設受管理的收集器和收集器群組至新 Panorama 虛擬設備。

從舊 Panorama 虛擬設備載入設定（第 7 步），將移除 Panorama 模式下，各 Panorama 虛擬設備上預定義的，預設受管理收集器和受管理群組。

1. 設定受管理收集器（Panorama 虛擬設備的本機收集器）。
2. 為預設的受管理收集器設定收集器群組。
3. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後將您的變更 **Commit**（提交）至 Panorama 組態。

STEP 10 | （Legacy mode only（僅限傳統模式））如果在傳統模式下從 Panorama 虛擬設備匯出 Panorama 設定，設定日誌轉送至 Panorama。

© 2019 Palo Alto Networks, Inc.

STEP 11 | 將新 Panorama 虛擬設備與防火牆同步，以恢復防火牆管理。

請在維護時段內完成此步驟，將網路斷線的情況降到最低。

1. 在新 Panorama 虛擬設備上，選取 **Panorama** > **Managed Devices**（受管理的裝置），並確認裝置狀態欄顯示防火牆 **Connected**（已連線）。

   此時，共用原則（裝置群組）和範本欄顯示防火牆 **Out of sync**（不同步）。
2. 將您的變更推送至裝置群組和範本：
   1. 選取 **Commit**（提交）> **Push to Devices**（推送至裝置）和 **Edit Selections**（編輯選擇）。
   2. 選取 **Device Groups**（裝置群組），選取每個裝置群組，以及 **Include Device and Network Templates**（包括裝置和網路範本），然後按一下 **OK**（確定）。
   3. **Push**（推送）您的變更。
3. 在 **Panorama** > **Managed Devices**（受管理的設備）頁面中，確認共用原則和範本欄顯示防火牆 **In sync**（同步）。

從 M-Series 設備移轉至 Panorama 虛擬設備

您可以將 Panorama 組態從 M-100、M-200、M-500 或 M-600 設備移轉至 Panorama 模式的 Panorama 虛擬設備。但是，您無法轉移日誌，因為 M-Series 設備與 Panorama 虛擬設備上的日誌格式不相容。因此，如果想要繼續存取 M-Series 設備上儲存的舊日誌，您必須在移轉之後將 M-Series 設備繼續當作專用日誌收集器執行，並新增至 Panorama 虛擬設備成為管理的收集器。

如果您的 Panorama 管理伺服器為高可用性設定的一部分，則您必須部署相同管理程序或雲端環境的次要 Panorama 虛擬設備，並購買必要的裝置管理和支援授權。請參閱Panorama HA 先決條件以瞭解完整 HA 需求清單。

STEP 1 | 規劃轉移。

- 在移轉至 Panorama 虛擬設備之前，先將 M-Series 設備升級為 Panorama 10.0 或更新版本。若要升級 Panorama，請參閱安裝 Panorama 的內容與軟體更新。如需瞭解軟體版本的重要詳細資訊，請參閱 Panorama、日誌收集器、防火牆和 WildFire 版本相容性。
- 為轉移排程維護時段。雖然防火牆可以在 M-Series 設備離線後緩衝日誌，並在 Panorama 虛擬設備上線後轉送日誌，但最好在維護時段完成轉移，以盡量降低日誌在轉移至不同 Panorama 型號期間超出緩衝容量的風險。

STEP 2 | 為新的 Panorama 虛擬設備購買管理和支援授權。

1. 聯絡您的銷售代表以購買新的裝置管理和支援授權。
2. 將您計劃要逐步淘汰的 M-Series 設備的序號、您購買新的 Panorama 虛擬設備時收到的序號及支援驗證碼，以及從舊裝置移轉至新虛擬設備的預期完成日期，提供給您的銷售代表。在移轉日期之前，請在新虛擬設備上註冊序號，並啟動支援驗證碼，以便開始移轉。在您提供的預期移轉完成日期，會自動移除舊 M-Series 設備上的容量驗證碼。

STEP 3 | 執行 Panorama 虛擬設備的初始設定。

1. 設定 Panorama 虛擬設備。
2. 執行 Panorama 虛擬設備的初始設定，以定義啟動授權和安裝更新所需的網路連線。
3. 註冊 Panorama。
4. 啟動 Panorama 支援授權。
5. 在 Panorama 虛擬設備與網際網路連線時，啟動/擷取防火牆管理授權
6. 安裝 Panorama 的內容與軟體更新。安裝 M-Series 設備上所執行的相同版本。

STEP 4 | 編輯 M-Series 設備 Panorama 介面的設定為僅能使用管理介面。

© 2019 Palo Alto Networks, Inc.

Panorama 虛擬設備僅支援裝置管理和日誌收集用管理介面。

1. 登入 Panorama 網頁介面（M-Series 設備）。
2. 選取 **Panorama** > **Setup**（設定）> **Management**（管理）。
3. 編輯一般設定，修改 **Hostname**（主機名稱），然後按一下 **OK**（確定）。
4. 選取 **Interfaces**（介面）然後編輯 **Management**（管理）介面以啟用必要服務。
5. 停用剩餘介面服務。
6. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**）。

STEP 5 | 新增新 Panorama 虛擬設備的 IP 位址。

在 M-Series 設備上，將 Panorama 虛擬設備的公共 IP 位址新增為次要 Panorama 伺服器，以管理來自新 Panorama 管理伺服器的裝置。如果 Panorama 虛擬設備正部署在 AWS、Azure 或 Google™ Cloud Platform 上，則使用公共 IP 位址。

1. 選取 **Device**（裝置）> **Setup**（設定）。
2. 在範本內容下拉式清單中，選取包含 Panorama 伺服器設定的範本或範本堆疊。
3. 編輯 Panorama 設定。
4. 輸入 Panorama 虛擬設備公共 IP 位址,然後按一下 **OK**（確定）。
5. 選取 **Commit**（提交）> **Commit and Push**（提交並推送）。

STEP 6 | 從 M-Series 設備匯出設定。

1. 選取 **Panorama** > **Setup**（設定）> **Operations**（操作）。
2. 按一下 **Save named Panorama configuration snapshot**（儲存具名 **Panorama** 組態快照），輸入 **Name**（名稱）以識別設定，然後按一下 **OK**（確定）。
3. 按一下 **Export named Panorama configuration snapshot**（匯出具名 **Panorama** 組態快照），選取您剛儲存的設定 **Name**（名稱），然後按一下 **OK**（確定）。Panorama 以 XML 檔案格式匯出設定至您的用戶端系統。將設定儲存至 Panorama 設備外部的位置。

STEP 7 | 關閉 M-Series 設備電源或指派新 IP 位址給管理（MGT）介面。

若 *M-Series* 設備設定為 *Panorama* 模式且有日誌儲存在本機日誌收集器上，則您需要進入新的 *Panorama* 虛擬設備，變更 *M-Series* 設備上的 *IP* 位址，以將其新增至 *Panorama* 虛擬設備，作為受管理的日誌收集器使用。

- 關閉 **M-Series** 設備電源：

1. 登入 Panorama 網頁介面。
2. 選取 **Panorama** > **Setup**（設定）> **Operations**（操作），在 Device Operations（裝置操作）下，選取 **Shutdown Panorama**（關閉 **Panorama**）。按一下 **Yes**（是）以確認關機。

- 變更 **M-Series** 設備上的 **IP** 位址：

1. 登入 Panorama 網頁介面。
2. 選取 **Panorama** > **Setup**（設定）> **Management**（管理），然後編輯 [管理介面設定]。
3. 輸入新 **IP Address**（**IP** 位址），然後按一下 **OK**（確定）。
4. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

STEP 8 | 將您從 M-Series 設備匯出的 Panorama 組態快照載入 Panorama 虛擬設備。

1. 登入 Panorama 虛擬設備的 Panorama 網頁介面，然後選取 **Panorama** > **Setup**（設定）> **Operations**（操作）。
2. 按一下 **Import named Panorama configuration snapshot**（匯入具名 **Panorama** 組態快照），**Browse**（瀏覽）至您從 M-Series 設備匯出的 Panorama 組態檔案，然後按一下 **OK**（確定）。

© 2019 Palo Alto Networks, Inc.

3. 按一下 **Load named Panorama configuration snapshot**（載入具名 **Panorama** 組態快照），選取您剛匯入的設定 **Name**（名稱），選取 **Decryption Key**（解密金鑰）（Panorama 主要金鑰），然後按一下 **OK**（確定）。Panorama 透過載入的設定覆寫其當前應徵者設定。Panorama 顯示載入設定檔時所發生的任何錯誤。

如果發生錯誤，請將錯誤儲存至本機檔案。解決各錯誤，確保轉移設定有效。一旦提交成功就已載入設定。

STEP 9 | 將 M-Series 設備變更為日誌收集器模式以保留現在日誌資料。

如果您在日誌記錄磁碟仍舊插在 *M-Series* 設備內時變更為日誌收集器模式，則日誌記錄資料將被消除。日誌記錄磁碟必須在變更模式前先移除，以避免日誌資料遺失。

各磁碟配對產生中繼資料時均會重新建立索引。因此，此程序視資料大小而定，可能需要較長的時間完成。若要加速程序，您可以啟動多個 *CLI* 工作階段並在各工作階段中執行中繼資料重新產生的命令，為每個配對同時完成程序。詳細資訊，請參閱重新產生 M-Series 設備 RAID 配對的中繼資料。

1. 將 RAID 磁碟從舊 M-Series 設備中移除。
   1. 按下電源按鈕，直至系統關機，關閉 M-Series 設備。
   2. 移除磁碟配對。詳情請參閱 M-Series 設備硬體參考指南中的磁碟更換程序。
2. 按下電源按鈕，開啟 M-Series 設備。
3. 設定 `admin`（管理員）superuser administrator account（超級使用者管理員帳戶）。

   如果已建立 `admin`（管理員）管理員帳戶，請繼續下一步驟。

   切換至日誌收集器模式之前，必須先建立具有超級使用者權限的 *`admin`*（管理員）帳戶，否則切換模式之後，您就無法存取 *M-Series* 設備。
4. 登入 Panorama CLI（在舊 M-Series 設備上）。
5. 從 Panorama 模式切換至日誌收集器模式。
   - 輸入下列命令，切換至日誌收集器模式：

     ```
     > request system system-mode logger
     ```
   - 輸入 **`Y`** 以確認模式變更。M-Series 設備重新啟動。重新啟動會終止終端機模擬軟體的工作階段並重新連線至 M-Series 設備以顯示 Panorama 登入提示。

     如果您看到 ***`CMS Login`***（*CMS* 登入）提示，則表示日誌收集器未完成重新啟動。在提示框中按 *Enter*，而不輸入使用者名稱或密碼。
   - 重新登入 CLI。
   - 確認已成功切換至日誌收集器模式：

     ```
     > show system info | match system-mode
     ```

     如果模式變更成功，則輸出顯示為：

     ```
     > system-mode: logger
     ```
6. 將磁碟插回舊的 M-Series 設備。詳情請參閱 M-Series 設備硬體參考指南中的磁碟更換程序。

   您必須保留磁碟配對關聯。儘管您可以將A1/A2 槽的磁碟配對裝入 B1/B2 槽，您必須將磁碟放在相同的槽內；否則，Panorama 可能無法順利恢復資料。
7. 透過執行下列各配對的 CLI 命令，啟用磁碟配對：

© 2019 Palo Alto Networks, Inc.

```
> request system raid add <slot> force no-format
```

例如：

```
> request system raid add A1 force no-format
> request system raid add A2 force no-format
```

force 和**no-format** 引數是必要的。**force** 引數將磁碟配對與新設備關聯。**no-format** 引數可防止磁碟機的重新格式化，並保留磁碟上儲存的日誌。

8. 為每個磁碟配對產生中繼資料。

```
> request metadata-regenerate slot <slot_number>
```

例如：

```
> request metadata-regenerate slot 1
```

9. 啟用日誌收集器和 Panorama 管理伺服器之間的連線。

   在日誌收集器 CLI 上輸入以下命令，其中 *<IPaddress1>* 單獨（非 Ha）或主動 (HA) Panorama 的 MGT 介面，*<IPaddress2>* 是被動 (HA) Panorama 的 MGT 介面（如果適用）。

```
> configure
# set deviceconfig system panorama-server <IPaddress1> panorama-server-2
 <IPaddress2>
# commit
# exit
```

STEP 10 | 將 Panorama 虛擬設備與防火牆同步，以恢復防火牆管理。

請在維護時段內完成此步驟，將網路斷線的情況降到最低。

1. 在 Panorama 虛擬設備上，選取 **Panorama** > **Managed Devices**（受管理的裝置），並確認 裝置狀態欄顯示防火牆為 **Connected**（已連線）。

   此時，共用原則（裝置群組）和範本欄顯示防火牆 **Out of sync**（不同步）。
2. 將您的變更推送至裝置群組和範本：
   1. 選取 **Commit**（提交）> **Push to Devices**（推送至裝置）和 **Edit Selections**（編輯選擇）。
   2. 選取 **Device Groups**（裝置群組），選取每個裝置群組，以及 **Include Device and Network Templates**（包括裝置和網路範本）。
   3. 選取 **Collector Groups**（收集器群組），並選取每個收集器群組，然後按一下 **OK**（確定）。
   4. **Push**（推送）您的變更。
3. 在 **Panorama** > **Managed Devices**（受管理的設備）頁面中，確認共用原則和範本欄顯示防火牆 **In sync**（同步）。

STEP 11 | （僅限 HA）設定 Panorama HA 配對。

如果 Panorama 管理伺服器位在高可用性設定內，則請在 HA 配對上執行以下步驟。

1. 執行 Panorama 虛擬設備的初始設定。
2. 編輯 M-Series 設備 Panorama 介面的設定為僅能使用管理介面。

© 2019 Palo Alto Networks, Inc.

3. 新增新 Panorama 虛擬設備的 IP 位址。
4. 關閉 M-Series 設備電源或指派新 IP 位址給管理（MGT）介面。
5. 將 M-Series 設備變更為日誌收集器模式以保留現在日誌資料。

STEP 12 | （僅限 HA）修改 Panorama 虛擬設備 HA 配對設定。

1. 在 HA 配對上，登入至 Panorama 網頁介面，選取**Panorama** > **High Availability**（高可用性）然後編輯 **Setup**（設定）。
2. 在**Peer HA IP Address**（配對 **HA IP** 位址）欄位中，輸入指派給端點設備的 IP 位址，然後按一下 **OK**（確定）。
3. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更
4. 在 HA 配對的另一個端點上重覆這些步驟。

STEP 13 | （僅限 HA）將 Panorama 配對同步化。

1. 在一個 HA 配對上存取 **Dashboard**（儀表板），並選取 **Widgets** > **System**（系統）> **High Availability**（高可用性）來顯示 HA Widget。
2. **Sync to peer**（同步至對等），按一下 **Yes**（是），等待 **Running Config**（執行中設定）顯示 **Synchronized**（已同步）。
3. 存取剩餘 HA 配對上的 **Dashboard**（儀表板），並選取 **Widgets** > **System**（系統）> **High Availability**（高可用性）來顯示 HA Widget。
4. 確認 **Running Config**（執行中設定）顯示 **Synchronized**（已同步）。

從 M-100 設備移轉至 M-500 設備

您可以在 Panorama 模式中從 M-100 設備轉移 Panorama 組態和防火牆日誌至 M-500 設備（Panorama 管理伺服器）。您也可以在日誌收集器模式中從 M-100 設備轉移防火牆日誌至 M-500 設備（專用日誌收集器）。由於收集器群組內的所有日誌收集器必須為相同 Panorama 型號，收集器群組中的 M-100 設備必須全部移轉或都不移轉。

在下列程序中，Panorama 管理伺服器被部署在主動/被動高可用性 (HA) 設定中，您將轉移兩個設定和日誌，而 M-500 設備將重複使用來自 M-100 設備的 IP 位址。

此程序假定您不再使用 *M-100* 進行裝置管理或日誌收集。如果您計劃使用解除委任的 *M-100* 設備作為專用日誌收集器，則需要在 *M-100* 上準備裝置管理授權。如無裝置管理授權，您將無法使用 *M-100* 作為專用日誌收集器。

如果您不打算使用 *M-100* 裝置作為專用日誌收集器，但 *M-100* 設備包含您之後需要存取的日誌資料，您仍可以透過現有日誌資料查詢和產生報告。*Palo Alto Networks* 建議在對 *M-100* 設備解除委任之前，檢閱日誌保留原則。

如果您僅轉移日誌而不轉移 *Panorama* 組態，請執行移轉日誌至日誌收集器模式內的新 M-Series 設備或移轉日誌至 Panorama 模式內的新 M-Series 設備。

如果您要轉移至為採用 *HA* 設定部署的新 *Panorama* 管理伺服器，並且該新 *Panorama* 必須存取現有專用日誌收集器上的日誌，則請執行 非 HA Panorama 故障/ RMA 後轉移日誌收集器。

STEP 1 | 規劃轉移。

- 如果目前版本低於 7.0，在 M-100 設備上升級軟體；M-500 設備需要 Panorama 7.0 或更新的版本。如需瞭解軟體版本的重要詳細資訊，請參閱 Panorama、日誌收集器、防火牆和 WildFire 版本相容性。

© 2019 Palo Alto Networks, Inc.

- 將您想要保留 Panorama 和日誌收集器產生的日誌，在轉移前將系統和設定日誌轉送至外部目的地。Panorama 模式的 M-Series 設備會在其 SSD 上儲存這些日誌類型，此 SSD 無法在型號之間移動。您僅可以移動儲存防火牆日誌的 RAID 磁碟機。
- 為轉移排程維護時段。雖然防火牆可以在 M-100 設備離線後緩衝日誌，並在 M-500 設備上線後轉送日誌，但最好在維護時段完成轉移，以盡量避免日誌在 Panorama 型號之間轉移時超出緩衝容量並遺失。

STEP 2 | 購買新 M-500 設備，轉移您的訂閱至新設備。

1. 購買新 M-500 設備。
2. 購買新支援授權和轉移授權。
3. 在您購買新的 M-500 設備時，向銷售代表提供您逐漸淘汰的 M-100 虛擬設備序號和裝置管理驗證碼，以及您選擇的授權轉移日期。在收到您的 M-500 設備後，透過 Palo Alto Networks 提供的轉移和支援驗證碼，註冊設備並啟動轉至管理和支援授權。在轉移時，M-100 設備上的裝置管理授權被解除委任，您無法再透過 M-100 設備管理裝置或收集日誌。但是，支援授權將被保留，Panorama 設備仍受支援。您可以在生效日期之後完成轉移，但無法在已解除委任的 M-100 設備上提交任何組態變更。

STEP 3 | 從 Panorama 模式內的各 M-100 設備匯出 Panorama 組態。

在各 M-100 設備 HA 端點執行此工作：

1. 登入 M-100 設備，然後選取 **Panorama** > **Setup**（設定）> **Operations**（操作）。
2. 按一下 **Save named Panorama configuration snapshot**（儲存具名 **Panorama** 組態快照），輸入 **Name**（名稱）以識別設定，然後按一下 **OK**（確定）。
3. 按一下 **Export named Panorama configuration snapshot**（匯出具名 **Panorama** 組態快照），選取您剛儲存的設定 **Name**（名稱），然後按一下 **OK**（確定）。Panorama 以 XML 檔案格式匯出設定至您的用戶端系統。

STEP 4 | 關閉 Panorama 模式內的各 M-100 設備。

1. 登入您要關閉的 M-100 設備 HA 端點。
2. 選取 **Panorama** > **Setup**（設定）> **Operations**（操作），再按一下 **Shutdown Panorama**（關閉 **Panorama**）。

STEP 5 | 執行每個 M-500 設備的初始設定。

1. 在機架中安裝 M-500 設備。請參閱 M-500 設備硬體參考指南的指示。
2. 執行 M-Series 設備的初始設定以定義啟動授權和安裝更新所需的網路連線。
3. 註冊 Panorama。
4. 啟動 Panorama 支援授權。
5. 啟動防火牆管理授權。使用轉移授權相關的授權碼。
6. 安裝 Panorama 的內容與軟體更新。安裝 M-100 設備上所執行的相同版本。
7. （僅限專用日誌收集器）將 M-Series 設備設定為日誌收集器。

STEP 6 | 載入您在 Panorama 模式下從各 M-100 設備中匯出的 Panorama 組態快照至各 M-500 設備內（二者均為 HA 端點）。

在各 M-500 設備 HA 端點執行此工作：

1. 登入 M-500 設備，然後選取 **Panorama** > **Setup**（設定）> **Operations**（操作）。
2. 按一下 **Import named Panorama configuration snapshot**（匯入具名 **Panorama** 組態快照），**Browse**（瀏覽）從 M-100 設備匯出的設定檔，該設備與 M-500 設備的 HA 優先級（主要或次要）一致，然後按一下 **OK**（確定）。
3. 按一下 **Load named Panorama configuration snapshot**（載入具名 **Panorama** 組態快照），選取您剛匯入的設定 **Name**（名稱），選取 **Decryption Key**（解密金鑰）（Panorama 主要金鑰），然後按一

© 2019 Palo Alto Networks, Inc.

下 **OK**（確定）。Panorama 透過載入的設定覆寫其當前應徵者設定。Panorama 顯示載入設定檔時所發生的任何錯誤。如果發生錯誤，請將錯誤儲存至本機檔案。解決各錯誤，確保轉移設定有效。

4. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Validate Commit**（驗證提交）。繼續前解決任何錯誤。
5. **Commit**（提交）您對 Panorama 組態所做的變更。

STEP 7 | 在 Panorama 模式下同步 M-500 設備 HA 端點之間的設定。

1. 在主動 M-500 設備上，選取 **Dashboard**（儀表板）頁籤，並在高可用性 widget 中，按一下 **Sync to peer**（同步至端點）。
2. 在高可用性 widget 中，確認 **Local**（本機）（主要 M-500 設備）為 **active**（主動），**Peer**（端點）為被動，且 **Running Config**（運行設定）為 **synchronized**（已同步）。

STEP 8 | 從各 M-100 設備移動 RAID 磁碟機至其更換 M-500 設備，以轉移從防火牆收集的日誌。

在下列工作中，跳過您已在 M-500 設備上完成的任何步驟。

- 移轉日誌至 Panorama 模式內的新 M-Series 設備。轉移來自 M-100 設備的日誌，如果其為日誌收集使用預設受管理的收集器。
- 移轉日誌至日誌收集器模式內的新 M-Series 設備。

STEP 9 | 將 Panorama 模式內的主動 M-500 設備與防火牆同步，以恢復防火牆管理。



請在維護時段內完成此步驟，將網路斷線的情況降到最低。

1. 在主動 M-500 設備上，選取 **Panorama** > **Managed Devices**（受管理的裝置）並確認裝置狀態欄顯示防火牆 **Connected**（已連線）。

   此時，共用原則（裝置群組）和範本欄顯示防火牆 **Out of sync**（不同步）。
2. 將您的變更推送至裝置群組和範本：
   1. 選取 **Commit**（提交）> **Push to Devices**（推送至裝置）和 **Edit Selections**（編輯選擇）。
   2. 選取 **Device Groups**（裝置群組），選取每個裝置群組，以及 **Include Device and Network Templates**（包括裝置和網路範本），然後按一下 **OK**（確定）。
   3. **Push**（推送）您的變更。
3. 在 **Panorama** > **Managed Devices**（受管理的設備）頁面中，確認共用原則和範本欄顯示防火牆 **In sync**（同步）。

© 2019 Palo Alto Networks, Inc.

存取並導覽 Panorama 管理介面

Panorama 提供三個管理介面：

- **Web** 介面——Panorama網頁介面擁有與防火牆網頁介面相同的外觀及風格。如果您已熟悉後者，您可以從 Panorama網頁介面中，輕鬆地導覽和完成管理工作及產生報告。此圖形式介面可讓您使用 HTTPS 存取 Panorama，而且是執行管理工作的最佳方法。請參閱 登入 Panorama 網頁介面 和 導覽 Panorama 網頁介面。如果您必須允許經由 HTTP 存取 Panorama，請在 **Panorama** > **Setup**（設定）> **Management**（管理）頁籤上編輯 [管理介面設定]。
- 命令行介面 **(CLI)**—CLI 是一個未經修飾的介面，能讓您快速且連續地輸入命令以完成一連串工作。CLI 支援兩種命令模式（操作和設定），每一種模式都有它自己的命令和陳述式階層。當您熟悉命令的巢狀結構和語法時，CLI 即可加快回應時間並進行有效率的管理。請參閱登入 Panorama CLI。
- **XML API**—XML 式 API 是一種使用 HTTP/HTTPS 要求和回應所實作的 Web 服務。它能讓您順暢地操作，並整合內部開發的現有應用程式和儲存庫。如需關於使用 Panorama API 的詳細資訊，請參閱《PAN-OS 和 Panorama XML API 用法指南》。

登入 Panorama 網頁介面

STEP 1 | 啟動網際網路 瀏覽器，使用安全連線輸入 Panorama IP 位址 (https://<IP address>)。

STEP 2 | 根據帳戶所用的驗證類型，登入 Panorama。如果是首次登入 Panorama，使用者名稱和密碼都使用預設值 `admin`。

- **SAML**—按一下 **Use Single Sign-On**（使用單一登入）(SSO)。如果 Panorama 為管理員執行授權（角色指派），請輸入 **Username**（使用者名稱），然後 **Continue**（繼續）。如果由 SAML 識別提供者 (IdP) 執行授權，則 **Continue**（繼續）而不輸入 **Username**（使用者名稱）。在這兩種情況下，Panorama 會將您重新導向至 IdP，而提示您輸入使用者名稱和密碼。通過 IdP 的驗證後，將顯示 Panorama 網頁介面。
- 任何其他驗證類型—輸入使用者 **Name**（名稱）和 **Password**（密碼）。如果登入頁面上有橫幅和核取方塊，則閱讀登入橫幅並選取 **I Accept and Acknowledge the Statement Below**（我接受並確認下方陳述）。然後按一下 **Login**（登入）。

STEP 3 | 閱讀並 **Close**（關閉）當日訊息。

導覽 Panorama 網頁介面

使用 Panorama 網頁介面可設定 Panorama、管理和監控防火牆、日誌收集器及 WildFire 設備和設備叢集，以及透過 **Context**（內容）下拉清單來存取每個防火牆的網頁介面。關於各網頁介面頁籤中選項和欄位的詳細資訊，請參閱 Panorama 線上說明。以下是各頁籤的概覽：

頁籤	說明
儀錶盤	檢視 Panorama 型號與網路存取設定。此頁籤上包含的 Widget 會顯示應用程式、日誌、系統資源及系統設定等資訊。
ACC	根據 Panorama 自受管理防火牆所收集的資訊，顯示網路的整體風險和威脅層級。
監控	檢視與管理日誌和報告。

© 2019 Palo Alto Networks, Inc.

頁籤	說明
Device Groups（裝置群組）> **Policies**（政策）	建立集中式原則規則，並將其套用至多個防火牆/裝置群組。 您必須 新增裝置群組 才能顯示此頁籤。
Device Groups（裝置群組）> **Objects**（物件）	定義原則規則可參考，且受管理的防火牆/裝置群組可共用的原則物件。 您必須 新增裝置群組 才能顯示此頁籤。
Templates（範本）> **Network**（網路）	設定網路設定，例如網路設定檔，並將其套用至多個防火牆。 您必須 新增範本 才能顯示此頁籤。
Templates（範本）> **Device**（裝置）	設定裝置設定，例如伺服器設定檔和管理員角色，並將其套用至多個防火牆。 您必須 新增範本 才能顯示此頁籤。
Panorama	設定 Panorama、管理授權、設定高可用性、存取軟體更新和安全性警示、管理「管理存取權」，以及管理已部署的防火牆、日誌收集器及 WildFire 設備和設備叢集。

登入 Panorama CLI

您可以使用序列連接埠連線登入 Panorama CLI，或從遠端使用 Secure Shell (SSH) 用戶端。

- 使用 SSH 登入 Panorama CLI。

  相同的指示也適用於日誌收集器模式中的 M-Series 設備。

  或者，您可以 設定帶有基於 SSH 金鑰驗證的 CLI 管理員。

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

        ```
        admin@ABC_Sydney>
        ```

- 使用序列連接埠連線以登入 Panorama CLI。

  1. 確定您具備下列條件：
     - 一條 Null 資料機序列纜線，將 Panorama 連接到配備 DB-9 序列連接埠的電腦
     - 正在電腦上執行的終端機模擬程式

© 2019 Palo Alto Networks, Inc.

2. 在終端機模擬軟體中使用下列設定進行連線：9600 傳輸速率；8 資料位元；1 停止位元；無同位檢查；無硬體流量控制。
3. 出現提示時輸入您的管理存取認證。登入後，將顯示當日訊息，然後在操作模式中顯示 CLI 提示。

- **變更為設定模式。**

  若要切換至設定模式，請在提示上輸入下列命令：

  ```
  admin@ABC_Sydney> configure
  ```

  提示將變更為 `admin@ABC_Sydney#`。

© 2019 Palo Alto Networks, Inc.

設定對 Panorama 的管理存取權

Panorama 實行 以角色為基礎的存取控制 (RBAC) 以讓您可以指定存取權限和管理員責任。下列主題描述了如何建立管理員角色、存取網域和存取 Panorama 網頁介面和命令行介面 (CLI) 的帳戶：

- 設定管理員角色設定檔
- 設定存取網域
- 設定管理帳戶和驗證

設定管理員角色設定檔

管理員角色設定檔為自訂 管理角色，讓您可以定義精確的管理存取權限，以確保對敏感公司資訊和使用者隱私的保護。最佳作法是，建立管理員角色設定檔，允許管理員僅存取執行其工作所需的管理介面區域。

STEP 1 | 設定防火牆管理員角色設定檔。

您必須在防火牆上建立管理員角色設定檔，並將其指派到 Panorama 管理伺服器管理員角色設定檔，以允許管理員在 Panorama 和受管理防火牆 Web 介面之間進行內容切換。

STEP 2 | 選取 **Panorama** > **Admin Roles**（管理員角色），然後按一下 **Add**（新增）。

STEP 3 | 輸入設定檔的 **Name**（名稱），然後選取 **Role**（角色）類型：**Panorama** 或 **Device Group and Template**（裝置群組與範本）。

STEP 4 | 透過切換圖示至所需設定，設定對 Panorama (**Web UI**) 和防火牆 (**Context Switch UI**（內容切換 **UI**）) 各功能區域的存取權限：Enable (read-write)（啟用（讀取-寫入））、Read Only（唯讀）或 Disable（停用）。



如果帶有自訂角色的管理員將提交設備群組或範本變更至受管理的防火牆，您必須提供角色讀取-寫入存取至 *Panorama* > *Device Groups*（設備群組）和*Panorama* > *Templates*（範本）。如果您是從較早的 *Panorama* 版本升級，升級程序提供那些節點的唯讀存取。

您無法透過 Panorama 角色中的內容切換存取權限管理對防火牆 CLI 或 XML API 的存取。

STEP 5 | 如果 **Role**（角色）類型為 **Panorama**，透過切換各功能區域的啟用/停用圖示，設定對 **XML API** 的存取。

STEP 6 | 如果 **Role**（角色）類型為 **Panorama**，選取 **Command Line**（命令行）介面的存取等級：**None**（無）（預設）、**superuser**（超級使用者）、**superreader**（超級讀取者）或 **panorama-admin**（**panorama** 管理員）。

STEP 7 | 要啟用內容切換，請選取您在步驟 1 中建立的 **Device Admin Role**（裝置管理員角色）。

STEP 8 | 按一下 **OK**（確定）來儲存設定檔。

設定存取網域

使用 存取網域 定義特定裝置群組和範本的裝置群組和範本管理員存取，以及控制管理員切換內容至受管理防火牆網頁介面的能力。Panorama 支援最多 4,000 個存取網域。

STEP 1 | 選取**Panorama** > **Access Domain**（存取網域），然後按一下 **Add**（存取網域）。

© 2019 Palo Alto Networks, Inc.

STEP 2 | 輸入用來識別存取網域的 **Name**（名稱）。

STEP 3 | 選取 **Shared Objects**（共用物件）的存取權限：

- **write**（寫入）——管理員可以針對共用物件執行所有操作。這是預設值。
- **read**（讀取）——管理員可以顯示和複製共用物件，但無法針對這些物件執行任何其他操作。新增非共用物件或複製共用物件時，目的地必須是存取網域中的裝置群組，而非 Shared（共用）位置。
- **shared-only**（僅限共用）——管理員只可將物件新增至 Shared（共用）位置。管理員可以顯示、編輯和刪除共用物件，但無法移動或複製這些物件。

此選項的結果是除了顯示非共用物件以外，該管理員無法針對這些物件執行任何操作。選取此選項的原因是組織要求所有物件為單一，全域儲存庫。

STEP 4 | 切換 **Device Groups**（裝置群組）頁籤內的圖示，以啟用存取網域內裝置群組的讀取-寫入或唯讀存取。

如果您將 *Shared Objects*（共用物件）的存取權設定為 *shared-only*（僅限共用），*Panorama* 會將唯讀存取權套用至任何您指定讀取/寫入存取權的裝置群組內物件。

STEP 5 | 選取 **Templates**（範本）頁籤並 **Add**（新增）各個您想要指派至存取網域的範本。

STEP 6 | 選取 **Device Context**（裝置內容）頁籤，選取防火牆以指派至存取網域，並按一下 **OK**（確定）。管理員可以使用 Panorama 中的 **Context**（內容）下拉式清單存取這些防火牆的網頁介面。

設定管理帳戶和驗證

如果您已設定驗證設定檔，或不需要此設定檔來驗證管理員，則可以開始 設定 Panorama 管理員帳戶。否則，執行下列其他程序之一，以為特定驗證類型設定管理帳戶。

- 設定 Panorama 管理員帳戶
- 為 Panorama 管理員設定本機或外部驗證
- 設定 Panorama 管理員以基於憑證的驗證來存取網頁介面
- 設定帶有基於 SSH 金鑰驗證的 CLI 管理員
- 為 Panorama 管理員設定 RADIUS 驗證
- 為 Panorama 管理員設定 TACACS+ 驗證
- 為 Panorama 管理員設定 SAML 驗證

設定 *Panorama* 管理員帳戶

管理帳戶指定 Panorama 管理員的管理角色和驗證。您用於指派角色和執行驗證的服務，將決定您要在 Panorama、外部伺服器或這兩者上新增帳戶（請參閱管理驗證）。若為外部驗證服務，在新增管理帳戶之前，您必須先設定驗證設定檔（請參閱設定管理帳戶和驗證）。如果您已設定驗證設定檔，或您將使用 Panorama 本機的驗證機制，請執行以下步驟，在 Panorama 上新增管理帳戶。

您無法新增管理員帳戶至專用日誌收集器（日誌收集器模式中的 *M-Series* 設備）。專用日誌收集器上僅有預先定義的帶有預設使用者名稱 *(admin)* 的管理員帳戶可用。

STEP 1 | 選取 **Panorama** > **Administrators**（管理員），然後 **Add**（新增）帳戶。

STEP 2 | 輸入管理員的使用者 **Name**（名稱）。

STEP 3 | 如果您已為管理員設定任何一項，則選取 **Authentication Profile**（驗證設定檔）或順序。

© 2019 Palo Alto Networks, Inc.

如果 Panorama 將使用 Kerberos SSO 或外部服務進行驗證，則此為必要步驟。

如果 Panorama 要使用本機驗證，將 **Authentication Profile**（驗證設定檔）設為 **None**（無）並輸入 **Password**（密碼）然後 **Confirm Password**（確認密碼）。

STEP 4 | 選取 **Administrator Type**（管理員類型）：

- **Dynamic**（動態）——選取預先定義的管理員角色。
- **Custom Panorama Admin**（自訂 **Panorama** 管理員）—選取您為此管理員建立的管理員角色 **Profile**（設定檔）（請參閱設定管理員角色設定檔）。
- **Device Group and Template Admin**（裝置群組和範本管理員）—將存取網域對應至下一步所述的管理角色。

STEP 5 | （僅限裝置群組和範本管理員）在 Access Domain to Administrator Role（存取網域至管理員角色）部分中，按一下 **Add**（新增），從下拉式清單中選取存取網域（請參閱設定存取網域），按一下相鄰的 Admin Role（管理員角色）資料格，然後選取管理員角色設定檔。

STEP 6 | 按一下 **OK**（確定）儲存您的變更。

STEP 7 | 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

為 *Panorama* 管理員設定本機或外部驗證

您可以使用外部驗證服務或 Panorama 本機的服務，以驗證存取 Panorama 的管理員。這些驗證方法將提示管理員回應一個或多個驗證挑戰，例如輸入使用者名稱和密碼的登入頁面。



如果您使用外部服務來管理驗證和授權（角色和存取網域指派），請參閱：

- 為 Panorama 管理員設定 RADIUS 驗證
- 為 Panorama 管理員設定 TACACS+ 驗證
- 為 Panorama 管理員設定 SAML 驗證

若要在不使用挑戰回應機制的情況下驗證管理員，您可以設定 Panorama 管理員以基於憑證的驗證來存取網頁介面和設定管理員以基於 SSH 金鑰的驗證來存取 CLI。

STEP 1 | （僅限外部驗證）可讓 Panorama 連線至外部伺服器來驗證管理員。

1. 選取 **Panorama** > **Server Profiles**（伺服器設定檔），選取服務類型（**RADIUS**、**TACACS+**、**SAML**、**LDAP** 或 **Kerberos**），並設定伺服器設定檔：
   - 為 Panorama 管理員設定 RADIUS 驗證。

     您可以使用 *RADIUS* 伺服器以支援 *RADIUS* 驗證服務或多重要素驗證 (MFA) 服務。

   - 為 Panorama 管理員設定 TACACS+ 驗證。
   - 新增 SAML IdP 伺服器設定檔。無法組合使用 Kerberos 單一登入 (SSO) 和 SAML SSO；您只能使用一種類型的 SSO 服務。
   - 新增 Kerberos 伺服器設定檔。
   - 新增 LDAP 伺服器設定檔。

STEP 2 | (選用) 如果 Panorama 使用本機驗證，請定義密碼複雜度和到期設定。

這些設定讓攻擊者難以猜測密碼，有助於保護 Panorama 免受未經授權的存取。

© 2019 Palo Alto Networks, Inc.

1. 定義所有本機管理員的全域密碼複雜性及到期設定。
    1. 選取 **Panorama** > **Setup**（設定）> **Management**（管理），然後編輯 Minimum Password Complexity（最小密碼複雜度）設定。
    2. 選取 **Enabled**（已啟用）。
    3. 定義密碼設定，然後按一下 **OK**（確定）。
2. 定義 Password Profile（密碼設定檔）。

    將設定檔指派給您要覆寫全域密碼過期設定的管理員帳戶。

    1. 選取 **Panorama** > **Password Profiles**（密碼設定檔），然後 **Add**（新增）設定檔。
    2. 輸入用來識別設定檔的 **Name**（名稱）。
    3. 定義密碼到期設定，然後按一下 **OK**（確定）。

STEP 3 | （僅限 Kerberos SSO）建立 Kerberos 金鑰標籤。

Keytab 是一個檔案，包含 Panorama 的 Kerberos 帳戶資訊。您的網路必須有 Kerberos 基礎結構才能支援 Kerberos SSO。

STEP 4 | 設定驗證設定檔。



如果您的管理帳戶儲存在多種類型的伺服器上，則可以為每種類型建立一個驗證設定檔，並將所有設定檔新增至驗證順序。

在驗證設定檔中，指定驗證服務的 **Type**（類型）和相關設定：

- 外部服務—選取外部服務的 **Type**（類型），然後選取您為其建立的 **Server Profile**（伺服器組態）。
- 本機驗證—將 **Type**（類型）設定為 **None**（無）。
- **Kerberos SSO**—指定 **Kerberos Realm**（**Kerberos** 領域），然後 **Import**（匯入）您建立的 **Kerberos Keytab**。

STEP 5 | （僅限裝置群組和範本管理員）設定存取網域。

設定一個或多個存取網域。

STEP 6 | （僅限自訂角色）設定管理員角色設定檔。

設定一個或多個管理員角色設定檔。

若為自訂 Panorama 管理員，此設定檔定義帳戶的存取權限。若為裝置群組和範本管理員，此設定檔定義與帳戶相關聯的一個或多個存取網域的存取權限。

STEP 7 | 設定管理員。

1. 設定 Panorama 管理員帳戶。
    - 指派您所設定的 **Authentication Profile**（驗證設定檔）或順序。
    - （僅限裝置群組和範本管理員）將存取網域對應至管理員角色設定檔。
    - （僅限本機驗證）選取 **Password Profile**（密碼設定檔）（如果已設定）。
2. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。
3. （選用）測試驗證伺服器連線，以驗證 Panorama 是否能使用驗證設定檔來驗證管理員。

設定 *Panorama* 管理員以基於憑證的驗證來存取網頁介面

作為比密碼式驗證更安全的對 Panorama Web 介面的驗證方法，您可以設定憑證式管理員帳戶驗證，該驗證為 Panorama 本機驗證。憑證式驗證涉及交換及驗證數位特徵碼，而非密碼。

© 2019 Palo Alto Networks, Inc.

為任何管理員設定憑證式驗證，將停用 *Panorama* 上所有管理員的使用者名稱/密碼登入，之後所有的管理員都需要憑證方可登入。

STEP 1 | 在 Panorama 上產生憑證授權單位 CA 憑證。

您將使用此 CA 憑證來簽署每個管理員的用戶端憑證。

建立自我簽署根　CA 憑證。

或者，您可以從您的企業 *CA* 匯入憑證。

STEP 2 | 設定憑證設定檔以安全存取網頁介面。

1. 選取 **Panorama** > **Certificate Management**（憑證管理）> **Certificate Profile**（憑證設定檔），再按一下 **Add**（新增）。
2. 輸入憑證設定檔的 **Name**（名稱），然後將 **Username Field**（使用者名稱欄位）設為 **Subject**（主體）。
3. 選取 CA Certificates（CA 憑證）部分中的 **Add**（新增），然後選取您剛建立的 **CA Certificate**（**CA** 憑證）。
4. 按一下 **OK**（確定）來儲存設定檔。

STEP 3 | 設定 Panorama 以使用憑證設定檔驗證管理員。

1. 選取 **Panorama** > **Setup**（設定）> **Management**（管理），再編輯 [驗證設定]。
2. 選取您剛建立的 **Certificate Profile**（憑證設定檔），再按一下 **OK**（確定）。

STEP 4 | 將管理員帳戶設定為使用用戶端憑證驗證。

設定 Panorama 管理員帳戶 對於將存取 Panorama 網頁介面的每個管理員。選取 **Use only client certificate authentication (Web)**（僅使用用戶端憑證驗證 **(Web)**）核取方塊。

如果您已部署您的企業 CA 產生的用戶端憑證，請跳至步驟 8。否則，請繼續步驟 5。

STEP 5 | 針對每個管理員產生用戶端憑證。

在 Panorama 上產生憑證。在 **Signed By**（簽署者）欄位中，選取您建立的 CA 憑證。

STEP 6 | 匯出用戶端憑證。

1. 匯出憑證。
2. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

   Panorama 重新啟動並終止您的登入工作階段。之後管理員只能從擁有您產生之用戶端憑證的用戶端系統存取網頁介面。

STEP 7 | 將用戶端憑證匯入將存取網頁介面之每個管理員的用戶端系統。

根據需要參考您的 web 瀏覽器文件，完成此步驟。

STEP 8 | 確認管理員可以存取 Web 介面。

1. 在電腦上的瀏覽器中打開有用戶端憑證的 Panorama IP 位址。
2. 出現提示時，選取您匯入憑證，並按一下 **OK**（確定）。瀏覽器會顯示憑證警告。
3. 將憑證新增至瀏覽器例外狀況清單。
4. 按一下 **Login**（登入）。網頁介面會顯示出來，而不會提示您輸入使用者名稱或密碼。

© 2019 Palo Alto Networks, Inc.

設定帶有基於 *SSH* 金鑰驗證的 *CLI* 管理員

對於使用 Secure Shell (SSH) 存取 Panorama CLI 的管理員，SSH 金鑰提供比密碼更安全的驗證方法。SSH 金鑰幾乎可以消除暴力密碼破解攻擊的風險，提供雙因素驗證 (私密金鑰與複雜密碼) 的選項，且不會透過網路傳送密碼。SSH 金鑰也可以啟用自動指令碼來存取 CLI。

STEP 1 | 使用 SSH 金鑰產生工具，在管理員用戶端系統上建立非對稱金鑰配對。

支援的金鑰格式是 IETF SECSH 與 Open SSH。支援的演算法是 DSA (1024 位元) 和 RSA (768 - 4,096 位元)。

關於產生金鑰配對的命令，請參考您的 SSH 用戶端文件。

公開金鑰與私密金鑰是不同的檔案。將二者儲存在 Panorama 可以存取的位置。為了增加安全性，請輸入複雜密碼來加密私人金鑰。Panorama 在登入時提示管理員提供此密碼。

STEP 2 | 將管理員帳戶設定為使用公開金鑰驗證。

1. 設定 Panorama 管理員帳戶。
   - 設定兩種驗證方法之一，以便在 SSH 金鑰驗證失敗時作為後援方法使用：

     外部驗證服務—選取 **Authentication Profile**（驗證設定檔）。

     本機驗證 - 將 **Authentication Profile**（驗證設定檔）設為 **None**（無），並輸入 **Password**（密碼）和 **Confirm Password**（確認密碼）。
   - 選取 **Use Public Key Authentication**（使用私人金鑰驗證）(SSH) 核取方塊，按一下 **Import Key**（匯入金鑰），**Browse**（瀏覽）至您剛產生的公開金鑰，並按一下 **OK**（確定）。
2. 按一下 **OK**（確定）以儲存管理帳戶。
3. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

STEP 3 | 設定 SSH 用戶端，使用私人金鑰向 Panorama 進行驗證。

對管理員的用戶端系統執行此工作。根據需要參考您的 SSH 用戶端文件，完成此步驟。

STEP 4 | 確認管理員可以使用 SSH 金鑰驗證存取 Panorama CLI。

1. 在管理員用戶端系統上使用瀏覽器前往 Panorama IP 位址。
2. 以管理員身份登入 Panorama CLI。輸入使用者名稱之後，您將看到下列輸出 (金鑰值為範例)：

   使用公開金鑰「`dsa-key-20130415`」驗證
3. 如果出現提示，請輸入您在建立金鑰時所定義的複雜密碼。

為 *Panorama* 管理員設定 *RADIUS* 驗證

您可以使用 RADIUS 伺服器來驗證對 Panorama 網頁介面的管理存取。您也可以在 RADIUS 伺服器上定義廠商特定屬性 (VSA) 來進行管理員授權管理。使用 VSA 可讓您透過目錄服務快速變更管理員的角色、存取網域和使用者群組，這通常比在 Panorama 上重新設定更加簡單。



您可以使用 RADIUS 伺服器來驗證對 *Panorama* 網頁介面的管理存取。您也可以在 *RADIUS* 伺服器上定義廠商特定屬性 (VSA) 來進行管理員授權管理。使用 *VSA* 可讓您透過目錄服務快速變更管理員的角色、存取網域和使用者群組，這通常比在 *Panorama* 上重新設定更加簡單。

您可以將 Palo Alto 網路 RADIUS 詞典 匯入 *RADIUS* 伺服器，以定義 *Panorama* 和 *RADIUS* 伺服器之間通訊所需的驗證屬性。

您也可以使用 *RADIUS* 伺服器來對管理員實作多因素驗證 (MFA)。

© 2019 Palo Alto Networks, Inc.

STEP 1 | 新增 RADIUS 伺服器設定檔。

該設定檔定義 Panorama 如何連接至 RADIUS 伺服器。

1. 選取 **Panorama** > **Server Profiles**（伺服器設定檔）> **RADIUS**，然後 **Add**（新增）設定檔。
2. 輸入用來識別伺服器設定檔的 **Profile Name**（設定檔名稱）。
3. 輸入 **Timeout**（逾時）間隔時間（單位為秒），超過此時間後，驗證要求將逾時（預設值為 3；範圍為 1-20）。



如果您使用伺服器設定檔來整合 *Panorama* 與 *MFA* 服務，請輸入讓管理員有足夠時間回應驗證挑戰的間隔。例如，如果 *MFA* 服務提示輸入一次性密碼 *(OTP)*，管理員需要時間才能在其端點裝置上看到 *OTP*，然後在 *MFA* 登入頁面中輸入 *OTP*。

4. 選取 Panorama 用於向 RADIUS 伺服器驗證的 **Authentication Protocol**（驗證通訊協定）（預設值為 **CHAP**）。



選取 *CHAP*（如果 *RADIUS* 伺服器支援此通訊協定）；它比 *PAP* 更安全。

5. **Add**（新增）每個 RADIUS 伺服器，然後輸入下列資訊：
   - 用來識別伺服器的 **Name**（名稱）
   - **RADIUS Server**（**RADIUS** 伺服器）IP 位址或 FQDN
   - **Secret**（密碼）/**Confirm Secret**（確認密碼）（用於加密使用者名稱和密碼的金鑰）
   - 用於驗證要求的伺服器 **Port**（連接埠）（預設值為 1812）
6. 按一下 **OK**（確定）來儲存伺服器設定檔。

STEP 2 | 將 RADIUS 伺服器設定檔指派給驗證設定檔。

驗證設定檔中定義一群管理員通用的驗證設定。

1. 選取 **Panorama** > **Authentication Profile**（驗證設定檔），然後 **Add**（新增）設定檔。
2. 輸入用來識別驗證設定檔的 **Name**（名稱）。
3. 將 **Type**（類型）設為 **RADIUS**。
4. 選取您設定的 **Server Profile**（伺服器設定檔）。
5. 選取 **Retrieve user group from RADIUS**（從 **RADIUS** 擷取使用者群組），以從 RADIUS 伺服器上定義的 VSA 收集使用者群組資訊。

   Panorama 會比對群組資訊與您在驗證設定檔「允許清單」中指定的群組。
6. 選取 **Advanced**（進階），然後在 Allow List（允許清單）中，**Add**（新增）允許使用此驗證設定檔進行驗證的管理員。
7. 按一下 **OK**（確定）來儲存驗證設定檔。

STEP 3 | 將 Panorama 設定為針對所有管理員使用驗證設定檔。

1. 選取 **Panorama** > **Setup**（設定）> **Management**（管理），然後編輯 Authentication Settings（驗證設定）。
2. 選取您所設定的 **Authentication Profile**（驗證設定檔），再按一下 **OK**（確定）。

STEP 4 | 設定角色和存取網域，定義管理員的授權設定。

1. 如果管理員使用自訂角色而非預定義（動態）角色，則設定管理員角色設定檔。
2. 如果管理員使用「裝置群組和範本」角色，請設定存取網域。

STEP 5 | Commit（提交）您的變更。

選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

STEP 6 | 設定　RADIUS 伺服器。

© 2019 Palo Alto Networks, Inc.

關於執行下列步驟的特定說明，請參閱 RADIUS 伺服器文件：

1. 新增 Panorama IP 位址或主機名稱做為 RADIUS 用戶端。
2. 新增管理員帳戶。

   若 *RADIUS* 伺服器設定檔將 *CHAP* 指定為 *Authentication Protocol*（驗證通訊協定），則您必須為帳戶定義可反轉的加密密碼。否則，*CHAP* 驗證將失敗。
3. 定義 Panorama 的廠商代碼 (25461)，然後分別為每個管理員的角色、存取網域和使用者群組定義 RADIUS VSA。

   當您預先定義使用者的動態管理員角色時，使用小寫字母指定角色（例如，輸入 **`superuser`**，而不是 **`SuperUser`**）。

STEP 7 | 確認 RADIUS 伺服器是否對管理員執行驗證和授權。

1. 使用您新增至 RADIUS 伺服器的管理員帳戶登入 Panorama 網頁介面。
2. 確認您是否只能存取允許該管理員關聯的角色存取的 Web 介面頁面。
3. 在 **Monitor**（監控）、**Policies**（原則）和 **Objects**（物件）頁籤中，驗證您是否只能存取管理員相關聯的存取網域所允許的裝置群組。

為 *Panorama* 管理員設定 *TACACS+* 驗證

您可以使用 TACACS+ 伺服器來驗證對 Panorama 網頁介面的管理存取。您也可以在 TACACS+ 伺服器上定義廠商特定屬性 (VSA) 來進行管理員授權管理。使用 VSA 可讓您透過目錄服務快速變更管理員的角色、存取網域和使用者群組，這通常比在 Panorama 上重新設定更加簡單。

STEP 1 | 新增 TACACS+ 伺服器設定檔。

該設定檔定義 Panorama 如何連接至 TACACS+ 伺服器。

1. 選取 **Panorama** > **Server Profiles**（伺服器設定檔）> **TACACS+**，然後 **Add**（新增）設定檔。
2. 輸入用來識別伺服器設定檔的 **Profile Name**（設定檔名稱）。
3. 輸入 **Timeout**（逾時）間隔時間（單位為秒），超過此時間後，驗證要求將逾時（預設值為 3；範圍為 1-20）。
4. 選取 Panorama 用於向 TACACS+ 伺服器驗證的 **Authentication Protocol**（驗證通訊協定）（預設值為 **CHAP**）。

   選取 *CHAP*（如果 *TACACS+* 伺服器支援此通訊協定）；它比 *PAP* 更安全。
5. **Add**（新增）每個 TACACS+ 伺服器，然後輸入下列資訊：
   - 用來識別伺服器的 **Name**（名稱）
   - **TACACS+ Server**（**TACACS+** 伺服器）IP 位址或 FQDN
   - **Secret**（密碼）/**Confirm Secret**（確認密碼）（用於加密使用者名稱和密碼的金鑰）
   - 用於驗證要求的伺服器 **Port**（連接埠）（預設值為 49）
6. 按一下 **OK**（確定）來儲存伺服器設定檔。

STEP 2 | 將 TACACS+ 伺服器設定檔指派給驗證設定檔。

驗證設定檔中定義一群管理員通用的驗證設定。

1. 選取 **Panorama** > **Authentication Profile**（驗證設定檔），然後 **Add**（新增）設定檔。
2. 輸入用來識別設定檔的 **Name**（名稱）。
3. 將 **Type**（類型）設為 **TACACS+**。
4. 選取您設定的 **Server Profile**（伺服器設定檔）。

© 2019 Palo Alto Networks, Inc.

5. 選取 **Retrieve user group from TACACS+**（從 **TACACS+** 擷取使用者群組），以從 TACACS+ 伺服器上定義的 VSA 收集使用者群組資訊。

   Panorama 會比對群組資訊與您在驗證設定檔「允許清單」中指定的群組。
6. 選取 **Advanced**（進階），然後在 Allow List（允許清單）中，**Add**（新增）允許使用此驗證設定檔進行驗證的管理員。
7. 按一下 **OK**（確定）來儲存驗證設定檔。

STEP 3 | 將 Panorama 設定為針對所有管理員使用驗證設定檔。

1. 選取 **Panorama** > **Setup**（設定）> **Management**（管理），然後編輯 Authentication Settings（驗證設定）。
2. 選取您所設定的 **Authentication Profile**（驗證設定檔），再按一下 **OK**（確定）。

STEP 4 | 設定角色和存取網域，定義管理員的授權設定。

1. 如果管理員將使用自訂角色而非預定義（動態）角色，則設定管理員角色設定檔。
2. 如果管理員使用「裝置群組和範本」角色，請設定存取網域。

STEP 5 | Commit（提交）您的變更。

選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

STEP 6 | 設定 TACACS+ 伺服器以驗證和授權管理員。

關於執行下列步驟的特定說明，請參閱 TACACS+ 伺服器文件：

1. 新增 Panorama IP 位址或主機名稱作為 TACACS+ 用戶端。
2. 新增管理員帳戶。

   若將 *CHAP* 選為 *Authentication Protocol*（驗證通訊協定），則您必須為帳戶定義可反轉的加密密碼。否則，*CHAP* 驗證將失敗。
3. 分別為每個管理員的角色、存取網域和使用者群組定義 TACACS+ VSA。

   當您預先定義使用者的動態管理員角色時，使用小寫字母指定角色（例如，輸入 ***superuser***，而不是 ***SuperUser***）。

STEP 7 | 確認 TACACS+ 伺服器是否對管理員執行驗證和授權。

1. 使用您新增至 TACACS+ 伺服器的管理員帳戶登入 Panorama 網頁介面。
2. 確認您是否只能存取允許該管理員關聯的角色存取的 Web 介面頁面。
3. 在 **Monitor**（監控）、**Policies**（原則）和 **Objects**（物件）頁籤中，驗證您是否只能存取允許該管理員關聯的粗存取網域存取的虛擬系統。

為 *Panorama* 管理員設定 *SAML* 驗證

您可以使用安全性聲明標記語言 (SAML) 2.0 來控制對 Panorama 網頁介面（但不是 CLI）的管理存取。您也可以使用 SAML 屬性來進行管理員授權管理。SAML 屬性可讓您透過目錄服務快速變更管理員的角色、存取網域及使用者群組，而不必在 Panorama 上重新設定。

若要設定 SAML 單一登入 (SSO) 和單一登出 (SLO)，您必須將 Panorama 和識別提供者 IdP 相互註冊，它們之間才能通訊。若 IdP 提供包含註冊資訊的中繼資料檔案，您可以將其匯入 Panorama，以註冊 IdP 並建立 IdP 伺服器設定檔。該伺服器設定檔定義了如何連線至 IdP 並指定了 IdP 用於簽署 SAML 訊息的憑證。您還可以使用憑證讓 Panorama 簽署 SAML 訊息。使用憑證是選擇性，但建議使用，以確保 Panorama 與 IdP 之間的通訊安全。

STEP 1 | （建議）取得 IdP 和 Panorama 將用於簽署 SAML 資訊的憑證。

© 2019 Palo Alto Networks, Inc.

如果這些憑證未指定金鑰用途屬性，則預設會允許各種用途，包括簽署訊息。在這種情況下，您可以透過任何方式取得憑證。

如果憑證明確指定金鑰用途屬性，則其中一個屬性必須是 Digital Signature（數位簽章），而您在 Panorama 上產生的憑證並無此屬性。在這種情況下，您必須匯入憑證：

- **Panorama** 用於簽署 **SAML** 訊息的憑證—從企業憑證授權單位 (CA) 或第三方 CA 匯入憑證。
- **IdP** 用於簽署 **SAML** 訊息的憑證—從 IdP 匯入包含憑證的中繼資料檔案（請參閱下一步）。IdP 憑證限於下列演算法：
  - 公開金鑰演算法—RSA（1,024 位元以上）和 ECDSA（所有大小）。
  - 簽署演算法—SHA1、SHA256、SHA384 和 SHA512。

STEP 2 | 新增 SAML IdP 伺服器設定檔。

該伺服器設定檔會向 Panorama 註冊 IdP，並定義它們的連線方式。

在此範例中，您將從 IdP 匯入 SAML 中繼資料檔案，以便 Panorama 能夠自動建立伺服器設定檔並填入連線、註冊和 IdP 憑證資訊。



如果 *IdP* 未提供中繼資料檔案，請選取 *Panorama* > *Server Profiles*（伺服器設定檔）> *SAML Identity Provider*（*SAML* 識別提供者），然後 *Add*（新增）伺服器設定檔，再手動輸入相關資訊（請向 *IdP* 管理員查詢相關的值）。

1. 從 IdP 將 SAML 中繼資料檔案匯出到 Panorama 可存取的用戶端系統。

   該檔案中指定的憑證必須符合前一步中所列的要求。關於匯出檔案的說明，請參閱 IdP 文件。
2. 選取 **Panorama** > **Server Profiles**（伺服器設定檔）> **SAML Identity Provider**（**SAML** 識別提供者），然後將中繼資料檔案 **Import**（匯入）Panorama。
3. 輸入用來識別伺服器設定檔的 **Profile Name**（設定檔名稱）。
4. **Browse**（瀏覽）至**Identity Provider Metadata**（識別提供者中繼資料）檔案。
5. （建議）選取**Validate Identity Provider Certificate**（驗證識別提供者憑證）（預設值），讓 Panorama 驗證 **Identity Provider Certificate**（識別提供者憑證）。

   只有在您將伺服器設定檔指派給驗證設定檔並 **Commit**（交付）之後，才會進行驗證。Panorama 將使用驗證設定檔中的 **Certificate Profile**（憑證設定檔）驗證憑證。

   驗證憑證時增強安全性的最佳做法。
6. 輸入 **Maximum Clock Skew**（最大時鐘誤差），即在 Panorama 驗證 IdP 訊息的瞬間，IdP 與 Panorama 系統時間之間允許的秒差（預設值為 60；範圍為 1 至 900）。若差值超過此值，則驗證失敗。
7. 按一下 **OK**（確定）來儲存伺服器設定檔。
8. 按一下伺服器設定檔名稱，以顯示設定檔組態。確認所匯出的資訊是否正確，並在必要時編輯。

STEP 3 | 設定驗證設定檔。

驗證設定檔指定 SAML IdP 伺服器設定檔，並定義驗證程序的選項，例如 SLO。

1. 選取 **Panorama** > **Authentication Profile**（驗證設定檔），然後 **Add**（新增）設定檔。
2. 輸入用來識別設定檔的 **Name**（名稱）。
3. 將 **Type**（類型）設為 **SAML**。
4. 選取您設定的 **IdP Server Profile**（**IdP** 伺服器設定檔）。
5. 選取 **Certificate for Signing Requests**（用於簽署要求的憑證）。

   Panorama 使用此憑證來簽署要傳送至 IdP 的訊息。
6. （選用）**Enable Single Logout**（啟用單一登出）（預設為停用）。

© 2019 Palo Alto Networks, Inc.

7. 選取 Panorama 用於驗證 **Identity Provider Certificate**（識別提供者憑證）的 **Certificate Profile**（憑證設定檔）。
8. 輸入 IdP 訊息用於識別使用者的 **Username Attribute**（使用者名稱屬性）（預設值為 **username**）。

   當您預先定義使用者的動態管理員角色時，使用小寫字母指定角色（例如，輸入 ***superuser***，而不是 ***SuperUser***）。如果您透過 *IdP* 識別身分存放區進行管理員授權管理，則還要指定 *Admin Role Attribute*（管理員角色屬性）和*Access Domain Attribute*（存取網域屬性）。
9. 選取 **Advanced**（進階），然後 **Add**（新增）允許使用此驗證設定檔進行驗證的管理員。
10. 按一下 **OK**（確定）來儲存驗證設定檔。

STEP 4 | 將 Panorama 設定為針對所有管理員使用驗證設定檔。

1. 選取 **Panorama** > **Setup**（設定）> **Management**（管理），編輯 Authentication Settings（驗證設定），然後選取您所設定的 **Authentication Profile**（驗證設定檔）。
2. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），讓您的變更在 Panorama 上生效，以及驗證您指派給 SAML IdP 伺服器設定檔的 **Identity Provider Certificate**（識別提供者憑證）。

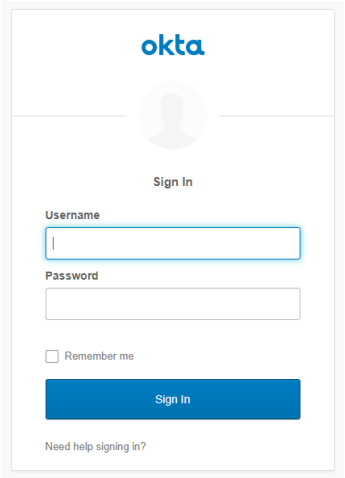
STEP 5 | 建立 SAML 中繼資料檔案將 Panorama 註冊在 IdP。

1. 選取 **Panorama** > **Authentication Profile**（驗證設定檔），然後在您所設定的驗證設定檔的 Authentication（驗證）欄中，按一下 **Metadata**（中繼資料）。
2. 將 **Management Choice**（管理選擇）設為 **Interface**（介面）（已選取預設值），然後選取管理 (MGT) 介面。
3. 按一下 **OK**（確定），將中繼資料檔案儲存至用戶端系統。
4. 將中繼資料檔案匯入 IdP 伺服器來註冊 Panorama。相關說明，請參閱 IdP 文件。

STEP 6 | 確認管理員可以使用 SAML SSO 進行驗證。

1. 移至 Panorama 網頁介面的 URL。
2. 按一下 **Use Single Sign-On**（使用單一登入）。
3. 按一下 **Continue**（繼續）。

   Panorama 會將您重新導向來向 IdP 驗證，此時會顯示登入頁面。例如：



4. 使用 SSO 使用者名稱和密碼登入。

   在 IdP 上成功驗證後，將重新導向回 Panorama，此時會顯示網頁介面。
5. 使用 Panorama 管理員帳戶來要求存取其他 SSO 應用程式。

   成功存取表示 SAML SSO 驗證成功。

© 2019 Palo Alto Networks, Inc.

設定使用自訂憑證進行驗證

依預設，Palo Alto Networks 裝置會使用預先定義的憑證相互驗證，以建立 SSL 連線來用於管理存取和裝置間通訊。不過，您可以設定改用自訂憑證進行驗證。此外，您也可以使用自訂憑證來保護 Panorama HA 對等之間的高可用性 (HA) 連線安全。自訂憑證可讓您建立唯一的信任鏈，以確保 Panorama 與受管理的防火牆和日誌收集器之間的相互驗證。請參閱憑證管理，瞭解憑證及如何部署在 Panorama、日誌收集器和防火牆上的詳細資訊。

下列主題說明如何使用 Panorama 設定與管理自訂憑證。

- SSL/TLS 連線如何相互驗證？
- 在 Panorama 上設定使用自訂憑證進行驗證
- 在受管理的裝置上設定使用自訂憑證進行驗證
- 新增用戶端裝置
- 變更憑證

SSL/TLS 連線如何相互驗證？

在一般 SSL 連線中，只有伺服器需要出示憑證向用戶端表明自己的身分。不過，在相互 SSL 驗證中，用戶端也會向伺服器出示憑證。Panorama、主要 Panorama HA 配對、日誌收集器、WildFire 設備和 PAN-DB 設備可以充當伺服器。防火牆、日誌收集器、WildFire 設備和次要 Panorama HA 對等可以充當用戶端。裝置扮演的角色視部署而定。例如，在下圖中，Panorama 管理一些防火牆和一個收集器群組，並充當防火牆和日誌收集器的伺服器。對於送來日誌的防火牆，日誌收集器充當這些防火牆的伺服器。

若要部署自訂憑證以便於您的部署中相互驗證，您需要：

- **SSL/TLS** 服務設定檔—SSL/TLS 服務設定檔會參考您的自訂憑證，並建立 SSL/TLS 通訊協定版本，供伺服器裝置用來與用戶端裝置進行通訊，以定義連線的安全性。
- 伺服器憑證和設定檔—伺服器角色中的裝置需要憑證和憑證設定檔，才能向用戶端裝置表明自己的身分。您可以從企業公開金鑰基礎結構 (PKI) 部署此憑證、向信任的第三方 CA 購買憑證，或在本機產生自我簽署憑證。伺服器憑證的憑證通用名稱 (CN) 或主體別名中，必須包含裝置管理介面的 IP 位址或 FQDN。用戶端防火牆或日誌收集器會根據伺服器的 IP 位址或 FQDN，比對伺服器出示的憑證中的 CN 或主體別名，以驗證伺服器的識別。

  此外，請使用憑證設定檔來定義憑證撤銷狀態 (OCSP/CRL)，以及根據撤銷狀態所採取的動作。
- 用戶端憑證和設定檔—每個受管理的裝置都需要用戶端憑證和憑證設定檔。用戶端裝置使用其憑證向伺服器裝置表明自己的身份。您可以使用 Simple Certificate Enrollment Protocol（簡易憑證註冊通訊協定 - SCEP）從企業 PKI 部署憑證、向信任的第三方 CA 購買憑證，或在本機產生自我簽署憑證。

  自訂憑證可以是每個用戶端裝置特有，或所有裝置共有。唯一裝置憑證使用受管理裝置序號和 CN 的雜湊。伺服器會根據用戶端裝置已設定的序號，以比對 CN 或主體別名。若要根據 CN 來驗證用戶端憑證，使用者名稱必須設為主體通用名稱。用戶端憑證行為也適用於 Panorama HA 對等連線。

  您可以在每個用戶端裝置上設定用戶端憑證和憑證設定檔，或隨著範本將設定從 Panorama 推送至每個裝置。

© 2019 Palo Alto Networks, Inc.

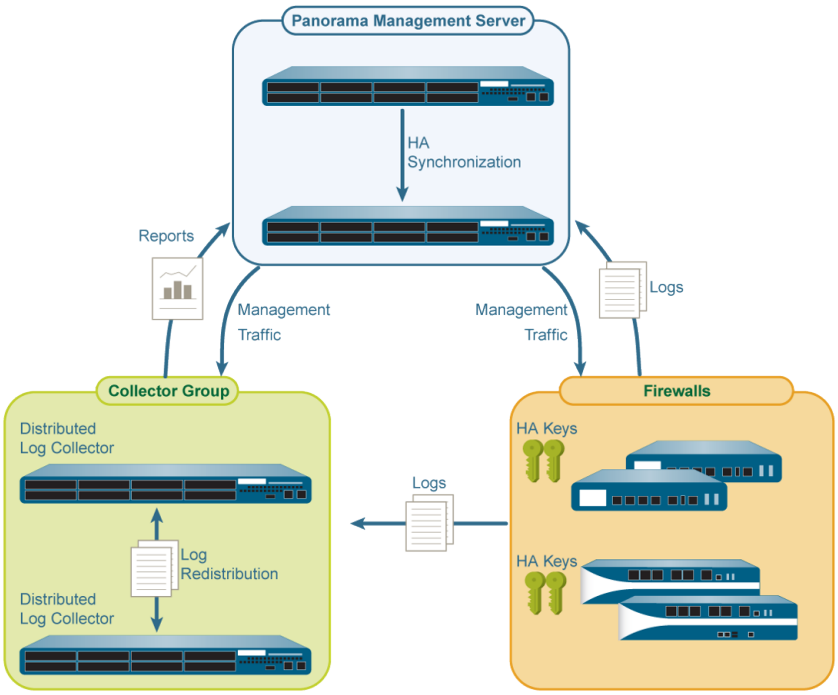


圖 11: SSL/TLS 驗證

在 Panorama 上設定使用自訂憑證進行驗證

完成下列程序，將伺服器端 (Panorama) 設定為使用自訂憑證（而非預先設定的憑證），以便與部署中的受管理裝置相互驗證。請參閱 設定在 HA 對等之間使用自訂憑證進行驗證，在 Panorama HA 配對上設定自訂憑證。

STEP 1 | 部署伺服器憑證。

您可以在 Panorama 上產生自我簽署憑證，或從企業憑證授權單位 (CA) 或信任的第三方 CA 取得憑證，就能在 Panorama 或伺服器日誌收集器上部署憑證。

STEP 2 | 在 Panorama 上，設定憑證設定檔。此憑證設定檔中定義使用哪個憑證，以及在哪個憑證欄位中尋找 IP 位址或 FQDN。

1. 選取 **Panorama** > **Certificates Management**（憑證管理）> **Certificate Profile**（憑證設定檔）。
2. 設定憑證設定檔。

如果您在憑證設定檔中設定中繼 *CA*，則必須同時包含 *root CA*。

STEP 3 | 設定 SSL/TLS 服務設定檔。

1. 選取 **Panorama** > **Certificate Management**（憑證管理）> **SSL/TLS Service Profile**（**SSL/TLS** 服務設定檔）。
2. 設定 SSL/TLS 設定檔，以定義憑證和通訊協定供 Panorama 及其受管理的裝置用於 SSL/TLS 服務。

STEP 4 | 在 Panorama 或伺服器角色的日誌收集器上設定安全伺服器通訊。

1. 選取下列其中一個導覽路徑：
   - Panorama：**Panorama** > **Setup**（設定）> **Management**（管理），然後 **Edit**（編輯）安全通訊設定

© 2019 Palo Alto Networks, Inc.

- 日誌收集器：**Panorama** > **Managed Collectors**（受管理的收集器）> **Add**（新增）> **Communication**（通訊）。

2. 選取 **Customize Secure Server Communication**（自訂安全伺服器通訊）選項。
3. 確認未選取 **Allow Custom Certificate Only**（僅允許自訂憑證）核取方塊。這樣可讓您在移轉至自訂憑證期間繼續管理所有裝置。

   選取 *Custom Certificate Only*（僅限自訂憑證）核取方塊時，*Panorama* 不會使用預先定義的憑證來驗證裝置，也無法使用這種憑證來管理裝置。
4. 選取 **SSL/TLS Service Profile**（**SSL/TLS** 服務設定檔）。此 SSL/TLS 服務設定檔會套用至 Panorama、防火牆、日誌收集器和 Panorama HA 對等之間的所有 SSL 連線。
5. 選取 **Certificate Profile**（憑證設定檔），以識別與用戶端（例如防火牆）建立安全通訊時所使用的憑證。
6. （選用）設定授權清單。授權清單可在憑證驗證之外多加一層安全性。授權清單會檢查用戶端憑證「主體」或「主體別名」。如果伴隨用戶端憑證一起出現的主體或主體別名不符合授權清單上的識別項，則會拒絕驗證。

   您也可以根據序號來授權用戶端裝置。

   1. **Add**（新增）授權清單。
   2. 在憑證設定檔中，選取 **Subject**（主體）或 **Subject Alt Name**（主體別名）作為識別項類型。
   3. 如果識別項是主體，請輸入通用名稱，如果識別項是主體別名，請輸入 IP 位址、主機名稱或電子郵件。
   4. 按一下 **OK**（確定）。
   5. 選取 **Check Authorization List**（檢查授權清單）以強制執行授權清單。
7. 選取 **Authorize Client Based on Serial Number**（根據序號來授權用戶端），讓伺服器根據受管理裝置的序號來驗證用戶端。用戶端憑證中的 CN 或主體必須有特殊關鍵字 $UDID，才能啟用這種驗證類型。
8. 在 **Customize Communication**（自訂通訊）區段中選取 **Data Redistribution**（資料重新散佈）選項，以使用自訂憑證來保護與資料重新散佈用戶端進行的傳出通訊。
9. 在 **Disconnect Wait Time (min)**（中斷連線等候時間（分鐘））中，指定 Panorama 在終止目前與其受管理裝置間的工作階段和重新建立連線之前應該等候多久。依預設，此欄位是空白，範圍是 0 至 44,640 分鐘。此欄位保持空白相當於設為 0。

   直到您提交新設定，中斷連線等候時間才會開始倒數計時。
10. 按一下 **OK**（確定）。
11. **Commit**（提交）您的變更。

在受管理的裝置上設定使用自訂憑證進行驗證

完成下列程序，將用戶端（防火牆或日誌收集器）設定為使用自訂憑證（而非預先設定的憑證），以便與部署中的受管理裝置相互驗證。

STEP 1 | 升級每個受管理的防火牆或日誌收集器。所有受管理的裝置必須執行 PAN-OS 8.0 或更新版本，才能強制執行自訂憑證驗證。

升級防火牆。升級之後，每個防火牆會使用預先定義的預設憑證來連接至 Panorama。

STEP 2 | 取得或產生裝置憑證。

您可以在 Panorama 上產生自我簽署憑證，或從企業憑證授權單位 (CA) 或信任的第三方 CA 取得憑證，就能在 Panorama 或伺服器日誌收集器上部署憑證。

如果是根據序號來授權用戶端裝置，請將通用名稱設為 $UDID 或將主體設為 CN=$UDID（在 SCEP 設定檔中）。

© 2019 Palo Alto Networks, Inc.

- 您可以在 Panorama 上產生自我簽署憑證，或從企業 CA 或信任的第三方 CA 取得憑證。
- 如果您使用 SCEP 傳送裝置憑證，請設定 SCEP 設定檔。SCEP 可讓您將憑證自動部署至受管理的裝置。當具有 SCEP 設定檔的新用戶端裝置嘗試向 Panorama 驗證時，SCEP 伺服器會將憑證傳送至裝置。

STEP 3 | 為用戶端裝置設定憑證設定檔。

您可以在每個用戶端裝置上個別設定這一項，也可以隨著範本將此設定推送至受管理的裝置。

1. 選取下列其中一個導覽路徑：
   - 防火牆 - 選取 **Device**（裝置）> **Certificates Management**（憑證管理）> **Certificate Profile**（憑證設定檔）。
   - 日誌收集器 - 選取 **Panorama** > **Certificates Management**（憑證管理）> **Certificate Profile**（憑證設定檔）。
2. 設定憑證設定檔。

STEP 4 | 將自訂憑證部署在每個防火牆或日誌收集器。

1. 選取下列其中一個導覽路徑：
   - 防火牆：選取 **Device**（裝置）> **Setup**（設定）> **Management**（管理），然後 **Edit**（編輯）Panorama 設定
   - 日誌收集器：選取 **Panorama** > **Managed Collectors**（受管理的收集器），然後 **Add**（新增）新的日誌收集器，或選取現有日誌收集器。選取 **Communication**（通訊）。
2. 選取 **Secure Client Communication**（安全用戶端通訊）核取方塊（僅限防火牆）。
3. 選取 **Certificate Type**（憑證類型）。
   - 如果您使用本機裝置憑證，請選取 **Certificate**（憑證）和 **Certificate Profile**（憑證設定檔）。
   - 如果您使用 SCEP 來部署裝置憑證，請選取 **SCEPC Profile**（**SCEP** 設定檔）和 **Certificate Profile**（憑證設定檔）。
   - 如果您正在使用預設的 Panorama 憑證，請選取 **Predefined**（預先定義）。
4. （選用）啟用 **Check Server Identity**（檢查伺服器識別）。防火牆或日誌收集器會根據 Panorama 的 IP 位址或 FQDN，檢查伺服器憑證中的 CN，以驗證其識別。
5. 按一下 **OK**（確定）。
6. **Commit**（提交）您的變更。

   提交您的變更之後，在「中斷連線等候時間」結束之前，受管理的裝置不會終止目前與 Panorama 之間的工作階段。

STEP 5 | 選取您想要為其使用自訂憑證的傳入通訊類型：

- **HA** 通訊
- **WildFire** 通訊
- 資料重新散佈

STEP 6 | 將自訂憑證部署在所有受管理的裝置之後，強制使用自訂憑證進行驗證。

WildFire 設備目前不支援自訂憑證。如果 *Panorama* 正在管理 *WildFire* 設備，請勿選取 *Allow Custom Certificates Only*（僅允許自訂憑證）。

1. 選取 **Panorama** > **Setup**（設定）> **Management**（管理），再 **Edit**（編輯）[Panorama 設定]。
2. 選取 **Allow Custom Certificate Only**（僅允許自訂憑證）。
3. 按一下 **OK**（確定）。
4. **Commit**（提交）您的變更。

© 2019 Palo Alto Networks, Inc.

提交此變更之後，Panorama 管理的所有裝置都必須使用自訂憑證。否則，Panorama 和裝置之間的驗證會失敗。

新增用戶端裝置

將新的防火牆或日誌收集器新增至 Panorama 時，工作流程取決於這些裝置是否設定為只使用自訂憑證相互驗證。

- 如果在 Panorama 上未選取 Custom Certificates Only（僅限自訂憑證），您可以將裝置新增至 Panorama，然後按照步驟在受管理的裝置上設定使用自訂憑證進行驗證中開始的程序來部署自訂憑證。
- 如果在 Panorama 上已選取 Custom Certificates Only（僅限自訂憑證），您必須先將自訂憑證部署在防火牆，再新增至 Panorama。否則，受管理的裝置無法使用 Panorama 驗證。這可透過防火牆網頁介面或 bootstrap.xml 檔案中的啟動程序來手動完成。

變更憑證

如果部署中的自訂憑證已過期或撤銷而需要更換，您可以完成下列其中一項工作。

- 變更伺服器憑證
- 變更用戶端憑證
- 變更 Root 或中繼 CA 憑證

變更伺服器憑證

完成下列工作來更換伺服器憑證。

STEP 1 | 部署新的伺服器憑證。

您可以在 Panorama 上產生自我簽署憑證，或從企業 CA 或信任的第三方 CA 取得憑證，就能在 Panorama 或伺服器日誌收集器上部署憑證。

STEP 2 | 在 SSL/TLS 服務設定檔中變更憑證。

1. 選取 **Panorama** > **Certificate Management**（憑證管理）> **SSL/TLS Service Profile**（**SSL/TLS** 服務設定檔），然後選取 SSL/TLS 服務設定檔。
2. 選取 **Certificate**（憑證）。
3. 按一下 **OK**（確定）。

STEP 3 | 重新建立伺服器（Panorama 或日誌收集器）與用戶端裝置之間的連線。

1. 若為 Panorama，請選取 **Panorama** > **Setup**（設定）> **Management**（管理），並 **Edit**（編輯）Panorama 設定，若為日誌收集器，請選取 **Panorama** > **Managed Collectors**（受管理的收集器）> **Add**（新增）> **Communication**（通訊）。
2. 設定 **Disconnect Wait Time**（中斷連線等候時間）。
3. 按一下 **OK**（確定）。
4. **Commit**（提交）您的變更。

變更用戶端憑證

完成下列工作來更換用戶端憑證。

STEP 1 | 取得或產生裝置憑證。

您可以在 Panorama 上產生自我簽署憑證，或從企業 CA 或信任的第三方 CA 取得憑證，就能在 Panorama 或伺服器日誌收集器上部署憑證。

© 2019 Palo Alto Networks, Inc.

如果是根據序號來授權用戶端裝置，請將通用名稱設為 $UDID 或將主體設為 CN=$UDID（在 SCEP 設定檔中）。

- 您可以在 Panorama 上產生自我簽署憑證，或從企業 CA 或信任的第三方 CA 取得憑證。
- 如果您使用 SCEP 傳送裝置憑證，請設定 SCEP 設定檔。SCEP 可讓您將憑證自動部署至受管理的裝置。當具有 SCEP 設定檔的新用戶端裝置嘗試向 Panorama 驗證時，SCEP 伺服器會將憑證傳送至裝置。

STEP 2 | 在憑證設定檔中變更憑證。

1. 選取 **Device**（裝置）> **Certificate Management**（憑證管理）> **Certificates Profile**（憑證設定檔），然後選取憑證設定檔。
2. 在 CA Certificates（CA 憑證）下，**Add**（新增）要指派給憑證設定檔的新憑證。
3. 按一下 **OK**（確定）。
4. **Commit**（提交）您的變更。

變更 *Root* 或中繼 *CA* 憑證

完成下列工作來更換 root 或中繼 CA 憑證。

STEP 1 | 設定伺服器接受來自用戶端預先定義的憑證。

1. 選取 **Panorama** > **Setup**（設定）> **Management**（管理），再 **Edit**（編輯）[Panorama 設定]。
2. 取消核取 **Custom Certificate Only**（僅限自訂憑證）。
3. 從 Certificate Profile（憑證設定檔）下拉式清單中選取 **None**（無）。
4. 按一下 **OK**（確定）。
5. **Commit**（提交）您的變更。

STEP 2 | 部署新的 root 或中繼 CA 憑證。

您可以在 Panorama 上產生自我簽署憑證，或從企業 CA 或信任的第三方 CA 取得憑證，就能在 Panorama 或伺服器日誌收集器上部署憑證。

STEP 3 | 在伺服器憑證設定檔中更新 CA 憑證。

1. 選取 **Panorama** > **Certificate Management**（憑證管理）> **Certificates Profile**（憑證設定檔），然後選取要更新的憑證設定檔。
2. **Delete**（刪除）舊的 CA 憑證。
3. **Add**（新增）新的 CA 憑證。
4. 按一下 **OK**（確定）。

STEP 4 | 產生或匯入新的用戶端憑證。

1. 選取 **Device**（裝置）> **Certificate Management**（憑證管理）> **Certificates**（憑證）。
2. 建立自我簽署根 CA 憑證或從企業 CA 匯入憑證。

STEP 5 | 在用戶端憑證設定檔中更新 CA 憑證。

1. 若為防火牆，請在 Panorama Settings（Panorama 設定）中選取 **Device**（裝置）> **Setup**（設定）> **Management**（管理），並按一下 **Edit**（編輯）圖示，若為日誌收集器，請選取 **Panorama** > **Managed Collectors**（受管理的收集器）> **Add**（新增）> **Communication**（通訊），然後選取要更新的憑證設定檔。
2. **Delete**（刪除）舊的 CA 憑證。
3. **Add**（新增）新的 CA 憑證。
4. 按一下 **OK**（確定）。

STEP 6 | 在所有受管理的裝置上更新 CA 憑證之後，強制執行自訂憑證驗證。

© 2019 Palo Alto Networks, Inc.

1. 選取 **Panorama** > **Setup**（設定） > **Management**（管理），再 **Edit**（編輯）[Panorama 設定]。
2. 選取 **Custom Certificate Only**（僅限自訂憑證）。
3. 按一下 **OK**（確定）。
4. **Commit**（提交）您的變更。

   提交此變更之後，Panorama 管理的所有裝置都必須使用自訂憑證。否則，Panorama 和裝置之間的驗證會失敗。

管理防火牆

若要使用 Panorama™ 管理伺服器來管理 Palo Alto Networks 防火牆，您必須將防火牆新增為受管理的裝置，然後將指派給裝置群組及範本或範本堆疊。下列工作適用於首次部署防火牆。繼續進行前，請先檢閱規劃 Panorama 部署以瞭解部署選項。

> 將防火牆新增為受管理的裝置
> 安裝受管理防火牆的裝置憑證
> 設定零接觸佈建
> 管理裝置群組
> 管理範本與範本堆疊
> 從 Panorama 管理主要金鑰
> 重新散佈資料到受管理防火牆
> 設定企業資料遺失防護 (DLP)
> 移轉防火牆至 Panorama 進行管理
> Panorama 上的裝置監控
> 使用案例：使用 Panorama 設定防火牆

若要檢視 Panorama 網頁介面上的 **Objects**（物件）和 **Policies**（原則）頁籤，您必須先建立至少一個裝置群組。若要檢視 **Network**（網路）和 **Device**（裝置）頁籤，您必須建立至少一個範本。這些頁籤包含設定及管理網路上防火牆所需要的選項。

將防火牆新增為受管理的裝置

若要使用 Panorama 來管理防火牆，您需要啟用防火牆和 Panorama 之間的連線。成功的連線要求您在每個 Panorama 管理的防火牆上輸入 Panorama IP 位址，還有在 Panorama 上輸入每個防火牆的序號。當您新增防火牆作為受管理裝置時，您可以在初始部署時，將新防火牆與裝置群組、範本堆疊、收集器群組和日誌收集器關聯。此外，您可以選擇當防火牆首次連線至 Panorama 時，自動推送組態至您新增的防火牆，從而確保立即完成該防火牆的設定，並保證您的網路安全。



您僅可以大量匯入由 *Panorama* 管理的 *vsys* 防火牆。

防火牆會使用 Panorama 管理伺服器 IP 位址來設定 SSL 連線，以便向 Panorama 註冊。Panorama 和防火牆使用 2,048 位元憑證和 AES-256 加密 SSL 連線來彼此驗證，以便管理組態和收集日誌。準備 Panorama 和每個防火牆，如下所示：

STEP 1 | 設定防火牆與 Panorama 進行通訊。

針對 Panorama 將管理的每個防火牆重複此步驟。

1. 在防火牆上執行初始設定，讓防火牆可供存取，並且能透過網路與 Panorama 通訊。
2. 針對您打算在防火牆上使用的資料介面，設定每個資料介面，並附加至安全性區域，以便從 Panorama 推送設定和原則。
3. 將 Panorama IP 位址新增至防火牆。
    1. 選取 **Device**（裝置）> **Setup**（設定）> **Management**（管理），再編輯 [Panorama 設定]。
    2. 在第一個欄位中輸入 Panorama IP 位址。

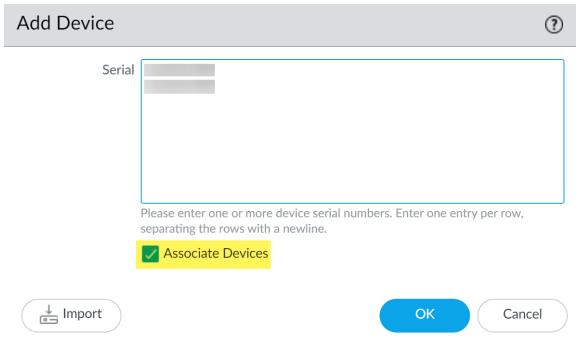
        

        Panorama 發佈裝置管理、日誌收集、報告和動態更新的單 *IP* 位址。輸入外部、網際網路界線 *IP* 位址以確保 *Panorama* 可以成功存取已有和新的受管理裝置以及日誌收集器。如果設定了內部 *Panorama IP* 位址，您可能無法管理某些裝置。例如，如果您 在 AWS 上安裝 Panorama 並輸入內部 *IP* 位址，*Panorama* 無法管理 *AWS* 安全群組以外的裝置或日誌收集器。
    3. （選用）如果您已在 Panorama 中設定高可用性 (HA) 對等，請在第二個欄位中輸入次要 Panorama 的 IP 位址。
    4. 按一下 **OK**（確定）。
    5. 選取 **Commit**（提交）並 **Commit**（提交）您的變更。

STEP 2 | 向 Panorama 新增一個或多個防火牆。

- 新增一個或多個防火牆。
    1. 新增一個新的受管理裝置（**Panorama** > **Managed Devices**（受管理裝置）> **Summary**（摘要））。
    2. 輸入防火牆 **Serial**（序）號。如果您新增多個防火牆，在分隔行上輸入各個序號。如果您想要將新防火牆與裝置群組、範本堆疊、收集器群組或日期收集器關聯進行初始部署，繼續下一步。要手動指派各防火牆，按一下 **OK**（確定）並繼續第 3 步。
    3. 選取 **Associate Devices**（關聯裝置）核取方塊，然後按一下 **OK**（確定）。

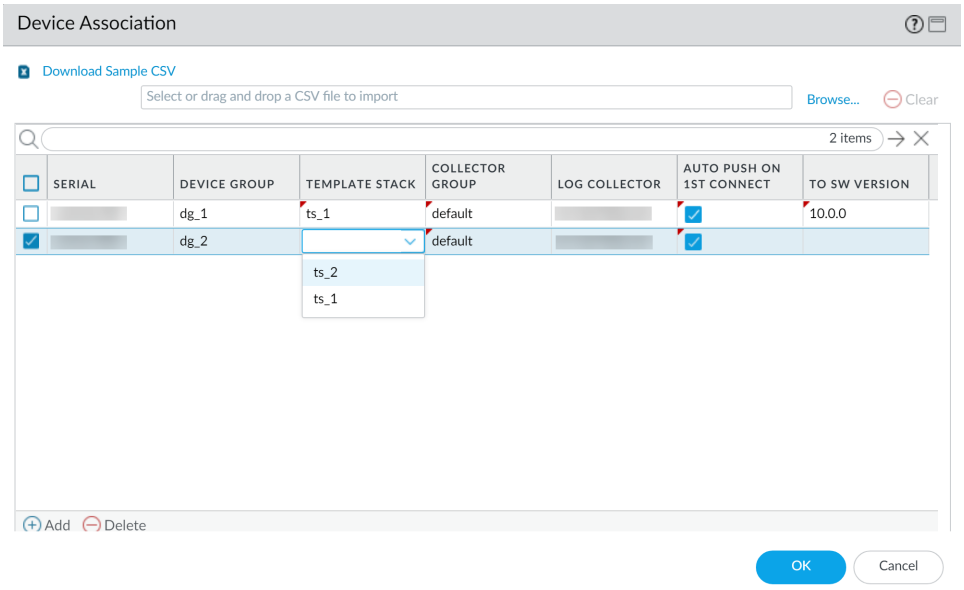
© 2019 Palo Alto Networks, Inc.



4. 根據需要從下拉式清單中為各列指派 **Device Group**（裝置群組）、**Template Stack**（範本堆疊）、**Collector Group**（收集器群組）和 **Log Collector**（日誌收集器）。
5. 啟用 **Auto Push on 1st connect**（首次連線時自動推送）核取方塊，在新裝置成功連線至 Panorama 時，自動推送裝置群組和範本堆疊組態至新裝置。

   Auto Push on 1st connect（首次連線時自動推送）選項僅在執行 *PAN-OS 8.1* 或更高版本的防火牆上受支援。`commit all` 工作從 *Panorama* 執行至運行 *PAN-OS 8.1* 和更新版本的受管理裝置。
6. （選用）在 **To SW Version**（至軟體版本）欄中選取 PAN-OS 發行版本，以便在成功連線到 Panorama 時開始將受管理防火牆自動升級到指定的 PAN-OS 發行版本。

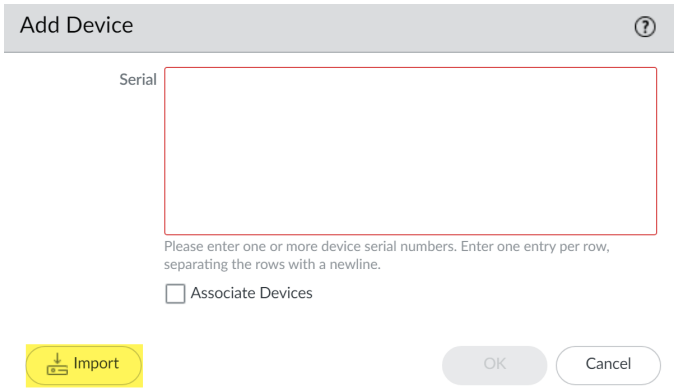
   如果您不想要自動升級受管理防火牆，則將此欄留空。
7. 按一下 **OK**（確定）來新增裝置。



- 透過逗號隔開的值 (CSV) 檔案大量匯入多個防火牆。

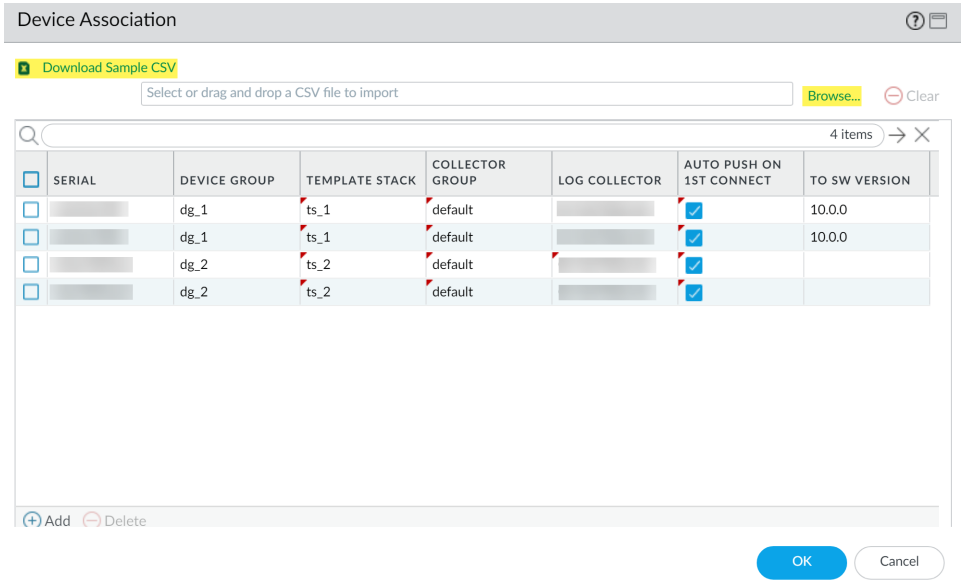
  1. 新增一個新的受管理裝置（**Panorama** > **Managed Devices**（受管理裝置）> **Summary**（摘要））。
  2. 按一下 **Import**（匯入）。

© 2019 Palo Alto Networks, Inc.



3. **Download Sample CSV**（下載範本 **CSV**）並透過您新增的防火牆編輯下載的 CSV 檔案。您可以選擇從 CSV 指派防火牆至裝置群組、範本堆疊、收集器群組和日誌收集器，或僅輸入防火牆序號並從 Web 介面進行指派。在完成編輯後，儲存 CSV。
4. **Browse**（瀏覽）並選取您在之前步驟中編輯的 CSV 檔案。
5. 如未在 CSV 中指派，根據需要，為各列從下拉清單中對防火牆指派 **Device Group**（裝置群組）、**Template Stack**（範本堆疊）、**Collector Group**（收集器群組）和 **Log Collector**（日誌收集器）。
6. 如未在 CSV 中啟用，啟用 **Auto Push on 1st connect**（首次連線時自動推送）核取方塊，在新裝置成功連線至 Panorama 時，自動推送裝置群組和範本堆疊組態至新裝置。
7. （選用）在 **To SW Version**（至軟體版本）欄中選取 PAN-OS 發行版本，以便在成功連線到 Panorama 時開始將受管理防火牆自動升級到指定的 PAN-OS 發行版本。

   如果您不想要自動升級受管理防火牆，則將此欄留空。
8. 按一下 **OK**（確定）來新增裝置。



STEP 3 | （選用）新增 **Tag**（標籤）。標籤可讓您更輕易地從大型清單中找出防火牆；它們可協助您動態地篩選和調整顯示的防火牆清單。例如，如果您新增名為分公司的標籤，即可跨網路篩選所有分公司防火牆。

1. 選擇各防火牆，並按一下 **Tag**（標籤）。
2. 按一下 **Add**（新增），並輸入最多 31 個字元（無空白字元）的字串，然後按一下**OK**（確定）。

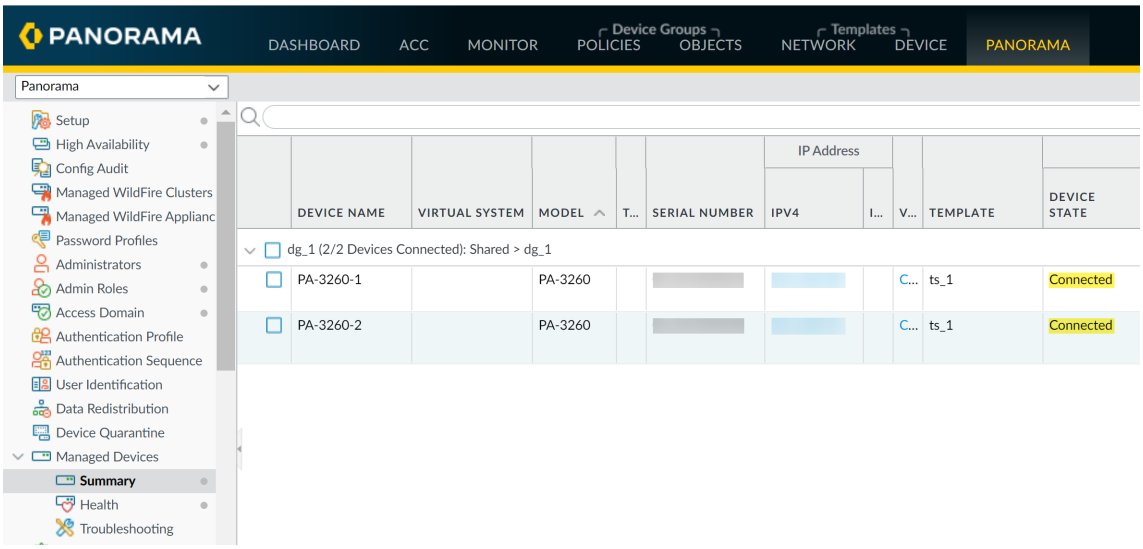
© 2019 Palo Alto Networks, Inc.

STEP 4 | 如果您的部署使用自訂憑證在 Panorama 和受管理的裝置之間驗證，請部署自訂用戶端裝置憑證。如需詳細資訊，請參閱設定使用自訂憑證進行驗證和新增用戶端裝置。

STEP 5 | 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

STEP 6 | 驗證已將防火牆連接至 Panorama。

1. 按一下 **Panorama** > **Managed Devices**（受管理的裝置）> **Summary**（摘要）。
2. 確認每個防火牆的 **Device State**（裝置狀態）為 `Connected`（已連線）。



© 2019 Palo Alto Networks, Inc.

安裝受管理防火牆的裝置憑證

在 PAN-OS 10.0 及更新版本中，您必須在受管理防火牆上安裝裝置憑證以成功驗證受管理防火牆，然後才能使用裝置遙測、IoT 和企業資料遺失防護 (DLP) 等 Palo Alto Networks 雲端服務。您可以安裝一個也可同時安裝多個受管理防火牆的裝置憑證。

若要在本機安裝防火牆裝置憑證，請參閱 Device Certificates（裝置憑證）。

- 安裝受管理防火牆的裝置憑證
- 安裝多個受管理防火牆的裝置憑證

安裝受管理防火牆的裝置憑證

在 PAN-OS 10.0 和更高版本中，您必須從 Panorama 管理伺服器安裝受管理防火牆的裝置憑證。受管理防火牆必須具有網際網路存取權才能成功安裝裝置憑證。

STEP 1 | 註冊 Panorama 及 Palo Alto Networks 客戶支援入口網站 (CSP) 的受管理防火牆。

STEP 2 | 登入 Panorama 網頁介面 以管理員使用者身份。

STEP 3 | 設定網路時間協定 (NTP) 伺服器。

需要 NTP 伺服器驗證裝置憑證到期日，確定裝置憑證未提前到期或失效。

1. 選取 **Device**（裝置）> **Setup**（設定）> **Services**（服務），然後選取 **Template**（範本）。
2. 依據您的平台選取下列其中一項：
   - 針對多個虛擬系統平台，選取 **Global**（全域）並編輯服務區段。
   - 針對單一虛擬系統平台，編輯服務區段。
3. 選取 **NTP** 並輸入主機名稱 `pool.ntp.org` 作為 **Primary NTP Server**（主要 **NTP** 伺服器）或輸入主要 NTP 伺服器的 IP 位址。
4. （選用）輸入 **Secondary NTP Server**（次要 **NTP** 伺服器）位址。
5. （選用）若要驗證 NTP 伺服器的時間更新，為每個伺服器選取下列的 **Authentication Type**（驗證類型）。
   - 無—（預設）停用 NTP 驗證。
   - 對稱金鑰—防火牆使用對稱金鑰交換 (共用密碼）來驗證時間更新。
     - 金鑰 **ID**—輸入金鑰 ID (1-65534)
     - 演算法—選取在 NTP 驗證中要使用的演算法（**MD5** 或 **SHA1**）
6. 按一下 **OK**（確定）儲存組態變更。
7. 選取**Commit**（提交），然後 **Commit and Push**（提交並推送）組態變更到受管理的防火牆。

STEP 4 | 選取 **Panorama** > **Managed Devices**（受管理的裝置）> **Summary**（摘要）並選取受管理防火牆。

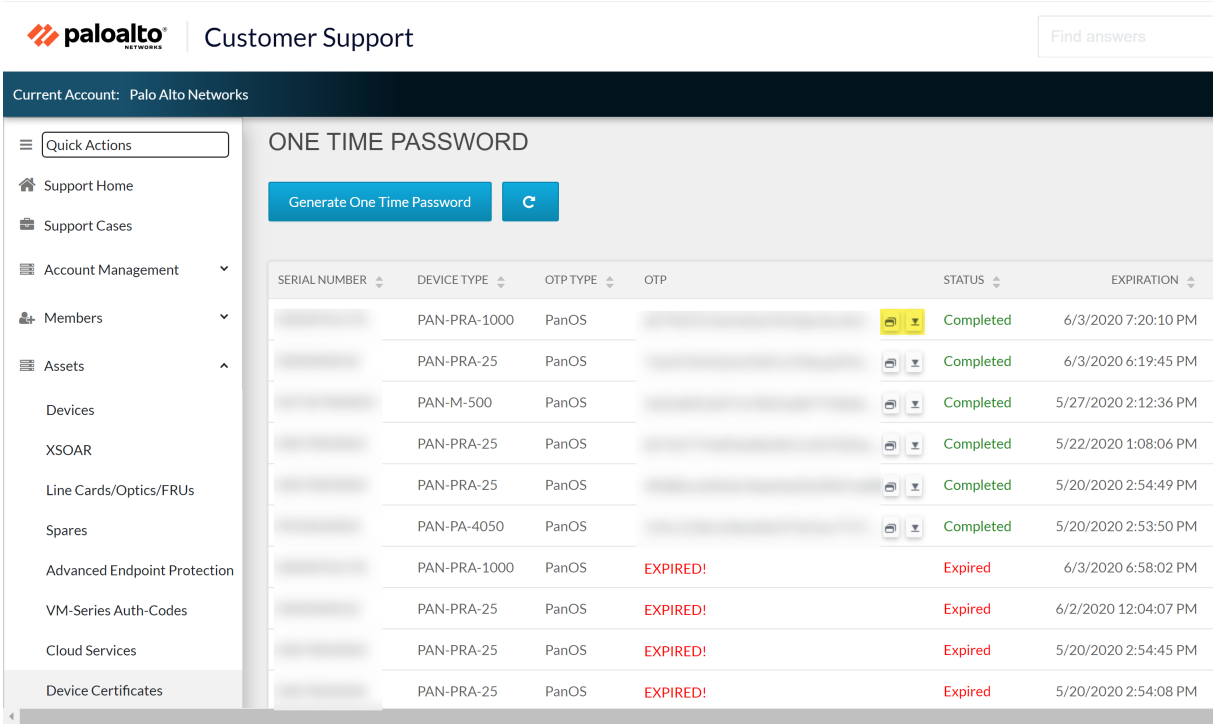
STEP 5 | 選取 **Request OTP From CSP**（向 **CSP** 要求 **OTP**）> **Custom selected devices**（自訂選取的裝置）。

STEP 6 | 複製整個 OTP 要求權杖。

STEP 7 | 產生受管理防火牆的一次性密碼 (OTP)。

© 2019 Palo Alto Networks, Inc.

1. 登入客戶支援入口網站。
2. 選取 **Assets**（資產）> **Device Certificates**（裝置憑證）及 **Generate OTP**（產生 **OTP**）。
3. 對於 **Device Type**（裝置類型），選取 **Generate OTP for Panorama managed firewalls**（產生 **Panorama** 受管理防火牆的 **OTP**）。
4. 貼上在上一步中複製的 OTP 要求，然後 **Generate OTP**（產生 **OTP**）。
5. 按一下 **Done**（完成），然後等待幾分鐘以便成功產生 OTP。如果未顯示新 OTP，您可以重新整理頁面。
6. **Copy to Clipboard**（複製到剪貼簿）或 **Download**（下載）OTP。



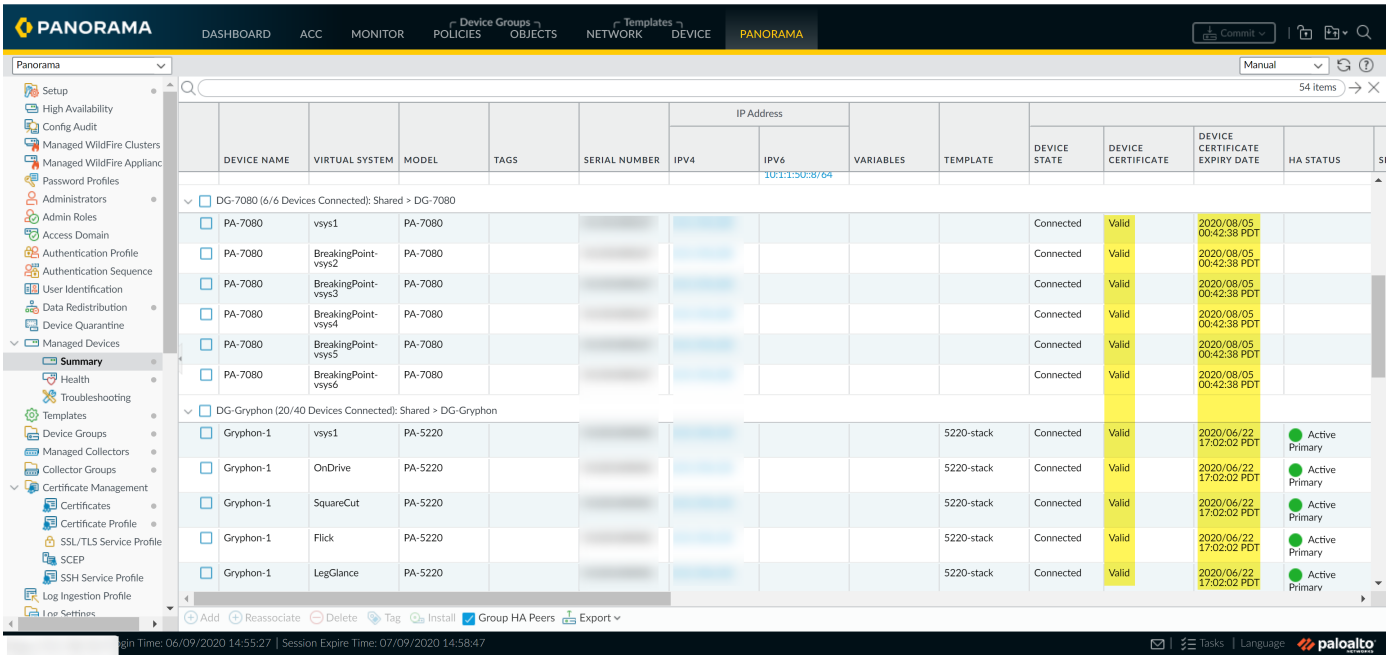
STEP 8 | 登入 Panorama 網頁介面 以管理員使用者身份。

STEP 9 | 選取 **Panorama** > **Managed Devices**（受管理的裝置）> **Summary**（摘要）及 **Upload OTP**（上傳 **OTP**）。

STEP 10 | 貼上您產生的 OTP，然後按一下 **Upload**（上傳）。

STEP 11 | 確認 **Device Certificate**（裝置憑證）欄顯示為 `Valid`（有效），且 **Device Certificate Expiry Date**（裝置憑證到期日期）顯示一個到期日期。

© 2019 Palo Alto Networks, Inc.



安裝多個受管理防火牆的裝置憑證

在 PAN-OS 10.0 和更高版本中，您必須從 Panorama 管理伺服器安裝受管理防火牆的裝置憑證。受管理防火牆必須具有網際網路存取權才能成功安裝裝置憑證。

STEP 1 | 註冊 Panorama 及 Palo Alto Networks 客戶支援入口網站 (CSP) 的受管理防火牆。

STEP 2 | 登入 Panorama 網頁介面 以管理員使用者身份。

STEP 3 | 設定網路時間協定 (NTP) 伺服器。

需要 NTP 伺服器驗證裝置憑證到期日，確定裝置憑證未提前到期或失效。

1. 選取 **Device**（裝置）> **Setup**（設定）> **Services**（服務），然後選取 **Template**（範本）。
2. 依據您的平台選取下列其中一項：
   - 針對多個虛擬系統平台，選取 **Global**（全域）並編輯服務區段。
   - 針對單一虛擬系統平台，編輯服務區段。
3. 選取 **NTP** 並輸入主機名稱 `pool.ntp.org` 作為 **Primary NTP Server**（主要 **NTP** 伺服器）或輸入主要 NTP 伺服器的 IP 位址。
4. （選用）輸入 **Secondary NTP Server**（次要 **NTP** 伺服器）位址。
5. （選用）若要驗證 NTP 伺服器的時間更新，為每個伺服器選取下列的 **Authentication Type**（驗證類型）。
   - 無—（預設）停用 NTP 驗證。
   - 對稱金鑰—防火牆使用對稱金鑰交換 (共用密碼）來驗證時間更新。
     - 金鑰 **ID**—輸入金鑰 ID (1-65534)
     - 演算法—選取在 NTP 驗證中要使用的演算法（**MDS** 或 **SHA1**）
6. 按一下 **OK**（確定）儲存組態變更。
7. 選取**Commit**（提交），然後 **Commit and Push**（提交並推送）組態變更到受管理的防火牆。

STEP 4 | 選取 **Panorama** > **Managed Devices**（受管理的裝置）> **Summary**（摘要）。

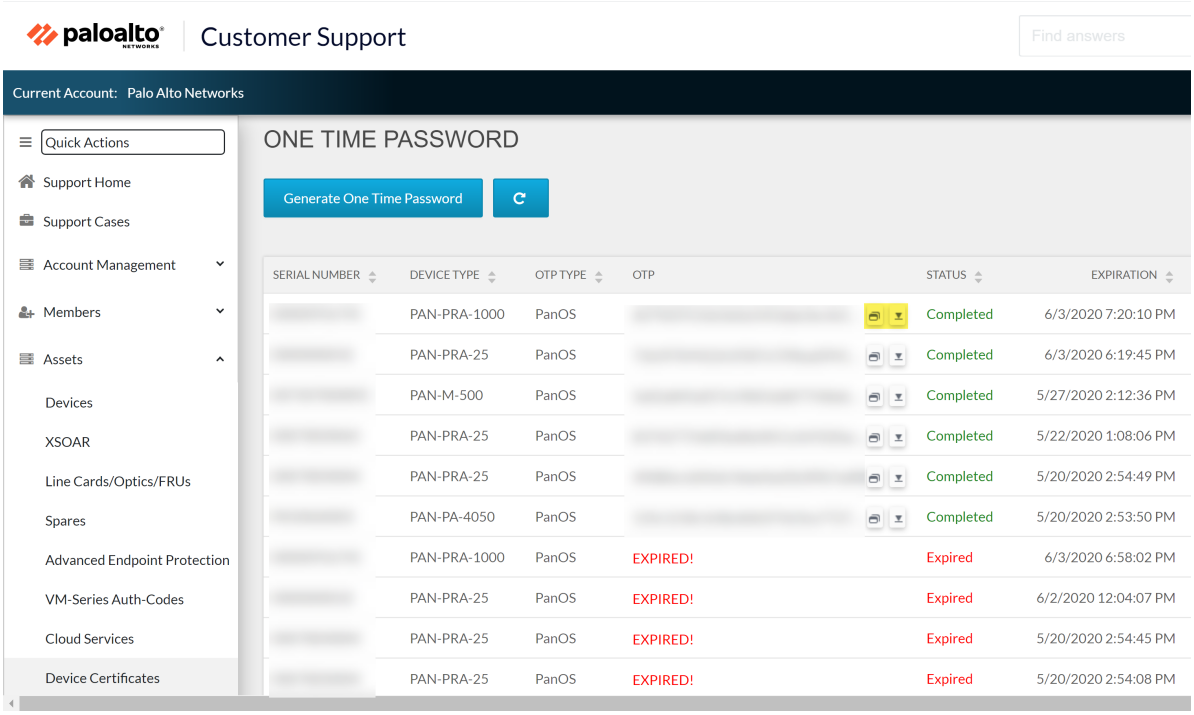
© 2019 Palo Alto Networks, Inc.

STEP 5 | 選取 **Request OTP From CSP**（向 **CSP** 要求 **OTP**）> **Select all devices without a certificate**（選取沒有憑證的所有裝置）。

STEP 6 | 複製整個 OTP 要求權杖。

STEP 7 | 產生受管理防火牆的一次性密碼 (OTP)。

1. 登入客戶支援入口網站。
2. 選取 **Assets**（資產）> **Device Certificates**（裝置憑證）及 **Generate OTP**（產生 **OTP**）。
3. 對於 **Device Type**（裝置類型），選取 **Generate OTP for Panorama managed firewalls**（產生 **Panorama** 受管理防火牆的 **OTP**）。
4. 貼上在上一步中複製的 OTP 要求，然後 **Generate OTP**（產生 **OTP**）。
5. 按一下 **Done**（完成），然後等待幾分鐘以便成功產生 OTP。如果未顯示新 OTP，您可以重新整理頁面。
6. **Copy to Clipboard**（複製到剪貼簿）或 **Download**（下載）OTP。



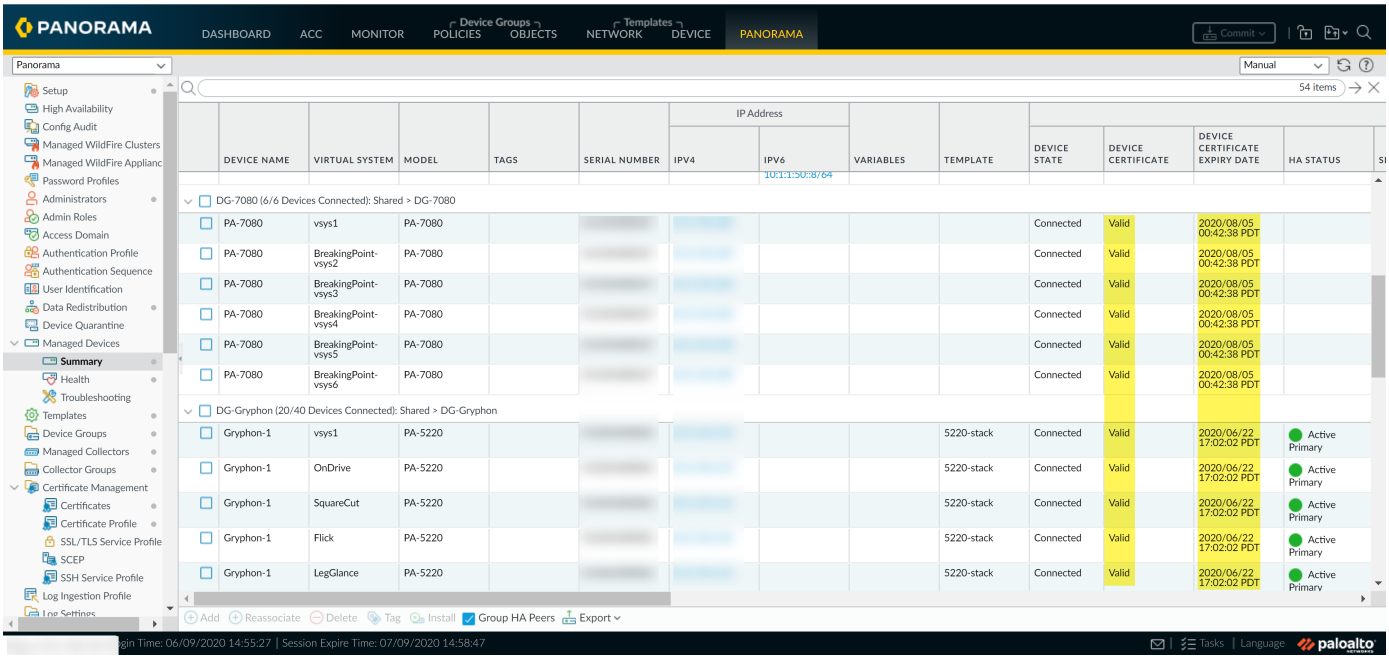
STEP 8 | 登入 Panorama 網頁介面 以管理員使用者身份。

STEP 9 | 選取 **Panorama** > **Managed Devices**（受管理的裝置）> **Summary**（摘要）及 **Upload OTP**（上傳 **OTP**）。

STEP 10 | 貼上您產生的 OTP，然後按一下 **Upload**（上傳）。

STEP 11 | 確認 **Device Certificate**（裝置憑證）欄顯示為 `Valid`（有效），且 **Device Certificate Expiry Date**（裝置憑證到期日期）顯示一個到期日期。

© 2019 Palo Alto Networks, Inc.



© 2019 Palo Alto Networks, Inc.

設定零接觸佈建

設定零接觸佈建 (ZTP)，藉由自動化新的受管理防火牆安裝，無需網路管理員手動佈建防火牆，從而簡化防火牆初始部署。

要成功利用 *ZTP* 服務，請在升級到 *PAN-OS 10.0.0* 或更高版本之前，安裝原廠預設 *PAN-OS* 版本的 *ZTP* 防火牆。

PAN-OS 10.0.1 和更新版本支援 *ZTP*。

- ZTP 概要
- 安裝 ZTP 外掛程式
- 設定 ZTP 安裝程式管理員帳戶
- 新增 ZTP 防火牆至 Panorama
- 使用 CLI 以進行 ZTP 工作
- 解除安裝 ZTP 外掛程式

ZTP 概要

進一步瞭解零接觸佈建 (ZTP) 外掛程式及其組態元素。

- 關於 ZTP
- ZTP 組態元素

關於 *ZTP*

零接觸佈建 (ZTP) 旨在簡化及自動化 Panorama™ 管理伺服器上新防火牆的安裝。ZTP 允許網路管理員將受管理的防火牆直接運送至分公司，且在 ZTP 防火牆成功連線至 Palo Alto Networks ZTP 服務後，自動將防火牆新增至 Panorama™ 管理伺服器，從而簡化防火牆的初始部署流程。由於無需 IT 管理員手動佈建受管理的新防火牆，所以當企業在分公司部署新防火牆時，可以節省時間及資源。成功安裝後，Panorama 將提供設定及管理您的 ZTP 組態和防火牆的方法。

檢閱並訂閱 ZTP 服務狀態事件，以獲得有關排程維護時間、中斷和因應措施的通知。

下列執行 PAN-OS 9.1.3 和更新版本的 ZTP 防火牆上支援 ZTP：

- PA-220-ZTP 及 PA-220R-ZTP
- PA-820-ZTP 及 PA-850-ZTP
- PA-3220-ZTP、PA-3250-ZTP 及 PA-3260-ZTP

ZTP 組態元素

以下元素一起運作，透過使用 ZTP 服務將防火牆自動新增到 Panorama 管理伺服器，讓您能夠快速安裝新部署的 ZTP 受管理防火牆。

- **ZTP Plugin**（**ZTP** 外掛程式）—ZTP 外掛程式允許 Panorama 連線到 ZTP 服務，並索取 ZTP 防火牆以簡化安裝。
- 客戶入口網站 **(CSP)**—Palo Alto Networks 客戶入口網站用於註冊您的 Panorama 以連線至 CSP，從而自動註冊新增的 ZTP 防火牆。
- **One-time Password**（一次性密碼，**OTP**）—一次性密碼由 Palo Alto Networks 提供，用於在 Panorama 上擷取和安裝憑證，以便其與 CSP 和 ZTP 服務通訊。

© 2019 Palo Alto Networks, Inc.

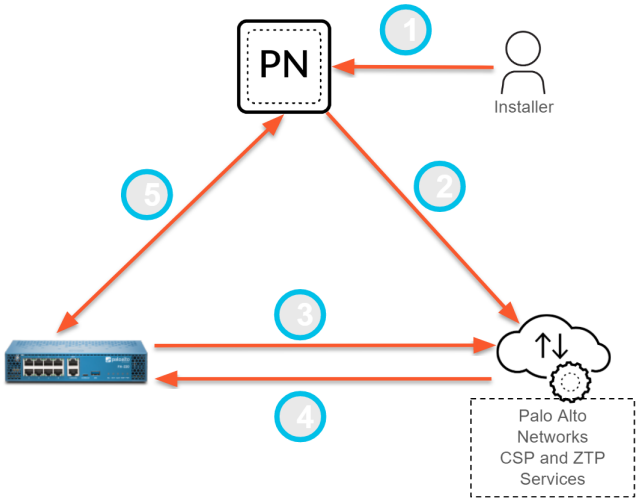
- 安裝程式—使用 `installeradmin` 管理員角色所建立的管理員使用者，用於安裝 ZTP 防火牆。此管理員使用者具有存取 Panorama 網頁介面的有限權限，僅允許在 CSP 及 Panorama 上輸入 ZTP 防火牆序號及索取金鑰，以註冊防火牆。安裝程式管理員可以在 Panorama 上建立或使用遠端驗證建立，例如 RADIUS、SAML 或 TACACS+。
- 索取金鑰—貼在 ZTP 防火牆上的實體八位數字金鑰，用於向 CSP 註冊 ZTP 防火牆。
- **To-SW-Version**（至軟體版本）—指定 ZTP 防火牆的 PAN-OS 軟體版本（**Panorama** > **Managed Devices**（受管理的裝置）> **Summary**（摘要））。選取目標 PAN-OS 版本，如果防火牆執行的版本比指定版本更舊，則防火牆開始升級循環，直到成功安裝目標 PAN-OS 版本。

Panorama 僅能管理 *PAN-OS* 版本與 *Panorama* 相同或更舊的防火牆。

在 Panorama 上成功安裝 ZTP 外掛程式並向 ZTP 服務註冊 Panorama 後，ZTP 安裝程序將按以下方式繼續：

1. 安裝程式或 IT 管理員透過使用防火牆序號和索取金鑰將防火牆新增到 Panorama，從而註冊 ZTP 防火牆。
2. Panorama 向 CSP 註冊防火牆。成功註冊防火牆後，防火牆將與 ZTP 服務中與 Panorama 相同的 ZTP 租戶關聯。

   向 ZTP 服務註冊成功的 ZTP 防火牆將自動新增為 Panorama 上的受管理防火牆（**Panorama** > **Managed Devices**（受管理的裝置））。
3. 當防火牆連線到網際網路時，ZTP 防火牆要求 CSP 提供裝置憑證以連線到 ZTP 服務。
4. ZTP 服務將 Panorama IP 或 FQDN 推送到 ZTP 防火牆。
5. ZTP 防火牆連線到 Panorama，且裝置群組和範本設定將被從 Panorama 推送到 ZTP 防火牆。



安裝 ZTP 外掛程式

在您的 Panorama™ 管理伺服器上安裝 ZTP 外掛程式以向 ZTP 服務註冊 Panorama，從而簡化 ZTP 防火牆的安裝。

如果您的 Panorama 為高可用性 (HA) 設定，則安裝 ZTP 外掛程式，並向 ZTP 服務註冊兩個 Panorama HA 對等。

- 在 Panorama 上安裝 ZTP 外掛程式
- 向 ZTP 服務註冊 Panorama

在 *Panorama* 上安裝 *ZTP* 外掛程式

在您的 Panorama 管理伺服器上安裝 ZTP 外掛程式，從而簡化 ZTP 防火牆的安裝和管理。

© 2019 Palo Alto Networks, Inc.

STEP 1 | 安裝 Panorama 裝置憑證。

STEP 2 | 以超級使用者或 Panorama 管理員身分登入 Panorama Web 介面以取得 Panorama 外掛程式存取權（**Panorama** > **Plugins**（外掛程式））。

STEP 3 | 選取 **Panorama** > **Plugins**（外掛程式），然後搜尋 `ztp` 外掛程式。

STEP 4 | **Download**（下載）及 **Install**（安裝）最新版本 ZTP 外掛程式。

向 *ZTP* 服務註冊 *Panorama*

向 ZTP 服務註冊 Panorama™ 管理伺服器以用於新的及現有部署。

- 向 ZTP 服務註冊 Panorama 以用於新部署
- 向 ZTP 服務註冊 Panorama 以用於現有部署

向 **ZTP** 服務註冊 **Panorama** 以用於新部署

在 Panorama™ 管理伺服器上安裝 ZTP 外掛程式後，您必須向 ZTP 服務註冊 Panorama，才能透過 ZTP 服務使 ZTP 防火牆與 Panorama 相關聯。在新 ZTP 部署的註冊程序過程中，會自動產生將您的 ZTP 防火牆連線至 ZTP 服務所需的裝置群組及範本設定。自動產生裝置群組及範本後，您必須將您的 ZTP 防火牆新增至裝置群組及範本，使其首次連線至 Panorama 後，可以與 ZTP 服務連線。

STEP 1 | 安裝 Panorama 裝置憑證。

STEP 2 | 登入 Palo Alto Networks 客戶支援入口網站 (CSP)。

STEP 3 | 使您的 Panorama 與 Palo Alto Networks CSP 上的 ZTP 服務相關聯。

ZTP 服務支援與至多兩個 Panoramas 相關聯，但其必須在高可用性 (HA) 組態中。如果 Panorama 不在 HA 組態中，則僅可與一個 Panoramas 相關聯。

1. 選取 **Assets**（資產）> **ZTP Service**（**ZTP** 服務）及 **Associate Panorama(s)**（關聯 **Panorama**）。
2. 選取管理您的 ZTP 防火牆的 Panorama 序號。
3. （僅限 HA）選取 Panorama HA 對等的序號。
4. 按一下 **OK**（確定）。

STEP 4 | 登入 Panorama 網頁介面。

STEP 5 | 選取 **Panorama** > **Zero Touch Provisioning**（零接觸佈建）> **Setup**（設定）並且編輯 **General**（一般）ZTP 設定。

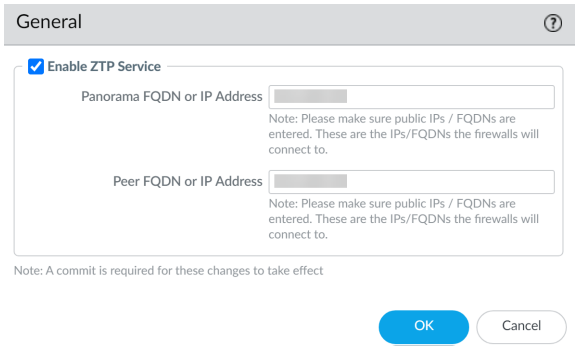
STEP 6 | 向 ZTP 服務註冊 Panorama。

1. 啟用 **ZTP** 服務。
2. 輸入 **Panorama FQDN or IP Address**（**Panorama FQDN** 或 **IP** 位址）。

   這是安裝 ZTP 外掛程式以及 CSP 推送到 ZTP 防火牆的 Panorama 的 FQDN 或公用 IP 位址。
3. （僅限 HA）輸入 **Peer FQDN or IP Address**（對等 **FQDN** 或 **IP** 位址）。

   這是發生容錯移轉時安裝 ZTP 外掛程式以及 CSP 推送到 ZTP 防火牆的 Panorama 對等的 FQDN 或公用 IP 位址。
4. 按一下 **OK**（確定）儲存組態變更。

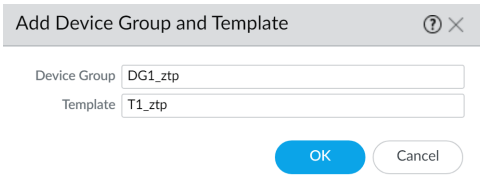
© 2019 Palo Alto Networks, Inc.



STEP 7 | 建立預設的裝置群組及範本，以自動產生將您的 ZTP 防火牆連線至 Panorama 所需的組態。

新增裝置群組及範本會自動產生含有預設組態的裝置群組及範本，以使 Panorama 與 ZTP 防火牆連線。

1. **Add Device Group and Template**（新增裝置群組與範本）。
2. 輸入 **Device Group**（裝置群組）名稱。
3. 輸入 **Template**（範本）名稱。
4. 按一下 **OK**（確定）儲存組態變更。



STEP 8 | 將您的 ZTP 防火牆新增至上一步指定的裝置群組與範本。

1. 選取 **Panorama** > **Device Groups**（裝置群組），並選取自動建立的裝置群組。
2. 選取 ZTP **Devices**（裝置）。
3. 按一下 **OK**（確定）儲存組態變更。
4. 選取 **Panorama** > **Templates**（範本）和 **Add Stack**（新增堆疊）。
5. 在 **Templates**（範本）區段，**Add**（新增）自動產生的範本。
6. 選取 ZTP **Devices**（裝置）。
7. 按一下 **OK**（確定）儲存組態變更。

STEP 9 | 確認已成功產生所需的裝置群組與範本組態。

1. 選取 **Network**（網路）> **Interfaces**（介面）> **Ethernet**（乙太網路），並且選取在上一步建立的 **Template**（範本）。
2. 確認 `ethernet1/1` 設有 IP 位址、虛擬路由器及安全性區域。
3. 選取 **Network**（網路）> **Interfaces**（介面）> **Loopback**（回送），並且選取在上一步建立的 **Template**（範本）。
4. 確認已成功建立 `loopback.900` 介面。
5. 選取 **Policies**（原則）> **Security**（安全性）> **Pre Rules**（預先規則），並且選取在上一步建立的 **Device Group**（裝置群組）。
6. 確認已成功建立 `rule1`。
7. 選取 **Policies**（原則）> **NAT** > **Pre Rules**（預先規則），並且選取在上一步建立的 **Device Group**（裝置群組）。
8. 確認已成功建立 `ztp-nat`。

STEP 10 | 視需要修改裝置群組與範本。

© 2019 Palo Alto Networks, Inc.

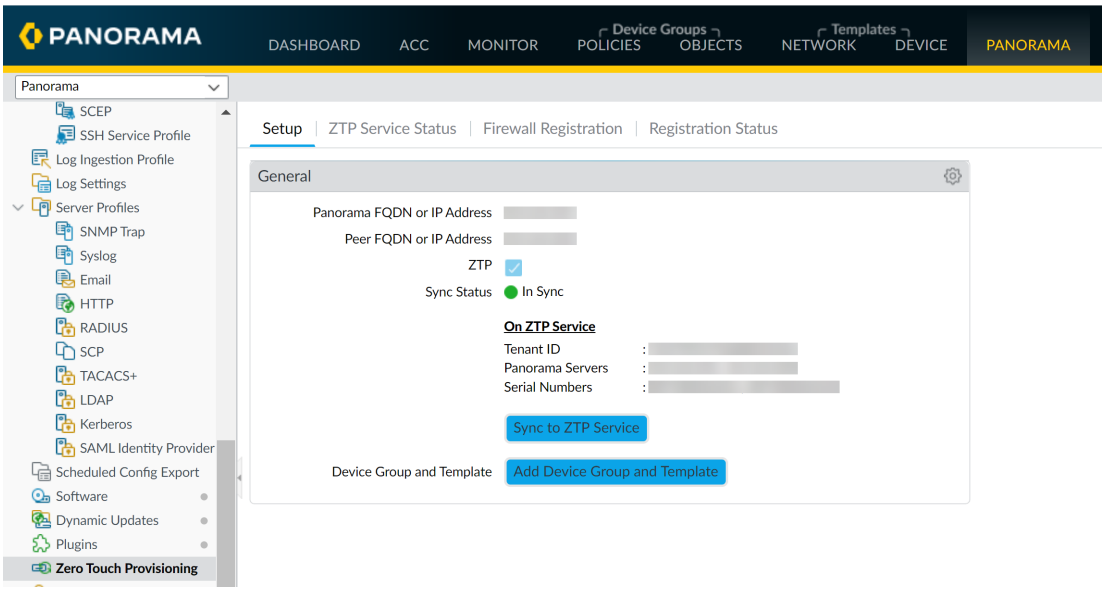
建立並設定新或現有的裝置群組及範本以完成部署。

當考量您範本堆疊中的 device group hierarchy（裝置群組階層）及 template priority（範本優先順序）時，請確定含有使 ZTP 防火牆與 Panorama 能夠通訊之必要 ZTP 組態的裝置群組及範本具有較高優先順序，使得在組態有衝突的情況中，此組態不會被覆寫。

切勿修改 *ethernet1/1* 介面、*loopback.900* 回送介面、*rule1* 安全性原則規則或 *ztp-nat* NAT 原則規則的 *IP* 位址、虛擬路由器及安全性區域。這些是將您的 *ZTP* 防火牆連線至 *Panorama* 所需的組態。

STEP 11 | 選取 **Commit**（認可）和 **Commit to Panorama**（向 **Panorama** 認可）。

STEP 12 | **Sync to ZTP Service**（同步至 **ZTP** 服務），並且確認 Panorama 同步狀態顯示為 **In Sync**（同步）。



向 **ZTP** 服務註冊 **Panorama** 以用於現有部署

在 Panorama™ 管理伺服器上安裝 ZTP 外掛程式後，您必須向 ZTP 服務註冊 Panorama，才能使 ZTP 服務將防火牆與 Panorama 相關聯。在註冊程序過程中，將您的 ZTP 防火牆新增至含有必要 ZTP 組態的裝置群組及範本中，以在 ZTP 服務首次連線至 Panorama 後，使 ZTP 防火牆與 ZTP 服務連線。

STEP 1 | 安裝 Panorama 裝置憑證。

STEP 2 | 登入 Palo Alto Networks 客戶支援入口網站 (CSP)。

STEP 3 | 使您的 Panorama 與 Palo Alto Networks CSP 上的 ZTP 服務相關聯。

ZTP 服務支援與至多兩個 Panoramas 相關聯，但其必須在高可用性 (HA) 組態中。如果 Panorama 不在 HA 組態中，則僅可與一個 Panoramas 相關聯。

1. 選取 **Assets**（資產）> **ZTP Service**（**ZTP** 服務）及 **Modify Association**（修改關聯性）。
2. 選取管理您的 ZTP 防火牆的 Panorama 序號。
3. （僅限 HA）選取 Panorama HA 對等的序號。
4. 按一下 **OK**（確定）。

STEP 4 | 登入 Panorama 網頁介面。

© 2019 Palo Alto Networks, Inc.

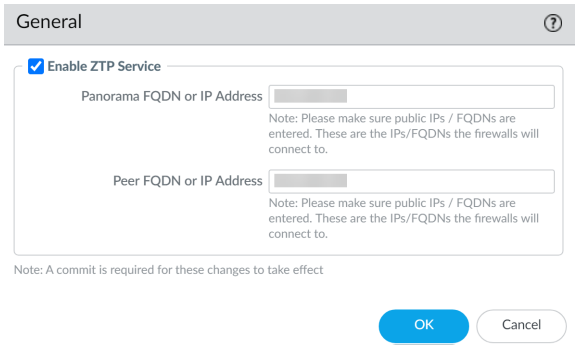
STEP 5 | 選取 **Panorama** > **Zero Touch Provisioning**（零接觸佈建） > **Setup**（設定）並且編輯 **General**（一般） ZTP 設定。

STEP 6 | 向 ZTP 服務註冊 Panorama。

1. 啟用 **ZTP** 服務。
2. 輸入 **Panorama FQDN or IP Address**（**Panorama FQDN** 或 **IP** 位址）。

   這是安裝 ZTP 外掛程式以及 CSP 推送到 ZTP 防火牆的 Panorama 的 FQDN 或公用 IP 位址。
3. （僅限 HA）輸入 **Peer FQDN or IP Address**（對等 **FQDN** 或 **IP** 位址）。

   這是發生容錯移轉時安裝 ZTP 外掛程式以及 CSP 推送到 ZTP 防火牆的 Panorama 對等的 FQDN 或公用 IP 位址。
4. 按一下 **OK**（確定）儲存組態變更。



STEP 7 | 將您的 ZTP 防火牆新增至含有必要 ZTP 組態的裝置群組及範本。

1. 選取 **Panorama** > **Device Groups**（裝置群組），並且選取將含有必要 ZTP 組態的裝置群組。
2. 選取 ZTP **Devices**（裝置）。
3. 按一下 **OK**（確定）儲存組態變更。
4. 選取 **Panorama** > **Templates**（範本）並且選取包含將具有必要 ZTP 組態的範本的範本堆疊。
5. 選取 ZTP **Devices**（裝置）。
6. 按一下 **OK**（確定）儲存組態變更。

STEP 8 | 視需要修改裝置群組與範本。

當考量您範本堆疊中的 device group hierarchy（裝置群組階層）及 template priority（範本優先順序）時，請確定含有使 ZTP 防火牆與 Panorama 能夠通訊之必要 ZTP 組態的裝置群組及範本具有較高優先順序，使得在組態有衝突的情況中，此組態不會被覆寫。

1. 設定 Ethernet1/1 介面。
   1. 選取 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路），選取含有 ZTP 組態的 **Template**（範本）並且選取 **ethernet1/1**。
   2. 對於 **Interface Type**（介面類型），選取 **Layer3**。
   3. 選取 **Config**（組態）並且設定 **Virtual Router**（虛擬路由器）且將 **Security Zone**（安全性地區）設定為 **Untrust**（不受信任）。
   4. 選取 **Ipv4**，而對於 **Type**（類型），選取 **DHCP Client**（**DHCP** 用戶端）。

      ZTP 防火牆需要 *DHCP* 用戶端才能與 *ZTP* 服務通訊。
   5. 按 **OK**（確定）儲存組態變更。
2. 建立回送介面

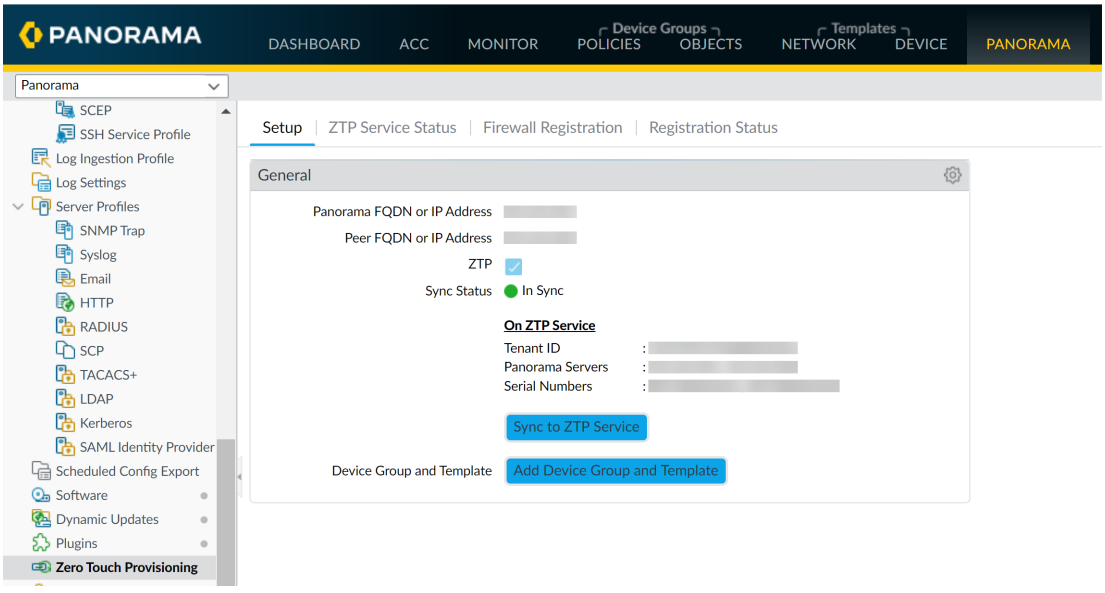
© 2019 Palo Alto Networks, Inc.

1. 選取 **Network**（網路）> **Interfaces**（介面）> **Loopback**（回送），選取含有 ZTP 組態的 **Template**（範本）並且 **Add**（新增）回送介面。
2. 對於 **Interface Name**（介面名稱），輸入 `loopback` 並且輸入 `900` 尾碼。
3. 選取 **Config**（組態），選取 **Virtual Router**（虛擬路由器）且將 **Security Zone**（安全性地區）設定為 **Trust**（受信任）。
4. 按 **OK**（確定）儲存組態變更。

3. 建立安全性原則規則以允許 ZTP 防火牆與 Panorama 通訊。
   1. 選取 **Policies**（原則）> **Security**（安全性）> **Pre Rules**（預先規則），選取含有 ZTP 原則規則的 **Device Group**（裝置群組），並且 **Add**（新增）新規則。
   2. 輸入原則規則的描述性 **Name**（名稱）。
   3. 選取 **Source**（來源）> **Source Zone**（來源區域）並且 **Add**（新增）**Trust**（信任）區域。
   4. 選取 **Destination**（目的地）> **Destination Zone**（目的地區域）並且 **Add**（新增）**Untrust**（不受信任）區域。
   5. 選取 **Action**（動作）> **Action Settings**（動作設定）> **Action**（動作）並且選取 **Allow**（允許）。
4. 建立 NAT 原則規則以允許 ZTP 防火牆與 Panorama 通訊。
   1. 選取 **Policies**（原則）> **NAT** > **Pre Rules**（預先規則），選取含有 ZTP 原則規則的 **Device Group**（裝置群組），並且 **Add**（新增）新規則。
   2. 輸入原則規則的描述性 **Name**（名稱）。
   3. 選取 **Original Packet**（原始封包）並設定以下選項：
      1. 對於 **Source Zone**（來源區域），**Add**（新增）**Trust**（信任）區域。
      2. 對於 **Destination Zone**（目的地區域），選取 **Untrust**（不受信任）區域。
      3. 對於 **Destination Interface**（目的地介面），選取 **ethernet1/1** 介面。
   4. 按一下 **OK**（確定）儲存組態變更。

STEP 9 | 選取 **Commit**（認可）和 **Commit to Panorama**（向 **Panorama** 認可）。

STEP 10 | **Sync to ZTP Service**（同步至 **ZTP** 服務），並且確認 Panorama 同步狀態顯示為 `In Sync`（同步）。



© 2019 Palo Alto Networks, Inc.

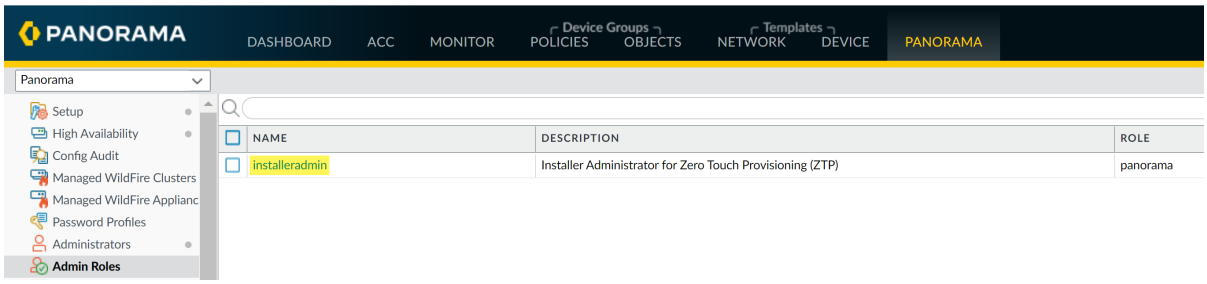
設定 ZTP 安裝程式管理員帳戶

ZTP 安裝程式管理員使用者是為非 IT 員工或安裝承包商所建立的管理員帳戶，以安裝新的 ZTP 防火牆。安裝程式管理員使用自動建立的 `installeradmin` 管理員角色，限制對 Panorama 網頁介面的可視性，並且僅允許安裝程式在 Panorama 上輸入 ZTP 防火牆索取金鑰及序號的能力。

STEP 1 | 登入 Panorama 網頁介面。

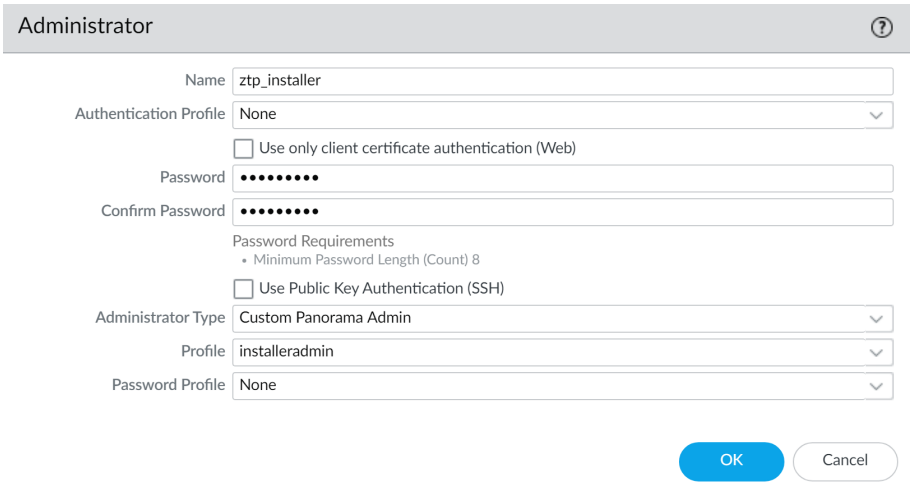
STEP 2 | 選取 **Panorama** > **Admin Roles**（管理員角色）並且確認已建立 **`installeradmin`** 管理員角色。

您成功在 Panorama 上安裝 ZTP 外掛程式後，會自動建立 `installeradmin`。



STEP 3 | 設定 ZTP 安裝程式管理員使用者。

1. 選取 **Panorama** > **Administrators**（管理員），然後 **Add**（新增）新的管理員使用者。
2. 輸入 ZTP 安裝程式管理員使用者的描述性 **Name**（名稱）。
3. 輸入安全的 **Password**（密碼）并 **Confirm Password**（確認密碼）。
4. 對於 **Administrator Type**（管理員類型），選取 **Custom Panorama Admin**（自訂 Panorama 管理員）。
5. 對於 **Profile**（設定檔），選取 **installeradmin**
6. 按一下 **OK**（確定）儲存組態變更。



STEP 4 | 按一下 **Commit**（提交）和 **Commit to Panorama**（提交至 **Panorama**）。

新增 ZTP 防火牆至 Panorama

您可以新增一個或匯入多個 ZTP 防火牆至 Panorama™ 管理伺服器。

- 新增 ZTP 防火牆至 Panorama

© 2019 Palo Alto Networks, Inc.

- 匯入多個 ZTP 防火牆至 Panorama

新增 *ZTP* 防火牆至 *Panorama*

以超級使用者、Panorama 管理員或 ZTP 安裝程式管理員身份登入 Panorama™ 管理伺服器的網頁介面，以新增 ZTP 防火牆至 Panorama。若要新增 ZTP 防火牆，您必須輸入 Palo Alto Networks 所提供的防火牆序號和索取金鑰，然後向 ZTP 服務註冊防火牆。註冊防火牆意味著防火牆將成為客戶支援入口網站中您帳戶的資產，並且允許 ZTP 服務將防火牆與 Panorama 相關聯。

在新增 *ZTP* 防火牆到 *Panorama* 時，在步驟 4 中驗證防火牆已成功新增到 *Panorama* 之前，不要在 *ZTP* 防火牆上執行任何提交。在 *ZTP* 防火牆上執行本機提交會停用 *ZTP* 功能並導致無法成功將防火牆新增到 *Panorama*。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 新增 ZTP 防火牆至 Panorama。

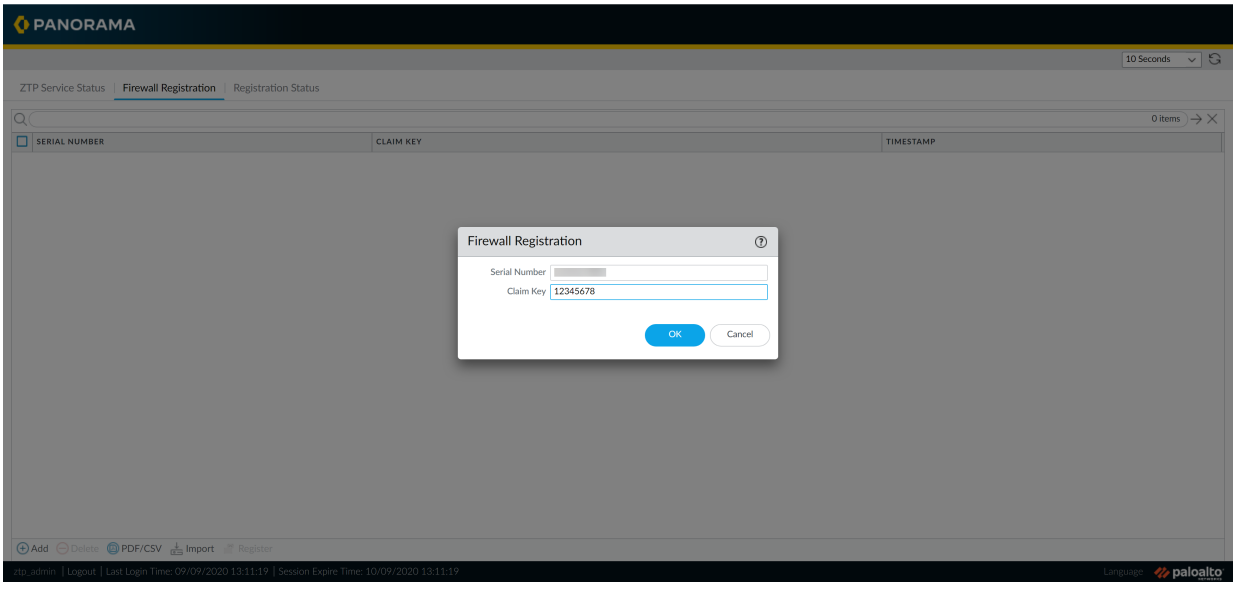
您必須連線 *ZTP* 防火牆上的 *Eth1/1* 介面，才能向 *CSP* 成功註冊 *ZTP* 防火牆，並推送原則和網路設定。

1. 選取 **Firewall Registration**（防火牆註冊）及 **Add**（新增）新的 ZTP 防火牆。
2. 輸入 ZTP 防火牆的序號。
3. 輸入 Palo Alto Networks 所提供的 ZTP 防火牆的索取金鑰。

   八位數的索取金鑰印刷在您從 Palo Alto Networks 收到的 ZTP 防火牆背面上貼的實體標籤上。



4. 按一下 **OK**（確定）儲存組態變更。



STEP 3 | 註冊 ZTP 防火牆。

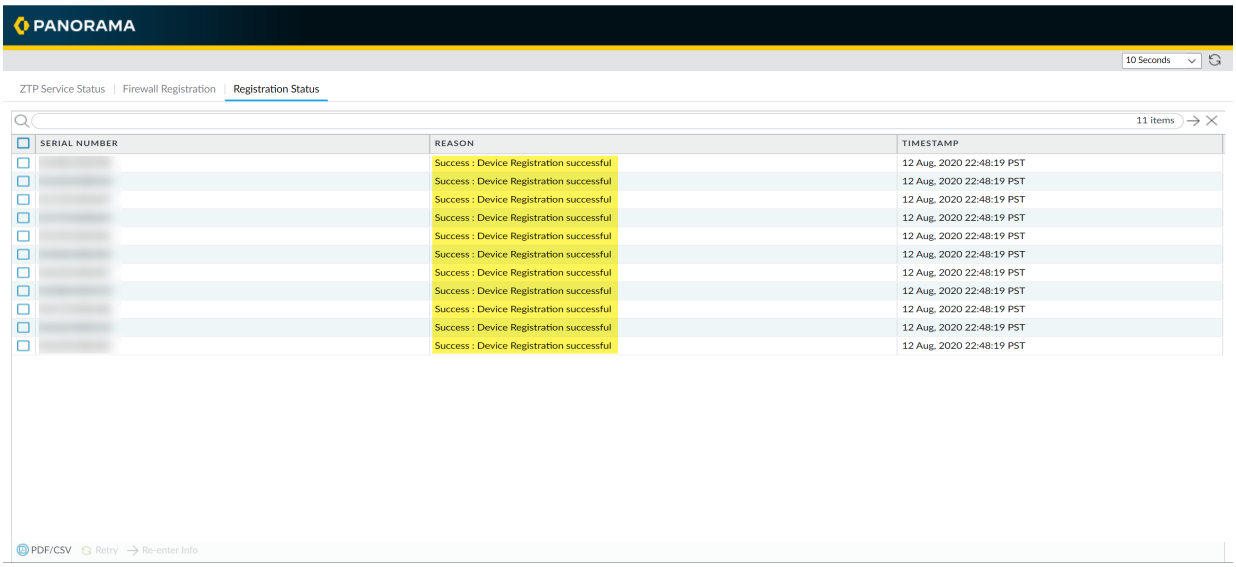
© 2019 Palo Alto Networks, Inc.

1. 選取新增的 ZTP 防火牆並并 **Register**（註冊）防火牆。
2. 出現提示時，按一下 **Yes**（是）以確認註冊 ZTP 防火牆。

STEP 4 | 確認已成功向 CSP 註冊防火牆。

必須向 *CSP* 成功註冊防火牆才能成功獲得裝置憑證。

1. 選取 **Registration Status**（註冊狀態）並確認已成功向 CSP 註冊 ZTP 防火牆。



2. 登入 Panorama 網頁介面 使用管理員認證。
3. 選取 **Panorama** > **Managed Devices**（受管理的裝置）> **Summary**（摘要），並確認 ZTP 防火牆已成功新增為受管理的防火牆。

務必確定 *To SW Version*（至軟體版本）欄設定為正確的 *PAN-OS* 版本，使防火牆不會無意地升級或降級。僅 *PAN-OS 10.0.1* 和更新版本支援 *ZTP* 功能。此外，*PAN-OS* 版本必須與 *Panorama* 上執行的 *PAN-OS* 版本相同或是較舊版本。

如需詳細資訊，請參閱升級 ZTP 防火牆。

STEP 5 | 新增 ZTP 防火牆至裝置群組及範本堆疊。

您必須新增 ZTP 防火牆至裝置群組及範本堆疊才能讓您的防火牆顯示為 `Connected`（已連線），以便推送原則及網路設定。

1. 登入 Panorama 網頁介面 使用管理員認證。
2. 選取 **Panorama** > **Device Groups**（裝置群組），新增一個裝置群組，然後新增 ZTP 防火牆到該裝置群組。

   Add a device group（新增裝置群組）以建立及設定新的裝置群組，以包含您的 ZTP 防火牆的原則物件及規則。
3. 選取 **Panorama** > **Templates**（範本），設定範本堆疊，然後將 ZTP 防火牆新增到範本堆疊。

   Configure a template stack（設定範本堆疊）以建立及設定新的範本堆疊，以包含您的 ZTP 防火牆的網路組態。

© 2019 Palo Alto Networks, Inc.

匯入多個 *ZTP* 防火牆至 *Panorama*

以超級使用者、Panorama 管理員或 ZTP 安裝程式管理員身份登入 Panorama™ 管理伺服器的網頁介面，以匯入多個 ZTP 防火牆至 Panorama。若要匯入多個 ZTP 防火牆，您必須匯入 Palo Alto Networks 所提供的 ZTP 防火牆序號及索取金鑰的 CSV 檔案，然後向 ZTP 服務註冊防火牆。註冊防火牆意味著防火牆將成為客戶支援入口網站中您帳戶的資產，並且允許 ZTP 服務將防火牆與 Panorama 相關聯。

在新增 *ZTP* 防火牆到 *Panorama* 時，在步驟 5 中驗證防火牆已成功新增到 *Panorama* 之前，不要在 *ZTP* 防火牆上執行任何提交。在 *ZTP* 防火牆上執行本機提交會停用 *ZTP* 功能並導致無法成功將防火牆新增到 *Panorama*。

STEP 1 | 蒐集您的 ZTP 防火牆序號及索取金鑰。

八位數的索取金鑰印刷在您從 Palo Alto Networks 收到的 ZTP 防火牆背面上貼的實體標籤上。



STEP 2 | 建立含有 ZTP 防火牆序號及索取金鑰的 CSV 檔案。第一欄必須含有序號，第二欄必須含有該防火牆的對應索取金鑰。請參閱下列範例。

	A	B
1	Serial Number	Claim Key
2	abcd1234	123456789
3	xyz7890	987654321

STEP 3 | 匯入 ZTP 防火牆至 Panorama。

您必須連線 *ZTP* 防火牆上的 *Eth1/1* 介面，才能向 *CSP* 成功註冊 *ZTP* 防火牆，並推送原則和網路設定。

1. 登入 Panorama 網頁介面 使用 ZTP 安裝程式管理員認證。
2. 選取 **Panorama** > **Zero Touch Provisioning**（零接觸佈建）> **Firewall Registration**（防火牆註冊）并 **Import**（匯入）ZTP 防火牆。
3. **Browse**（瀏覽）並選取含有 ZTP 防火牆資訊的 CSV 檔案，然後按一下 **OK**（確認）。

STEP 4 | 註冊 ZTP 防火牆。

1. 選取新增的 ZTP 防火牆並 **Register**（註冊）防火牆。
2. 出現提示時，按一下 **Yes**（是）以確認註冊 ZTP 防火牆。

STEP 5 | 確認已成功向 ZTP 服務註冊防火牆。

1. 選取 **Registration Status**（註冊狀態）並且確認已成功向 ZTP 服務註冊防火牆。
2. 登入 Panorama 網頁介面 使用管理員認證。
3. 選取 **Panorama** > **Managed Devices**（受管理裝置）> **Summary**（摘要），然後確認 ZTP 防火牆已成功新增為受管理的防火牆。

© 2019 Palo Alto Networks, Inc.

務必確定 *To SW Version*（至軟體版本）欄設定為正確的 *PAN-OS* 版本，使防火牆不會無意地升級或降級。僅 *PAN-OS 10.0.1* 和更新版本支援 *ZTP* 功能。此外，*PAN-OS* 版本必須與 *Panorama* 上執行的 *PAN-OS* 版本相同或是較舊版本。

如需詳細資訊，請參閱升級 ZTP 防火牆。

STEP 6 | 新增 ZTP 防火牆至裝置群組及範本堆疊。

您必須新增 ZTP 防火牆至裝置群組及範本堆疊才能讓您的防火牆顯示為 `Connected`（已連線），以便推送原則及網路設定。

1. 登入 Panorama 網頁介面 使用管理員認證。
2. 選取 **Panorama** > **Device Groups**（裝置群組），然後將防火牆指派給適當的裝置群組。

   Add a device group（新增裝置群組）以建立及設定新的裝置群組，以包含您的 ZTP 防火牆的原則物件及規則。
3. 選取 **Panorama** > **Templates**（範本），然後將防火牆指派給適當的範本堆疊。

   Configure a template stack（設定範本堆疊）以建立及設定新的範本堆疊，以包含您的 ZTP 防火牆的網路組態。

使用 CLI 以進行 ZTP 工作

使用下列 CLI 命令執行零接觸佈建 (ZTP) 工作，並且檢視 ZTP 服務狀態。

如果您想要 ...	使用 ...
從防火牆 **CLI** 管理防火牆	
顯示到 ZTP 服務的連線狀態。	`> show system ZTP status`
顯示到 Panorama 管理伺服器的連線狀態。	`> show panorama status`
顯示 ZTP 型號和防火牆系統資訊。	`> show system info`
停用防火牆上的 ZTP 狀態機器。 執行此命令不會刪除任何現有 ZTP 設定。 在從 *CLI* 停用防火牆上的 *ZTP* 狀態機器後，您無法再將其重新啟用。 如要重新啟用，您必須將防火牆重設為原廠預設設定。	`> request disable ztp`
從 **Panorama** 註冊、設定和管理您的 **ZTP** 防火牆	

© 2019 Palo Alto Networks, Inc.

如果您想要 ...	使用 ...

建立含有必要組態的裝置群組或範本，以在 Eth1/1 介面上使用 ZTP 服務將受管理防火牆與 Panorama 連線。	`> request plugins ztp create dgroup-template device-group <device group name>`
	
	`> request plugins ztp create dgroup-template template <template name>`

新增 ZTP 防火牆至防火牆清單，以便未來向 ZTP 服務註冊。	`> request plugins ztp firewall-add <serial number> claim-key <claim key>`
修改已新增至防火牆清單的 ZTP 防火牆序號，以便未來向 ZTP 服務註冊。	`> request plugins ztp firewall-add-modify firewall <old serial number> claim-key <claim key> new-serial <new serial number>`
從防火牆清單刪除 ZTP 防火牆，以便未來向 ZTP 服務註冊。	`> request plugins ztp firewall-delete firewall <serial number>`
新增 ZTP 防火牆至防火牆清單，以便未來向 ZTP 服務重新註冊。 當 ZTP 防火牆最初無法向 ZTP 服務註冊但需要註冊時，使用此命令。	`> request plugins ztp firewall-re-enter-info firewall <serial number> claim-key <claim key>`
向 ZTP 服務註冊您的 Panorama™ 管理伺服器。	`> request plugins ztp panorama-registration`
向 ZTP 服務註冊 ZTP 防火牆。	`> request plugins ztp firewall-registration firewall <serial number> claim-key <claim key>`
向 ZTP 服務重新註冊 ZTP 防火牆。 當 ZTP 防火牆最初無法向 ZTP 服務註冊時，使用此命令開始重新註冊程序。	`> request plugins ztp firewall-register-retry firewall <serial number> claim-key <claim key>`
匯入 ZTP 防火牆序號及索取金鑰資訊。 指定的檔案必須是 CSV 格式。	`> request plugins ztp ztp-add-import import-path <file path>`
從 **Panorama** 檢視 **ZTP** 防火牆資訊及 **ZTP** 服務狀態	

© 2019 Palo Alto Networks, Inc.

如果您想要 ...	使用 ...
從 ZTP 服務擷取向 Panorama 註冊的 ZTP 防火牆清單。	`> request plugins ztp ztp-service-info` 顯示下列詳細資料： • `first-firewall-connect-time`—ZTP 防火牆首次連線至 ZTP 服務時的時間戳記。 • `last-firewall-connect-time`—ZTP 防火牆上次連線至 ZTP 服務時的時間戳記。 • `registration-time`—ZTP 防火牆向 ZTP 服務註冊時的時間戳記。 • `isZTPFirewall`—防火牆是否是 ZTP 防火牆。 • `created_by`—新增 ZTP 防火牆的管理使用者。 • `IP address`— ZTP 防火牆的 IP 位址。
檢視要向 ZTP 服務註冊的防火牆清單中的 ZTP 防火牆清單。	`> show plugins ztp device-add-list`
檢視您的 ZTP 防火牆的註冊狀態。	`> show plugins ztp device-reg-status`
檢視 ZTP 防火牆的 ZTP 服務同步狀態。	`> request plugins ztp ztp-sync-status`
顯示完整管理平面 ZTP 連線歷程記錄。 這有助於對到 ZTP 服務的連線進行疑難排解。	`> tail follow yes mp-log ms.log`

解除安裝 ZTP 外掛程式

根據程序從您的 Panorama™ 管理伺服器移除 ZTP 設定和解除安裝 ZTP 外掛程式。如果您的 Panorama 採用高可用性 (HA) 設定，則在兩個 Panorama HA 對等上重複這些步驟。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 刪除 ZTP 安裝程式管理員帳戶。

1. 選取 **Panorama** > **Administrators**（管理員），然後選取您之前設定的 ZTP 安裝程式管理員帳戶。
2. **Delete**（刪除）ZTP 安裝程式管理員帳戶。
3. 選取 **Panorama** > **Administrators**（管理員），然後選取 `installeradmin` 管理員角色。
4. **Delete**（刪除）`installeradmin` 管理員角色。
5. 按一下 **Commit**（提交）和 **Commit to Panorama**（提交至 **Panorama**）。

STEP 3 | 解除安裝 ZTP 外掛程式

1. 選取 **Panorama** > **Plugins**（外掛程式），然後導覽至 Panorama 上安裝的 ZTP 外掛程式。
2. 在「動作」欄中，**Remove Config**（移除設定）以從 Panorama 刪除 ZTP 相關設定
3. 當系統提示時按一下 **OK**（確定）以確認從 Panorama 移除 ZTP 設定。
4. 按一下 **Commit**（提交）和 **Commit to Panorama**（提交至 **Panorama**）。
5. **Uninstall**（解除安裝）ZTP 外掛程式。

© 2019 Palo Alto Networks, Inc.

6. 當系統提示時按一下 **OK**（確定）以從 Panorama 解除安裝 ZTP 外掛程式。

© 2019 Palo Alto Networks, Inc.

管理裝置群組

- 新增裝置群組
- 建立裝置群組階層
- 建立共用或裝置群組原則中使用的物件
- 還原至繼承的物件值
- 管理未使用的共用物件
- 管理繼承物件的優先順序
- 移動或複製原則規則或物件至不同的裝置群組
- 在 Panorama 上選取 URL 篩選廠商
- 將原則規則推送至防火牆子集
- 管理規則階層

新增裝置群組

在新增防火牆後（請參閱 將防火牆新增為受管理的裝置），您可以將其組成群組至 裝置群組（最多 1,024 個），如下所示。確保將主動被動高可用性 (HA) 設定的防火牆指派至相同的裝置群組，以便 Panorama 將相同的原則規則和物件推送至這些防火牆。PAN-OS 不會在 HA 端點之間同步推送的規則。若要在組織內不同管理層級上管理規則和物件，建立裝置群組階層。

STEP 1 | 選取 **Panorama** > **Device Groups**（設備群組），然後按一下 **Add**（新增）。

STEP 2 | 輸入唯一的 **Name**（名稱）及 **Description**（描述）以識別裝置群組。

STEP 3 | 在裝置部分中，選取核取方塊以指派防火牆至群組。若要搜尋防火牆的長清單，使用篩選器。



您可以將任何防火牆指派至一個裝置群組。您可以將防火牆上的每個虛擬系統指派至不同的裝置群組。

STEP 4 | 在參照範本部分中，**Add**（新增）任何範本或範本堆疊，物件參照裝置群組組態。

您必須指派適當的範本或範本堆疊參照至裝置群組，以將範本或範本堆疊關聯至裝置群組。這讓您可以參照範本或範本堆疊中設定的物件，而無需新增無關裝置至範本堆疊。

如果裝置群組組態沒有參照任何範本或範本堆疊中設定的物件，跳過此步驟。

STEP 5 | （選用）針對身為 HA 對等的防火牆，選取 **Group HA Peers**（群組 **HA** 對等）。

只有當受管理防火牆 HA 對等在同一裝置群組中時，您才可對其進行分組。



被動或主動次要端點防火牆名稱位於括弧內。分組 *HA* 對等是視覺變更且未發生組態變更。

STEP 6 | 在裝置群組階層中選取位於您建立裝置上方的 **Parent Device Group**（父系裝置群組）（預設為 **Shared**（共用））。

STEP 7 | 如果您的原則規則會參考使用者和群組，指派一個 **Master**（主）防火牆。

這將是 Panorama 收集使用者名稱和使用者群組資訊的裝置群組唯一防火牆。

STEP 8 | 按一下 **OK**（確定）儲存您的變更。

© 2019 Palo Alto Networks, Inc.

STEP 9 | 選取 **Commit**（提交）> **Commit and Push**（提交並推送），然後將您的變更 **Commit and Push**（提交並推送）至 Panorama 組態和您新增的裝置群組。

建立裝置群組階層

STEP 1 | 規劃裝置群組階層。

1. 決定裝置群組等級，以及您指派至各裝置群組和共用位置的防火牆和虛擬系統。您可以將任一防火牆或虛擬系統 (vsys) 指派至一個裝置群組。如果裝置群組將作為低階裝置群組的組織容器，您無需向其指派防火牆。
2. 如果指派內容不符合您計劃的階層，從現有裝置群組移除防火牆或 vsys 指派。
   1. 選取 **Panorama** > **Device Groups**（設備群組），並選取設備群組。
   2. 在設備部分中，清除您想要移除的防火牆和虛擬系統核取方塊，然後按一下 **OK**（確定）。
3. 若有必要，新增您將指派至裝置群組的更多防火牆：請參閱將防火牆新增為受管理的裝置。
4. 如果您使用多個 Panorama 外掛程式來執行端點監控，則包含部署在特定超管理器中的防火牆的裝置群組不能是包含部署在其他超管理器中的防火牆的裝置群組的子系或父系。如需詳細資訊，請參閱 裝置群組階層。

STEP 2 | 對於各頂級裝置群組，新增裝置群組。

1. 在 **Panorama** > **Device Groups**（設備群組）頁面中，按一下 **Add**（新增）並輸入 **Name**（名稱）以識別設備群組。
2. 在設備部分中，選取核取方塊以指派防火牆和虛擬系統至裝置群組。
3. 保留 **Parent Device Group**（父系裝置群組）選項位於 **Shared**（共用）（預設）位置，然後按一下 **OK**（確定）。

STEP 3 | 對於各低階裝置群組，新增裝置群組。

- 對於各低階新設備群組，重複先前步驟，但設定 **Parent Device Group**（父系設備群組）為下一級上方的設備群組。
- 對於各現有裝置群組，在 **Device Groups**（裝置群組）頁面中，選取裝置群組以對其進行編輯，選取 **Parent Device Group**（父系裝置群組），然後按一下 **OK**（確定）。



如果您移動裝置群組至不同的父系，其所有子系裝置群組會隨其移動，同時移動的還有所有與裝置群組及其子系關聯的防火牆、原則規則和物件。如果新父系位於另一個存取網域中，移動的裝置群組將不再在原存取網域中擁有成員資格。如果新存取網域有父系裝置群組的讀寫存取權限，其也會擁有移動的裝置群組的讀寫存取權限。如果新存取網域有父系裝置群組的唯讀存取權限，其沒有移動的裝置群組的存取權限。若要重新設定裝置群組的存取，請參閱設定存取網域。

STEP 4 | 根據需要設定、移動和複製物件和原則規則，來說明裝置群組階層內的繼承。

- 建立共用或裝置群組原則中使用的物件，或編輯現有物件。

您僅可以在物件的位置對其進行編輯：即裝置群組被指派的位置。子系裝置群組從該位置繼承物件的唯讀實例。但是，您可以選擇參考步驟取代繼承的物件值。

- 建立或編輯原則。
- 移動或複製原則規則或物件至不同的裝置群組。

STEP 5 | 取代繼承的物件值。

僅當特定裝置群組中的物件值必須與從上階裝置群組繼承的值不一致時適用。

在取代一個物件後，您可以在子系裝置群組中再次將其取代。不過，您無法取代共用或預先定義（預設）物件。

© 2019 Palo Alto Networks, Inc.

在 **Objects**（物件）頁籤中，繼承的物件在名稱欄中有一個綠色圖示，且位置欄顯示上階裝置群組。

1. 在 **Objects**（物件）頁籤中，選取物件類型（例如，**Objects**（物件）> **Addresses**（位址））。
2. 選取有取代實例的 **Device Group**（裝置群組）。
3. 選取物件並按一下 **Override**（取代）。
4. 編輯值。您無法編輯 **Name**（名稱）或 **Shared**（共用）設定。
5. 按一下 **OK**（確定）。名稱欄顯示物件的黃色和綠色重疊圖示，表示其已被取代。



若有必要，您稍後可以還原至繼承的物件值。

STEP 6 | 儲存並提交您的變更。



對階層進行任何變更之後，提交至 *Panorama*，並推送至裝置群組。

如果範本參考裝置群組內的物件（例如，介面參考位址），且由於階層變更，指派給範本的防火牆不再指派給該裝置群組，則您還必須將變更推送至範本。

選取 **Commit**（提交）> **Commit and Push**（提交並推送），然後將您的變更 **Commit and Push**（提交並推送）至 Panorama 組態和您新增或變更的裝置群組。

建立共用或裝置群組原則中使用的物件

您可以使用任何原則規則內的物件，該原則規則位於共用位置、與物件相同的裝置群組，或裝置群組子系中（如需詳細資訊，請參閱 裝置群組物件）。



如果您希望利用動態位址群組，以建立自動適應網路內變更的原則，參閱 在原則中使用動態位址群組 以確認 *Panorama* 上支援的註冊 *IP* 位址數量。

- 建立共用物件。

  在此範例中，我們會針對想要觸發警示的 URL 篩選類別新增共用物件。

  1. 選取 **Objects**（物件）> **Security Profiles**（安全性設定檔）> **URL Filtering**（URL 篩選）頁籤，然後按一下 **Add**（新增）。

     Objects（物件）頁籤僅在您 新增裝置群組 後顯示（至少一個）。
  2. 輸入 **Name**（名稱）及 **Description**（描述）。
  3. 選取 **Shared**（共用）。
  4. **Disable Override**（停用取代）選項預設為清除，這表示您可以在所有裝置群組中取代物件的繼承實例。若要針對物件停用取代，請選取此核取方塊。
  5. 在 **Categories**（類別）頁籤中，選取您想獲得通知的每個類別。
  6. 在 **Action**（動作）欄中，選取 **Alert**（轉送）。
  7. 按一下 **OK**（確定）以儲存物件的變更。
  8. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

- 建立裝置群組物件。

  在此範例中，我們將為您網路上的特定網頁伺服器新增位址物件。

  1. 選取 **Objects**（物件）> **Addresses**（位址）並選取您將使用物件的 **Device Group**（設備群組）。
  2. 按一下 **Add**（新增），並輸入用來識別物件的 **Name**（名稱）。

© 2019 Palo Alto Networks, Inc.

3. 確定 **Shared**（共用）選項維持已清除。
4. **Disable Override**（停用取代）選項預設為清除，這表示您可以在裝置群組中取代物件的繼承實例，而這些裝置群組為所選 **Device Group**（裝置群組）的子系。若要針對物件停用取代，請選取 **Disable Override**（停用取代）選項。
5. 選取位址物件的 **Type**（類型）和相關值。例如，選取 **IP Range**（IP 範圍）並輸入網頁伺服器的 IP 位址範圍。
6. 按一下 **OK**（確定）以儲存物件的變更。
7. 選取 **Commit**（提交）> **Commit and Push**（提交並推送），然後將您的變更 **Commit and Push**（提交並推送）至 Panorama 組態和您新增物件的裝置群組。

- 檢視 Panorama 中的共用物件和裝置群組物件。

  Objects（物件）頁籤頁面中，位置欄顯示物件是共用，還是裝置群組所特有。

  1. 在 **Objects**（物件）頁籤中，選取物件類型（在本示例中，**Objects**（物件）> **Addresses**（位址））。
  2. 選取您新增物件的 **Device Group**（裝置群組）。

     Objects（物件）頁籤僅顯示所選 *Device Group*（裝置群組）內的物件，或從上階裝置群組或共用位置繼承的物件。
  3. 確認顯示裝置群組物件。注意位址欄內的裝置群組名稱符合 **Device Group**（裝置群組）下拉式清單中的選擇。

還原至繼承的物件值

在取代裝置群組物件從上階裝置群組繼承的值後，您可以隨時將物件還原至其上階值。在 **Objects**（物件）頁籤中，取代的物件在名稱欄內有一個黃色和綠色重疊的圖示（）。

如果您希望推送上階值至所有取代物件，而非還原某個特定物件，請參閱管理繼承物件的優先順序。

關於取代值的步驟，請參閱步驟 5

對於物件繼承和取代的詳細資訊，請參閱 裝置群組物件。

STEP 1 | 在 **Objects**（物件）頁籤中，選取物件類型（例如，**Objects**（物件）> **Addresses**（位址））並選取具有物件取代實例的 **Device Group**（設備群組）。

STEP 2 | 選取該物件，按一下 **Revert**（還原），然後按一下 **Yes**（是）。名稱欄顯示物件的綠色圖示，表示其從上階裝置群組繼承了所有值。

STEP 3 | 選取 **Commit**（提交）> **Commit and Push**（提交並推送），然後將您的變更 **Commit and Push**（提交並推送）至 Panorama 組態和您還原物件的裝置群組。

管理未使用的共用物件

當您將組態變更推送至 裝置群組 時，依預設，無論任何共用或裝置群組原則規則是否參考共用物件，Panorama 會將所有共用物件推送至防火牆。但是，您可以設定 Panorama 僅推送規則在裝置群組中參考的共用物件。**Share Unused Address and Service Objects with Devices**（與裝置共用未使用的位址與服務物件）選項可讓您限制 Panorama 推送至受管理防火牆的物件。

當 *Share Unused Address and Service Objects with Devices*（與裝置共用未使用的位址與服務物件）被停用時，*Panorama* 在您 將原則規則推送至防火牆子集 時忽略 *Target*（目標）防火牆。這意味著任何規則引用的物件將被推送至裝置群組內的所有防火牆。

© 2019 Palo Alto Networks, Inc.

要限制被推送至一組受管理防火牆的物件數量，根據需要新增原則規則至子裝置群組和參照共用物件。參閱 建立裝置群組階層 獲取關於建立子裝置群組的更多資訊。

在低階型號上（例如 PA-220），請考慮只將相關的共用物件推送至受管理的防火牆。這是因為低階型號上可儲存的物件數目，遠低於中階至高階型號可儲存的數目。此外，如果您有許多未使用的位址和服務物件，則清除 **Share Unused Address and Service Objects with Devices**（與裝置共用未使用的位址與服務物件）可大幅減少防火牆上的提交時間，因為推送至每一個防火牆的設定較小。不過，停用此選項可能會增加 Panorama 上的提交時間，因為 Panorama 必須動態檢查原則規則是否參考特定物件。

STEP 1 | 選取 **Panorama** > **Setup**（設定）> **Management**（管理），再編輯 Panorama 設定。

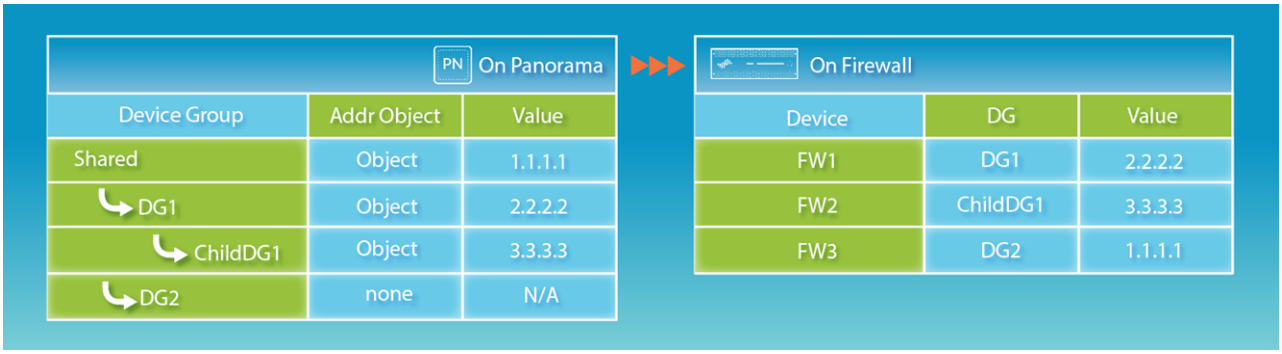
STEP 2 | 清除 **Share Unused Address and Service Objects with Devices**（與裝置共用未使用的位址與服務物件）選項會僅推送規則參考的共用物件，而選取此選項可重新啟用推送所有共用物件。

STEP 3 | 按一下 **OK**（確定）儲存您的變更。

STEP 4 | 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

管理繼承物件的優先順序

依預設，當 裝置群組階層 內不同等級的裝置群組擁有相同名稱的物件，但值不同時（例如，由於發生取代），子系裝置群組中的原則規則適用該子系裝置群組中的物件值，而非從上階裝置群組中繼承的物件值。或者，您可以還原優先順序以將含有物件的最高上階值推送至所有子系裝置群組。當您啟用此選項後，下次將設定變更推送至裝置群組時，繼承物件的值會取代子系裝置群組中任何被取代物件的值。下圖展示了裝置群組內繼承物件的優先順序：



如果防火牆擁有本機定義的物件，且該物件與 *Panorama* 所推送的共用或裝置群組物件同名，則將發生提交失敗。

如果您希望還原特定的被取代物件至其上階值而非推送上階值至所有被取代的物件，請參閱 還原至繼承的物件值。

STEP 1 | 選取 **Panorama** > **Setup**（設定）> **Management**（管理），再編輯 [Panorama 設定]。

STEP 2 | 如果您希望反轉預設的優先順序，請選取 **Objects defined in ancestors will take higher precedence**（父系中定義的物件將擁有較高優先順序）。之後對話方塊顯示 **Find Overridden Objects**（尋找被取代物件）連結，提供選項，以查看在提交此變更後，多少被取代（鏡像）物件將具有上階值。您可以暫留在數量訊息上以顯示物件名稱。

如果您希望還原為預設的優先順序，請清除 **Objects defined in ancestors will take higher precedence**（父系中定義的物件將擁有較高優先順序）。

© 2019 Palo Alto Networks, Inc.

Find Overridden Objects（尋找被取代物件）僅偵測與裝置群組內另一個物件共用名稱的共用裝置群組物件。

STEP 3 | 按一下 **OK**（確定）儲存您的變更。

STEP 4 | 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

STEP 5 | （選用）如果您選取 **Objects defined in ancestors will take higher precedence**（父系中定義的物件將擁有較高優先順序），Panorama 會在您將設定變更推送至裝置群組之後，才推送父系物件：選取 **Commit**（提交）> **Push to Devices**（推送至裝置），然後 **Push**（推送）您的變更。

移動或複製原則規則或物件至不同的裝置群組

在 Panorama 上，如果您移動或從裝置群組複製的原則規則或物件擁有目標裝置群組中不可用的物件參考（**Destination**（目的地）），您必須在相同操作中移動或複製被參考物件和參考規則或物件。在裝置群組階層中，請牢記參考物件可能在整個繼承中都可用。例如，共用物件在整個裝置群組中都可用。您可以執行全域尋找檢查參考。如果您移動或複製被取代的物件，請確保該物件在 **Destination**（目的地）父系裝置群組中啟用了取代（請參閱建立共用或裝置群組原則中使用的物件）。

在複製多個原則規則時，您選取規則時的順序將決定規則複製到裝置群組的順序。例如，如果您有規則 *1-4*，您的選擇順序為 *2-1-4-3*，將複製這些規則的裝置群組會以相同的順序顯示規則。但是，複製成功後，您可以按照您任何合適的順序重新整理這些規則。

STEP 1 | 登入 Panorama 並選取規則庫（例如，**Policy**（高可用性）> **Security**（安全性）> **Pre Rules**（預先規則））或物件類型（例如，**Objects**（物件）> **Addresses**（位址））。

STEP 2 | 選取 **Device Group**（裝置群組）並選取一個或多個規則或物件。

STEP 3 | 執行下列其中一個步驟：

- （僅限規則）**Move**（移動）> **Move to other device group**（移動至其他設備群組）
- （僅限物件）**Move**（移動）
- （規則或物件）**Clone**（複製）

STEP 4 | 在 **Destination**（目的地）下拉式清單中，選取新裝置群組或 **Shared**（共用）。預設為之前選取的 **Device Group**（設備群組）。

STEP 5 | （僅限規則）選取 **Rule order**（規則順序）：

- **Move top**（移至頂部）（預設）—規則將位於所有其他規則之前。
- **Move bottom**（移至底部）—規則將位於所有其他規則之後。
- **Before rule**（規則之前）—在相鄰下拉式清單中，選取所選規則後的規則。
- **After rule**（規則之後）—在相鄰下拉式清單中，選取所選規則前的規則。

STEP 6 | **Error out on first detected error in validation**（驗證過程中顯示首次偵測到的錯誤）核取方塊預設為被選取，這表示 Panorama 會顯示發現的第一個錯誤，並停止檢查更多錯誤。例如，若 **Destination**（目的地）裝置群組沒有您要移動之原則規則所參照的物件，則會發生錯誤。當您同時移動或複製多個項目時，選取此核取方塊可簡化疑難排解。若您清除核取方塊，則 Panorama 將找出所有錯誤再加以顯示。無論此設定如何，在您修復所有所選項目的錯誤之前，Panorama 都不會移動或複製任何內容。

© 2019 Palo Alto Networks, Inc.

STEP 7 | 按一下 **OK**（確定）以啟動錯誤驗證。如果 Panorama 發現錯誤，修復錯誤並重試移動或複製操作。如果 Panorama 未發現錯誤，其將執行操作。

STEP 8 | 選取 **Commit**（提交）> **Commit and Push**（提交並推送）、在推送範圍中 **Edit Selections**（編輯選擇）、選取 **Device Groups**（裝置群組）、選取原始和目的地裝置群組，按一下 **OK**（確定），然後將您的變更 **Commit and Push**（提交並推送）至 Panorama 組態和裝置群組。

在 Panorama 上選取 URL 篩選廠商

URL 篩選可允許防火牆監控與控制使用者的 Web 存取行為。您設定用於控制 Web 存取的原則規則（安全性、QoS、網頁認證與解密規則）會參照 URL 類別。您在 Panorama 上選取的 URL 篩選廠商會決定您新增至裝置群組並推送至防火牆的規則中可參照哪些 URL 類別。

Panorama 預設使用 PAN-DB，其為緊密整合到 PAN-OS 以及 Palo Alto Networks 威脅情報雲的 URL 篩選資料庫。PAN-DB 提供高效能的本機快取以最大化 URL 查詢的線內效能。另一個廠商選項為 BrightCloud，這是一個協力廠商 URL 資料庫。

與防火牆不同，*Panorama* 不會下載 *URL* 資料庫，也不需要 *URL* 篩選授權。

下列主題描述了如何在 Panorama 上或同時在 Panorama 和受管理防火牆上變更 URL 篩選廠商。您還可以僅在防火牆上變更 URL 篩選廠商。

- Panorama 和防火牆必須要有相符的 URL 篩選廠商嗎？
- 在 HA Panorama 上變更 URL 篩選廠商
- 在非 HA Panorama 上變更 URL 篩選廠商
- 將 Panorama 和 HA 防火牆從 BrightCloud 轉移至 PAN-DB
- 將 Panorama 和非 HA 防火牆從 BrightCloud 轉移至 PAN-DB

Panorama 和防火牆必須要有相符的 *URL* 篩選廠商嗎？

在任何單一 Panorama 管理伺服器或防火牆上，只有一個 URL 篩選廠商可以為作用中：PAN-DB 或 BrightCloud。為 Panorama 選取廠商時，您必須考量受管理防火牆的廠商與 PAN-OS 版本：

- PAN-OS 5.0.x 與更早版本—Panorama 與防火牆需要相符的 URL 篩選廠商。
- PAN-OS 6.0 或更新版本—Panorama 與防火牆不需要相符的 URL 篩選廠商。如果偵測到廠商不符合，防火牆會將在 URL 篩選設定檔中的 URL 類別及其從 Panorama 收到的規則，對應至與防火牆上啟用的廠商其類別符合的 URL 類別。

因此若有一個部署，其中部分的防火牆執行 PAN-OS 6.0 或更新版本，部分的防火牆執行舊版的 PAN-OS，則 Panorama 使用的 URL 篩選廠商必須與執行舊版 PAN-OS 的防火牆相同。例如，如果執行 PAN-OS 5.0 的防火牆使用 PAN-DB，執行 PAN-OS 7.0 的防火牆使用 BrightCloud，則 Panorama 必須使用 PAN-DB。

在 *HA Panorama* 上變更 *URL* 篩選廠商

對於高可用性 (HA) 部署，在變更 URL 篩選廠商時，每個 Panorama 端點都必須處於非運作狀態。因此，為了避免中斷 Panorama 的運作，在被動 Panorama（此範例中為 Panorama2）上變更 URL 篩選廠商，然後觸發容錯移轉，再在主動 Panorama（此範例中為 Panorama1）上變更廠商。

STEP 1 | 在每個 Panorama HA 端點上變更 URL 篩選廠商。

先在 *Panorama2*（被動端點）上完成變更，然後在 *Panorama1*（主動端點）上完成變更。

1. 登入 Panorama 網頁介面。

© 2019 Palo Alto Networks, Inc.

2. 選取 **Panorama** > **High Availability**（高可用性），然後 **Suspend local Panorama**（暫停本機 **Panorama**）。

   在 Panorama1 上執行此步驟時，會發生容錯轉移，並且 Panorama2 的狀態變為主動。
3. 選取 **Panorama** > **Setup**（設定）> **Management**（管理），再編輯 [一般設定]。
4. 選取 **URL Filtering Database**（**URL** 篩選資料庫）廠商：**paloaltonetworks** (PAN-DB) 或 **brightcloud**。
5. 選取 **Panorama** > **High Availability**（高可用性），然後 **Make local Panorama functional**（讓本機 **Panorama** 運作）。

   在 Panorama1 上執行此步驟時（ 兩個 HA 端點均啟用先佔）Panorama1 會自動恢復主動狀態，而 Panorama2 則恢復被動狀態。

STEP 2 | 確認 URL 類別可在原則中供參照之用。

1. 選取 **Objects**（物件）> **Security Profiles**（安全性設定檔）> **URL Filtering**（**URL** 篩選）。
2. 按一下 **Add**（新增），並確認 URL Filtering profile（URL 篩選設定檔）對話方塊的 **Categories**（類別）頁籤中顯示這些與所選廠商相關的 URL 類別。

在非 *HA Panorama* 上變更 *URL* 篩選廠商

在並非部署為高可用性 (HA) 設定的 Panorama 管理伺服器上執行此程序，以變更 URL 篩選廠商。

STEP 1 | 變更 URL 篩選廠商。

1. 選取 **Panorama** > **Setup**（設定）> **Management**（管理），再編輯 [一般設定]。
2. 選取 **URL Filtering Database**（**URL** 篩選資料庫）廠商：**paloaltonetworks** (PAN-DB) 或 **brightcloud**。

STEP 2 | 確認 URL 類別可在原則中供參照之用。

1. 選取 **Objects**（物件）> **Security Profiles**（安全性設定檔）> **URL Filtering**（**URL** 篩選）。
2. 按一下 **Add**（新增），並確認 URL Filtering profile（URL 篩選設定檔）對話方塊的 **Categories**（類別）頁籤中顯示這些與所選廠商相關的 URL 類別。

將 *Panorama* 和 *HA* 防火牆從 *BrightCloud* 轉移至 *PAN-DB*

當防火牆採用高可用性 (HA) 設定部署時，執行此程序，以將 Panorama 和防火牆上的 URL 篩選廠商從從 BrightCloud 轉移至 PAN-DB。在此範例中，主動（或主動-主要）防火牆命名為 fw1，被動（或主動-次要）防火牆命名為 fw2。轉移操作會自動將 BrightCloud URL 類別對應至 PAN-DB URL 類別。

STEP 1 | 確定哪些防火牆需要新的 PAN-DB URL 篩選授權。

1. 登入 Panorama，然後選取 **Panorama** > **Device Deployment**（設備部署）> **Licenses**（授權）。
2. 檢查 URL 欄以確定哪些防火牆具有 PAN-DB 授權以及這些授權是否有效或已到期。

   防火牆會具有 BrightCloud 與 PAN-DB 兩者的有效授權，但只有一個授權可以為作用中。

   如果您不確定 *PAN-DB URL* 篩選授權是否有效，則存取防火牆 *Web* 介面，選取 *Device*（設備）> *Licenses*（授權），然後確認 *PAN-DB URL* 篩選區段中的 *Active*（有效）欄位是否顯示 *Yes*（是）。
3. 為沒有有效 PAN-DB 授權的防火牆購買新的授權。

   在 HA 部署中，每個防火牆端點都需要不同的 PAN-DB 授權和授權碼。Palo Alto Networks 將傳送一封電子郵件，其中載有您所購買授權的啟動碼。如果您找不到該電子郵件，請在繼續操作前聯絡客戶支援。

STEP 2 | 在 Panorama 上將 URL 篩選廠商變更為 PAN-DB。

© 2019 Palo Alto Networks, Inc.

存取 Panorama Web 介面並執行下列工作之一：

- 在 HA Panorama 上變更 URL 篩選廠商
- 在非 HA Panorama 上變更 URL 篩選廠商

STEP 3 | 在兩個防火牆 HA 端點上進行 TCP 工作階段設定，確保當您暫停其中一個端點是，未同步的工作階段將進行容錯移轉。

登入每個防火牆的 CLI 並執行下列命令：

```
> set session tcp-reject-non-syn no
```

STEP 4 | 在每個防火牆 HA 端點上將 URL 篩選廠商轉移至 PAN-DB。

先在 *fw2*（被動或主動-次要端點）上完成變更，然後在 *fw1*（主動或主動-主要端點）上完成變更。

1. 存取防火牆 Web 介面，選取 **Device**（設備）> **High Availability**（高可用性）> **Operational Commands**（操作命令），然後 **Suspend local device**（暫停本機設備）。

   在 fw1 上執行此步驟將觸發向 fw2 容錯轉移。
2. 選取 **Device**（裝置）> **Licenses**（授權）。
3. 在授權管理區段中，選取**Activate feature using authorization code**（使用授權碼啟動功能），輸入 **Authorization Code**（授權碼），然後按一下 **OK**（確定）。

   啟動 PAN-DB 授權將自動停用 BrightCloud 授權。
4. 在 PAN-DB URL 篩選區段中，**Download**（下載）種子檔案，選取您所在的地區，然後按一下 **OK**（確定）。
5. 提交並推送您的設定變更：
   1. 存取 Panorama Web 介面。
   2. 選取 **Commit**（提交）> **Commit and Push**（提交並推送），然後在 Push Scope（推送範圍）中 **Edit Selections**（編輯選擇）
   3. 選取 **Device Groups**（裝置群組），選取防火牆，然後按一下 **OK**（確定）。
   4. 將您的變更 **Commit and Push**（提交並推送）至 Panorama 組態和裝置群組。
6. 存取防火牆 Web 介面，選取 **Device**（設備）> **High Availability**（高可用性）> **Operational Commands**（操作命令），然後 **Make local device functional**（讓本機設備運作）。

   在 fw1 上執行此步驟時（兩個防火牆均啟用先佔），fw1 會自動還原至主動（或主動-主要）狀態，而 fw2 則還原至被動（或主動-次要）狀態。

STEP 5 | 將兩個防火牆 HA 端點還原至原始 TCP 工作階段設定。

在每個防火牆的 CLI 上執行下列命令：

```
> set session tcp-reject-non-syn yes
```

將 *Panorama* 和非 *HA* 防火牆從 *BrightCloud* 轉移至 *PAN-DB*

當防火牆未採用高可用性 (HA) 設定部署時，執行此程序，以將 Panorama 和防火牆上的 URL 篩選廠商從從 BrightCloud 轉移至 PAN-DB。轉移操作會自動將 BrightCloud URL 類別對應至 PAN-DB URL 類別。

STEP 1 | 確定哪些防火牆需要新的 PAN-DB URL 篩選授權。

1. 登入 Panorama，然後選取 **Panorama** > **Device Deployment**（設備部署）> **Licenses**（授權）。

© 2019 Palo Alto Networks, Inc.

2. 檢查 URL 欄以確定哪些防火牆具有 PAN-DB 授權以及這些授權是否有效或已到期。

   防火牆會具有 BrightCloud 與 PAN-DB 兩者的有效授權，但只有一個授權可以為作用中。

   如果您不確定 *PAN-DB URL* 篩選授權是否有效，則存取防火牆 *Web* 介面，選取 *Device*（設備）> *Licenses*（授權），然後確認 *PAN-DB URL* 篩選區段中的 *Active*（有效）欄位是否顯示 *Yes*（是）。
3. 為沒有有效 PAN-DB 授權的防火牆購買新的授權。

   Palo Alto Networks 將傳送一封電子郵件，其中載有您所購買授權的啟動碼。如果您找不到該電子郵件，請在繼續操作前聯絡客戶支援。

STEP 2 | 在 Panorama 上將 URL 篩選廠商變更為 PAN-DB。

存取 Panorama Web 介面並執行下列工作之一：

- 在 HA Panorama 上變更 URL 篩選廠商
- 在非 HA Panorama 上變更 URL 篩選廠商

STEP 3 | 在每個防火牆上將 URL 篩選廠商轉移至 PAN-DB。

1. 存取防火牆 Web 介面，選取 **Device**（裝置）> **Licenses**（授權）。
2. 在授權管理區段中，選取**Activate feature using authorization code**（使用授權碼啟動功能），輸入 **Authorization Code**（授權碼），然後按一下 **OK**（確定）。

   啟動 PAN-DB 授權將自動停用 BrightCloud 授權。
3. 在 PAN-DB URL 篩選區段中，**Download**（下載）種子檔案，選取您所在的地區，然後按一下 **OK**（確定）。
4. 提交並推送您的設定變更：
   1. 存取 Panorama Web 介面。
   2. 選取 **Commit**（提交）> **Commit and Push**（提交並推送），然後在 Push Scope（推送範圍）中 **Edit Selections**（編輯選擇）
   3. 選取 **Device Groups**（裝置群組），選取防火牆，然後按一下 **OK**（確定）。
   4. 將您的變更 **Commit and Push**（提交並推送）至 Panorama 組態和裝置群組。

將原則規則推送至防火牆子集

原則目標可讓您指定裝置群組中的防火牆，以便將原則規則推送到這些設備。它能讓您排除一或多個防火牆或虛擬系統，或僅將規則套用到裝置群組中的特定防火牆或虛擬系統。

隨著規則庫的發展和推送新或修改的規則至防火牆，除非您在建立和修改規則時封存此資訊，否則變更和稽核資訊會逐漸遺失。使用稽核註解封存檔檢視所選規則的稽核註解和設定日誌記錄，以及將兩個原則規則版本進行對比以查看規則的變更。從 Panorama 推送的規則稽核註解記錄僅可以從 Panorama 管理伺服器檢視。然而，您可以在從受管理防火牆轉送至 Panorama 的設定日誌中檢視稽核註解。但是，對於在防火牆本機建立或修改的規則，無法檢視稽核註解封存檔。為確保在規則建立或修改時擷取該稽核註解，強制執行原則規則、說明、標記和稽核註解。

能夠針對規則可讓您確保原則集中於 Panorama 上。目標規則允許您在 Panorama 上定義規則（作為共用或裝置群組前期或後期規則），並在管理規則時提高可見度和效率（請參閱 裝置群組原則）。稽核註解封存檔透過允許您追踪原則規則變更的方式和原因，進一步增加可見度，讓您可以在規則的整個生命週期內稽核規則的演進。

STEP 1 | （最佳做法）強制執行原則規則的稽核註解。

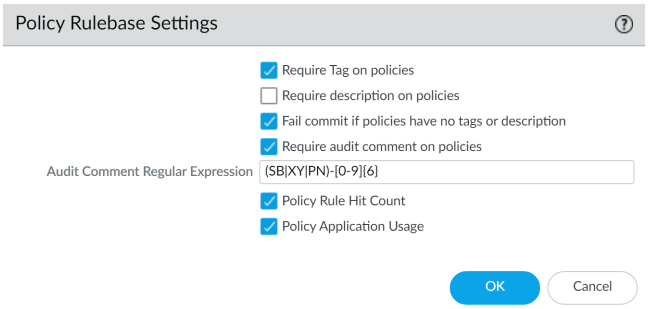
雖然此步驟為可選項，其仍是為原則規則強制執行稽核註解的最佳做法，從而確保您可以為建立或修改規則擷取原因。其還有助於保留準確的規則歷程記錄以用於稽核目的。

© 2019 Palo Alto Networks, Inc.

1. 選取 **Panorama** > **Setup**（設定） > **Management**（管理），然後編輯 Policy Rulebase Settings（原則規則庫設定）。
2. 啟用選項以 **Require audit comment on policies**（要求原則稽核註解）。
3. 設定 Audit Comment Regular Expression（稽核註解規則運算式）以指定稽核註解格式。

   當建立或修改規則時，要求透過指定字母和數字運算式，讓這些稽核註解遵循適合業務和稽核需求的特定格式。例如，您可使用以下設定來指定與票證號碼格式相符的規則運算式：

   - **`[0-9]{<Number of digits>}`**—要求稽核註解包含數值介於 0 到 9 之間的最少數字數。例如，**`[0-9]{6}`** 要求數字運算式包含最少六位數值介於 0 到 9 之間的數字。根據需要設定最少位數。
   - **`<Letter Expression>`**—要求稽核註解包含字母運算式。例如，**`Reason for Change-`** 要求管理員設定以此字母運算式開頭的稽核註解。
   - **`<Letter Expression>-[0-9]{<Number of digits>}`**—要求稽核註解包含一個設定的前置字元，後接數值介於 0 到 9 之間的最少數字數。例如，**`SB-[0-9]{6}`** 要求稽核註解格式以 **`SB-`** 開頭，後接包含最少六位數（數值介於 0 到 9 之間）的數字運算式，如 **`SB-012345`**。
   - **`(<Letter Expression>)|(<Letter Expression>)|(<Letter Expression>)|-[0-9]{<Number of digits>}`**—要求稽核註解包含一個首碼，該首碼使用任意一個預先確定的字母運算式，並包含數值介於 0 到 9 之間的最少數字數。例如，**`(SB|XY|PN)-[0-9]{6}`** 要求稽核註解格式以 **`SB-`**、**`XY-`** 或 **`PN-`** 開頭，後接包含最少六位數（數值介於 0 到 9 之間）的數字運算式，如 **`SB-012345`**、**`XY-654321`** 或 **`PN-012543`**。
4. 按一下 **OK**（確定）以套用新的原則規則庫設定。



5. 按一下 **Commit**（提交）和 **Commit to Panorama**（提交至 **Panorama**）。

STEP 2 | 建立規則。

例如，在安全性規則庫中定義預先規則，允許內部網路上的使用者存取 DMZ 中的伺服器。

1. 選取 **Policies**（原則）頁籤，然後選取要定義規則的 **Device Group**（裝置群組）。
2. 選取規則庫。例如，選取 **Policies**（原則） > **Security**（安全性） > **Pre-Rules**（預先規則）並 **Add**（新增）一個規則。
3. 在 **General**（一般）頁籤，輸入說明性規則 **Name**（名稱）並輸入 **Audit Comment**（稽核註解）。
4. 在 **Source**（來源）頁籤中，設定 **Source Zone**（來源地區）為 **Trust**（信任）。
5. 在 **Destination**（目的地）頁籤中，將 **Destination Zone**（目的地區域）設定為 **DMZ**。
6. 在 **Service/ URL Category**（服務/URL 類別）頁籤中，將 **Service**（服務）設定為 **application-default**。
7. 在 **Actions**（動作）頁籤中，將 **Actions**（動作）設定為 **Allow**（允許）。
8. 所有其他選項保持預設值不變。

STEP 3 | 將規則的目標指定為包含或排除防火牆的子集。

若要將原則套用到選取的防火牆集：

1. 在 Policy Rule（原則規則）對話方塊中選取 **Target**（目標）頁籤。

© 2019 Palo Alto Networks, Inc.

2. 選取您要套用規則的防火牆。

   如果您未選取作為目標的防火牆，則規則會新增至裝置群組中所有 (未核取) 的防火牆。

   依預設，雖然裝置群組內的虛擬系統核取方塊已停用，所有虛擬系統將繼承提交時的規則，除非您選取一個或多個您想要套用規則的系統。

3. （選用）要從繼承規則中排除防火牆子集，**Install on all but specified devices**（安裝在指定裝置除外的所有裝置上）並選取您想要排除的防火牆。

   如果您選取 *Install on all but specified devices*（安裝在指定裝置除外的所有裝置上），且未選取任何防火牆，則規則不會新增至裝置群組中的任何一個防火牆。

4. 按一下 **OK**（確定）來新增規則。

STEP 4 | 提交並推送設定變更。

1. 選取 **Commit**（提交）> **Commit and Push**（提交並推送），然後在 Push Scope（推送範圍）中 **Edit Selections**（編輯選擇）。
2. 選取 **Device Groups**（裝置群組），選取您新增規則的裝置群組，然後按一下 **OK**（確定）。
3. 將您的變更 **Commit and Push**（提交並推送）至 Panorama 組態和裝置群組。

STEP 5 | 疑難排解原則規則流量匹配 確認規則依據所需允許和拒絕流量。

管理規則階層

原則規則順序對網路的安全至關重要。在任何原則層面（共用、裝置群組或本機定義規則）和規則庫（例如，共用安全預先規則）內，防火牆根據規則在 **Policies**（原則）頁籤內的順序，從上至下對其進行評估。防火牆會對照第一個符合所定義條件的規則來比對封包，而且忽略後續的規則。由此，若要強制執行特定的匹配，將特定規則移動至一般規則上方。



若要瞭解防火牆根據層級和類型（預先規則、後續規則和預設規則）在整個設備群組階層中評估規則的順序，請參閱設備群組原則。

STEP 1 | 檢視每一個規則庫的規則階層。

1. 選取 **Policies**（原則）頁籤，再按一下 **Preview Rules**（預覽規則）。
2. 依據 **Rulebase**（規則庫）（例如，**Security**（安全）或 **QoS**）篩選預覽。
3. 篩選預覽以顯示特定 **Device Group**（裝置群組）的規則和其從共用位置和上階裝置群組繼承的規則。您必須選取被指派了防火牆的裝置群組。
4. 依據 **Device**（裝置）篩選預覽，以顯示其本機定義規則。
5. 按一下綠色箭頭圖示，將您的篩選器選取套用至預覽（請參閱裝置群組原則）。
6. 完成規則預覽後，關閉組合規則預覽對話方塊。

STEP 2 | 如有必要，刪除或停用規則。



若要決定防火牆目前不使用的規則，在 *Panorama Context*（內容）下拉式清單中選取防火牆，選取規則庫（例如，*Policies*（原則）> *Security*（安全性）），然後選取 *Highlight Unused Rules*（反白顯示不使用的規則）核取方塊。虛線的橘色背景表示防火牆未使用的規則。

1. 選取包含您將要刪除或停用的規則的規則庫（例如，**Policies**（原則）> **Security**（安全性）> **Pre Rules**（預先規則））。
2. 選取包含規則的 **Device Group**（裝置群組）。
3. 選取規則，然後視需要按一下 **Delete**（刪除）或 **Disable**（停用）。停用的規則將以斜體字型顯示。

© 2019 Palo Alto Networks, Inc.

STEP 3 | 如有必要，在規則庫內重新置放規則。



若要在防火牆上重新置放本機規則，在執行此步驟前，在 *Context*（內容）下拉式清單中選取防火牆，以存取其 *Web* 介面。

1. 選取包含您將要移動的規則的規則庫（例如，**Policies**（原則）> **Security**（安全性）> **Pre Rules**（預先規則））。
2. 選取包含規則的 **Device Group**（裝置群組）。
3. 選取規則，選取 **Move**（移動），然後選取：
   - **Move Top**（移動至頂部）—在裝置群組中將規則移動至所有其他規則上方（但非共用或上階裝置群組繼承規則上方）。
   - **Move Up**（上移）—將規則移動至其前方規則上方（但非共用或上階裝置群組繼承規則上方）。
   - **Move Down**（下移）—將規則移動至其後續規則下方。
   - **Move Bottom**（移動至底部）—將規則移動至所有其他規則下方。
   - 移至其他設備群組 — 請參閱移動或複製原則規則或物件至不同的設備群組。

STEP 4 | 如果修改規則，請提交並推送變更。

1. 選取 **Commit**（提交）> **Commit and Push**（提交並推送），然後在 Push Scope（推送範圍）中 **Edit Selections**（編輯選擇）。
2. 選取 **Device Groups**（裝置群組），選取包含您已變更或刪除的規則的裝置群組，然後按一下 **OK**（確定）。
3. 將您的變更 **Commit and Push**（提交並推送）至 Panorama 組態和裝置群組。

© 2019 Palo Alto Networks, Inc.

管理範本與範本堆疊

使用範本和範本堆疊定義一般基礎設定，該設定啟用防火牆以在您的網路內操作。在決定將哪些防火牆新增至哪些範本時，將範本在堆疊內排序以管理普通層級和防火牆群組特定設定時，以及使用防火牆特定值取代範本設定時，請參閱範本與範本堆疊以瞭解需要考慮問題的概要。



若要刪除範本，您必須先在防火牆上本機停用/移除範本設定。僅擁有超級使用者角色的管理員可以停用範本。

- 範本功能與例外狀況
- 新增範本
- 設定範本堆疊
- 設定範本或範本堆疊變數
- 匯入及覆寫現有範本堆疊變數
- 取代範本設定
- 停用/移除範本設定

範本功能與例外狀況

您可以使用範本和範本堆疊定義各種設定，但您僅可在各受管理的防火牆上執行下列工作：

- 設定裝置封鎖清單。
- 清除日誌。
- 啟用操作模式，如一般模式、多重虛擬系統模式或 FIPS-CC 模式。
- 設定 HA 配對中防火牆的 IP 位址。
- 設定主要金鑰和診斷。
- 比較組態檔案（組態稽核）。



若要為防火牆管理授權和更新（軟體或內容），請使用 *Panorama* > *Device Management*（裝置管理）頁籤選項，而非範本。

- 重新命名多重虛擬系統防火牆上的虛擬系統。

新增範本

在 Panorama™ 顯示在防火牆上定義網路設定元件和設備設定元件時所需要的 **Device**（裝置）和 **Network**（網路）頁籤前，您必須至少新增一個範本。Panorama 支援最多 1,024 個範本。每個受管理的防火牆必須屬於一個範本堆疊。當範本包含受管理的裝置設定時，範本堆疊允許您管理並推送範本設定到所有指派給範本堆疊的受管理防火牆。



將範本整合至堆疊，以避免在範本中複製許多設定（請參閱範本和範本堆疊與設定範本堆疊）。

STEP 1 | 新增範本。

1. 請選取 **Panorama** > **Templates**（範本）。
2. 按一下 **Add**（新增），並輸入用來識別物件的唯一 **Name**（名稱）。
3. （選用）輸入範本的 **Description**（說明）。
4. 按一下 **OK**（確定）來儲存範本。
5. 如果範本有帶設定的虛擬系統（例如介面），且您希望將 Panorama 將設定推送至無虛擬系統的防火牆，請從 **Default VSYS**（預設 **VSYS**）下拉式清單中選取 vsys，然後按一下**OK**（確定）。

© 2019 Palo Alto Networks, Inc.

6. 選取 **Commit**（提交）> **Commit and Push**（提交並推送），然後將您的變更 **Commit and Push**（提交並推送）至 Panorama 組態和範本。

STEP 2 | 驗證範本可用。

新增第一個範本後，Panorama 上顯示 **Device**（裝置）和 **Network**（網路）頁籤。這些頁籤顯示 **Template**（範本）下拉式清單。檢查下拉式清單是否顯示您剛新增的範本。

STEP 3 | 設定範本堆疊並新增範本至範本堆疊。

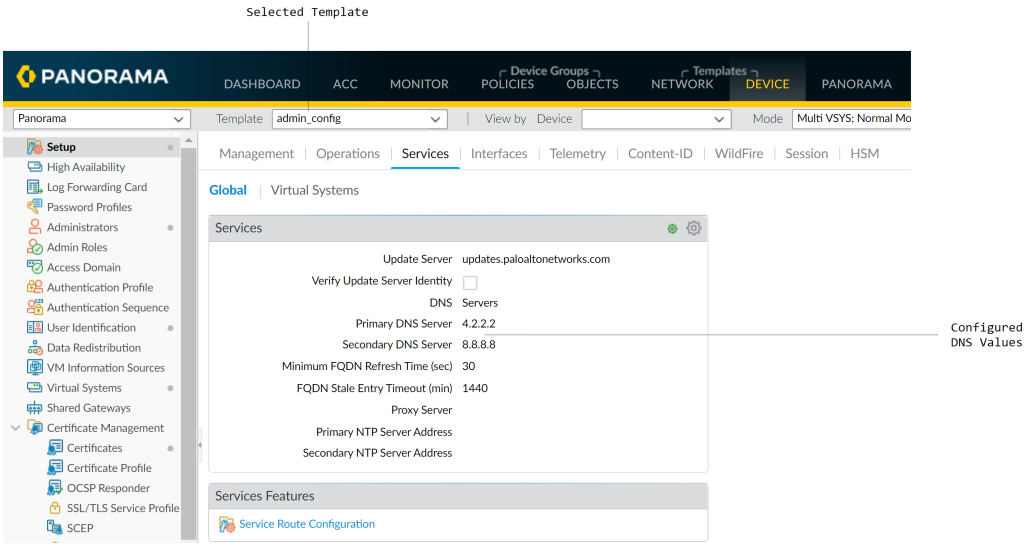
STEP 4 | 使用範本推送設定變更至防火牆。

如果僅允許在本機防火牆而非 *Panorama* 上重新命名 *vsys*，會有全新的 *vsys*，或者新的 *vsys* 名稱可能對應至防火牆上錯誤的 *vsys*。

例如，在範本防火牆內定義主要網域名稱系統 (DNS) 伺服器。

您也可以設定範本或範本堆疊變數，以推送特定的裝置值到受管理的裝置上。

1. 在 **Device**（裝置）頁籤中的下拉式清單中選取 **Template**（範本）。
2. 選取 **Device**（設備）> **Setup**（設定）> **Services**（服務）> **Global**（全域），然後編輯 [服務] 部分。
3. 輸入 **Primary DNS Server**（主要 **DNS** 伺服器）的 IP 位址。

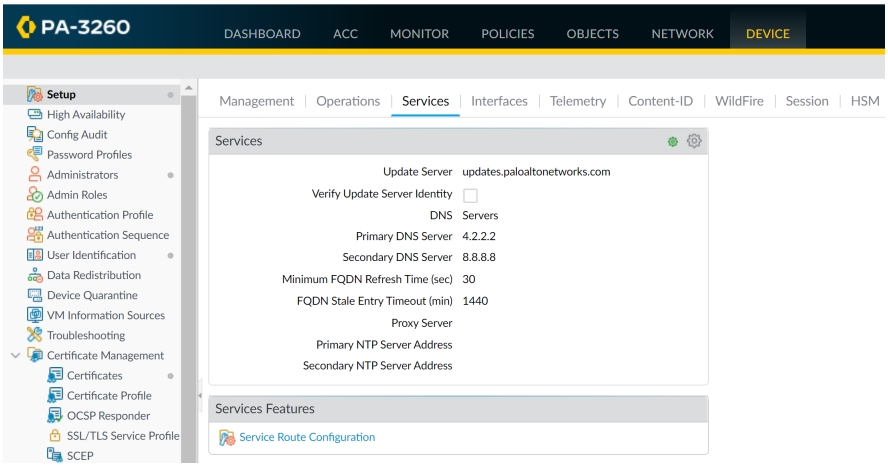


4. 選取 **Commit**（提交）> **Commit and Push**（提交並推送），然後將您的變更 **Commit and Push**（提交並推送）至 Panorama 組態和範本。

STEP 5 | 驗證防火牆是使用您從 Panorama 推送的範本設定所設定。

1. 在 **Context**（內容）下拉式清單中，選取推送範本設定的防火牆之一。
2. 選取 **Device**（裝置）> **Setup**（設定）> **Services**（服務）> **Global**（全域）。顯示您使用範本所推送的 IP 位址。服務部分標頭顯示範本圖示（ ）以表示此部分內的設定帶有從範本推送的值。

© 2019 Palo Alto Networks, Inc.



STEP 6 | 疑難排解網路資源連線 確認您的防火牆可以存取您的網路資源。

設定範本堆疊

範本堆疊是可設定的，且允許結合多個範本以推送完整設定到受管理的防火牆。當範本為可在不同堆疊上重複使用的防火牆組態模組部分時，您也可以設定範本堆疊，以填充您需要套用至指派給該堆疊所有防火牆的其餘設定。Panorama 支援最多 1,024 個範本堆疊，每個堆疊最多可指派給它 8 個範本。您可以參考屬於範本堆疊的範本中的範本堆疊來設定物件。若範本堆疊和堆疊中的範本出現值衝突，則推送範本堆疊中設定的值。如需詳細資訊和規劃，請參閱範本與範本堆疊。

新增範本以設定介面、*VLAN*、*Virtual Wires*、*IPSec* 通道、*DNS Proxy* 和虛擬系統。必須設定這些物件，並透過範本而非範本堆疊推送。透過範本推送後，您可以取代範本堆疊中除虛擬系統外的物件。

STEP 1 | 規劃堆疊內的範本及其順序。

新增範本 您計劃指派給範本堆疊。

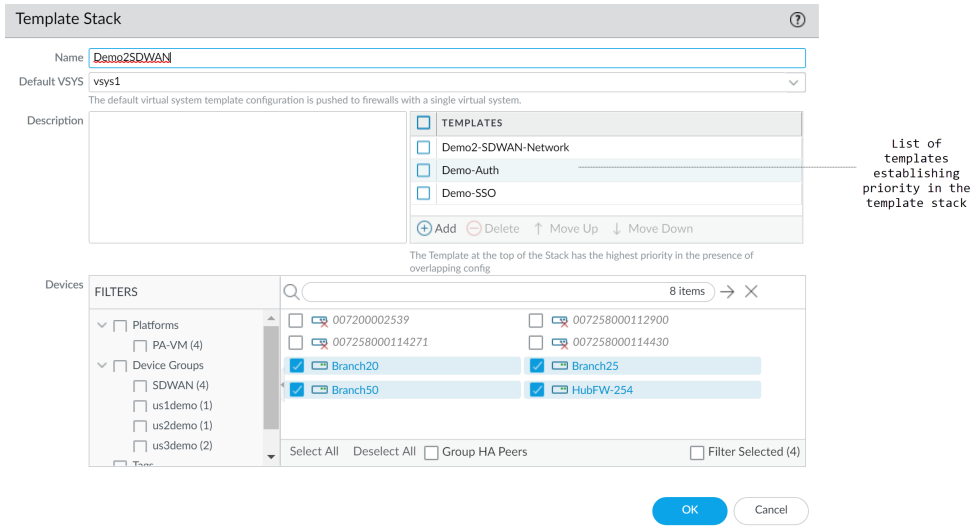
當在堆疊內（為重疊設定）規劃範本的優先順序時，您必須檢查順序以免設定錯誤。例如，堆疊在以太網 *1/1* 介面為類型 *Layer 3* 的 *Template_A* 內但在 *Template_B* 內為帶 *VLAN* 的類型 *Layer 2*。如果 *Template_A* 有較高的優先權限，*Panorama* 將推送以太網 *1/1* 作為類型 *Layer 3* 但指派至 *VLAN*。

還請注意，即使兩個範本位於相同的堆疊，範本設定仍無法參考其他範本中的設定。例如，Template_A 內的區域設定無法參考 Template_B 內的區域保護設定檔。

STEP 2 | 建立範本堆疊。

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. 針對堆疊將合併的各範本（最多 8 個），**Add**（新增）並選取該範本。對話方塊以列出對應重複設定優先級順序中新增的範本，較高範本中的值取代清單中較低範本的值。若要變更順序，請選取範本，並 **Move Up**（上移）或 **Move Down**（下移）。

© 2019 Palo Alto Networks, Inc.



4. 在裝置部分中，選取防火牆以指派它們至堆疊。對於有多個虛擬系統的防火牆，您無法指派個別虛擬系統，而僅能指派整個防火牆。您可以將任何防火牆指派至僅一個範本堆疊。

   每當您將新的受管理防火牆新增至 *Panorama* 時，您必須將它指派給適當的範本堆疊；*Panorama* 不會自動指派新的防火牆給範本或範本堆疊。當您將設定變更推送至範本時，*Panorama* 會將設定推送至每個指派給該範本堆疊的防火牆。

5. （選用）選取 **Group HA Peers**（群組 **HA** 對等），只顯示單一核取方塊來含括 high availability (高可用性 - HA) 設定中的防火牆。圖示表示 HA 狀態：綠色表示主動，黃色表示被動。次要端點防火牆名稱位於括弧內。

   對於主動/被動 HA，新增兩種端點至相同範本，讓兩者都會接收設定。對於主動/主動 HA，是否新增兩種端點至相同範本視乎各端點是否需要相同的設定而定。對於 PAN-OS 在 HA 端點之間同步的設定清單，請參閱高可用性同步。

6. 按一下 **OK**（確定）來儲存範本堆疊。

STEP 3 | （可選用）設定範本或範本堆疊變數。

STEP 4 | 必要時，編輯 **Network**（網路）和 **Device**（裝置）設定。

僅允許在本機防火牆上重新命名 *vsys*。如果在 *Panorama* 上重新命名 *vsys*，會有全新的 *vsys*，或者新的 *vsys* 名稱可能對應至防火牆上錯誤的 *vsys*。

在單一防火牆內容中，您可以取代 Panorama 從堆疊推送的設定，方式與取代從範本推送的設定一致：請參閱覆蓋範本或範本堆疊值。

1. 篩選頁籤以僅顯示您希望編輯的指定模式設定：

   在 *Panorama* 僅推送指定模式設定至支援這些模式的防火牆時，此選取性推送不會對指定模式值進行調整。例如，如果範本有聯邦資訊處理標準 *(FIPS)* 模式的防火牆，還有使用非 *FIPS* 演算法的 *IKE Crypto* 設定檔，範本推送會失敗。若要避免此錯誤，使用 *Network*（網路）和 *Device*（裝置）頁籤下的 *Mode*（模式）下拉式清單篩選指定模式功能和值選項。

   - 在 **Mode**（模式）下拉式清單中，選取或清除 **Multi VSYS**（多 **VSYS**）、**Operational Mode**（操作模式）和 **VPN Mode**（**VPN** 模式）篩選器選項。
   - 設定所有 **Mode**（模式）選項以反射特定防火牆的模式設定，具體方法是在 **Device**（裝置）下拉式清單中將其選取。

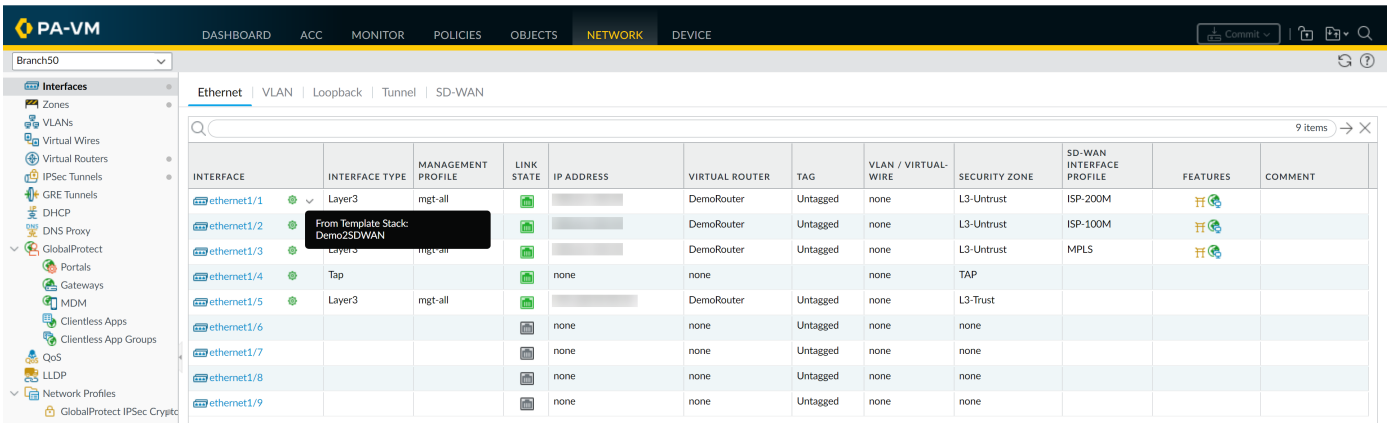
2. 設定介面和網路連線。舉例來說，設定區域與介面以分割網路管理並控制通過防火牆的流量。

© 2019 Palo Alto Networks, Inc.

3. 根據需要編輯設定。
4. 選取 **Commit**（提交）> **Commit and Push**（提交並推送）、在 Push Scope（推送範圍）中 **Edit Selections**（編輯選取）、選取 **Templates**（範本）、選取指派給範本堆疊的防火牆，然後將您的變更 **Commit and Push**（提交並推送）至 Panorama 組態和範本堆疊。

STEP 5 | 確認範本堆疊正常工作。

1. 從 **Context**（內容）下拉式清單中選取一個指派給範本堆疊的裝置。
2. 選取使用範本堆疊將設定變更推送到的頁籤。
3. 透過範本堆疊推送的值會顯示範本圖示（ ），以表示此部分內的設定帶有從範本堆疊推送的值。將滑鼠懸停在堆疊上以檢視值為哪一個範本堆疊推送出去的。



STEP 6 | 疑難排解網路資源連線 確認您的防火牆可以存取您的網路資源。

設定範本或範本堆疊變數

要讓您更輕鬆地重覆使用範本或範本堆疊，您可以使用範本和範本堆疊變數以取代 IP 位址、群組 ID 和設定中的介面。範本變數在範本或範本堆疊層級中定義，且您可以使用變數以取代 IP 位址、IP 範圍、FQDN、在 IKE、VPN、和 HA 設定中的介面以及群組 ID。在範本中定義的變數取代了在範本堆疊中的變數，因為範本設定與範本堆疊設定相比，有較高的優先次序。變數讓您可以減少需要管理的範本和範本堆疊總數量，同時讓您可以保留任何防火牆或設備特定的值。舉例來說，如果您有一個附基本設定的範本堆疊，您可以使用變數建立不套用在範本或範本堆疊中所有防火牆的值。此讓您能夠管理並從較少的範本和範本堆疊中推送設定，同時在您可以建立新範本或範本堆疊前，所需要任何防火牆特定或設備特定值。

若要建立範本或範本堆疊變數：

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 建立範本與範本堆疊。

1. 新增範本
2. 設定範本堆疊。

STEP 3 | 選取 **Panorama** > **Templates**（範本）並 **Manage**（管理）（變數欄）您想要建立變數的範本或範本堆疊。

STEP 4 | **Add**（新增）新變數。

變數名稱必須以錢字號（$）開頭。

1. 命名新變數。在本例中，變數名稱為 `$DNS-primary` 和 `$DNS-secondary`。
2. 選取變數 **Type**（類型），然後為所選變數類型輸入相應的值。

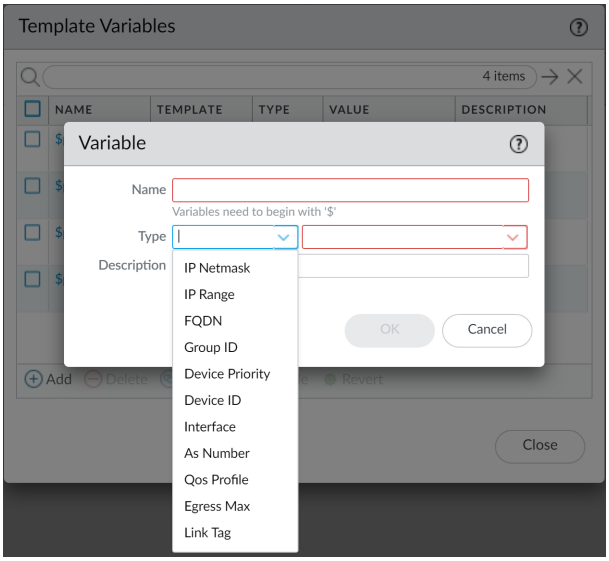
© 2019 Palo Alto Networks, Inc.

對於此範例，選取 **IP Netmask**（**IP 網路遮罩**）。

3. （選用）輸入變數的說明。
4. 按一下 **OK**（確定）與 **Close**（關閉）。



也可以建立變數內嵌於支援的變數。

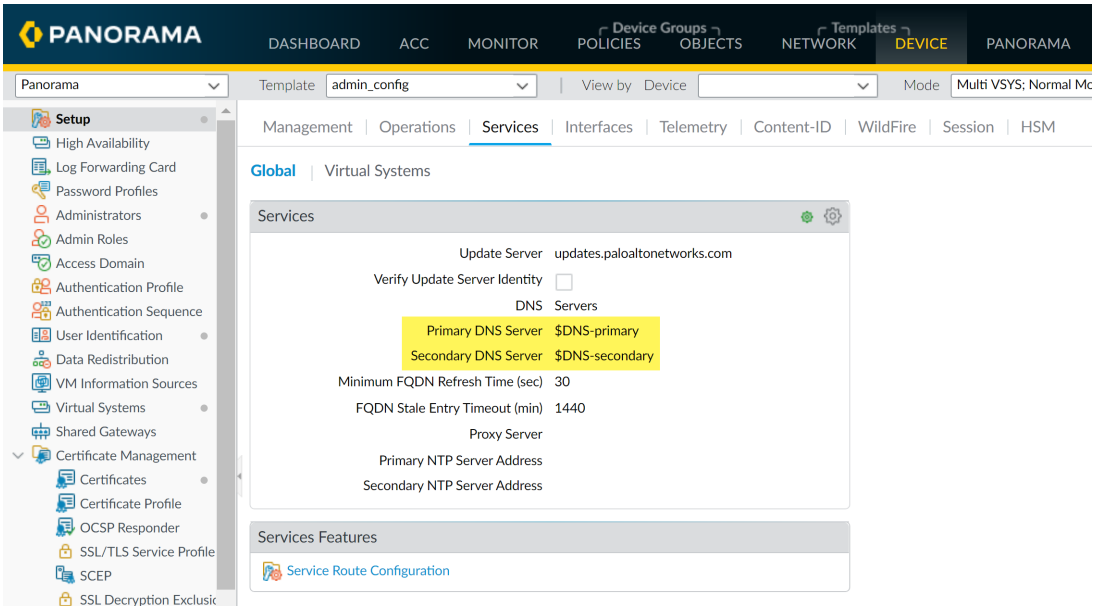


STEP 5 | 從 **Template**（範本）下拉式選單中，選取變數所屬的範本或範本堆疊。

STEP 6 | 在適當位置輸入變數。

就本例來說，參考之前定義的 DNS 值。

1. 選取 **Device**（裝置）> **Setup**（設定）> **Services**（服務），然後編輯服務。
2. 輸入 **`$DNS-primary`** 或從 **Primary DNS Server**（主要 **DNS** 伺服器）下拉式選單中選取它。
3. 輸入 **$DNS-secondary**或從 **Secondary DNS Server**（次要 **DNS** 伺服器）下拉式選單中選取它。
4. 按一下 **OK**（確定）。



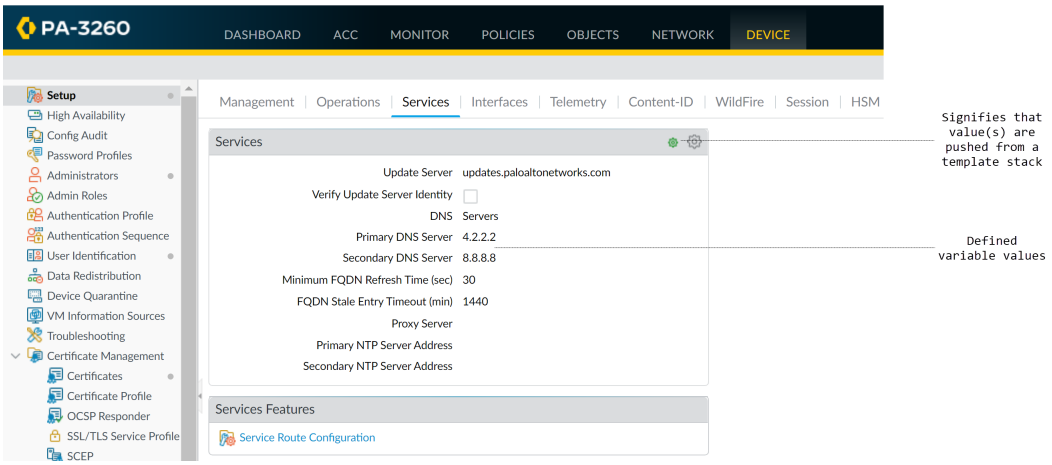
© 2019 Palo Alto Networks, Inc.

STEP 7 | 按一下 **Commit**（提交）並 **Commit and Push**（提交並推送）您的變更至受管理的防火牆。

當您將裝置群組組態與參考推送至範本或範本堆疊變量時，您必須 *Edit Selections*（編輯選擇）並 *Include Device and Network Templates*（包含裝置與網路範本）。

STEP 8 | 確認所有變數的值都已推送至受管理的裝置。

1. 從 **Context**（內容）下拉式清單，選取屬於建立變數的範本堆疊的防火牆。
2. 選取 **Device**（裝置）> **Setup**（設定）> **Services**（服務）。
3. 以範本或範本堆疊定義的值設定乃透過範本符號（.）表示。將游標停留在項目上以檢視變數定義所屬的範本和範本堆疊。當從防火牆檢視內容時，變數會顯示為您為變數設定的 IP 位址。



STEP 9 | 疑難排解網路資源連線 確認您的防火牆可以存取您的網路資源。

匯入及覆寫現有範本堆疊變數

使用範本堆疊變數來取代 IP 位址、IP 範圍、FQDN、介面、或您的防火牆組態中的群組 ID。變數讓您可以減少需要管理的範本和範本堆疊總數量，同時讓您可以保留任何防火牆特定值。

匯入範本堆疊變數可讓您覆寫多個現有變數的值，但匯入時您不能建立新的範本堆疊變數。如需更多有關如何建立新的範本或範本堆疊變數的資訊，請參閱 設定範本或範本堆疊變數。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 匯入現有範本堆疊變數。

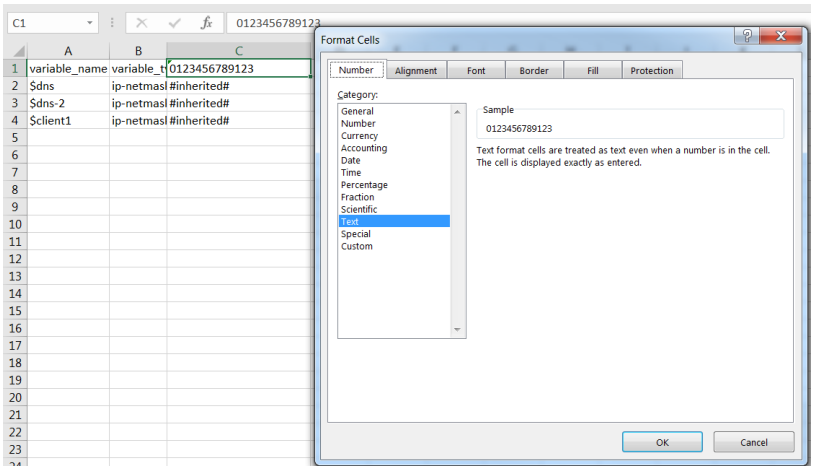
1. 選取 **Panorama** > **Templates**（**Panorama** 範本），並且選取範本或範本堆疊。
2. 選取 **Variable CSV**（變數 **CSV**）> **Export**（匯出）。設定的範本堆疊變數會在本機以 CSV 檔案格式下載。
3. 開啟匯出的 CSV。

STEP 3 | 編輯包含範本堆疊變數的 CSV 檔案，以下列格式匯入至 Panorama：

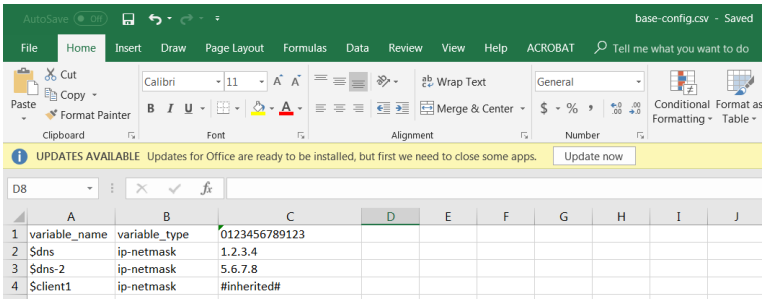
顯示為 `#inherited#` 的值是範本堆疊中定義的值。

1. 更正包含防火牆序號的資料格編號。針對 CSV 檔案中的所有防火牆重複這些步驟。
   1. 在包含防火牆序號的資料格上按一下滑鼠右鍵，然後選取 **Format Cells**（格式資料格。
   2. 選取 **Number**（編號）> **Text**（文字），然後按一下 **OK**（確定）。
   3. 在序號開頭加上 **0**。

© 2019 Palo Alto Networks, Inc.



2. 輸入所需範本變數的新值。
3. 選取 **File**（檔案）> **Save As**（另存新檔），然後以 **CSV UTF-8** 格式儲存檔案。



STEP 4 | 匯入 CSV 檔案至範本堆疊。

1. 登入 Panorama 網頁介面。
2. 選取 **Panorama** > **Templates**（範本），然後選取您要在 步驟 2 匯出變數的範本堆疊。
3. 選取 **Variable CSV**（變數 CSV）> **Import**（匯入）及 **Browse**（瀏覽）在步驟 3 中編輯的 CSV 檔案。
4. 按一下 **OK**（確定）來匯入範本堆疊變數。

STEP 5 | 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

STEP 6 | 在適當位置輸入變數。

STEP 7 | 按一下 **Commit**（提交）並 **Commit and Push**（提交並推送）您的變更至受管理的防火牆。

當您將裝置群組組態與參考推送至範本或範本堆疊變量時，您必須 *Edit Selections*（編輯選擇）並 *Include Device and Network Templates*（包含裝置與網路範本）。

取代範本或範本堆疊值

雖然範本與範本堆疊能讓您套用基礎設定至多個防火牆，但您可能會想要設定防火牆特有的設定，且這些設定不會套用至範本或範本堆疊中的所有防火牆。相反地，您可能想要取代範本設定以建立範本堆疊設定，以套用至所有受管理的防火牆，作為基本設定。取代可讓您針對設定需求來設定例外或進行修改。例如，如果使用範本建立基礎設定，但測試實驗室環境有一些防火牆需要針對網域名稱系統 (DNS) 伺服器 IP 位址或網路時間協定 (NTP) 伺服器進行不同的設定，則您可以取代範本和範本堆疊設定。

© 2019 Palo Alto Networks, Inc.

如果您想要停用或移除防火牆上的所有範本或堆疊設定，而非取代單一值，請參閱停用/移除範本設定。

您可以使用以下任一種方式取代範本或範本堆疊值：

- 取代防火牆的範本值l或使用變數取代範本或範本堆疊值—有兩種取代推送自範本或範本堆疊值的方法。第一種為在防火牆上定義本機的值，以取代推送自範本或範本堆疊的值。第二種為定義防火牆特定變數，以取代推送自範本或範本堆疊的值。
- 使用範本堆疊取代範本值—定義範本堆疊上的值或變數以取代推送自範本的值。

取代防火牆上的範本值

取代從範本或範本堆疊推送的本機防火牆上的設定，以建立特定防火牆組態。這讓您可以自 Panorama™ 管理基本範本或範本堆，同時維護未套用在其他防火牆上的任何特定防火牆組態。

STEP 1 | 存取防火牆 Web 介面。

透過在瀏覽器 URL 欄內輸入 IP 位址直接存取防火牆，或使用 Panorama 中的 **Context**（內容）下拉式清單切換至防火牆內容。

STEP 2 | 取代從範本或範本堆疊推送的值。

在此範例中，您會取代您使用新增範本中的範本所指定的 DNS 伺服器 IP 位址

1. 選取 **Device**（裝置）> **Setup**（設定）> **Services**（服務），然後編輯服務部分。
2. 按一下 **Primary DNS Server**（主要 **DNS** 伺服器）的範本圖示（ ）以啟用該欄的取代。
3. 輸入 **Primary DNS Server**（主要 **DNS** 伺服器）的新 IP 位址。範本取代符號（ ）表示範本值已被取代。
4. 按一下 **OK**（確定）並 **Commit**（交付）變更。

使用範本堆疊取代範本值

您可以使用範本堆疊以取代從範本推送至受管理防火牆的設定，以建立可用來管理來自 Panorama™受管理防火牆的基本設定。這讓您可以利用 Panorama 的管理容量從單一位置推送設定變更至多個裝置。在這個例子中，您將使用範本堆疊以取代從範本推送出來，被稱為 `$DNS` 的主要 DNS 伺服器 IP 位址變數。

Panorama 支援使用範本堆疊覆寫範本中設定的介面，彙總介面的 *Layer2* 子介面除外。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 從 **Template**（範本）下拉式清單中，選取將覆寫範本設定的範本堆疊。

STEP 3 | 取代推送的範本設定。

1. 選取 **Device**（裝置）> **Setup**（設定）> **Services**（服務），然後編輯服務部分。
2. 用 IP 位址設定 **Primary DNS**（主要 **DNS**）以取代推送範本設定，並按一下 **OK**（確認）。

STEP 4 | **Commit and Push**（提交並推送）設定變更。

使用範本堆疊變數取代範本值

您可以使用範本堆疊值和變數以取代從範本推送至受管理防火牆的設定，以建立可用來管理來自 Panorama™受管理防火牆的基本設定。這讓您可以利用 Panorama 的管理容量從單一位置推送設定變更至多個防火牆。在這個例子中，您將透過取代稱為 `$DNS` 的主要 DNS 伺服器 IP 位址變數，以建立一個範本堆疊變數。

© 2019 Palo Alto Networks, Inc.

Panorama 支援使用範本堆疊覆寫範本中設定的介面，彙總介面的 *Layer2* 子介面除外。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 取代範本變數。

1. 請選取 **Panorama** > **Templates**（範本）。
2. **Manage**（管理）（變數欄）範本堆疊所含您需要取代的範本變數。
3. 找出並選取 **$DNS** 變數。
4. 選取 **Override**（取代）。
5. 輸入新變數值，然後按一下 **OK**（確定）。

STEP 3 | **Commit and Push**（提交並推送）您的變更。

使用變數取代範本或範本堆疊值

您可以使用特定防火牆變數以取代從範本或範本堆疊推送至受管理的防火牆的變數，以建立特定防火牆組態。這讓您可以管理基本範本或範本堆疊，同時維護未套用在其他防火牆上的任何特定防火牆組態—全部來自 Panorama™。這讓您可以利用 Panorama 管理容量的同時，計算任何個別防火牆需要的特定配置。在本例中，自範本推送出來的主要 DNS 伺服器 IP 位址變數（稱做 `$DNS`）將被取代以建立指定防火牆變數。

您可以取代尚未取代的範本或範本堆疊變數。如果範本或範本堆疊變數已被取代，則 *Revert*（復原）取代以建立特定防火牆變數。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 取代範本或範本堆疊變數。

1. 選取 **Panorama** > **Managed Devices**（受管理的裝置）> **Summary**（摘要）。
2. **Edit**（編輯）（變數欄）防火牆所含您需要取代的變數。
3. 找出並選取 **$DNS** 變數。
4. 選取 **Override**（取代）。
5. 輸入新防火牆特定 IP 位址，然後按一下 **OK**（確定）。

STEP 3 | **Commit and Push**（提交並推送）您的變更。

停用/移除範本設定

若要停止使用範本或範本堆疊來管理受管理防火牆上的設定，您可以停用範本或堆疊。停用時，您可以複製範本/堆疊值至防火牆本機設定或刪除該值。

如果您希望取代單一設定而非停用或移除各副本或堆疊設定，請參閱覆蓋範本設定。

請參閱範本與範本堆疊以取得如何使用這些內容管理防火牆的詳細資訊。

STEP 1 | 以帶有超級使用者角色的管理員身份存取受管理的防火牆網頁介面。您可以在瀏覽器的 URL 欄位中輸入防火牆的 IP 位址，以直接存取防火牆，或是在 Panorama 的 **Context**（內容）下拉式清單中選取該防火牆。

STEP 2 | 選取 **Device**（裝置）> **Setup**（設定）> **Management**（管理），再編輯 [Panorama 設定]。

STEP 3 | 選取 **Disable Device and Network Template**（停用裝置與網路範本）。

© 2019 Palo Alto Networks, Inc.

STEP 4 | （選用）選取 **Import Device and Network Template before disabling**（停用前匯入裝置與網路範本），將組態設定儲存在防火牆本機。如果您未選取此選項，PAN-OS 將會刪除防火牆中所有由 Panorama 推送的設定。

STEP 5 | 按一下 **OK**（確定）兩次，然後 **Commit**（提交）變更。

© 2019 Palo Alto Networks, Inc.

從 Panorama 管理主要金鑰

Panorama、防火牆、日誌收集器和 WF-500 設備使用主要金鑰加密設定內的敏感元素，並帶有預設主要金鑰用於加密密碼和設定元素。

作為標準安全做法的一部分，您應更換預設主要金鑰，並在過期前變更各單個防火牆、日誌收集器、WildFire 設備和 Panorama 上的金鑰。您必須對您的所有受管理裝置部署相同的主要金鑰，並設定 Panorama 上的主要金鑰，以成功從 Panorama 向您的受管理裝置推送組態。要確保統一的金鑰部署，從 Panorama 直接向多個防火牆、日誌收集器和 WF-500 設備部署一個新的主要金鑰或更新過期的金鑰。請參閱 設定主要金鑰 ，獲取關於設定主要金鑰的更多資訊。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | （ 最佳做法 ）選取 **Commit**（提交）和 **Commit and Push**（提交與推送）任何擱置組態變更。

Panorama 必須使用新的主要金鑰重新加密資料。要確保所有設定元素均透過新主要金鑰加密，您應在部署新的主要金鑰之前，提交所有擱置變更。

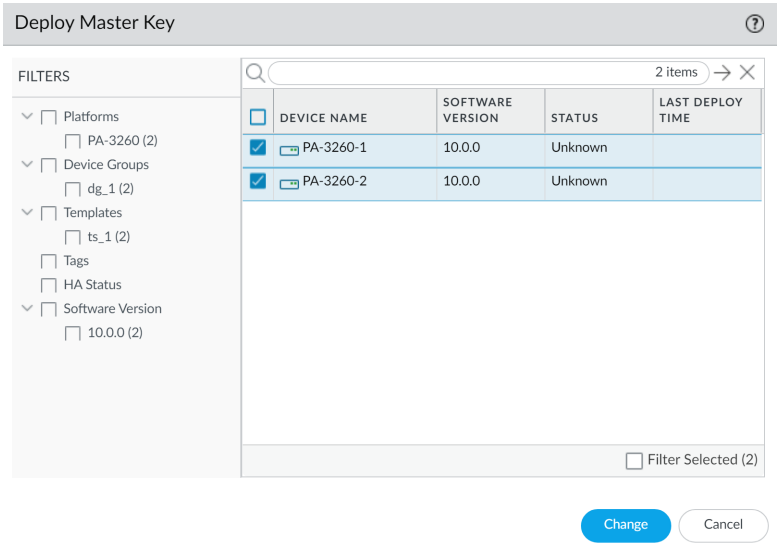
STEP 3 | 設定防火牆、日誌收集器和 WildFire 設備主要金鑰，以在金鑰生命週期結束後，透過相同的主要金鑰自動更新。

自動更新主要金鑰讓您可以在維護窗口前的金鑰過期時，保持設定的加密，但這不是金鑰生命週期過期之後部署新主要金鑰的替代方法。考慮設定主要金鑰以在其存留時間到期後自動更新時，距離下一個可用維護窗口的天數。

1. 選取 **Device**（裝置）> **Master Key and Diagnostics**（主要金鑰與診斷）），然後編輯 Master Key（主要金鑰）設定。
2. 設定 Panorama 以在指定的天數和小時數內 **Auto Renew with Same Master Key**（透過相同的主要金鑰自動更新）。

STEP 4 | 部署主要金鑰至受管理的防火牆。

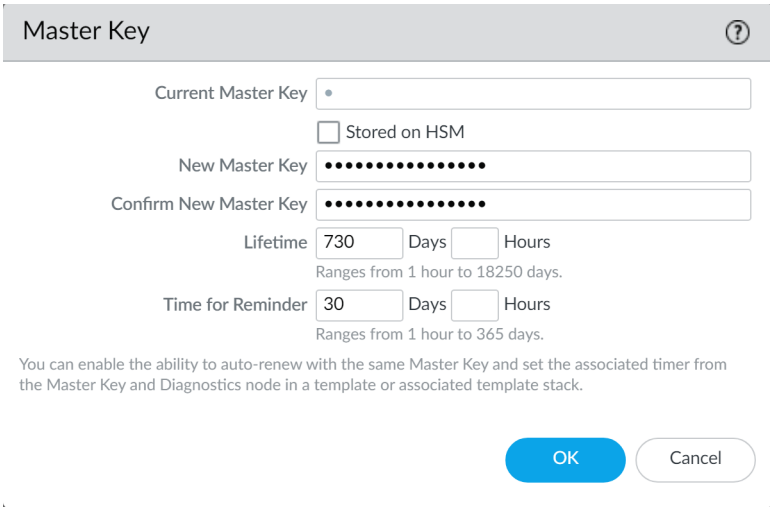
1. 選取 **Panorama** > **Managed Devices**（受管理的裝置）> **Summary**（摘要）並 **Deploy Master Key**（部署主要金鑰）。
2. 選取所有壯漢子並 **Change**（變更）主要金鑰。



3. 設定主要金鑰：

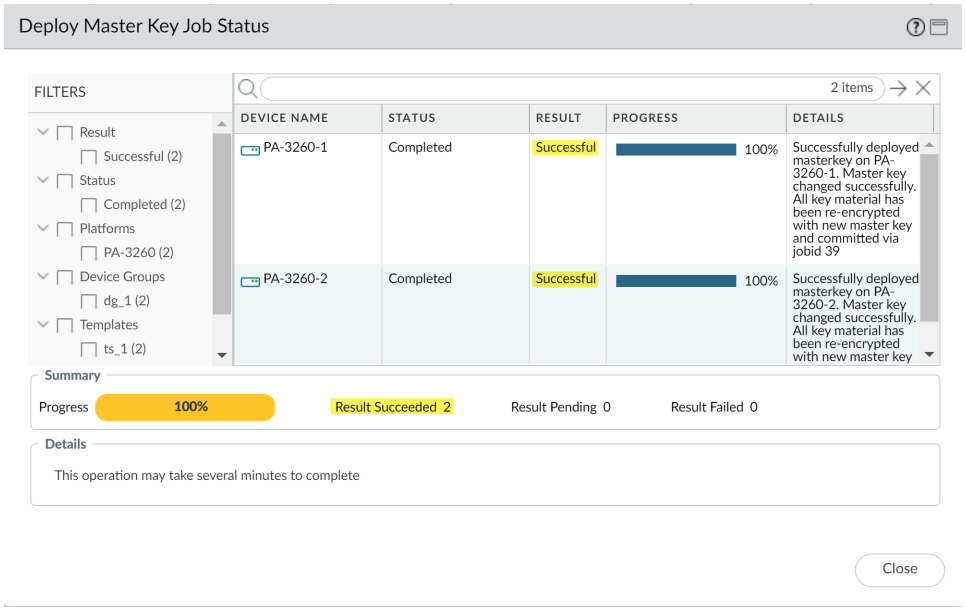
© 2019 Palo Alto Networks, Inc.

1. 如果要更新主要金鑰，輸入 **Current Master Key**（當前主要金鑰）。如果您透過新的主要金鑰更換預設主要金鑰，不得指定 **Current Master Key**（當前主要金鑰）。
2. 指定 **New Master Key**（新主要金鑰）並 **Confirm Master Key**（確認主要金鑰）。
3. 設定主要金鑰 **Lifetime**（生命週期）與 **Time for Reminder**（提醒時間）。
4. 按一下 **OK**（確定）。



4. 確認主要金鑰已成功部署至所有已選裝置。

   當您從 Panorama 部署新的主要金鑰時，系統日誌產生。



STEP 5 | 部署主要金鑰至日誌收集器。主要緊要必須與第 3 步中部署的金鑰一致。

1. 選取 **Panorama** > **Managed Devices**（受管理的裝置）和 **Deploy Master Key**（部署主要金鑰）。
2. 選取所有壯漢子並 **Change**（變更）主要金鑰。
3. 設定主要金鑰：
   1. 如果要更新主要金鑰，輸入 **Current Master Key**（當前主要金鑰）。如果您透過新的主要金鑰更換預設主要金鑰，不得指定 **Current Master Key**（當前主要金鑰）。
   2. 指定 **New Master Key**（新主要金鑰）並 **Confirm Master Key**（確認主要金鑰）。
   3. 設定主要金鑰 **Lifetime**（生命週期）與 **Time for Reminder**（提醒時間）。

© 2019 Palo Alto Networks, Inc.

4. 按一下 **OK**（確定）。

4. 確認主要金鑰已成功部署至所有已選裝置。

   當您從 Panorama 部署新的主要金鑰時，系統日誌產生。

STEP 6 | 部署主要金鑰至受管理的 WildFire 設備。主要緊要必須與第 3 步中部署的金鑰一致。

1. 選取 **Panorama** > **Managed WildFire Appliances**（受管理的 **WildFire** 設備）和 **Deploy Master Key**（部署主要金鑰）。
2. 選取所有壯漢子並 **Change**（變更）主要金鑰。
3. 設定主要金鑰：
   1. 如果要更新主要金鑰，輸入 **Current Master Key**（當前主要金鑰）。如果您透過新的主要金鑰更換預設主要金鑰，不得指定 **Current Master Key**（當前主要金鑰）。
   2. 指定 **New Master Key**（新主要金鑰）並 **Confirm Master Key**（確認主要金鑰）。
   3. 設定主要金鑰 **Lifetime**（生命週期）與 **Time for Reminder**（提醒時間）。
   4. 按一下 **OK**（確定）。
4. 確認主要金鑰已成功部署至所有已選裝置。

   當您從 Panorama 部署新的主要金鑰時，系統日誌產生。

STEP 7 | 設定 Panorama 上的主要金鑰。主要金鑰必須與透過第 3 步至第 5 步部署至防火牆、日誌收集器和 WildFire 設備上的金鑰一致。

1. 選取 **Panorama** > **Master Key and Diagnostics**（主要金鑰與診斷），然後設定主要金鑰。
   1. 如果要更新主要金鑰，輸入 **Current Master Key**（當前主要金鑰）。如果您透過新的主要金鑰更換預設主要金鑰，不得指定 **Current Master Key**（當前主要金鑰）。
   2. 設定 **New Master Key**（新主要金鑰）並 **Confirm Master Key**（確認主要金鑰）。
   3. 設定主要金鑰 **Lifetime**（生命週期）與 **Time for Reminder**（提醒時間）。
   4. 按一下 **OK**（確定）。
2. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

© 2019 Palo Alto Networks, Inc.

設定企業資料遺失防護 (DLP)

使用企業資料遺失防護 (DLP) 來執行組織的資料安全性標準，以防止意外的資料誤用、遺失或被盜。

- 企業資料遺失防護 (DLP) 概要介紹
- 企業資料遺失防護 (DLP) 支援什麼？
- 預先定義的資料篩選設定檔
- 安裝企業資料遺失防護 (DLP) 外掛程式
- 建立資料模式
- 建立資料篩選設定檔
- 啟用企業資料遺失防護 (DLP)
- 檢視企業資料遺失防護 (DLP) 日誌詳細資料
- 編輯企業資料遺失防護 (DLP) 設定
- 啟用現有資料模式和篩選設定檔
- 解除安裝企業資料遺失防護 (DLP) 外掛程式

企業資料遺失防護 (DLP) 概要介紹

資料遺失防護 (DLP) 是一組工具和程序，可幫助您保護敏感資料，以防被未經授權存取、誤用、擷取或共用。DLP 外掛程式安裝在 Panorama 管理伺服器上，您可以在其中集中管理強制執行組織資料安全標準的資料模式和資料篩選設定檔，並防止受管理防火牆在行動使用者和遠端網路中丟失敏感資料。資料模式和資料篩選設定檔設計用於在執行 PAN-OS 10.0.2 和更高版本的所有受支援 Panorama 和防火牆型號上工作，以在所有位置提供一致的資料安全性。要利用企業 DLP，Panorama 和受管理防火牆必須具有網際網路連線。

企業 DLP 是一項基於雲端的服務，使用受監督的機器學習演算法進行文件分類，將敏感文件分為財務、法律、醫療和其他類別，防止暴露、資料遺失和資料外洩。這些模式可以識別流經網路的流量中的敏感資訊，並保護它們免遭暴露。

企業 DLP 允許您透過以下方式保護敏感資料：

- 防止檔案上傳洩露到未經認可的 **Web** 應用程式—探索並有條件地阻止敏感資料洩露到不受信任的 Web 應用程式。
- 監控到認可 **Web** 應用程式的上傳—探索並監控上傳到經認可企業應用程式的敏感資料。

為幫助您檢查內容和分析正確上下文中的資料，以便您能夠準確地識別敏感資料，並提供保護以防止發生意外，企業 DLP 將透過雲端服務啟用。企業 DLP 支援超過 380 種資料模式和許多預先定義的資料篩選設定檔。企業 DLP 可在新模式和設定檔新增到雲端服務後，立即自動使其可在安全性原則規則中使用。使用以下工具設定企業 DLP：

- 資料模式—幫助您偵測敏感內容，以及如何在網路上共用和存取該內容。

  預先定義的資料模式和內建設定讓您可以輕鬆保護包含特定檔案屬性（如文件標題或作者）、信用卡號、不同國家的監管資訊（如駕照編號）和協力廠商 DLP 標籤的檔案。要提高組織中敏感資料的偵測率，您可以建立特定於您的內容偵測和資料保護要求的自訂資料模式，作為預先定義資料模式的補充。在自訂資料模式中，您還可以定義規則運算式和檔案屬性，以在檔案的自訂或擴充屬性中查找中繼資料或屬性，並在資料篩選設定檔中使用。
- 資料篩選設定檔—支援資料分類並監控受管理防火牆上可用的功能，以防止資料遺失並減少業務風險。

  資料篩選設定檔是資料模式的集合，這些資料模式被重新分組在一起以掃描特定的物件或內容類型。為執行內容分析，預先定義的資料篩選設定檔具有包括行業標準資料識別碼、關鍵字和內建邏輯（以機器學習、規則運算式以及法律和財務資料模式總和檢查碼的形式）的資料模式。當您在安全性原則規則中使用資料篩選設定檔時，防火牆可以檢查流量中的相符項並採取動作。

  在利用資料模式（無論是預先定義還是自訂）後，您可以從 Panorama 管理資料篩選設定檔。您可以使用預先定義的資料篩選設定檔，或建立新設定檔，然後向其新增資料模式。然後建立安全性原則，並將您

© 2019 Palo Alto Networks, Inc.

新增的設定檔套用到建立的原則。如果使用者上傳一個檔案，且檔案中的資料與原則中的準則相符，則受管理防火牆會建立一個警示通知或封鎖檔案上傳。

當您將資料篩選設定檔套用到安全性原則規則時，受管理防火牆會產生資料篩選日誌，其中包含與資料篩選設定檔中一個或多個資料模式相符之流量的詳細資訊。日誌詳細資料可讓您驗證上傳的檔案是產生了警示通知還是被封鎖，從而進行鑑識。

您可在資料篩選日誌中檢視程式碼片段。依預設，受管理防火牆使用資料遮罩部分遮罩程式碼片段，以防止洩露敏感資料。您可以設定受管理防火牆完全遮罩敏感資訊、不遮罩程式碼片段或停用程式碼片段擷取和檢視。

要提高偵測準確性並減少誤報，您還可以指定：

- 鄰近關鍵字—當關鍵字在運算式 200 個字元的距離內時，會為資產分配較高的準確性概率。如果在一個文件中，一個 16 位數後緊跟 `Visa` 字樣，這很可能是信用卡號。但如果 Visa 是文字的標題，16 位數位於這個 22 頁文件的最後一頁，則不太可能是信用卡號。

  您還可以在一個關鍵字群組中使用多個關鍵字，並包括或排除關鍵字，以查找特定單詞是否出現在運算式的 200 個字元之內。
- 信賴等級—信賴等級與鄰近關鍵字一起，可讓您指定一個模式相符項中鄰近關鍵字出現的可能性。當信賴等級為 **Low**（低）時，受管理防火牆不會使用鄰近關鍵字來識別相符項；當信賴等級為 **High**（高）時，受管理防火牆在將檔案中的資料模式視為相符項之前，會在模式中規則運算式的 200 個字元內查找鄰近關鍵字。
- 基本和加權規則運算式—規則運算式描述如何搜尋特定文字模式，然後在找到模式相符項時顯示相符項出現次數。有兩種類型的規則運算式—*basic*（基本）和 *weighted*（加權）。
  - 基本規則運算式搜尋特定文字模式。當找到模式相符項時，服務會顯示相符項出現次數。
  - 加權規則運算式會向文字項目指派一個分數。當超過分數閾值時，服務會返回模式的一個相符項。

    為減少誤報和最大化規則運算式的搜尋效能，您可以在建立資料模式時使用加權規則運算式建立器指派分數，以查找對您而言重要的資訊並為其計算分數。評分會採用一個比對閾值，當超過分數閾值時，例如，當一個模式有足夠多的運算式與一項資產相符時，該資產將被表示為該模式的相符項。

    如需更多資訊，包括使用案例和最佳做法，請參閱 Prisma SaaS 管理員指南中的設定規則運算式。

企業資料遺失防護 (DLP) 支援什麼？

除執行 PAN-OS 10.0.2 或更高版本且具有最低應用程式和威脅內容版本 8334-6362 的 CN-Series 防火牆外，所有基於硬體的防火牆和 VM-Series 防火牆均支援企業資料遺失防護 (DLP)。

以下是可以與企業資料遺失防護 (DLP) 一起使用的受支援應用程式和操作參數。

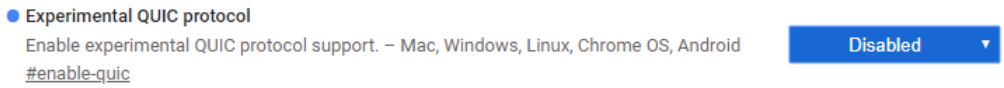
Web 應用程式	PDF	doc/docx	ppt/pptx	xls/xlsx	rtf	Csv	多檔案上傳	檔案大小
Web 瀏覽	是	是	是	是	是	是	是	20MB
Onedrive Web 應用程式	是	是	是	是	是	是	是	20MB
Sharepoint Web 應用程式	是	是	是	是	是	是	是	20MB

© 2019 Palo Alto Networks, Inc.

Web 應用程式	PDF	doc/docx	ppt/pptx	xls/xlsx	rtf	Csv	多檔案上傳	檔案大小
Gmail Web 應用程式	是	是	是	是	是	是	是	20MB
Box Web App	是	是	是	是	是	是	是	20MB
Slack Web 應用程式	是	是	是	是	是	是	是	20MB

- 應用程式—您可以為以下應用程式基於 Web（基於 HTTP 或 HTTPS）的上傳執行 DLP：
  - Box（App-ID 為 boxnet-uploading）
  - Gmail（App-ID 為 gmail-uploading）

    要使用 *Gmail*，您必須停用 *QUIC* 通訊協定。*Palo Alto Networks* 推薦在 *Chrome* 中停用 *QUIC*。要執行此操作，請在 *Chrome* 的 *URL* 列中指定 `chrome://flags/`，找到實驗性 *QUIC* 通訊協定，然後選取 *Disabled*（已停用）。

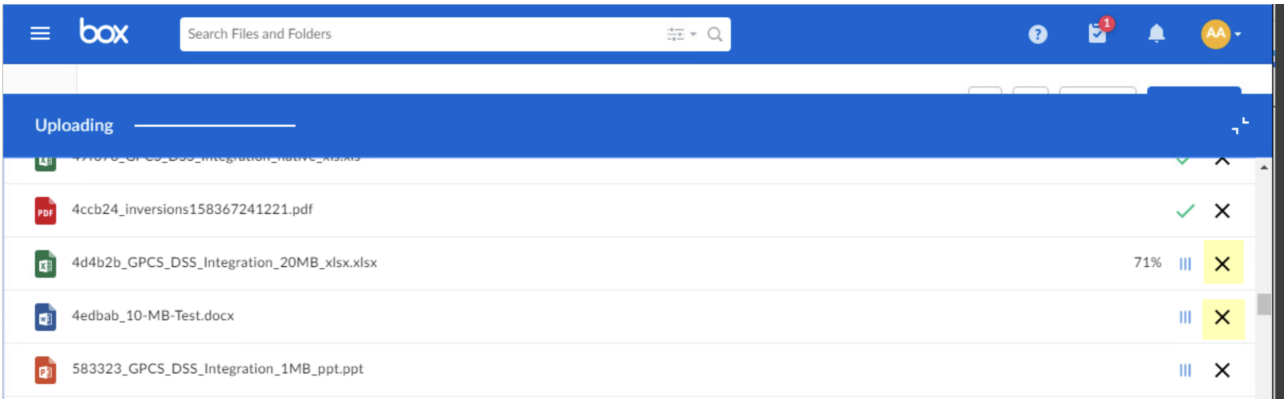
    

  - Microsoft OneDrive（App-ID 為 sharepoint-online-uploading）
  - Microsoft SharePoint（App-ID 為 sharepoint-online-uploading）
  - Slack（App-ID 為 slack-uploading）
  - Web 瀏覽（App-ID 為 web-browsing）
- 檔案操作—您可以使用採用 HTTP/1.1 的 HTTP 和 HTTPS（不是 FTP 或 SMTP）上傳檔案。

  一些應用程式（如 *SharePoint* 和 *OneDrive*）預設使用 *HTTP/2*。要透過 *HTTP/1.1* 使用 *HTTP/2* 檔案，您需要建立一個解密設定檔和安全原則，去除 *ALPN* 標頭。如需詳細資訊，請參閱 啟用企業資料遺失防護 (DLP)。
- 資料流程—支援檔案上傳（不支援下載）。
- 同時檔案上傳—支援 25 個檔案同時上傳。
- 檔案大小—支援最大 20 MB 的檔案。

  如果您使用 Box 上傳多個檔案，且其中一個或多個檔案大於 20 MB，則將無法上傳全部檔案。如要繼續，請找出 Box 中大於 20 MB 的檔案，按一下 **X** 以停止上傳這些檔案。

© 2019 Palo Alto Networks, Inc.



- 檔案類型—Microsoft Office (.doc、.docx、.ppt、.pptx、.xls、.xlsx) 、.csv、.pdf 和 .rtf。
- 回應—對 HTTP 和 HTTPS 檔案支援「封鎖」和「警示」動作。「封鎖」頁面不會顯示受管理防火牆封鎖的檔案的名稱。
- 資料模式和資料篩選設定檔—使用預先定義的資料模式和資料篩選設定檔，或建立您自己的資料模式和資料篩選設定檔。當前不支援資料模式複製；但是，如果要在現有設定檔中新增、移除或修改資料識別碼，則可以複製預先定義的資料篩選設定檔。

  對於每個資料篩選設定檔，企業 DLP 最多允許 10 個資料模式用於「封鎖」規則，50 個資料模式用於「警示」規則。

  預先定義的資料模式對掃描的檔案進行基於機器學習或 regex 的偵測。企業 DLP 對最多 1MB 的掃描檔案返回以下基於預先定義機器學習的資料模式的裁定：

  - 銀行 – 破產申請
  - 銀行 – 對賬單
  - 財務 – 財務會計
  - 財務 – 通用
  - 財務 – 發票
  - 財務 – 個人財務
  - 健康 – 通用
  - 法律 – 通用
  - 法律 – 法律訴訟
  - 法律 – 併購
  - 法律 – 專利申請
  - 法律 – 標準商業協定
  - 原始碼– `Cfamily`
  - 原始碼– 通用
  - 原始碼– `java`
  - 原始碼– `javascript`
  - 原始碼– `perl`
  - 原始碼– `powershell`
  - 原始碼– `python`
  - 原始碼– `r`
  - 原始碼– `ruby`
  - 原始碼– `vbs`
  - 原始碼– `verilog`
  - 原始碼– `vhdl`
  - 原始碼– `x86_assembly`

© 2019 Palo Alto Networks, Inc.

預先定義的資料篩選設定檔

下表描述了企業資料遺失防護 (DLP) 隨附的預先定義資料篩選設定檔：

預先定義的資料篩選設定檔	掃描
大量 CCN	信用卡號或 Voyager 信用卡號（超過 100）。
CCPA	《加利福尼亞消費者隱私法案》合規性。
公司財務文件	財務會計和通用財務資訊。
財務資訊	銀行對賬單、銀行路由號碼、信用卡號（嚴格檢查）、破產申請。
GDPR	駕照編號、稅務登記號、居民身分證號、護照號碼。
金融服務現代化法案 (GLBA)	信用卡號、Voyager 信用卡號、磁條資訊、美國稅務登記號 (TIN)、美國居民身分證號、社會安全號碼 (SSN)。
醫療	《臨床實驗室改進修正案》(CLIA) 編號、藥品執行管理局 (DEA) 編號和其他醫療文件。
智慧財產權	原始碼、AWS 密碼金鑰、存取金鑰、公司機密。 有兩種類型的智慧財產權。智慧財產權 - 基本資料篩選設定檔包含智慧財產權資料篩選設定檔中包含的資料模式的子集。
法律	法律文件，包括法律訴訟、企業併購、標準商業協定、專利、破產申請。
惡意軟體	所有 Microsoft Office 文件、PDF 和可攜式執行檔，以及針對 WildFire 的已知威脅。裁定基於雜湊，這是檔案的唯一指紋。
個人可識別資訊 (PII)	稅務登記號、居民身分證號、護照號碼和駕照編號。
猥褻語言	被審查、個人、包括/排除、害怕同性戀、性。
自我傷害	自殺意圖。
敏感內容	居民身分證號、銀行資訊、AWS 密碼金鑰或存取金鑰、公司機密、CCN。
U.K.PIOCP	稅務登記號或居民身分證號。

安裝企業資料遺失防護 (DLP) 外掛程式

要在您的 Panorama™ 管理伺服器和受管理防火牆上安裝企業資料遺失防護 (DLP) 外掛程式，您必須從 Palo Alto Networks 客戶支援入口網站下載該外掛程式，將外掛程式上傳到 Panorama，然後才能安裝外掛程式。您必須在 Panorama 和受管理防火牆上安裝該外掛程式才能使用企業 DLP。

在 *Panorama* 上成功安裝企業 *DLP* 外掛程式後，您的現有資料模式（*Objects*（物件）> *Custom Objects*（自訂物件）> *Data Patterns*（資料模式））和資料篩選設定檔（*Objects*（物件）> *Security Profiles*（安全性設定檔）> *Data Filtering*（資料篩選））將自動隱藏。要顯示現有資料模式和篩選設定檔，請參閱 啟用現有資料模式和篩選設定檔。

© 2019 Palo Alto Networks, Inc.

STEP 1 | 向 Palo Alto Networks 客戶支援入口網站 (CSP) 註冊您的 Panorama 和受管理防火牆。

STEP 2 | 在 Panorama 上安裝 Panorama 裝置憑證。

STEP 3 | 安裝受管理防火牆的裝置憑證。

您必須在利用企業 DLP 的所有受管理防火牆上安裝裝置憑證。

STEP 4 | 在 Panorama 上安裝外掛程式。

1. 登入 Panorama 網頁介面。
2. 選取 **Panorama** > **Plugins**（外掛程式），然後搜尋 dlp 外掛程式的最新版本。
3. 在 Panorama 上 **Download**（下載）並 **Install**（安裝）企業 DLP 外掛程式。

STEP 5 | 在受管理防火牆上安裝外掛程式。

1. 選取 **Panorama** > **Device Deployment**（裝置部署） > **Plugins**（外掛程式），然後搜尋企業 DLP 外掛程式的最新版本。
2. 在受管理防火牆上 **Download**（下載）並 **Install**（安裝）企業 DLP 外掛程式。
3. 選取要安裝外掛程式的 **Devices**（裝置）。
4. 按一下 **OK**（確定）安裝外掛程式。

STEP 6 | 提交並推送到受管理防火牆以完成企業 DLP 外掛程式安裝。

要讓企業 DLP 資料篩選設定檔名稱顯示在資料篩選日誌中，必須進行此步驟。

儘管支援執行 *Commit and Push*（提交並推送），但不建議對企業 *DLP* 設定變更執行，您需要在「推送範圍選取」中手動選取受影響的範本和受管理防火牆。

1. 選取 **Commit**（提交） > **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的設定變更。
2. 選取 **Commit**（提交） > **Push to Devices**（推送至裝置） 和 **Edit Selections**（編輯選擇）。
3. 選取 **Device Groups**（裝置群組），以及 **Include Device and Network Templates**（包括裝置和網路範本）。
4. 按一下 **OK**（確定）。
5. 將您的設定變更 **Push**（推送）到受管理的防火牆。

STEP 7 | 在 Palo Alto Networks 客戶支援入口網站 (CSP) 上啟動企業 DLP 授權。

為利用企業 DLP 的所有防火牆重複此步驟。

1. 登入 Palo Alto Networks 客戶支援入口網站。
2. 選取 **Assets**（資產） > **Devices**（裝置），然後在「動作」欄中按一下編輯按鈕 ( )。
3. 在「裝置授權」視窗中，選取 **Activate Auth-Code**（啟動授權碼）並輸入 **Authorization Code**（授權碼）。

   在您購買企業 DLP 外掛程式授權後，Palo Alto Networks 會自動向您傳送一封電子郵件，提供該授權碼。
4. 按一下 **Agree and Submit**（同意並提交）。

STEP 8 | 建立 Palo Alto Networks 支援票證以在防火牆之間進行企業 DLP 授權傳輸。

要求企業 DLP 授權可傳輸，即表示您可將 DLP 授權傳輸到其他受管理防火牆。

在支援票證中，包含以下資訊：

- 要求對企業 DLP 授權進行防火牆傳輸。
- 您的 CSP 帳戶 ID 以及與 CSP 帳戶關聯的電子郵件。

© 2019 Palo Alto Networks, Inc.

- 受管理防火牆序號。如果您在多個受管理防火牆上啟動了企業 DLP 授權，則須在單個支援票證中包含所有受管理防火牆序號。
- 用於在受管理防火牆上啟動企業 DLP 授權的授權碼。
- （選用）如果您有屬於另一 CSP 帳戶的受管理防火牆，請提供這些受管理防火牆關聯的 CSP 帳戶 ID。

STEP 9 | 請確認 Panorama 和受管理防火牆屬於同一 CSP 帳戶。

Panorama 和受管理防火牆必須屬於同一 CSP 帳戶，這可讓您共用資料設定檔以執行一致的安全性原則。

1. 登入 Palo Alto Networks 客戶支援入口網站。
2. 選取 **Assets**（資產）> **Devices**（裝置）並找到您的 Panorama 和受管理防火牆。

STEP 10 | 在受管理防火牆上啟動企業 DLP 外掛程式。

1. 選取 **Panorama** > **Device Deployment**（裝置部署）> **License**（授權），然後 **Activate**（啟動）企業 DLP 外掛程式。
2. 為目標受管理防火牆輸入 **Auth Code**（授權碼）。

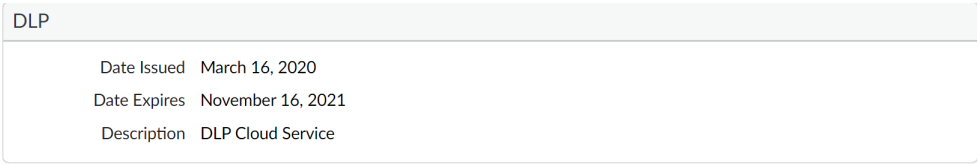
   在您購買企業 DLP 外掛程式授權後，Palo Alto Networks 會自動向您傳送一封電子郵件，提供該授權代碼。
3. 在受管理防火牆上 **Activate**（啟動）企業 DLP 外掛程式授權。

STEP 11 | 選取 **Objects**（物件）> **DLP** > **DLP Data Filtering**（**DLP** 資料篩選），並確認顯示了預先定義的資料篩選設定檔。

當 Panorama 成功連線到 DLP 雲端服務時，Panorama 會自動填入預先定義的資料篩選設定檔。

STEP 12 | 確認已在您的受管理防火牆上成功啟動企業 DLP 授權。

1. 啟動防火牆 Web 介面。
2. 選取 **Device**（裝置）> **Licenses**（授權），並確認已成功啟動授權。



建立資料模式

資料模式可讓您使用規則運算式、檔案屬性或代表網路上敏感資訊的關鍵字來指定比對準則和標識模式。建立的所有資料模式均跨全部裝置群組共用。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 選取 **Objects**（物件）> **DLP** > **DLP Data Patterns**（**DLP** 資料模式），然後指定 **Device Group**（裝置群組）。

STEP 3 | **Add**（新增）新資料模式。

STEP 4 | 為資料模式指定 **Type**（類型）和準則，並為其提供 **Name**（名稱）。

使用以下資料模式類型：

- 規則運算式—建立要在資料模式中使用的規則運算式。

© 2019 Palo Alto Networks, Inc.

您可以選擇 **Basic**（基本）或 **Advanced**（進階）資料模式。使用 **Advanced**（進階）資料模式來建立基本或加權規則運算式。使用加權規則運算式，會為每個文字項目指派一個分數，當超過分數閾值時，例如，當一個模式的足夠多運算式與一項資產相符時，該資產將被表示為該模式的相符項。

然後使用 **Regular Expressions**（規則運算式）區域中的查詢建立器來新增運算式，可以是常規（**Basic**（基本））或者加權（**Advanced**（進階））規則運算式。

您可以輸入一個或多個 **Proximity Keywords**（鄰近關鍵字）以便與資料篩選模式一起使用。在具有「高信賴等級」的資料篩選設定檔中使用鄰近關鍵字。當您上傳檔案時，受管理防火牆在將檔案中的指定資料模式視為相符項之前，會在規則運算式的 200 個字元內查找您指定的鄰近關鍵字。

- **File Property**（檔案屬性）—新增要進行比對的檔案屬性模式。

  要進行資料控管和資訊保護，如果您在 MS Office 和 PDF 文件中使用分類標籤或嵌入標籤以包含更多資訊用於稽核和追蹤，則可以建立檔案屬性資料模式來比對屬於檔案中自訂或擴充屬性的中繼資料或屬性。無論您是否使用 Titus 之類的自動分類機制或要求使用者新增標籤，都可以指定一個名稱-值配對，以比對檔案中嵌入的自訂或擴充屬性。

  企業 DLP 支援 MS Office 和 PDF 文件中的檔案屬性資料模式。OLE (.doc/.ppt) 和 XML (.docx/.pptx) 格式的 MS Office 均受支援。

  然後新增 **Tag Name**（標籤名稱）和 **Tag Value**（標籤值）。

  Tag Name（標籤名稱）和 **Tag Value**（標籤值）是一個關聯配對，用於指定您想要查找的屬性（例如，您可以將 **Tag Name**（標籤名稱）指定為 **Label**（標籤），將 **Tag Value**（標籤值）指定為 **Confidential**（機密））。您可以新增任意數量的檔案屬性。當您之後在資料篩選設定檔中引用檔案屬性資料模式時，比對準則中會使用布林運算「OR」進行比對。

STEP 5 | 按一下 **OK**（確定）以儲存資料模式。

STEP 6 | 提交設定變更並將其推送到利用企業 DLP 的受管理防火牆。

儘管支援執行 *Commit and Push*（提交並推送），但不建議對企業 *DLP* 設定變更執行，您需要在「推送範圍選取」中手動選取受影響的範本和受管理防火牆。

1. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的設定變更。
2. 選取 **Commit**（提交）> **Push to Devices**（推送至裝置）和 **Edit Selections**（編輯選擇）。
3. 選取 **Device Groups**（裝置群組），以及 **Include Device and Network Templates**（包括裝置和網路範本）。
4. 按一下 **OK**（確定）。
5. 將您的設定變更 **Push**（推送）到受管理的防火牆。

STEP 7 | 使用一個或多個資料模式建立資料篩選設定檔。

建立資料篩選設定檔

建立資料篩選設定檔以新增多個資料模式並指定相符項和信賴等級。所有預先定義和自訂資料篩選設定檔均在全部裝置群組可用。

在使用預先定義資料模式建立資料篩選設定檔時，請考慮預先定義資料模式使用的偵測類型，因為這決定了企業 DLP 如何對已掃描檔案作出裁定。例如，當您建立包括三個基於機器學習的資料模式和 7 個基於 Regex 的資料模式的資料篩選設定檔時，如果掃描的檔案超過 1MB，則企業 DLP 將根據 7 個基於 Regex 的模式返回裁定。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | （選用）建立一個或多個資料模式。

© 2019 Palo Alto Networks, Inc.

STEP 3 | 選取 **Objects**（物件）> **DLP** > **DLP Data Filters**（**DLP** 資料篩選器），然後指定 **Device Group**（裝置群組）。

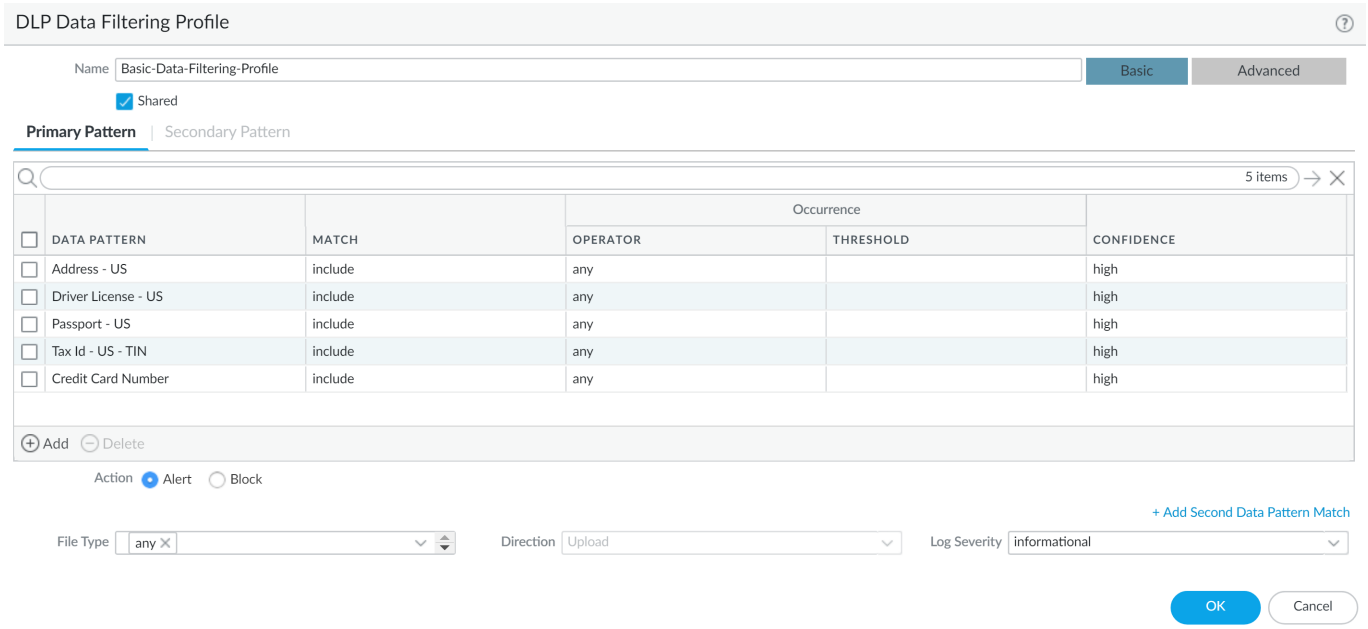
STEP 4 | **Add**（新增）新的資料篩選設定檔。

STEP 5 | 為資料篩選設定檔設定主要模式。

- 如果選取 **Basic**（基本）選項，請設定以下內容：
  - **Primary Pattern**（主要模式）—**Add**（新增）一個或多個資料模式以指定為比對準則。

    如果指定多個資料模式，受管理防火牆會在比對準則中使用布林運算「OR」進行比對。
  - **Match**（比對）—選取您指定的模式應當與指定標準相符（包括）還是不相符（排除）。
  - **Operator**（運算子）—選取一個運算子與 **Threshold**（閾值）參數搭配使用。指定 **Any**（任何）以忽略閾值。
  - **Threshold**（閾值）—指定一個值以便與您指定的 **Operator**（運算子）搭配使用。

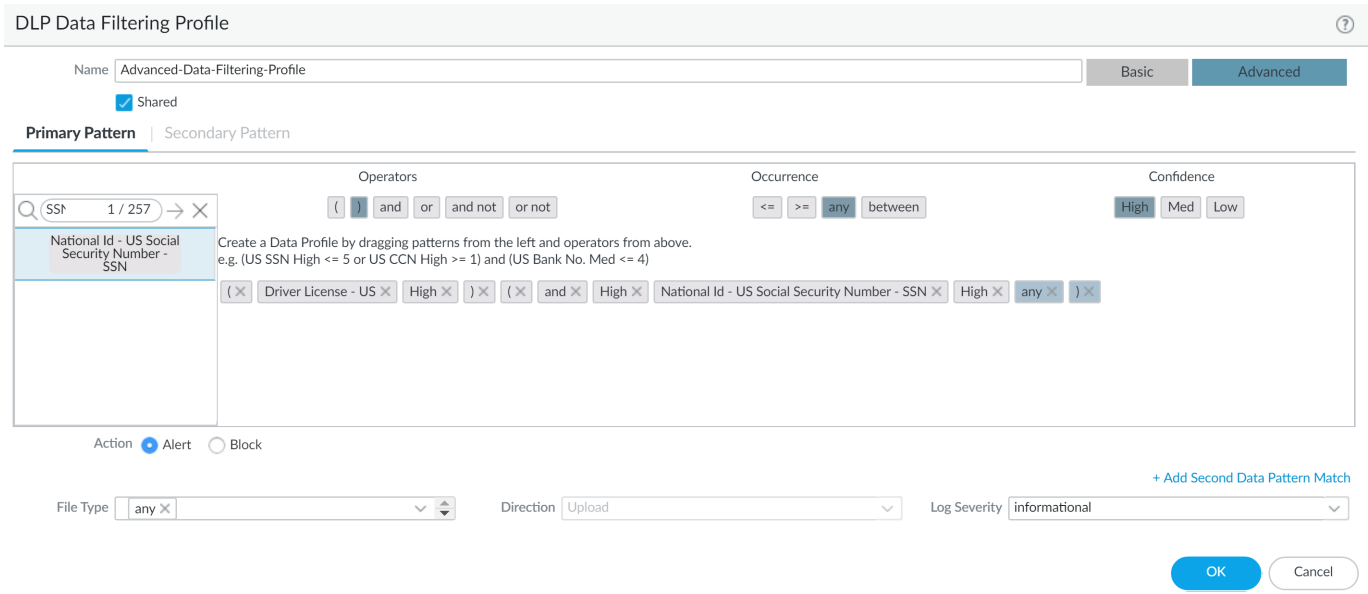
    例如，要比對一個在檔案中出現 3 次或以上的模式，請選取 **Operator**（運算子）**more_than_or_equal_to**，選取 **Threshold**（閾值） **3**。
  - **Confidence**（信賴）—將此項與您在建立的資料模式中指定的鄰近關鍵字一起使用。將信賴等級指定為 **Low**（低）意味著受管理防火牆不使用鄰近關鍵字。將信賴等級指定為 **High**（高）意味著受管理防火牆在將檔案中的資料模式視為相符項之前，會在模式中規則運算式的 200 個字元內查找模式中的鄰近關鍵字。



- 如果您選取 **Advanced**（進階）選項，則透過將資料模式、**Confidence**（信賴）等級、**Operators**（運算子）和**Occurrence**（發生頻率）值拖放到頁面中心的欄位來建立運算式。

  指定值以便其顯示在以下螢幕擷取畫面中（資料模式、**Confidence**（信賴）和 **Operator**（運算子）或 **Occurrence**（發生頻率）值）。

© 2019 Palo Alto Networks, Inc.



STEP 6 | 選取要在檔案上執行的 **Action**（動作）（**Alert**（警示）或 **Block**（封鎖））。

STEP 7 | 指定 **File Type**（檔案類型）。

將檔案類型保留為 **any**（任何）以比對任何受支援的檔案類型。

STEP 8 | 選取上傳的 **Direction**（方向）。

不支援下載。

STEP 9 | （選用）設定為與此規則相符的檔案記錄的 **Log Severity**（日誌嚴重性）。

預設嚴重性為 **Informational**（僅供參考）。

STEP 10 | 按一下 **OK**（確定）儲存組態變更。

STEP 11 | 將資料篩選設定檔附加於安全性原則規則。

1. 選取 **Policies**（原則）> **Security**（安全性），然後指定 **Device Group**（裝置群組）。
2. 選取想要向其新增資料篩選設定檔的安全性原則規則。
3. 選取 **Actions**（動作），然後將 **Profile Type**（設定檔類型）設定為 **Profiles**（設定檔）。
4. 選取您之前建立的 **Data Filtering**（資料篩選）。
5. 按一下 **OK**（確定）儲存組態變更。

STEP 12 | 提交設定變更並將其推送到利用企業 DLP 的受管理防火牆。

儘管支援執行 *Commit and Push*（提交並推送），但不建議對企業 *DLP* 設定變更執行，您需要在「推送範圍選取」中手動選取受影響的範本和受管理防火牆。

1. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的設定變更。
2. 選取 **Commit**（提交）> **Push to Devices**（推送至裝置）和 **Edit Selections**（編輯選擇）。
3. 選取 **Device Groups**（裝置群組），以及 **Include Device and Network Templates**（包括裝置和網路範本）。

© 2019 Palo Alto Networks, Inc.

4. 按一下 **OK**（確定）。
5. 將您的設定變更 **Push**（推送）到受管理的防火牆。

啟用企業資料遺失防護 (DLP)

按照以下步驟以設定受管理的防火牆以成功利用企業資料遺失防護 (DLP)。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | （僅限硬體防火牆）建立服務路由以便防火牆連線到網際網路。

必須設定服務路由這些防火牆平台才能成功利用企業 DLP。



為執行 *PAN-OS 10.0* 和更高版本的所有受支援防火牆型號建立服務路由。

1. 選取 **Device**（裝置）> **Setup**（設定）> **Services**（服務），然後選取包含企業 DLP 設定的範本
2. 按一下 **Service Features**（服務功能）中的 **Service Route Configuration**（服務路由設定），然後選取 **Customize**（自訂）。
3. 按一下 **Dataplane**（資料平面），然後設定 **Source Interface**（來源介面）和 **Source Address**（來源位址）。

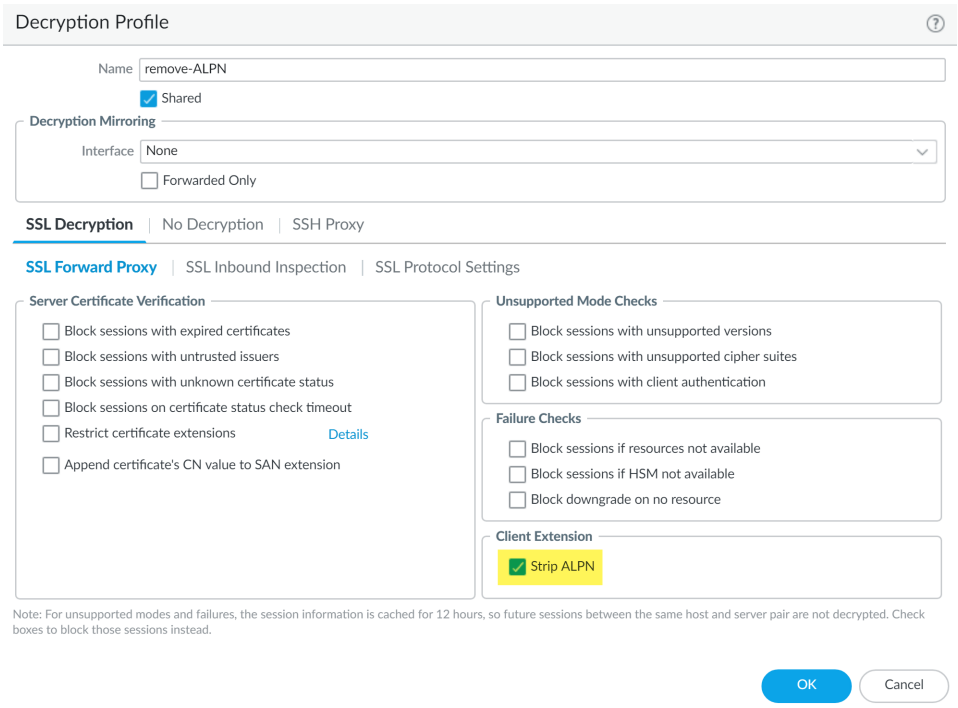
   來源介面必須具有網際網路連線。請參閱設定介面和建立位址物件以獲取有關建立來源介面和位址的更多資訊。
4. 選取（核取）**Dataplane**（資料平面），然後按一下 **OK**（確定）儲存您的設定變更。
5. 選取 **Device**（裝置）> **Setup**（設定）> **Content-ID**（內容 **ID**），然後復制 **Service URL Setting**（服務 **URL** 設定）區段中的 **Public Cloud Server**（公用雲端伺服器）FQDN。
6. 選取 **Policies**（原則）> **Security**（安全性），然後 **Add**（新增）一個允許流量從來源介面到公用雲端伺服器 FQDN 的安全性原則規則。

STEP 3 | 建立解密設定檔以從上傳的檔案中移除應用程式層通訊協定交涉 (ALPN) 標頭。

企業 DLP 支援 HTTP/1.1。一些應用程式（如 SharePoint 和 OneDrive）預設支援 HTTP/2 進行上傳。要讓從使用 HTTP/2 的應用程式上傳的檔案與企業 DLP 相容，請完成以下步驟：

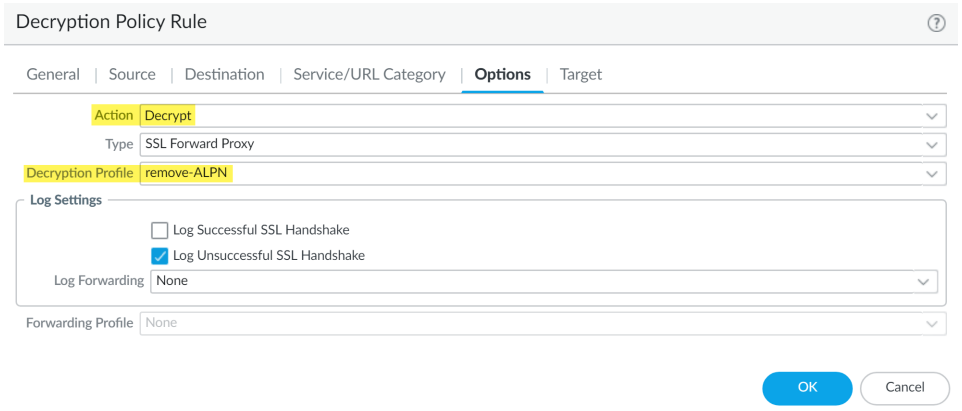
1. 選取 **Objects**（物件）> **Decryption**（解密）> **Decryption Profile**（解密設定檔），然後指定 **Device Group**（裝置群組）。
2. **Add**（新增）新的解密設定檔。
3. 輸入描述性的 **Name**（名稱）。
4. （選用）啟用（核取）**Shared**（共用）以使該解密設定檔在所有裝置群組中可用。
5. 選取 **SSL Decryption**（**SSL** 解密）> **SSL Forward Proxy**（**SSL** 正向 **Proxy**），然後啟用（核取）**Client Extension**（用戶端延伸）中的 **Strip ALPN**（除去 **ALPN**）
6. 按一下 **OK**（確定）儲存組態變更。

© 2019 Palo Alto Networks, Inc.



STEP 4 | 建立原則規則以從已上傳檔案中移除 ALPN 標頭。

1. 選取 **Policies**（原則）> **Decryption**（解密），然後指定 **Device Group**（裝置群組）。
2. **Add**（新增）新的解密原則規則，並根據需要進行設定。
3. 選取 **Options**（選項）。
4. 針對 **Action**（動作），選取 **Decrypt**（解密）。
5. 選取您建立的 **Decryption Profile**（解密設定檔）。
6. 按一下 **OK**（確定）儲存組態變更。



STEP 5 | 停用 QUIC 通訊協定以拒絕連接埠 80 和 443 上的流量。

許多受支援的 Web 應用程式（如 Gmail）要求您停用 QUIC 通訊協定，以便企業 DLP 能夠正確運作。

1. 選取 **Policies**（原則）> **Security**（安全性），然後指定 **Device Group**（裝置群組）。
2. **Add**（新增）一個安全性原則規則，拒絕使用 **quic** 應用程式的流量。
3. 選取 **Objects**（物件）> **Services**（服務），然後指定 **Device Group**（裝置群組）。
4. **Add**（新增）兩個服務：一個用於連接埠 80 上的 UDP，一個用於連接埠 443 上的 UDP。

© 2019 Palo Alto Networks, Inc.

QUIC 的較新版本可能被錯誤識別為 **unknown-udp**。對此，Palo Alto Networks 推薦為 UDP 連接埠 80 和 UDP 連接埠 443 新增服務，並建立額外的安全性原則以拒絕這些連接埠上的 UDP 流量。

5. 選取 **Policies**（原則）> **Security**（安全性），然後指定 **Device Group**（裝置群組）。
6. **Add**（新增）一個安全性原則規則，其中包括您建立的用於拒絕到 UDP 連接埠 80 和 443 的流量的服務。

   完成後，您將有兩個安全性原則：一個封鎖 QUIC 通訊協定，一個封鎖 UDP 連接埠 80 和 443 上的流量。

STEP 6 | 建立資料模式。

STEP 7 | 建立資料篩選設定檔。

STEP 8 | 將資料篩選設定檔附加於安全性原則規則。

請參閱建立安全性原則規則以獲取有關建立新安全性原則規則的更多資訊。

要將您的 *Panorama* 管理伺服器降級到之前的 *PAN-OS* 版本，您必須移除安全性原則規則中引用的所有企業 *DLP* 資料模式和資料篩選設定檔。在建立和組織引用企業 *DLP* 資料模式和篩選設定檔的原則規則時，請考慮到這一點。

例如，建立一個裝置群組包含所有安全性原則規則，其中包含對企業 *DLP* 資料模式和篩選設定檔的引用。這樣，當您需要降級 *Panorama PAN-OS* 版本時，可以快速修改相關原則規則。

1. 選取 **Policies**（原則）> **Security**（安全性）> **Pre Rules**（預先規則），然後指定**Device Group**（裝置群組）。
2. 選取想要向其新增資料篩選設定檔的安全性原則規則。
3. 選取 **Actions**（動作），然後將 **Profile Type**（設定檔類型）設定為 **Profiles**（設定檔）。
4. 選取您建立的 **Data Filtering**（資料篩選）設定檔。
5. 按一下 **OK**（確定）儲存組態變更。

STEP 9 | 提交設定變更並將其推送到利用企業 DLP 的受管理防火牆。

儘管支援執行 *Commit and Push*（提交並推送），但不建議對企業 *DLP* 設定變更執行，您需要在「推送範圍選取」中手動選取受影響的範本和受管理防火牆。

1. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的設定變更。
2. 選取 **Commit**（提交）> **Push to Devices**（推送至裝置）和 **Edit Selections**（編輯選擇）。
3. 選取 **Device Groups**（裝置群組），以及 **Include Device and Network Templates**（包括裝置和網路範本）。
4. 按一下 **OK**（確定）。
5. 將您的設定變更 **Push**（推送）到受管理的防火牆。

檢視企業資料遺失防護 (DLP) 日誌詳細資料

如果受管理防火牆在檔案上傳期間偵測到敏感內容，且您已建立「警示」或「封鎖」動作，則會產生資料篩選日誌。您可以篩选和檢視偵測到的流量的詳細日誌資料，如原則規則資訊、流量的來源和目的地，以及與資料模式關聯的資料設定檔。此外，詳細的日誌檢視會顯示相符流量的特定資料模式，並顯示資料模式相符的總唯一次數和總出現次數。僅可在 Panorama 上檢視詳細日誌。

如果受管理防火牆在檔案上傳期間偵測到敏感內容，且您已建立「警示」或「封鎖」動作時，它會產生一個日誌。然後，您可以從資料篩選日誌中檢視敏感內容，稱為 *snippet*（程式碼片段）。程式碼片段是與模式

© 2019 Palo Alto Networks, Inc.

相符項關聯的證據或可識別資訊。例如，如果您指定了「信用卡號」資料模式，則受管理防火牆將返回使用者的社會安全號碼作為相符的程式碼片段。依預設，受管理防火牆會返回程式碼片段。

受管理防火牆使用資料遮罩來遮罩程式碼片段中的資料。依預設，資料篩選日誌以純文字顯示值的後四位數（部分遮罩）。例如，資料篩選日誌將信用卡號的程式碼片段顯示為 `XXXX-XXXX-XXXX-1234`。您還可以指定以純文字完整顯示資料，或完全遮罩資料以隱藏所有值。

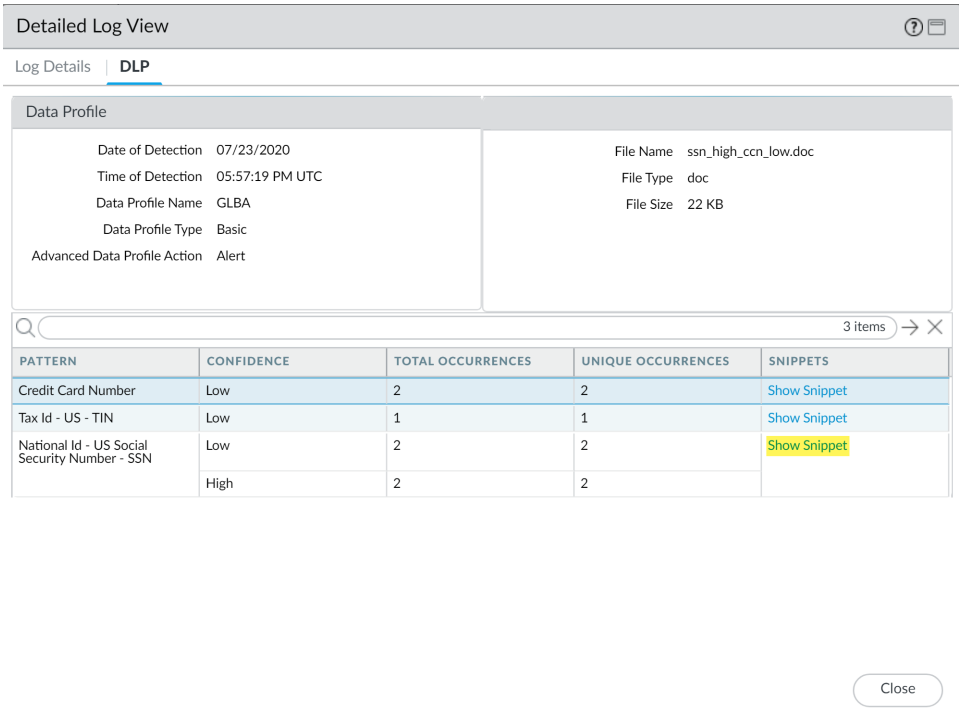
要檢視特定於 DLP 的日誌，包括檔案程式碼片段，請完成以下步驟。

STEP 1 | 啟用企業資料遺失防護 (DLP)。

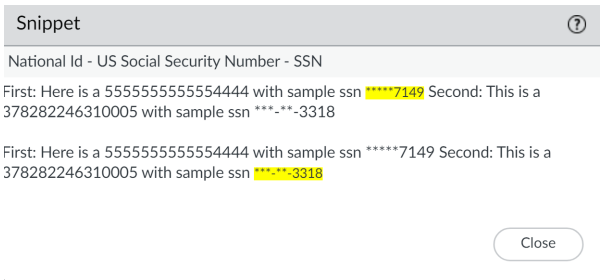
STEP 2 | 選取 **Monitor**（監控）> **Logs**（日誌）> **Data Filtering**（資料篩選），然後透過輸入 **`(subtype eq dlp)`** 來 **Filter**（篩選）資料篩選日誌。

STEP 3 | 檢視有關檔案的更多詳細資料，包括檔案程式碼片段。

1. 按一下您想要檢視更多詳細資料的特定日誌項目左邊的放大鏡 ()。
2. 選取 **DLP** 以檢視模式詳細資料。
3. 選取 **Show Snippet**（顯示程式碼片段）以檢視與特定資料模式相符的資料的程式碼片段。



4. 檢閱遮罩的程式碼片段以瞭解偵測到了什麼資料。



© 2019 Palo Alto Networks, Inc.

啟用現有資料模式和篩選設定檔

成功安裝企業資料遺失防護 (DLP) 外掛程式後，現有資料模式和篩選設定檔將不再顯示，但仍可以在安全性原則規則中引用。如果您已經設定了資料篩選模式和設定檔，需要在安裝企業 DLP 外掛程式後進行編輯，您可以重新將其顯示在 Panorama Web 介面中。

STEP 1 | 登入 Panorama CLI。

STEP 2 | 啟用現有資料模式和篩選設定檔。

```
admin> request plugins dlp hide-old-config no
```

Panorama 返回 `pass` 以確認現有資料模式和篩選設定檔現已顯示。

輸入以下命令以不再顯示現有資料模式和篩選設定檔。

```
admin> request plugins dlp hide-old-config yes
```

STEP 3 | 登入 Panorama 網頁介面。

STEP 4 | 編輯現有資料模式和篩選設定檔。

1. 選取 **Objects**（物件）> **Custom Objects**（自訂物件）> **Data Patterns**（資料模式），然後編輯您的資料模式。
2. 選取 **Objects**（物件）> **Security Profiles**（安全性設定檔）> **Data Filtering**（資料篩選），然後編輯您的資料篩選設定檔。

STEP 5 | 選取 **Policies**（原則）> **Security**（安全性），然後選取 **Device Group**（裝置群組）以根據需要修改安全性原則規則。

STEP 6 | 提交設定變更並將其推送到利用企業 DLP 的受管理防火牆。

儘管支援執行 *Commit and Push*（提交並推送），但不建議對企業 *DLP* 設定變更執行，您需要在「推送範圍選取」中手動選取受影響的範本和受管理防火牆。

1. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的設定變更。
2. 選取 **Commit**（提交）> **Push to Devices**（推送至裝置）和 **Edit Selections**（編輯選擇）。
3. 選取 **Device Groups**（裝置群組），以及 **Include Device and Network Templates**（包括裝置和網路範本）。
4. 按一下 **OK**（確定）。
5. 將您的設定變更 **Push**（推送）到受管理的防火牆。

編輯企業資料遺失防護 (DLP) 設定

編輯企業資料遺失防護 (DLP) 設定，以編輯檔案掃描的雲端內容設定、設定資料篩選設定以及設定在 DLP 程式碼片段中遮罩多少敏感資料。

- 編輯雲端內容設定
- 編輯企業資料遺失防護 (DLP) 資料篩選設定
- 編輯企業資料遺失防護 (DLP) 程式碼片段設定

© 2019 Palo Alto Networks, Inc.

編輯雲端內容設定

依預設，企業資料遺失防護 (DLP) 設定有雲端內容完全合格網域名稱 (FQDN)，這會自動解析到私密雲端服務伺服器來掃描您的企業 DLP 檔案。如果您有特定的資料落地要求，可以透過編輯雲端內容 FQDN 來指定區域性雲端服務伺服器，以傳送企業資料遺失防護 (DLP) 檔案進行掃描。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 選取 **Device**（裝置）> **Setup**（設定）> **Content-ID**（內容 **ID**），然後選取與利用企業 DLP 之受管理防火牆關聯的 **Template**（範本）。

STEP 3 | 編輯雲端內容 FQDN。

1. 編輯 **Cloud Content Settings**（雲端內容設定）。
2. 根據您的資料落地要求修改 **Public Cloud Server**（公用雲端伺服器）。
   - **APAC—apac.hawkeye.services-edge.paloaltonetworks.com**
   - **歐洲—eu.hawkeye.services-edge.paloaltonetworks.com**
   - **美國—us.hawkeye.services-edge.paloaltonetworks.com**
3. 按一下 **OK**（確定）儲存組態變更。

STEP 4 | 提交設定變更並將其推送到利用企業 DLP 的受管理防火牆。

儘管支援執行 *Commit and Push*（提交並推送），但不建議對企業 *DLP* 設定變更執行，您需要在「推送範圍選取」中手動選取受影響的範本和受管理防火牆。

1. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的設定變更。
2. 選取 **Commit**（提交）> **Push to Devices**（推送至裝置）和 **Edit Selections**（編輯選擇）。
3. 選取 **Device Groups**（裝置群組），以及 **Include Device and Network Templates**（包括裝置和網路範本）。
4. 按一下 **OK**（確定）。
5. 將您的設定變更 **Push**（推送）到受管理的防火牆。

編輯企業資料遺失防護 *(DLP)* 資料篩選設定

為掃描到企業資料遺失防護 (DLP) 雲端服務的檔案設定網路設定，並指定利用企業 DLP 的防火牆採取的動作。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 選取 **Device**（裝置）> **Setup**（設定）> **DLP**，然後選取與利用企業 DLP 之受管理防火牆關聯的 **Template**（範本）。

STEP 3 | 編輯資料篩選設定。

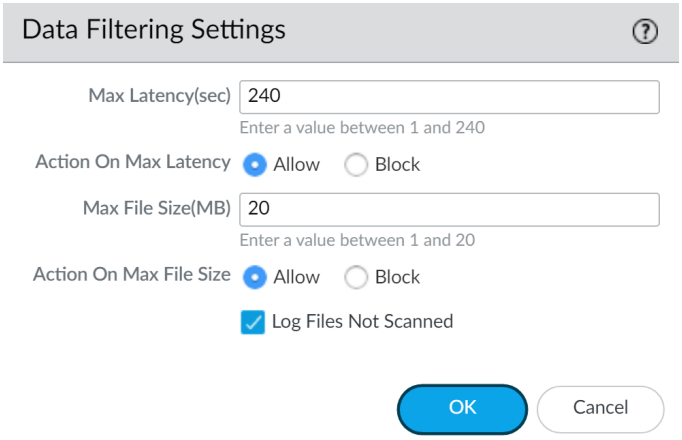
1. 針對檔案上傳，為防火牆採取的動作指定 **Max Latency (sec)**（最大延遲（秒））。
2. 指定當掃描以儲存到 DLP 雲端服務的檔案達到設定的 **Max Latency**（最大延遲）時防火牆採取的 **Action on Max Latency**（最大延遲動作）（**Block**（封鎖）或**Allow**（允許））。

   選取 *Block*（封鎖）僅套用至設定為封鎖檔案的企業 DLP 資料篩選設定檔。此設定不會影響設定為在掃描到包含敏感資料的流量時發出警示的企業 *DLP* 篩選設定檔。
3. 指定 **Max File Size (MB)**（最大檔案大小 **(MB)**）以對儲存在 DLP 雲端服務中的檔案強制執行最大檔案大小。

© 2019 Palo Alto Networks, Inc.

4. 指定當掃描到 DLP 雲端服務的檔案達到設定的 **Max File Size**（最大檔案大小）時防火牆採取的 **Action on Max File Size**（最大檔案大小動作）（**Block**（封鎖）或**Allow**（允許））。

   選取 *Block*（封鎖）僅套用至設定為封鎖檔案的企業 DLP 資料篩選設定檔。此設定不會影響設定為在掃描到包含敏感資料的流量時發出警示的企業 *DLP* 篩選設定檔。
5. 核取（啟用）**Log Files Not Scanned**（日誌檔案未掃描）以在無法將檔案掃描到 DLP 雲端服務時在資料篩選日誌中產生警示。
6. 按一下 **OK**（確定）儲存組態變更。



STEP 4 | 提交設定變更並將其推送到利用企業 DLP 的受管理防火牆。

儘管支援執行 *Commit and Push*（提交並推送），但不建議對企業 *DLP* 設定變更執行，您需要在「推送範圍選取」中手動選取受影響的範本和受管理防火牆。

1. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的設定變更。
2. 選取 **Commit**（提交）> **Push to Devices**（推送至裝置）和 **Edit Selections**（編輯選擇）。
3. 選取 **Device Groups**（裝置群組），以及 **Include Device and Network Templates**（包括裝置和網路範本）。
4. 按一下 **OK**（確定）。
5. 將您的設定變更 **Push**（推送）到受管理的防火牆。

編輯企業資料遺失防護 *(DLP)* 程式碼片段設定

設定防火牆以將與企業 DLP 資料模式相符的敏感資料程式碼片段儲存在 DLP 雲端服務中，以及設定在儲存的情況下如何遮罩敏感資料。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 選取 **Panorama** > **DLP** > **Configuration**（設定），然後編輯程式碼片段設定。

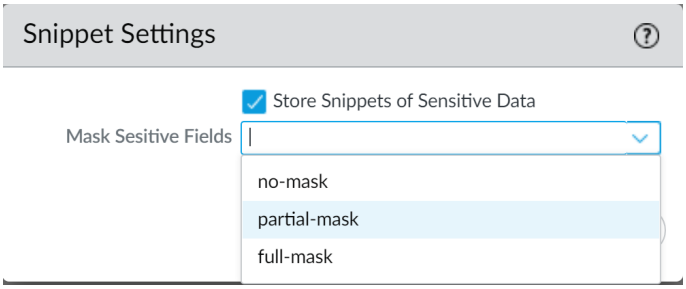
STEP 3 | 核取（啟用）**Store Snippets of Sensitive Data**（儲存敏感資料程式碼片段）以將與企業 DLP 資料模式相符的敏感資料程式碼片段儲存在 DLP 雲端服務中。

STEP 4 | 為 DLP 雲端服務中的儲存設定如何遮罩敏感欄位。

- **no-mask**（不遮罩）—當儲存在 DLP 雲端服務中時，相符的敏感資料程式碼片段不會被遮罩且完全可見。

© 2019 Palo Alto Networks, Inc.

- **partial-mask**（部分遮罩）—當儲存在 DLP 雲端服務中時，相符的敏感資料程式碼片段會被部分遮罩，只顯示四個字元。
- **full-mask**（完全遮罩）—當儲存在 DLP 雲端服務中時，相符的敏感資料程式碼片段將被完全遮罩。



STEP 5 | 按一下 **OK**（確定）儲存組態變更。

STEP 6 | 提交設定變更並將其推送到利用企業 DLP 的受管理防火牆。

儘管支援執行 *Commit and Push*（提交並推送），但不建議對企業 *DLP* 設定變更執行，您需要在「推送範圍選取」中手動選取受影響的範本和受管理防火牆。

1. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的設定變更。
2. 選取 **Commit**（提交）> **Push to Devices**（推送至裝置）和 **Edit Selections**（編輯選擇）。
3. 選取 **Device Groups**（裝置群組），以及 **Include Device and Network Templates**（包括裝置和網路範本）。
4. 按一下 **OK**（確定）。
5. 將您的設定變更 **Push**（推送）到受管理的防火牆。

解除安裝企業資料遺失防護 (DLP) 外掛程式

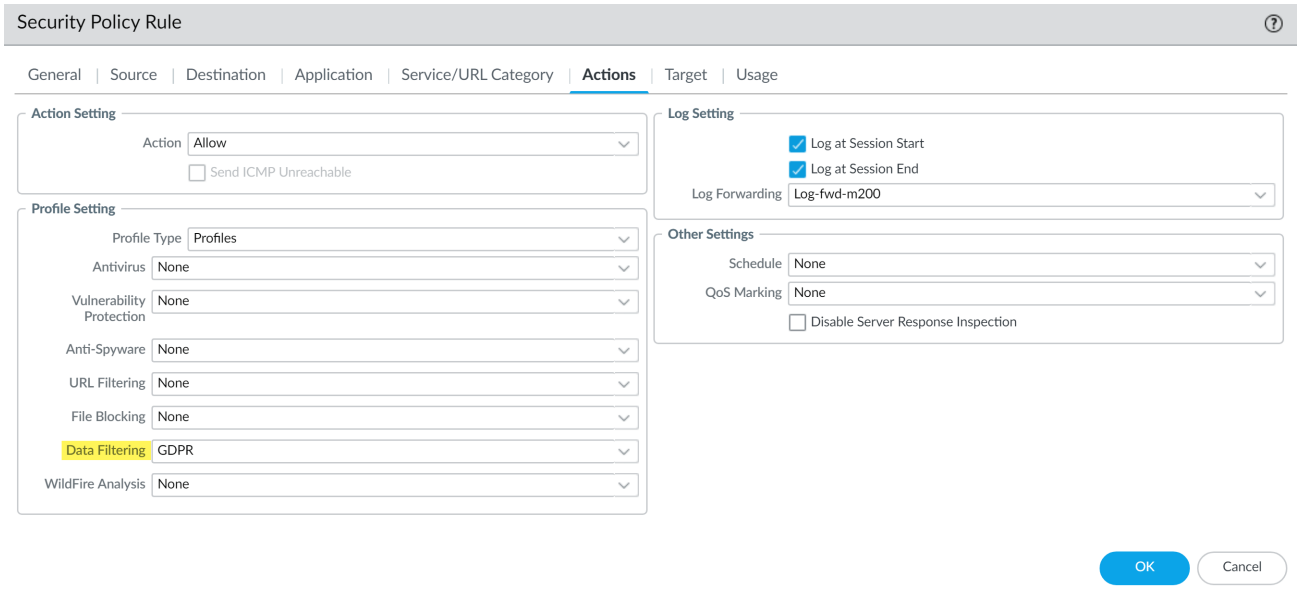
要解除安裝企業資料遺失防護 (DLP) 外掛程式，必須先從所有安全性原則規則中移除所有企業資料遺失防護 (DLP) 資料篩選設定檔引用，然後才能在 Panorama™ 管理伺服器和受管理防火牆上解除安裝該外掛程式。成功解除安裝外掛程式後，您可以繼續降級 Panorama 和受管理防火牆。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 選取 **Policies**（原則）> **Security**（安全性），然後從安全性原則規則移除所有企業 DLP 資料篩選設定檔。

需要完成此步驟才能成功解除安裝企業 DLP 外掛程式。

© 2019 Palo Alto Networks, Inc.



STEP 3 | 提交設定變更並將其推送到利用企業 DLP 的受管理防火牆。

儘管支援執行 *Commit and Push*（提交並推送），但不建議對企業 *DLP* 設定變更執行，您需要在「推送範圍選取」中手動選取受影響的範本和受管理防火牆。

1. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的設定變更。
2. 選取 **Commit**（提交）> **Push to Devices**（推送至裝置）和 **Edit Selections**（編輯選擇）。
3. 選取 **Device Groups**（裝置群組），以及 **Include Device and Network Templates**（包括裝置和網路範本）。
4. 按一下 **OK**（確定）。
5. 將您的設定變更 **Push**（推送）到受管理的防火牆。

STEP 4 | 從受管理防火牆解除安裝企業 DLP 外掛程式。

1. 存取受管理防火牆 CLI。
2. 使用以下命令解除安裝企業 DLP 外掛程式：

```
admin> request plugins uninstall dlp
```

在系統提示時，輸入 **y** 確認解除安裝企業 DLP 外掛程式。

STEP 5 | 從 Panorama 解除安裝企業 DLP 外掛程式。

1. 登入 Panorama 網頁介面。
2. 選取 **Panorama** > **Plugins**（外掛程式），然後 **Uninstall**（解除安裝）企業 DLP 外掛程式。

STEP 6 | 提交設定變更並將其推送到利用企業 DLP 的受管理防火牆。

儘管支援執行 *Commit and Push*（提交並推送），但不建議對企業 *DLP* 設定變更執行，您需要在「推送範圍選取」中手動選取受影響的範本和受管理防火牆。

1. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的設定變更。
2. 選取 **Commit**（提交）> **Push to Devices**（推送至裝置）和 **Edit Selections**（編輯選擇）。

© 2019 Palo Alto Networks, Inc.

3. 選取 **Device Groups**（裝置群組），以及 **Include Device and Network Templates**（包括裝置和網路範本）。
4. 按一下 **OK**（確定）。
5. 將您的設定變更 **Push**（推送）到受管理的防火牆。

© 2019 Palo Alto Networks, Inc.

重新散佈資料到受管理防火牆

要確保所有執行原則和產生報告的防火牆都具有原則規則所需的資料和驗證時間戳記，您可以利用 Panorama 基礎結構重新散佈對應和時間戳記。

- 設定 Panorama 管理伺服器以重新散佈資料。
  1. 將防火牆、虛擬系統或 Windows User-ID 代理程式作為重新散佈代理程式新增到 Panorama：
     1. 選取 **Panorama** > **Data Redistribution**（資料重新散佈）並 **Add**（新增）每個重新散佈代理程式。
     2. 輸入 **Name**（名稱）以標識重新散佈代理程式。
     3. 確認該代理程式 **Enabled**（已啟用）。
     4. 輸入防火牆上 MGT 介面的 **Host**（主機）名稱或 IP 位址。
     5. 輸入防火牆將接聽資料重新散佈查詢的 **Port**（連接埠）號（預設為 5007）。
     6. 如果重新散佈代理程式是防火牆或虛擬系統，請輸入 **Collector Name**（收集器名稱）和 **Collector Pre-Shared Key**（收集器預先共用金鑰）。
     7. 選取您想要重新散佈的 **Data type**（資料類型）。您可以選取所有資料類型，但必須選取以下資料類型中的至少一種：
        - **IP** 使用者對應
        - **IP** 標籤
        - 使用者標籤
        - **HIP**
        - 隔離清單
     8. 按一下 **OK**（確定）來儲存組態。
  2. 啟用 Panorama MGT 介面以回應來自防火牆的資料重新散佈查詢：

     如果 *Panorama* 管理伺服器具有高可用性 *(HA)* 設定，最佳作法是在每個 *HA* 對等上執行此步驟，以便 *Panorama* 容錯移轉時繼續重新散佈。

     1. 選取 **Panorama** > **Setup**（設定）> **Interfaces**（介面）和 **Management**（管理）。
     2. 在 Network Services（網路服務）區段中選取 **User-ID**，然後按一下 **OK**（確定）。
  3. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），讓您的變更在 Panorama 上生效。

- 設定防火牆以接收 Panorama 重新散佈的資料。
  1. 選取 **Device**（裝置）> **Data Redistribution**（資料重新散佈）> **Agents**（代理程式），然後選取要向其指派防火牆的 **Template**（範本）。
  2. **Add**（新增）代理程式並輸入 **Name**（名稱）。
  3. 選取要以何種方式新增代理程式：
     - **Serial Number**（序號）—從清單中選取您想要使用的 Panorama 的 **Serial Number**（序號）：
       - **panorama**—主動或單獨 Panorama
       - **panorama2**—（僅限 HA）被動 Panorama
     - **Host and Port**（主機和連接埠）—指定以下資訊：
       - 選取防火牆上 MGT 介面的 **Host**（主機）名稱或 IP 位址。
       - 選取主機是否是 **LDAP Proxy**。
       - 輸入防火牆將接聽資料重新散佈查詢的 **Port**（連接埠）號（預設為 5007）。
       - 如果重新散佈代理程式是防火牆或虛擬系統，請輸入 **Collector Name**（收集器名稱）和 **Collector Pre-Shared Key**（收集器預先共用金鑰）。

© 2019 Palo Alto Networks, Inc.

- 選取您想要重新散佈的 **Data type**（資料類型）。

4. 確認代理程式為 **Enabled**（已啟用），然後按一下 **OK**（確定）以儲存設定。
5. 選取 **Commit**（提交）> **Commit and Push**（提交並推送），讓您的變更在 Panorama 上生效，並將變更推送至防火牆。

- 確認 Panorama 和防火牆接收重新散佈的資料。
  1. 檢視代理程式統計資料（**Panorama** > **Data Redistribution**（資料重新散佈）> **Agents**（代理程式）），然後選取 **Status**（狀態）以檢視重新散佈代理程式的活動摘要，如用戶端防火牆接收的對應數量。
  2. 確認 User-ID 日誌（ **Monitor**（監控）> **Logs**（日誌）> **User-ID**）中的 **Source Name**（來源名稱），以確認防火牆從重新散佈代理程式接收對應。
  3. 檢視 IP-Tag 日誌（**Monitor**（監控）> **Logs**（日誌）> **IP-Tag**）以確認用戶端防火牆接收資料。
  4. 在重新散佈資料的防火牆或 Panorama 管理伺服器上存取 CLI。
  5. 執行下列命令，顯示所有使用者對應：

```
> show user ip-user-mapping all
```

  6. 記錄與任何一個使用者名稱相關聯的 IP 位址。
  7. 存取接收重新散佈資料之防火牆或 Panorama 管理伺服器的 CLI。
  8. 顯示您所記錄之 *<Ip-address>* 的對應資訊和驗證時間戳記：

```
> show user ip-user-mapping ip <IP-address>
IP address:     192.0.2.0 (vsys1)
User:           corpdomain\username1
From:           UIA
Idle Timeout:   10229s
Max. TTL:       10229s
MFA Timestamp: first(1) - 2016/12/09 08:35:04
Group(s):       corpdomain\groupname(621)
```



此範例輸出顯示對一個驗證挑戰（因素）做出回應的時間戳記。對於使用多因素驗證 *(MFA)* 的驗證規則，輸出會顯示多個時間戳記。

© 2019 Palo Alto Networks, Inc.

移轉防火牆至 Panorama 進行管理

如果您已部署 Palo Alto Networks 防火牆並在本機設定它們，但現在想要使用 Panorama 以集中管理這些防火牆，則必須執行預先移轉規劃工作。轉移涉及匯入防火牆組態至 Panorama 和確認在轉移之後防火牆功能正常。如果某些設定是單個防火牆專屬，您可以繼續存取這些防火牆以管理這些唯一設定。您可以透過從 Panorama 推送防火牆組態值，或在防火牆上執行本機設定來管理任何特定防火牆組態，但無法透過 Panorama 和防火牆二者同時管理設定。如果您希望從 Panorama 管理中排除某些防火牆組態，您可以：

- 轉移整個防火牆組態，然後在 Panorama 上刪除您會在防火牆上本機管理的設定。您也可以取代範本設定（由 Panorama 推送至防火牆的範本設定），而非在 Panorama 上將該設定刪除。
- 載入部分防火牆組態，包括您將僅使用 Panorama 管理的設定。



防火牆在轉移至 *Panorama* 管理時不會丟失日誌。

- 計劃移轉至 Panorama 進行管理
- 移轉防火牆至 Panorama 進行管理
- 移轉防火牆 HA 配對至 Panorama 進行管理
- 載入部分防火牆組態至 Panorama 中

計劃移轉至 Panorama 進行管理

下列工作是轉移防火牆至 Panorama 管理所需的高階規劃概覽：

- ❑ 決定要轉移的防火牆。
- ❑ 計劃維護時間並確保 Panorama 或防火牆上沒有擱置中的設定變更。
- ❑ 在移轉之前保留您的已知工作中 Panorama 和防火牆設定。
  - 匯出防火牆的裝置狀態。
  - 匯出正在執行的 Panorama 設定的已命名 Panorama 設定快照。
- ❑ 決定 Panorama 和防火牆軟體和內容版本，以及您將如何 管理授權與更新。如需重要詳細資訊，請參閱 Panorama、日誌收集器、防火牆和 WildFire 版本相容性。
- ❑ 規劃 Panorama 部署 包括 URL 篩選資料庫（BrighCloud 或 PAN-DB）、日誌收集和管理員角色方面。
- ❑ 規劃如何管理公用設定。

  規劃 裝置群組階層、範本與範本堆疊，以減少備援和流暢執行設定管理，相關設定在所有防火牆之間或防火牆設定內共用。在轉移過程中，您可以選取是否從防火牆上的共用位置匯入物件至 Panorama 的共用位置，下列情況除外：

  - 若共用的防火牆物件與現有共用的 Panorama 物件具有相同的名稱和值，則匯入會排除防火牆物件。
  - 若共用的防火牆物件與現有共用的 Panorama 物件不具有相同的名稱和值，則 Panorama 會將防火牆物件匯入至每個為匯入而建立的新裝置群組。
  - 如果被匯入範本的設定參考共用防火牆物件，或如果公共防火牆物件參考匯入範本的設定，Panorama 會將物件作為共用物件匯入，而無論您是否選取了 **Import devices' shared objects into Panorama's shared context**（匯入設備共用物件至 Panorama 共用內容）核取方塊。
- ❑ 確定防火牆是否有您不希望匯入的設定元件（原則、物件和其他設定），或者是因為 Panorama 已包含類似的元件或由於這些元件是防火牆指定（例如，時區設定）且您不會使用 Panorama 對其進行管理。您可以執行全域尋找以確定 Panorama 上是否有類似的元件。
- ❑ 為每一個裝置群組確定共同區域。這包括各裝置群組內防火牆和虛擬系統的區域命名策略。例如，如果您有名為 Branch LAN 和 WAN 的區域，Panorama 可推送參考這些區域的原則規則，而不必知道連接埠或媒體類型、型號或邏輯定址結構描述的變化。
- ❑ 建立轉移後測試規劃。

  您將使用測試規劃確認防火牆在轉移後是否與轉移之前一樣有效運行。規劃可能包括下列工作：

© 2019 Palo Alto Networks, Inc.

- 轉移後至少監控防火牆 24 小時。
- 監控 Panorama 和防火牆日誌是否異常。
- 檢查 Panorama 上的管理員登入。
- 測試來自多個源的各種流量類型。例如，檢查頻寬圖、工作階段計數和拒絕規則流量日誌項目（請參閱 使用 Panorama 增強可見度）。測試應涵蓋原則設定的代表樣本。
- 檢查您的網路操作中心 (NOC) 和安全操作中心 (SOC) 是否有任何使用者報告的問題。
- 包括任何其他幫助確認防火牆功能的測試準則。

移轉防火牆至 Panorama 進行管理

當您匯入防火牆組態時，Panorama 自動建立範本以包含匯入的網路和設備設定。若要包含匯入的原則和物件，Panorama 自動為每個防火牆建立一個裝置群組或為多 vsys 防火牆內的每個虛擬系統建立一個裝置群組。

當您執行下列步驟時，Panorama 匯入整個防火牆組態。或者，您可以載入部分防火牆組態至 Panorama 中。

Panorama 可以從運行 *PAN-OS 5.0* 或更新版本的防火牆匯入設定並可將設定推送至這些防火牆。但有一個例外，*Panorama 6.1* 和更新版本無法推送設定至運行 *PAN-OS 6.0.0* 至 *6.0.3* 的防火牆。

Panorama 可以從已經是受管理的裝置，但未被指派至裝置群組或範本的防火牆匯入設定。

STEP 1 | 規劃轉移。

請參閱計劃移轉至 Panorama 進行管理中的檢查清單。

STEP 2 | 將防火牆新增為受管理的裝置。

將防火牆新增為受管理的裝置：

1. 登入 Panorama，選取 **Panorama** > **Managed Devices**（受管理的裝置）> **Summary**（摘要），再按一下 **Add**（新增）。
2. 輸入防火牆的序號，然後按一下 **Add**（新增）。

   如果您要匯入多個防火牆組態，在分隔行上輸入各個序號。或者，您可以從 *Microsoft Excel* 工作表複製黏貼序號。
3. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

STEP 3 | 設定從防火牆至 Panorama 的連線。

1. 登入防火牆，選取 **Device**（設備）> **Setup**（設定），然後編輯 Panorama 設定。
2. 在 **Panorama Servers**（**Panorama** 伺服器）欄內，輸入 Panorama 管理伺服器的 IP 位址。
3. 按一下 **OK**（確定）與 **Commit**（提交）。

STEP 4 | 將防火牆組態匯入 Panorama。

如果您稍後決定重新匯入防火牆組態，請先移除當作成員的防火牆裝置群組和範本。如果裝置群組和範本名稱與防火牆主機名稱一致，您可以在重新匯入防火牆組態前刪除壯漢子群組和範本，或使用 *Device Group Name Prefix*（裝置群組名稱前置詞）欄位為透過重新匯入建立的裝置群組和範圍定義新名稱。此外，將防火牆從裝置群組或範本中移除時，防火牆不會丟失日誌。

© 2019 Palo Alto Networks, Inc.

1. 從 Panorama，選取 **Panorama** > **Setup**（設定）> **Operations**（操作），按一下 **Import device configuration to Panorama**（匯入設備組態至 **Panorama**），然後選取 **Device**（設備）。

   Panorama 無法從被指派至現有裝置群組或範本的防火牆匯入設定。

2. （Optional（選用））編輯 **Template Name**（範本名稱）。預設值為防火牆名稱。您無法使用現有範本或範本堆疊名稱。
3. （選用）編輯 **Device Group**（裝置群組）名稱。若為多重 vsys 防火牆，依預設，每個裝置群組都有 vsys 名稱，請各新增一個字元字串作為裝置群組名稱首碼。否則，預設值為防火牆名稱。您無法使用現有裝置群組的名稱。

   依預設會選取 *Import devices' shared objects into Panorama's shared context*（將裝置的共用物件匯入 *Panorama* 的共用內容）核取方塊，這表示 *Panorama* 比較會將屬於防火牆中「共用」位置的物件，匯入 *Panorama* 中的「共用」。如果匯入的物件不在防火牆的共用內容中，則會套用至每個要匯入的裝置群組。如果清除此核取方塊，*Panorama* 複製不會比較匯入的物件，而會將所有共用的防火牆物件套用至要匯入的裝置群組（而不是「共用」）。這會建立重複物件，因此，選取核取方塊在大多數情況下是最佳方法。若要理解將共用或重複物件匯入 *Panorama* 的結果，請參閱規劃如何管理公用設定。

4. 選取匯入原則規則的 **Rule Import Location**（規則匯入位置）：**Pre Rulebase**（預先規則庫）或 **Post Rulebase**（後續規則庫）。無論您的選取為何，Panorama 會將預設安全性規則（intrazone 規則和 interzone 規則）匯入至後續規則庫。

   若 *Panorama* 的規則與您所匯入之防火牆規則具有相同名稱，則 *Panorama* 會同時顯示兩個規則。執行 *Panorama* 提交前刪除一個規則，以避免提交出錯。

5. 按一下 **OK**（確定）。Panorama 顯示匯入狀態、結果、關於匯入內容的詳細資訊和任何警告。按一下 **Close**（關閉）。
6. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

STEP 5 | 從 Panorama 推送組態至新增的裝置。

要防止規則或物件名稱重複，從 Panorama 推送裝置群組組態至防火牆以避免提交錯誤。

此步驟是防火牆管理成功轉移至 *Panorama* 管理伺服器的必要步驟。未能成功執行此步驟將導致組態錯誤和提交失敗。

1. 登入 Panorama 網頁介面 選取 **Panorama** > **Setup**（設定）> **Operations**（操作），然後按一下 **Export or push device config bundle**（匯出或推送裝置設定組合）。
2. 按一下 **Export or push device config bundle**（匯出或推送裝置設定組合），從下拉式功能表選取 **Device**（裝置），然後按一下 **OK**（確定）。
3. 選取匯入設定的 **Device**（設備），按一下 **OK**（確定），然後按一下 **Push & Commit**（推送和提交）。Panorama 推送設定組合並在防火牆上啟動提交。
4. 在成功提交推送後，按一下 **Close**（關閉）。
5. Launch the Web Interface（啟動防火牆的 Web 介面）並確保設定已成功提交。如否，在防火牆上本機 **Commit**（提交）變更。
6. 在 Panorama Web 介面上，選取 **Panorama** > **Managed Devices**（受管理的裝置）> **Summary**（摘要），確認被動防火牆的裝置群組和範本已同步。確認被動防火牆上的原則規則、物件和網路設定符合主動防火牆。在防火牆 Web 介面上，確認組態物件顯示綠色齒輪（.），表示該組態物件從 Panorama 推送。
7. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

© 2019 Palo Alto Networks, Inc.

STEP 6 | 調整匯入的設定。

1. 在 Panorama 中，選取 **Panorama** > **Config Audit**（設定稽核），選取 **Running config**（運行設定）和 **Candidate config**（候選設定）用於對比，按一下 **Go**（前往），然後檢閱輸出。
2. 根據需要，依照設定稽核和 Panorama 在匯入後顯示的警告，更新裝置群組和範本設定。例如：
   - 刪除備援物件和原則規則。
   - 移動或複製原則規則或物件至不同的裝置群組。
   - 移動防火牆至不同裝置群組或範本。
   - 移動匯入時 Panorama 建立的裝置群組至不同的父系裝置群組：選取 **Panorama** > **Device Groups**（設備群組），選取您想要移動的設備群組，選取新 **Parent Device Group**（父系設備群組），然後按一下 **OK**（確定）。

STEP 7 | 推送防火牆組態組合至防火牆，以從其本機設定移除所有原則規則和物件。

此步驟是預防重複規則或物件名稱的必要步驟，否則可能在下一步中，當您從 Panorama 推送裝置群組設定至防火牆時，引起提交出錯。

1. 在 Panorama 中，選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。
2. 選取 **Panorama** > **Setup**（設定）> **Operations**（操作），然後按一下 **Export or push device config bundle**（匯出或推送裝置設定組合）。
3. 選取匯入設定的 **Device**（設備），按一下 **OK**（確定），然後按一下 **Push & Commit**（推送和提交）。Panorama 推送設定組合並在防火牆上啟動提交。

STEP 8 | 推送裝置群組和範本設定，以完成轉移至集中管理。

如果您正在轉移多個防火牆，請在繼續前為各防火牆執行所有先前步驟——包括此步。

1. 選取 **Commit**（提交）> **Commit and Push**（提交並推送），然後在 Push Scope（推送範圍）中 **Edit Selections**（編輯選擇）。
2. 選取 **Device Groups**（裝置群組），然後選取含有匯入之防火牆組態的裝置群組。
3. 選取 **Merge with Device Candidate Config**（與裝置候選設定合併）、**Include Device and Network Templates**（包含裝置與網路範本）以及 **Force Template Values**（強制範本值）。
4. 按一下 **Ok**（確定），以儲存您對 Push Scope（推送範圍）所做的變更。
5. **Commit and Push**（提交並推送）您的變更。

STEP 9 | 整合所有匯入的防火牆組態。

如果您正在轉移多個防火牆，必須執行此步驟。

1. 在匯入所有防火牆組態後，根據需要更新裝置群組和範本，以消除備援並簡化設定管理：請參閱 調整匯入的設定。（您無需再次推送防火牆組態組合。）
2. 進行任何防火牆特定設定。

   如果防火牆會帶有本機區域，您必須在執行裝置群組或範本提交之前建立本機區域；Panorama 無法輪詢防火牆獲得區域名稱或區域設定。如果您將使用本機防火牆規則，請確保其名稱的唯一（在 Panorama 中不重複）。如有必要，您可以透過用防火牆指定值 取代範本或範本堆疊值。
3. 提交並推送您的變更：
   1. 選取 **Commit**（提交）> **Commit and Push**（提交並推送），然後在 Push Scope（推送範圍）中 **Edit Selections**（編輯選擇）。
   2. 選取 **Device Groups**（裝置群組），選取您已變更的裝置群組，以及 **Include Device and Network Templates**（包括裝置和網路範本）。
   3. 按一下 **Ok**（確定），以儲存您對 Push Scope（推送範圍）所做的變更。
   4. **Commit and Push**（提交並推送）您的變更。

STEP 10 | 執行轉移後測試規劃。

© 2019 Palo Alto Networks, Inc.

執行轉移規劃時計劃的確認工作，以確認防火牆帶 Panorama 推送組態時與其帶原始本機設定時的效率一致：請參閱 建立移轉後測試計劃。

移轉防火牆 HA 配對至 Panorama 進行管理

如果 HA 設定中有您想要使用 Panorama 來管理的防火牆配對，您可以選擇將防火牆 HA 配對本機的設定匯入 Panorama，而不必重新建立任何設定或原則。您要先將防火牆組態匯入 Panorama，而這些設定會用於建立新裝置群組和範本。您將會以特殊方式將裝置群組和範本的設定推送至防火牆，以覆寫本機防火牆組態，並將防火牆與 Panorama 同步。

STEP 1 | 規劃轉移。

請參閱計劃移轉至 Panorama 進行管理中的檢查清單。

STEP 2 | 停用 HA 對等之間的設定同步。

針對 HA 配對中的兩個防火牆重複這些步驟。

1. 登入每個防火牆的網頁介面，選取 **Device**（裝置）> **High Availability**（高可用性）> **General**（一般），並編輯 Setup（設定）部分。
2. 清除 **Enable Config Sync**（啟用設定同步），然後按一下 **OK**（確定）。
3. 在每個防火牆上 **Commit**（提交）設定變更。

STEP 3 | 將每個防火牆連接至 Panorama。

如果 *Panorama* 已開始從這些防火牆接收日誌，則您不需要執行此步驟。繼續至步驟 5。

針對 HA 配對中的兩個防火牆重複這些步驟。

1. 登入每個防火牆的網頁介面，選取 **Device**（裝置）> **Setup**（設定）> **Management**（管理），然後編輯 Panorama 設定。
2. 在 **Panorama Servers**（**Panorama** 伺服器）欄位中，輸入 Panorama 管理伺服器的 IP 位址，確認 **Panorama Policy and Objects**（**Panorama** 原則與物件）和 **Device and Network Template**（裝置與網路範本）已啟用，然後選取 **OK**（確定）。
3. 在每個防火牆上 **Commit**（提交）設定變更。

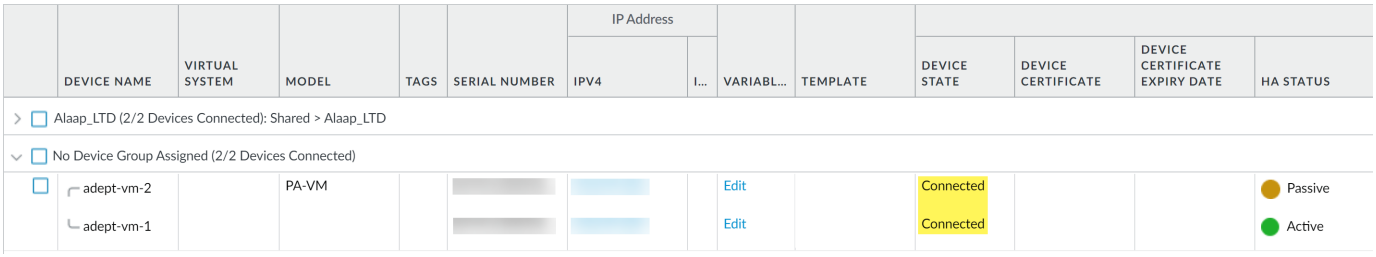
STEP 4 | 將每個防火牆新增為受管理的裝置。

如果 *Panorama* 已開始從這些防火牆接收日誌，則您不需要執行此步驟。繼續至步驟 5。

將防火牆新增為受管理的裝置。

1. 登入 Panorama 網頁介面，選取**Panorama** > **Managed Devices**（受管理的設備），再按一下 **Add**（新增）。
2. 輸入每個防火牆的序號並按一下 **Add**（新增）。
3. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。
4. 確認每個防火牆的 Device State（裝置狀態）為 Connected（已連線）。

© 2019 Palo Alto Networks, Inc.



	DEVICE NAME	VIRTUAL SYSTEM	MODEL	TAGS	SERIAL NUMBER	IP Address IPV4	I...	VARIABL...	TEMPLATE	DEVICE STATE	DEVICE CERTIFICATE	DEVICE CERTIFICATE EXPIRY DATE	HA STATUS
>	Alaap_LTD (2/2 Devices Connected): Shared > Alaap_LTD												
v	No Device Group Assigned (2/2 Devices Connected)												
	adept-vm-2		PA-VM					Edit		Connected			Passive
	adept-vm-1							Edit		Connected			Active

STEP 5 | 將每個防火牆組態匯入 Panorama。

在此步驟中，不要將任何裝置群組或範本堆疊設定推送到受管理防火牆。在此步驟推送裝置群組和範本堆疊設定會擦除後續步驟中的本機防火牆 *HA* 設定。

如果您稍後決定重新匯入防火牆組態，請先移除當作成員的防火牆裝置群組和範本。如果裝置群組和範本名稱與防火牆主機名稱一致，您可以在重新匯入防火牆組態前刪除壯漢子群組和範本，或使用 *Device Group Name Prefix*（裝置群組名稱前置詞）欄位為透過重新匯入建立的裝置群組和範圍輸入新名稱。此外，將防火牆從裝置群組或範本中移除時，防火牆不會丟失日誌。

1. 從 Panorama，選取 **Panorama** > **Setup**（設定）> **Operations**（操作），按一下 **Import device configuration to Panorama**（匯入設備組態至 **Panorama**），然後選取 **Device**（設備）。

   Panorama 無法從被指派至現有裝置群組或範本堆疊的防火牆匯入設定。

2. （Optional（選用））編輯 **Template Name**（範本名稱）。預設值為防火牆名稱。您無法使用現有範本或範本堆疊名稱。
3. （選用）編輯 **Device Group**（裝置群組）名稱。若為多重 vsys 防火牆，依預設，每個裝置群組都有 vsys 名稱，請各新增一個字元字串作為裝置群組名稱首碼。否則，預設值為防火牆名稱。您無法使用現有裝置群組的名稱。

   依預設會選取 *Import devices' shared objects into Panorama's shared context*（將裝置的共用物件匯入 *Panorama* 的共用內容）核取方塊，這表示 *Panorama* 比較會將屬於防火牆中「共用」位置的物件，匯入 *Panorama* 中的「共用」。如果匯入的物件不在防火牆的共用內容中，則會套用至每個要匯入的裝置群組。如果清除此核取方塊，*Panorama* 複製不會比較匯入的物件，而會將所有共用的防火牆物件套用至要匯入的裝置群組（而不是「共用」）。這會建立重複物件，因此，選取核取方塊在大多數情況下是最佳方法。若要理解將共用或重複物件匯入 *Panorama* 的結果，請參閱規劃如何管理公用設定。

4. **Commit to Panorama**（提交至 **Panorama**）。
5. 選取 **Panorama** > **Setup**（設定）> **Operations**（操作），然後 **Export or push device config bundle**（匯出或推送裝置設定組合）。選取 **Device**（裝置）、選取 **OK**（確定），然後 **Push & Commit**（推送與提交）設定。

   在推送裝置群組和範本堆疊之前，兩個防火牆上必須清除步驟 2 中的啟用設定同步設置。

6. 在防火牆 HA 對等上，啟動 Web 介面 並確保上一步推送的設定已成功提交。如否，在防火牆上本機 **Commit**（提交）變更。
7. 在第二個防火牆上重複上述步驟 1-6。此程序會為每個防火牆建立一個裝置群組和範本堆疊。

STEP 6 | 將 HA 防火牆對等新增至相同的裝置群組和範本堆疊。

如果 HA 防火牆對等在主動/主動設定中，請跳過此步驟。

© 2019 Palo Alto Networks, Inc.

1. 選取 **Panorama** > **Device Group**（裝置群組），選取第二個防火牆的裝置群組並 **Delete**（刪除）。
2. 選取第一個防火牆的裝置群組，選取第二個防火牆，按一下 **OK**（確定）並 **Commit to Panorama**（提交至 **Panorama**），以新增至與 HA 對等相同的裝置群組。
3. 選取 **Panorama** > **Templates**（範本），選取第二個防火牆的範本堆疊並 **Delete**（刪除）。
4. 選取第一個防火牆的範本堆疊，新增第二個防火牆，選取 **OK**（確定）並 **Commit to Panorama**（提交至 **Panorama**），以新增至與 HA 對等相同的範本堆疊。
5. 在與新移轉的防火牆關聯的範本中移除 HA 設定。
   1. 選取 **Device**（裝置）> **Setup**（設定）> **High Availability**（高可用性）
   2. 選取 **Remove All**（全部移除）。
   3. **Commit to Panorama**（提交至 **Panorama**）。
6. 將裝置群組和範本堆疊設定推送到受管理防火牆。

   先將裝置群組和範本堆疊設定推送到被動 *HA* 對等，然後推送到主動 *HA* 對等。

   1. 選取 **Commit**（提交）> **Push to Devices**（推送至裝置）和 **Edit Selections**（編輯選擇）。
   2. 啟用（選取）**Merge Device Candidate Config**（合併裝置候選設定）、**Include Device and Network Templates**（包含裝置與網路範本）以及 **Force Template Values**（強制範本值）。
   3. 按一下 **OK**（確定）。
   4. **Push**（推送）到您的受管理防火牆。
   5. 在主動 HA 對等上，啟動 Web 介面，然後選取 **Device**（裝置）> **High Availability**（高可用性）> **Operational Commands**（操作命令）以暫停本機裝置。

      在修改主動 HA 對等前容錯移轉到被動 HA 對等，以便在完成設定移轉時維持安全狀態。
   6. 為現在的被動 HA 對等重複步驟 1-4。
   7. 在現在的主動 HA 對等上，啟動 Web 介面，然後選取 **Device**（裝置）> **High Availability**（高可用性）> **Operational Commands**（操作命令）以暫停本機裝置。

      這會還原原始主動/被動 HA 對等角色。
7. 選取 **Panorama** > **Managed Devices**（受管理的裝置）> **Summary**（摘要），確認被動防火牆的裝置群組和範本已同步。確認被動防火牆上的原則規則、物件和網路設定符合主動防火牆。

STEP 7 | 啟用 HA 對等之間的設定同步。

如果您打算維護的本機設定需要同步，請針對 HA 配對中的兩個防火牆重複這些步驟。

1. 登入每個防火牆的網頁介面，選取 **Device**（裝置）> **High Availability**（高可用性）> **General**（一般），並編輯 Setup（設定）部分。
2. 選取 **Enable Config Sync**（啟用設定同步），然後按一下 **OK**（確定）。
3. 在每個防火牆上 **Commit**（提交）設定變更。

載入部分防火牆組態至 Panorama 中

如果防火牆上的部分組態設定與其他防火牆共用，您可以將特定設定載入 Panorama 然後將其推送至所有其他防火牆或特定裝置群組和範本內的防火牆。

載入組態至 Panorama 管理伺服器需要完整認可，並且必須由超級使用者執行。執行某些 Panorama 操作時需要完整認可，諸如還原及載入組態快照，並且不支援自訂管理員角色設定檔。

STEP 1 | 計劃移轉至 Panorama。

請參閱計劃移轉至 Panorama 進行管理中的檢查清單。

STEP 2 | 解決如何管理重複設定，重複設定是指在 Panorama 中與防火牆內名稱一致的設定。

© 2019 Palo Alto Networks, Inc.

載入部分防火牆組態之前，Panorama 和防火牆可能已有重複設定。載入防火牆組態可能還需要新增設定至 Panorama，該設定是其他受管理防火牆內設定的重複。

如果 *Panorama* 有與防火牆上原則規則或物件相同名稱的原則規則或物件，當您嘗試推送裝置群組設定至該防火牆時，可能出現提交失敗。如果 *Panorama* 範本設定與防火牆上範本設定名稱相同，當您推送範本時，範本值將取代防火牆值。

1. 在 Panorama 上，執行全域尋找以確定是否有重複的設定。
2. 如果要使用 Panorama 管理，則刪除或重新命名防火牆上的重複設定，或如果要使用防火牆管理，則刪除或重命名 Panorama 上的重複設定。如果您要使用防火牆管理裝置或網路設定，不需要刪除或重命名 Panorama 上的重複設定，您也可以從 Panorama 推送設定（步驟 6），然後在防火牆上以防火牆特定的值取代範本或範本堆疊值。

STEP 3 | 匯出整個防火牆組態至您的本機電腦。

1. 在防火牆上，選取 **Device**（裝置）> **Setup**（設定）> **Operations**（操作）。
2. 按一下 **Save named configuration snapshot**（儲存具名組態快照），輸入 **Name**（名稱）以識別設定，然後按一下 **OK**（確定）。
3. 按一下 **Export named configuration snapshot**（匯出具名組態快照），選取您剛儲存的設定 **Name**（名稱），然後按一下 **OK**（確定）。防火牆將設定匯出為 XML 檔案。

STEP 4 | 將防火牆組態快照匯入 Panorama。

1. 在 Panorama 上，選取 **Panorama** > **Setup**（設定）> **Operations**（操作）。
2. 按一下 **Import named Panorama configuration snapshot**（匯入具名 **Panorama** 組態快照），**Browse**（瀏覽）至您匯出至電腦的防火牆組態檔案，並按一下 **OK**（確定）。

在使用此選項匯入防火牆組態檔案後，您無法使用 *Panorama web* 介面加載。您必須如下一步中所述使用 *XML API* 或 *CLI*。

STEP 5 | 載入防火牆組態所需的部分至 Panorama 中。

若要指定設定部分（例如，所有應用物件），您必須識別：

- 源 xpath—來自載入防火牆組態檔案中的 XML 節點。
- 目的地 xpath—載入至 Panorama 組態的節點。

使用 XML API 或 CLI 識別和載入部分設定：

1. 使用防火牆 XML API 或 CLI 識別源 xpath。

   例如，防火牆 vsys1 中應用物件的 xpath 為：

```
/config/devices/entry[@name='localhost.localdomain']/vsys/
entry[@name='vsys1']/application
```

2. 使用 Panorama XML API 或 CLI 識別目的地 xpath。

   例如，若要載入應用物件至名稱為 US-West 的裝置群組中，xpath 為：

```
/config/devices/entry[@name='localhost.localdomain']/device-group/
entry[@name='US-West']/application
```

3. 使用 Panorama CLI 載入設定並提交變更：

```
# load config partial mode [append|merge|replace] from-xpath <source-
xpath> to-xpath <destination-xpath> from <filename>
```


© 2019 Palo Alto Networks, Inc.

```
# commit
```

例如，輸入以下內容從名稱為 fw1-config.xml 匯入防火牆組態上的 vsys1 載入應用物件至 Panorama 上名為 US-West 的裝置群組內：

```
# load config partial mode merge from-xpath devices/
entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/application
 to-xpath /config/devices/entry[@name='localhost.localdomain']/device-
group/entry[@name='US-West']/application from fw1-config.xml
# commit
```

STEP 6 | 從 Panorama 推送部分設定至防火牆，以完成轉移至集中管理。

1. 在防火牆上，刪除任何與 Panorama 上規則或物件相同名稱的規則或物件。如果該防火牆的裝置群組有帶 Panorama 中重複規則或物件的其他防火牆，也應在那些防火牆上執行這些步驟。詳細資訊，請參閱步驟 2。
2. 在 Panorama 上，將部分設定推送至防火牆。
   1. 選取 **Commit**（提交）> **Commit and Push**（提交並推送），然後在 Push Scope（推送範圍）中 **Edit Selections**（編輯選擇）。
   2. 選取 **Device Groups**（裝置群組），然後選取含有匯入之防火牆組態的裝置群組。
   3. 選取 **Merge with Device Candidate Config**（與裝置候選設定合併）、**Include Device and Network Templates**（包含裝置與網路範本）以及 **Force Template Values**（強制範本值）。
   4. 按一下 **Ok**（確定），以儲存您對 Push Scope（推送範圍）所做的變更。
   5. **Commit and Push**（提交並推送）您的變更。
3. 如果防火牆有您不會使用 Panorama 管理的裝置或網路設定，在防火牆上 取代範本或範本堆疊值。

STEP 7 | 執行轉移後測試規劃。

執行轉移規劃時計劃的確認工作，以確認防火牆帶 Panorama 推送設定時與其帶原始本機設定時的效率一致：請參閱建立轉移後測試規劃。

© 2019 Palo Alto Networks, Inc.

Panorama 上的裝置監控

在新增防火牆並設定政策規則後，您可以監控健康狀態，以確保您的防火牆在正常參數值內運作。對於原則規則，請監控規則流量以進行比對，識別哪一個規則符合您流量強制執行的需要。

- 監控裝置健康
- 監控原則規則使用狀況

監控裝置健康

監控您受管理的防火牆的健康資料，以在影響網路安全性之前找出並解決硬體問題。Panorama™ 和受管理的防火牆兩者都必須執行 PAN-OS® 8.1 或更新版本，但防火牆不需要為裝置群組或範本堆疊的一部分，才能監控他們的摘要工作階段、日誌記錄、資源與環境效能。Panorama 會儲存最近 90 天的受管理防火牆的健康監控統計數值，因此當您選取一個防火牆，您可以檢視工作階段、環境、介面、日誌記錄、資源和高可用性效能的時間趨勢圖形以及表格。Panorama 使用七天平均值和標準偏差計算每個度量標準的基準性能，以確定特定防火牆的正常操作範圍。除了追踪基準並比較時間趨勢的性能，您可以查看哪一個防火牆存在偏差指標，並在影響網路之前隔離與性能相關的問題。當 Panorama 識別出一個超過正常作業範圍度量值時，它會標記該度量值並用偏離的防火牆填入偏離裝置頁籤。

健康監控資料儲存在 Panorama 上，且在移除防火牆時保留。當防火牆從 Panorama 管理移除時，健康監控資料就不再顯示，但會保留 90 天。在 90 天後，所有移除防火牆的健康監控資料將從 Panorama 上移除。如果防火牆新增回 Panorama 管理，則最新健康監控數值將從防火牆移除的時間開始顯示。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 選取 **Panorama** > **Managed Devices**（受管理的裝置）> **Health**（健康）以監控受管理的防火牆健康。

檢視 **All Devices**（所有裝置）以觀看所有受管理的防火牆的清單，以及監控的健康度量。選取個別防火牆以檢視詳細的裝置視圖，其中附有監控度量的時間趨勢圖與表格。

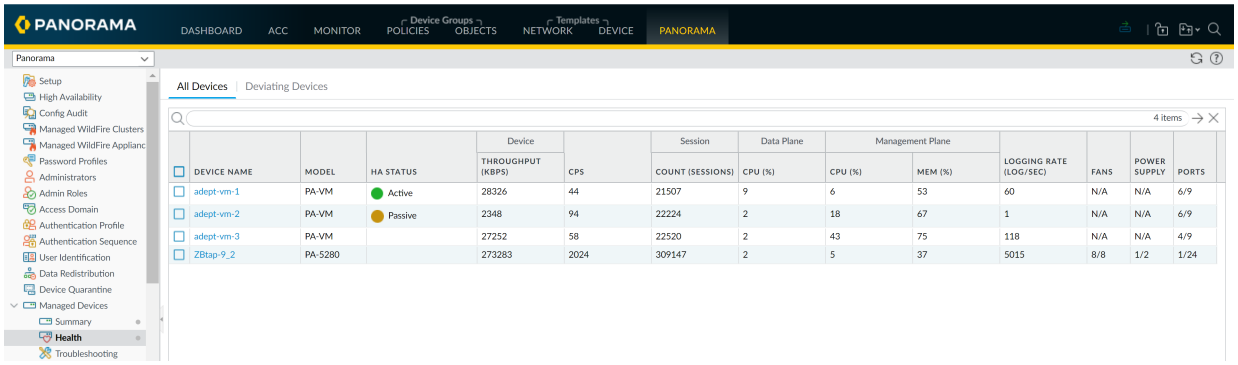


圖 12: 受管理的防火牆健康監控

© 2019 Palo Alto Networks, Inc.

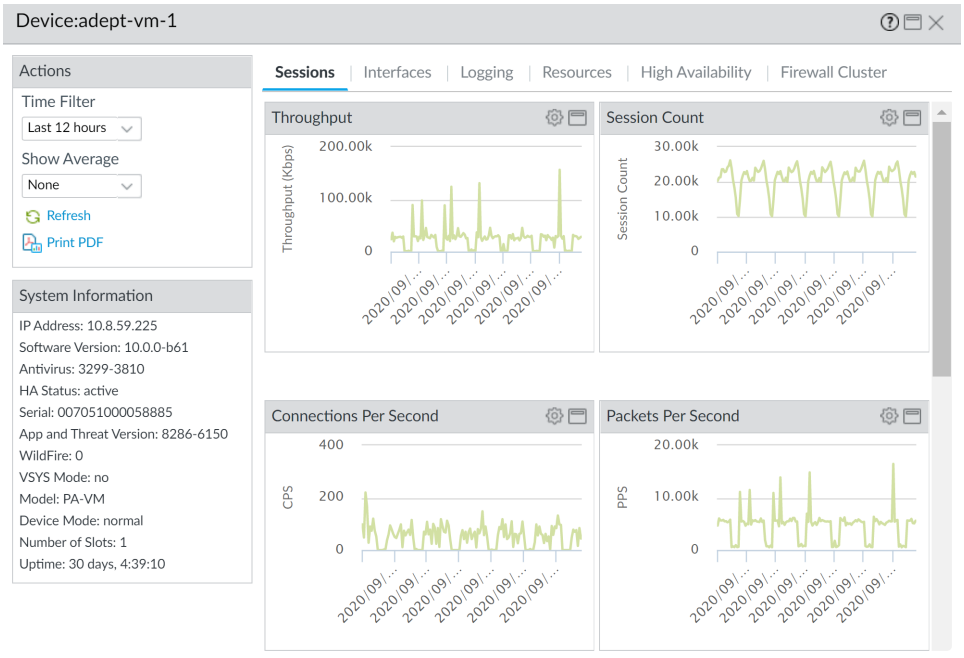
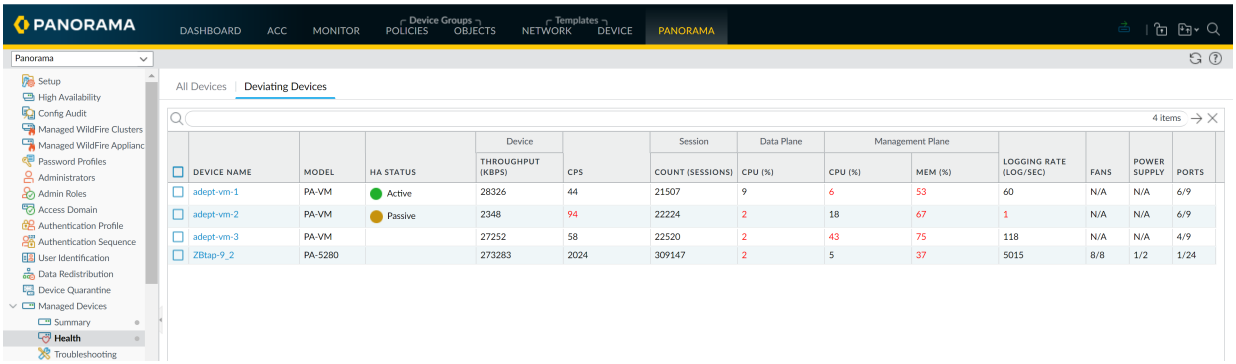


圖 13: 詳細裝置檢視

STEP 3 | 選取 **Deviating Devices**（偏離的裝置）以檢視帶有偏離超出計算基準的健康度量的防火牆。

Panaroma 列出所有回報偏離計算基準的防火牆，並以紅色顯示偏離度量。



監控原則規則使用狀況

由於您的原則變更，追蹤 Panorama 上的規則使用狀況可以幫助您評估您的原則實作是否能持續符合您強制需求。此可見度能幫助您找到並移除未使用的規則，以降低安全性風險，並讓您的原則規則庫井井有條。此外，規則使用狀況追蹤讓您能夠快速驗證新規則增加的部分，以及規則變更，並監控操作和疑難排解工作的規則使用狀況。在 Panorama 上，您可以檢視您推送原則的裝置群組中的防火牆規則使用狀況，以決定是全部、一些或是沒有防火牆的流量匹配，而不是僅能監控在裝置群組中所有防火牆的命中總數。您可以透過規則使用資料，在可自訂的時間範圍內快速篩選規則，如建立和修改日期。顯示的規則使用狀況資訊在重新啟動、資料平面重新啟動和升級過程中會持續存在。

在 Panorama 上，您可以檢視執行 PAN-OS 8.1 或更新版本的受管理防火牆規則使用詳細資料，啟用原則規則命中數（預設為啟用），以及透過裝置群組定義和推送原則規則。Panorama 無法為防火牆上本機設定的原則規則檢索規則使用詳細資料，因此您必須登入防火牆以檢視本機設定規則的規則使用詳細資料。

篩選原則規則庫後，管理員可以採取動作直接從原則最佳化工具中刪除、停用、啟用和標記原則規則。例如，您可以篩選未使用的規則，然後標記它們以進行檢閱，從而確定可以安全地刪除它們還是將其保留在規

© 2019 Palo Alto Networks, Inc.

則庫中。透過讓管理員能夠直接從原則最佳化工具中採取動作，可以減少進一步幫助簡化規則生命週期管理並確保防火牆沒有被過度佈建所需的管理負荷。

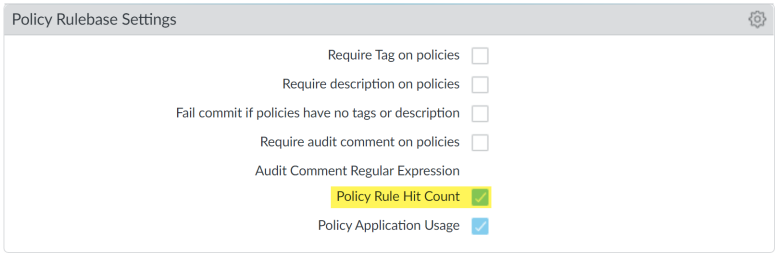
使用原則最佳化工具確定遷移或清除規則的優先順序時，原則規則使用情況資料也可能有用。

若要檢視任何共享規則或特定裝置群組的規則使用狀況：

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 確認是否已啟用 **Policy Rule Hit Count**（原則規則命中數）。

1. 導覽至 Policy Rulebase Settings（原則規則庫設定）（**Panorama** > **Setup**（設定）> **Management**（管理））。
2. 確認是否已啟用 **Policy Rule Hit Count**（原則規則命中數）。



STEP 3 | 選取 **Policies**（原則）> *<policy rule>* 以檢視規則。

STEP 4 | 變更裝置群組內容為 **Shared**（共用）或您想要檢視的特定裝置群組。

STEP 5 | 決定是否要使用規則（規則使用狀況）。原則規則使用狀況狀態為下列內容之一：

防火牆必須執行 PAN-OS 8.1 或更新版本，並為 Panorama 啟用攻策規則命中數以確定規則使用情況。

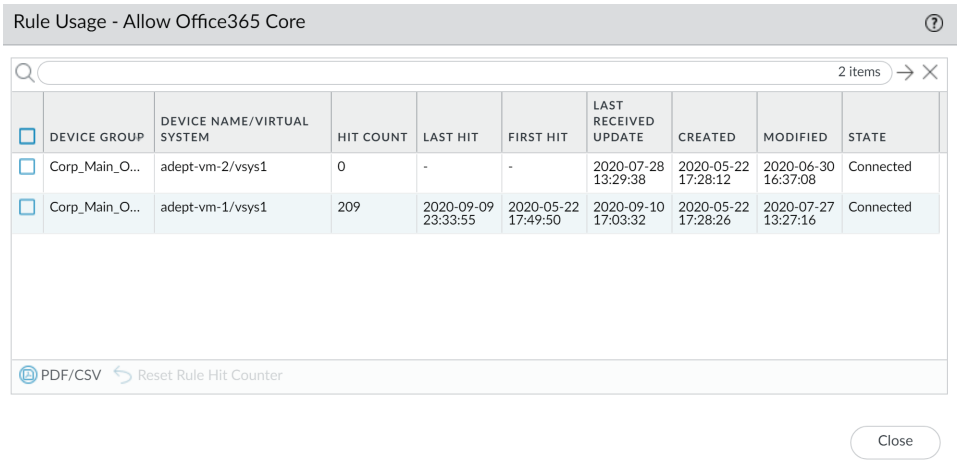
- 已使用—當您推送原則規則的裝置群組中的所有防火牆與原則規則的流量匹配時。
- 部分使用—當您推送原則規則的裝置群組中的一些防火牆與原則規則的流量匹配時。
- 未使用—當您推送原則規則的裝置群組中沒有防火牆與原則規則的流量匹配時。
- **Em-dash (—)**—當您推送原則規則的裝置群組中沒有防火牆已啟用原則則命中數，或可用 Panorama 決定規則使用情況時。
- 修改—原則規則上次修改的日期與時間。
- 建立—原則規則建立的日期與時間。

如果規則建立時 *Panorama* 執行 *PAN-OS 8.1* 並已啟用原則規則命中數設定，第一次命中日期與時間將用作升級至 *PAN-OS 9.0* 或更高版本時的建立日期與時間。如果規則在 *PAN-OS 8.1* 防火牆中建立並已停用原則規則命中數設定，或如果規則在 *Panorama* 執行 *PAN-OS 8.0* 或更早版本時建立，為原則規則建立日期將為您成功升級*Panorama*至 *PAN-OS 9.0* 或更高版本的日期與時間。

© 2019 Palo Alto Networks, Inc.

Rule Usage		DAYS WITH NO NEW APPS	MODIFIED	CREATED
RULE USAGE	APPS SEEN			
Used	6	150	2020-06-24 10:34:...	2020-04-09 11:34:03
Unused	0	-	2020-06-24 10:34:...	2020-04-16 11:42:46
Used	11	57	2020-06-24 10:34:...	2020-04-16 11:42:46
Partially Used	3	111	2020-06-24 10:34:...	2020-05-22 17:26:44
Unused	0	-	2020-06-24 10:34:...	2020-05-22 22:45:53

STEP 6 | 按一下規則使用情況狀態以檢視使用此規則的防火牆清單，以及與每個防火牆上規則匹配的流量的命中數資料。



STEP 7 | （選用）為在裝置群組內的個別防火牆檢視原則規則命中數資料。

1. 按一下 **Preview Rules**（預覽規則）。
2. 從裝置內容中選取您想要檢視原則規則使用情況資料的防火牆。

STEP 8 | 選取 **Policies**（原則），在原則最佳化工具對話方塊中，檢視 **Rule Usage**（規則使用情況）篩選器。

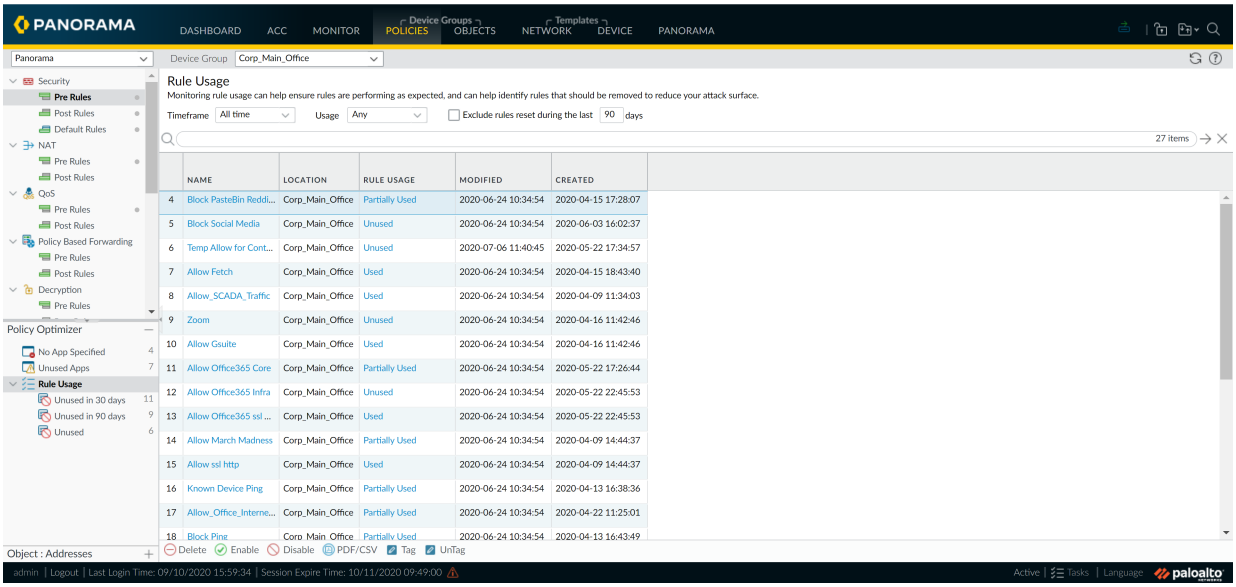
STEP 9 | 篩選所選規則庫中的規則。

您可以篩選從 Panorama 推送至防火牆的規則使用情況。Panorama 無法篩選在防火牆上本機設定的規則使用情況。

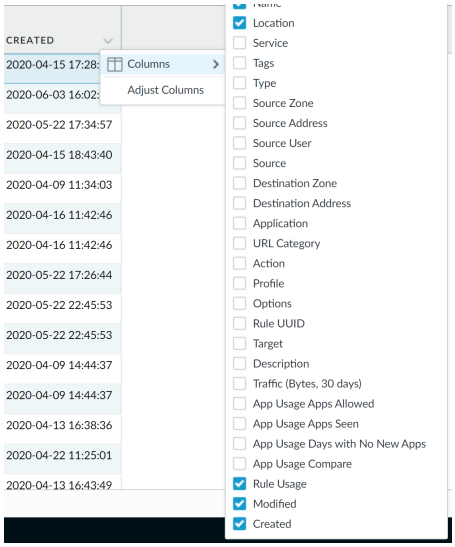
使用規則使用情況篩選器評估指定時段內的規則使用情況。例如，為 *30* 天內未使用的規則篩選所選的規則庫。您還可評估具有其他規則屬性的規則使用情況，例如建立與修改日期使您能夠篩選要檢視的正確規則集。您可以使用此資料幫助管理您的規則生命週期，並確定是否需要移除規則以減少網路受攻擊面。

1. 選取要篩選的 **Timeframe**（時間範圍），或指定 **Custom**（自訂）時間範圍。
2. 選取要篩選的規則 **Usage**（使用情況）。
3. （選用）如果您重設了任何規則的規則使用情況，請檢查排除最近 *<number of days>* 天內重設的規則，並確定根據自重設規則以來指定的天數排除規則的時間。僅在您指定天數之前重設的規則包含在篩選結果內。

© 2019 Palo Alto Networks, Inc.

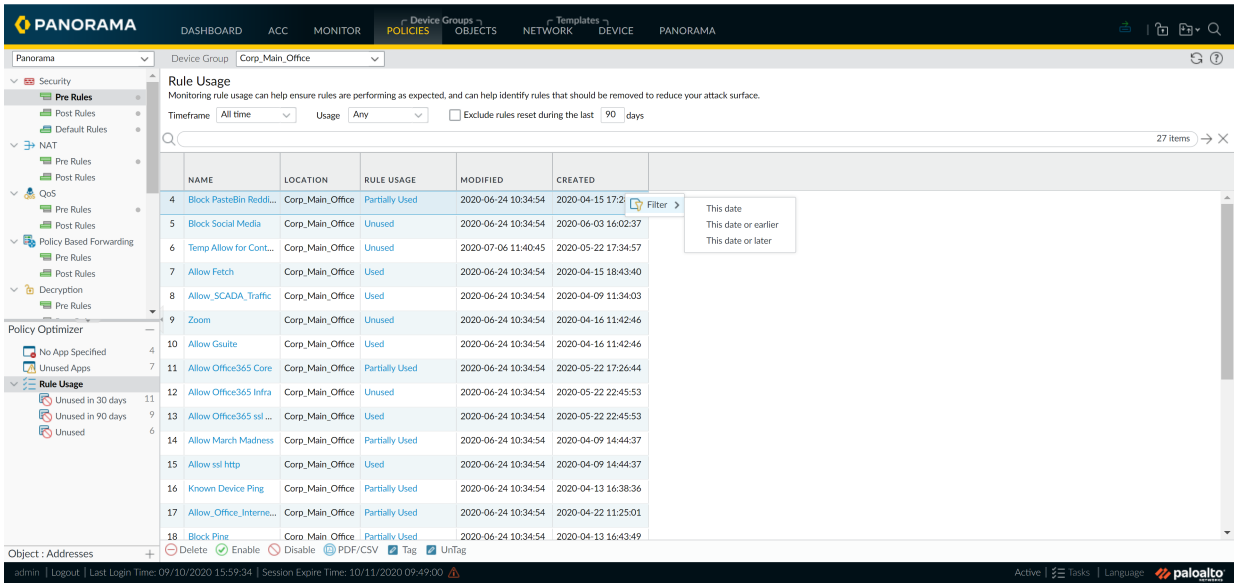


4. （選用）根據規則使用情況之外的其他規則資料指定搜尋篩選器。
   1. 將滑鼠懸停在欄標頭上，並從下拉式清單中選取 **Columns**（欄）。
   2. 新增任何要篩選或顯示的其他欄。



   3. 將滑鼠懸停在要篩選的欄資料上，並從下拉式清單中選取 **Filter**（篩選）。針對包含日期的資料，選取使用 **This date**（此日期）、**This date or earlier**（此日期或更高）或 **This date or later**（此日期或更遲）進行篩選。
   4. 按一下 **Apply Filter**（套用篩選器）（→）。

© 2019 Palo Alto Networks, Inc.



STEP 10 | 對一個或多個未使用的原則規則採取動作。

1. 選取一個或多個未使用的原則規則。
2. 執行下列其中一個動作：
   - 刪除—刪除一個或多個所選原則規則。
   - 啟用—在停用狀態下啟用一個或多個所選原則規則。
   - 停用—停用一個或多個所選原則規則。
   - 標記—將一個或多個群組標籤套用至一個或多個所選原則規則。群組標籤必須已經存在才可標記原則規則。
   - 取消標記—從一個或多個所選原則規則中移除一個或多個群組標籤。
3. 選取 **Commit**（提交），**Commit and Push**（提交並推送）您的變更。

© 2019 Palo Alto Networks, Inc.

使用案例：使用 Panorama 設定防火牆

讓我們假設您想要使用高可用性設定中的 Panorama，管理網路上的十二個防火牆；您跨六家分公司部署六個防火牆；在兩個資料中心的每一個資料中心上，於高可用性設定中部署一對防火牆；並在兩個地區總部的每一個總部上部署一個防火牆。

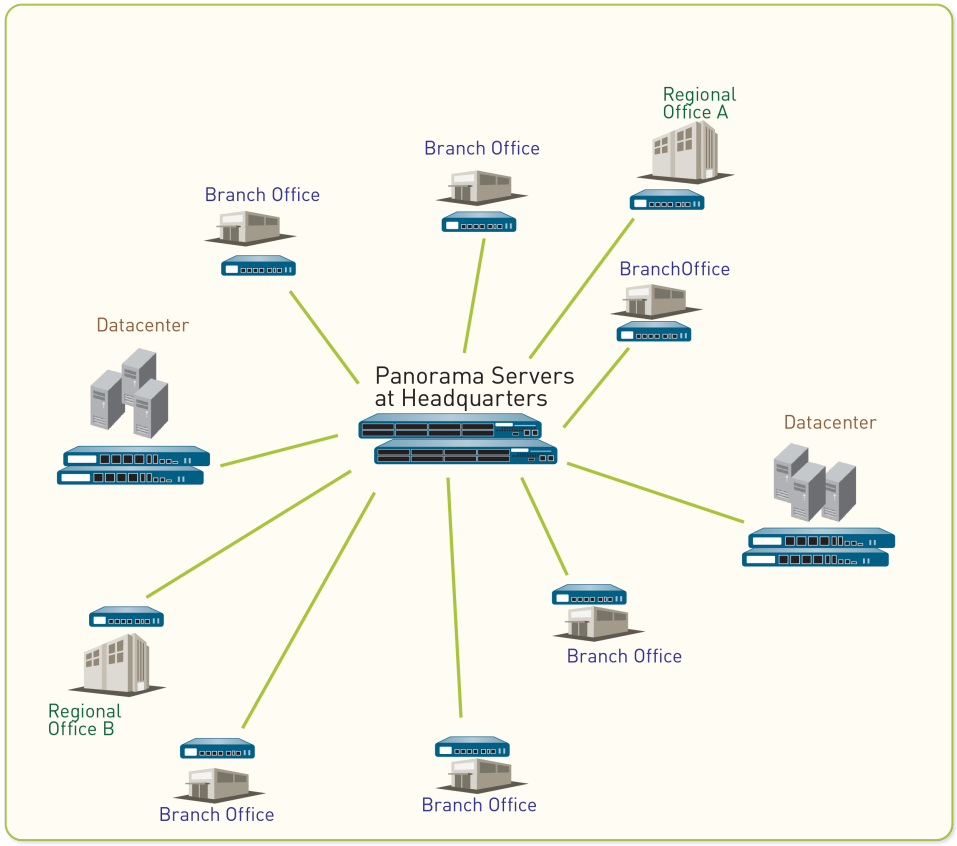


圖 14: 防火牆分散範例

建立中央管理策略的第一步是決定如何將防火牆分組至裝置群組與範本，從而有效率地從 Panorama 推送設定。您可以將防火牆的商務功能、地理位置或管理網域做為分組的依據。在此範例中，您將使用 Panorama 建立兩個裝置群組和三個範本來管理防火牆：

- 此使用案例中的裝置群組
- 此使用案例中的範本
- 設定您的中央設定與原則

此使用案例中的裝置群組

在 使用案例：使用 Panorama 設定防火牆 中，我們需要根據防火牆將執行的功能，定義兩個裝置群組：

- DG_BranchAndRegional，適用於針對在分公司和地區總部上做為安全性閘道運作的防火牆進行群組分配。我們會在相同的裝置群組中放置分公司防火牆和地區總部防火牆，因為具備類似功能的防火牆將需要類似的原則規則庫。
- DG_DataCenter，適用於群組用來保護資料中心之伺服器安全的防火牆。

我們接著會跨兩個裝置群組來管理共用原則規則，以及為地區總部和分公司群組管理不同的裝置群組規則。接下來為了增加靈活度，地區總部或分公司的本機管理員可建立本機規則來比對特定的來源、目的地和服務

© 2019 Palo Alto Networks, Inc.

流程，以存取該機構所需要的應用程式和服務。在此範例中，我們將為安全性規則建立下列階層；您可以針對任何其他規則庫使用類似的方法。

Device Groups	DG_BranchAndRegional		DG_DataCenter
Rules	Regional	Branch	Datacenter
Shared pre-rule	Allow DNS and SNMP services.		
	Acceptable use policy that denies access to specified URL categories and peer-to-peer traffic that is of risk level 3, 4, and 5.		
Device Group pre-rule	Allow Facebook to all users in the marketing group in the regional offices only.		Allow access to the Amazon cloud application for the specified hosts/servers in the datacenter.
Local rules on a device	None		
Device Group post-rule	None		
Shared post-rule	To enable logging for all Internet-bound traffic on your network, create a rule that allows or denies all traffic from the trust zone to the untrust zone.		

圖 15: 安全性規則階層

此使用案例中的範本

群組範本的防火牆時，我們必須考量網路設定中的差異。例如，如果介面設定不同（介面類型不相似、使用的介面在編號結構描述和連結容量方面不相似，或區域至介面的對應不同），則防火牆必須位於不同的範本。此外，設定防火牆來存取網路資源的方式也可能不同，因為防火牆散佈在各處；例如，它們存取的 DNS 伺服器、系統日誌伺服器和閘道可能不同。因此，若要取得最佳的基礎設定，在 使用案例：使用 Panorama 設定防火牆 中，我們必須將防火牆置於不同的範本中，如下所示：

- T_Branch，適用於分公司防火牆
- T_Regional，適用於地區總部防火牆
- T_DataCenter，適用於資料中心防火牆

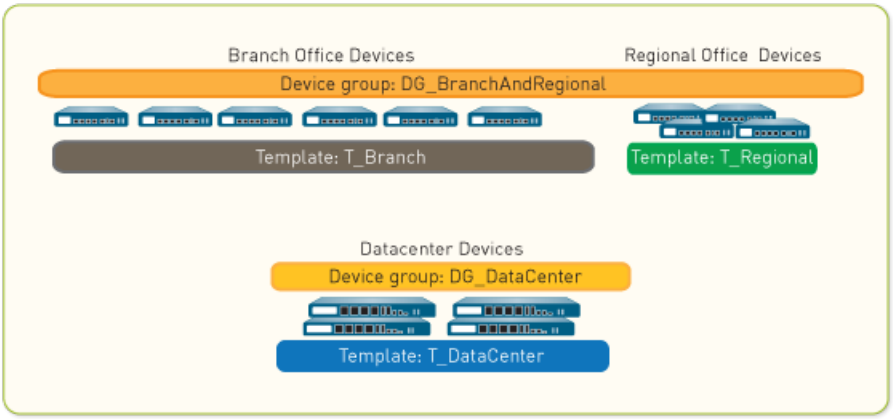


圖 16: 裝置群組範例

© 2019 Palo Alto Networks, Inc.

如果計劃在主動/主動 *HA* 設定中部署您的防火牆，請將 *HA* 配對的每個防火牆指定給不同的範本。這麼做能讓您為每個端點，彈性地進行不同的網路設定。例如，您可以針對每個端點，管理不同範本中的網路設定，讓每個端點都可以連線至不同的北向和南向路由器，並且可擁有不同的 *OSPF* 或 *BGP* 對等設定。

設定您的中央設定與原則

在 使用案例：使用 Panorama 設定防火牆 中，我們需要執行以下工作，以集中部署和管理防火牆：

- 新增受管理的防火牆和部署更新
- 使用範本管理基礎組態
- 使用裝置群組以推送原則規則
- 預覽規則與提交變更

新增受管理的防火牆和部署更新

使用案例：使用 Panorama 設定防火牆 中的第一項工作是新增防火牆作為受管理的裝置，並將內容更新和 PAN-OS 軟體更新部署至這些防火牆。

STEP 1 | 對於 Panorama 將管理的每個防火牆，將防火牆新增為受管理的裝置。

在此示例中，新增 12 道防火牆。

STEP 2 | 將內容更新部署至防火牆。如果您已購買威脅防範使用授權，就可以使用內容和防毒資料庫。先安裝 **Applications**（應用程式）或 **Applications and Threats**（應用程式和威脅）資料庫，其次安裝 **Antivirus**（防毒）。

若要檢閱 *Panorama* 上執行的所有工作的狀態或進度，請參閱 使用 Panorama 工作管理員。

1. 選取 **Panorama** > **Device Deployment**（設備部署）> **Dynamic Updates**（動態更新）。
2. 按一下 **Check Now**（立即檢查）以檢查最新更新。如果在 Action（動作）欄中的值為 **Download**（下載），這表示可進行該項更新。
3. 按一下 **Download**（下載）。完成下載後，Action（動作）欄中的值會變更為 **Install**（安裝）。
4. 在 **Action**（動作）欄中，按一下 **Install**（安裝）。使用篩選器或使用者定義的標籤來選取要安裝此更新的受管理防火牆。
5. 按一下 **OK**（確定），然後監控每個防火牆內容更新的狀態、進度和結果。**Result**（結果）欄會顯示安裝成功或失敗。

STEP 3 | 將軟體更新部署至防火牆。

1. 選取 **Panorama** > **Device Deployment**（設備部署）> **Software**（軟體）。
2. 按一下 **Check Now**（立即檢查）以檢查最新更新。如果在 Action（動作）欄中的值為 **Download**（下載），這表示可進行該項更新。
3. 尋找每個硬體型號需要的版本，然後按一下 **Download**（下載）。完成下載後，Action（動作）欄中的值會變更為 **Install**（安裝）。
4. 在 Action（動作）欄中，按一下 **Install**（安裝）連結。使用篩選器或使用者定義的標籤來選取要安裝此版本的受管理防火牆。
5. 啟用**Reboot device after install**（安裝後重新啟動裝置）或**Upload only to device (do not install)**（僅上傳至裝置（不要安裝））核取方塊，然後按一下 **OK**（確定）。**Results**（結果）欄會顯示安裝成功或失敗。

© 2019 Palo Alto Networks, Inc.

使用範本管理基礎組態

使用案例：使用 Panorama 設定防火牆 中的第二項工作是建立向防火牆推送基礎設定所需的範本。

STEP 1 | 對於每個您要使用的範本，先新增範本，然後將適當的防火牆指派給每個範本。

在此示例中，建立名為 T_Branch、T_Regional 和 T_DataCenter 的範本。

STEP 2 | 定義 DNS 伺服器、NTP 伺服器、系統日誌伺服器及登入橫幅。為每個範本重複此步驟。

1. 在 **Device**（裝置）頁籤中的下拉式清單中選取 **Template**（範本）。
2. 定義 DNS 和 NTP 伺服器：
    1. 選取 **Device**（設備）> **Setup**（設定）> **Services**（服務）> **Global**（全域），然後編輯 [服務]。
    2. 在 **Services**（服務）頁籤中，輸入 **Primary DNS Server**（主要 **DNS** 伺服器）的 IP 位址。

    對於擁有超過一個虛擬系統 (vsys) 的防火牆，對於每個 *vsys*，新增 DNS 伺服器設定檔至範本（*Device*（裝置）> *Server Profiles*（伺服器設定檔）> *DNS*）。
    3. 在 **NTP** 頁籤中，輸入 **Primary DNS Server**（主要 **DNS** 伺服器）的 IP 位址。
    4. 按一下 **OK**（確定）儲存您的變更。
3. 新增登入橫幅：選取 **Device** > **Setup**（設定）> **Management**（管理），編輯 [一般設定] 部分，輸入 **Login Banner**（登入橫幅）的文字，然後按一下 **OK**（確定）。
4. 設定系統日誌伺服器設定檔（**Device**（設備）> **Server Profiles**（伺服器設定檔）> **Syslog**（系統日誌））。

STEP 3 | 讓 HTTPS、SSH 和 SNMP 存取受管理防火牆的管理介面。為每個範本重複此步驟。

1. 在 **Device**（裝置）頁籤中的下拉式清單中選取 **Template**（範本）。
2. 選取 **Setup**（設定）> **Management**（管理），再編輯 [管理介面設定]。
3. 在 Services（服務）下，選取 **HTTPS**、**SSH** 與 **SNMP** 核取方塊，然後按一下 **OK**（確定）。

STEP 4 | 針對資料中心範本 (T_DataCenter) 中的防火牆建立區域防護設定檔。

1. 在 **Network**（網路）頁籤的 **Template**（範本）下拉式清單中選取 T_DataCenter。
2. 選取 **Network Profiles**（網路設定檔）> **Zone Protection**（區域防護），然後按一下 **Add**（新增）。
3. 此範例中針對 SYN Flood 啟用防禦—在 **Flood Protection**（洪流防禦）頁籤中，選取 **SYN** 核取方塊，將動作設為 **SYN Cookie**，將警示封包/秒設為 `100`，啟動封包/秒設為 `1000`，最大封包/秒設為 `10000`。
4. 以此範例說明，啟用警示—在 **Reconnaissance Protection**（偵察保護）頁籤中，選取 **TCP Port Scan**（**TCP** 連接埠掃描）、**Host Sweep**（主機掃描）及 **UDP Port Scan**（**UDP** 連接埠掃描）的 **Enable**（啟用）核取方塊。確定 Action（動作）值設為**alert**（警示）（預設值）。
5. 按一下 **OK**（確定）來儲存區域防護設定檔。

STEP 5 | 在資料中心範本 (T_DataCenter) 中設定介面與區域設定，然後附加您剛剛建立的區域防護設定檔。



執行此步驟之前，您必須已在防火牆的本機設定介面。至少對於每個介面，必須已定義介面類型、視需要將其指派給虛擬路由器，並附加安全性區域。

1. 在 **Network**（網路）頁籤的 **Template**（範本）下拉式清單中選取 T_DataCenter。
2. 選取 **Network**（網路）> **Interface**（介面），然後在 [介面] 欄中按一下介面名稱。
3. 從下拉式清單中選取 **Interface Type**（介面類型）。
4. 在 **Virtual Router**（虛擬路由器）下拉式清單中，按一下 **New Virtual Router**（新虛擬路由器）。定義虛擬路由器時，確定 **Name**（名稱）符合防火牆上定義的名稱。
5. 在 **Security Zone**（安全性區域）欄中，按一下 **New Zone**（新增區域）。定義區域時，確定 **Name**（名稱）符合防火牆上定義的名稱。

© 2019 Palo Alto Networks, Inc.

6. 按一下 **OK**（確定）以儲存對介面所做的變更。
7. 選取 **Network**（網路）> **Zones**（區域），再選取剛才建立的區域。驗證將正確的介面附加至區域。
8. 在 **Zone Protection Profile**（區域防護設定檔）下拉式清單中，選取您建立的設定檔，然後按一下 **OK**（確定）。

STEP 6 | 推送範本變更。

1. 選取 **Commit**（提交）> **Commit and Push**（提交並推送），然後在 Push Scope（推送範圍）中 **Edit Selections**（編輯選擇）。
2. 選取 **Templates**（範本），並選取指派給您已變更之範本的防火牆。
3. 將您的變更 **Commit and Push**（提交並推送）至 Panorama 組態和範本。

使用裝置群組以推送原則規則

使用案例：使用 Panorama 設定防火牆 中的第三項工作是建立裝置群組，以管理防火牆上的原則規則。

STEP 1 | 建立裝置群組，並將適當的防火牆指定給每個裝置群組：請參閱新增裝置群組。

在此示例中，建立名稱為 DG_BranchAndRegional 和 DG_DataCenter 的裝置群組。

當設定 DG_BranchAndRegional 裝置群組時，您必須指派 **Master**（主）防火牆。主防火牆是裝置群組中，唯一會針對原則評估收集使用者和群組對應資訊的防火牆。

STEP 2 | 建立共享預先規則以允許 DNS 和 SNMP 服務。

1. 建立 DNS 和 SNMP 服務的共享應用程式群組。
    1. 選取 **Objects**（物件）> **Application Group**（應用程式群組），然後按一下 **Add**（新增）。
    2. 輸入 **Name**（名稱），並選取 **Shared**（共享）核取方塊以建立共享的應用程式群組物件。
    3. 按一下新增並鍵入 **DNS**，再從清單中選取 **dns**。準備 SNMP 並選取 **snmp**、**snmp-trap**。
    4. 按一下 **OK**（確定）以建立應用程式群組。
2. 建立共享規則。
    1. 在 **Policies**（原則）頁籤的 **Device Group**（裝置群組）下拉式清單中選取 **Shared**（共享）。
    2. 選取 **Security**（安全性）> **Pre-Rules**（預先規則） 原則規則庫。
    3. 按一下 **Add**（新增），並輸入安全性原則規則的 **Name**（名稱）。
    4. 在規則的 **Source**（來源）和 **Destination**（目的地）頁籤中，按一下 **Add**（新增），並輸入流量的 **Source Zone**（來源區域）和 **Destination Zone**（目的地區域）。
    5. 在 **Applications**（應用程式）頁籤中按一下 **Add**（新增），並鍵入您剛剛建立的應用程式群組物件名稱，然後從下拉式清單中選取它。
    6. 在 **Actions**（動作）頁籤中，將 **Action**（動作）設定為 **Allow**（允許），然後按一下 **OK**（確定）。

STEP 3 | 定義企業中的所有辦公室都可接受的使用原則。在此範例中建立共享規則來限制存取部分 URL 類別，並拒絕存取風險等級 3、4 和 5 的點對點流量。

1. 在 **Policies**（原則）頁籤的 **Device Group**（裝置群組）下拉式清單中選取 **Shared**（共享）。
2. 選取 **Security**（安全性）> **Pre-Rules**（預先規則），然後按一下 **Add**（新增）。
3. 在 **General**（一般）頁籤上，輸入安全性規則的 **Name**（名稱）。
4. 在 **Source**（來源）和 **Destination**（目的地）頁籤中，按一下 **Add**（新增），針對流量 **Source Zone**（來源區域）和 **Destination Zone**（目的地區域），選取 **any**（任何）。
5. 在 **Application**（應用程式）頁籤中，定義應用篩選器：
    1. 按一下 **Add**（新增），在下拉式清單頁尾按一下 **New Application Filter**（新應用程式篩選器）。
    2. 輸入 **Name**（名稱），然後選取 **Shared**（共用）核取方塊。
    3. 在 [風險] 欄中，選取等級 **3**、**4** 及 **5**。
    4. 在 Technology（技術）欄中，按一下 **peer-to-peer**（點對點）。

© 2019 Palo Alto Networks, Inc.

5. 按一下 **OK**（確定）儲存新篩選器。
6. 在 **Service/URL Category**（服務/URL 類別）頁籤，按一下 **Add**（新增）並選取要封鎖的 URL 類別（例如 **streaming-media**、**dating** 和 **online-personal-storage**）。
7. 您也可以附加預設的 URL 篩選設定檔—在 **Actions**（動作）頁籤中的 Profile Setting（設定檔設定）區段中，然後選取 **Profile Type**（設定檔類型）選項中的 **Profiles**（設定檔），並選取 **URL Filtering**（**URL** 篩選）選項中的 **default**（預設）。
8. 按一下 **OK**（確定）儲存安全性預先規則。

STEP 4 | 僅允許向地區總部的行銷群組的所有使用者發送 Facebook。

根據使用者和群組啟用安全性規則有下列必要條件工作：

- 在防火牆上設定使用者 ID。
- 為每個區域啟用使用者 ID，這些區域均包含了您想要識別的使用者。
- 為 DG_BranchAndRegional 裝置群組定義主防火牆（請參閱步驟 1）。

1. 選取 **Policies**（原則）頁籤，然後在 **Device Group**（裝置群組）下拉式清單中選取 DG_BranchAndRegional。
2. 選取 **Security**（安全性）> **Pre-Rules**（預先規則）原則規則庫。
3. 按一下 **Add**（新增），並輸入安全性原則規則的 **Name**（名稱）。
4. 在 **Source**（來源）頁籤中，**Add**（新增）包含行銷群組使用者的源區域。
5. 在 **Destination**（目的地）頁籤中，**Add**（新增）目的地區域。
6. 在 **User**（使用者）頁籤中，**Add**（新增）行銷使用者群組至源使用者清單。
7. 在應用程式頁籤中，按一下新增並鍵入 **`Facebook`**，然後從下拉式清單選取它。
8. 在 **Action**（動作）頁籤中，將 **Action**（動作）設定為 **Allow**（允許）。
9. 在 **Target**（目標）頁籤中，選取地區總部防火牆並按一下 **OK**（確定）。

STEP 5 | 可針對資料中心的指定主機/伺服器存取 Amazon 雲端應用程式。

1. 針對資料中心內需要存取 Amazon 雲端應用程式的伺服器/主機，建立位址物件。
    1. 選取 **Objects**（物件）> **Addresses**（位址），然後在 **Device Group**（設備群組）下拉式清單中選取 DG_DataCenter。
    2. 按一下 **Add**（新增），並輸入位址群組物件的 **Name**（名稱）。
    3. 選取 **Type**（類型），然後指定 IP 位址和網路遮罩（**IP Netmask**（**IP** 網路遮罩）），IP 位址範圍（**IP Range**（**IP** 範圍）），或 **FQDN**。
    4. 按一下 **OK**（確定）儲存物件。
2. 建立安全規則，允許對 Amazon 雲應用進行存取。
    1. 選取 **Policies**（原則）> **Security**（安全性）> **Pre-Rules**（預先規則），然後在 **Device Group**（設備群組）下拉式清單中選取 DG_DataCenter。
    2. 按一下 **Add**（新增），並輸入安全性原則規則的 **Name**（名稱）。
    3. 選取 **Source**（來源）頁籤，**Add**（新增）資料中心的源區域，並 **Add**（新增）您剛定義的位址物件（源位址）。
    4. 選取 **Destination**（目的地）頁籤並 **Add**（新增）目的地區域。
    5. 選取 **Application**（應用程式）頁籤，按一下 **Add**（新增）並鍵入 **`amazon`**，再從清單中選取 Amazon 應用程式。
    6. 選取 **Action**（動作）頁籤，將 **Action**（動作）設定為 **Allow**（允許）。
    7. 按一下 **OK**（確定）來儲存規則。

STEP 6 | 若要為網路上的所有網際網路繫結流量啟用日誌記錄，請建立用於比對信任區域與不受信任區域的規則。

1. 在 **Policies**（原則）頁籤的 **Device Group**（裝置群組）下拉式清單中選取 **Shared**（共享）。
2. 選取 **Security**（安全性）> **Pre-Rules**（預先規則）原則規則庫。

© 2019 Palo Alto Networks, Inc.

3. 按一下 **Add**（新增），並輸入安全性原則規則的 **Name**（名稱）。
4. 在規則的 **Source**（來源）和 **Destination**（目的地）頁籤中，**Add**（新增）`trust_zone` 作為來源區域，並新增 `untrust_zone` 作為目的地區域。
5. 在 **Action**（動作）頁籤中，將動作設為 **Deny**（拒絕），**Log Setting**（日誌設定）設為 **Log at Session end**（同時連線結束時的日誌），然後按一下 **OK**（確定）。

預覽規則與提交變更

使用案例：使用 Panorama 設定防火牆 中的最後一項工作是檢閱規則，然後將您所做的變更提交至 Panorama、裝置群組和範本。

STEP 1 | 預覽規則。

此預覽能讓您以目視方式評估如何針對特殊的規則庫分層您的規則。

1. 選取 **Policies**（原則）和 **Preview Rules**（預覽規則）。
2. 選取 **Rulebase**（規則庫）、**Device Group**（裝置群組）和 **Device**（裝置）。
3. 完成時關閉預覽對話。

STEP 2 | 提交並推送您的設定變更。

1. 選取 **Commit**（提交）> **Commit and Push**（提交並推送），然後在 Push Scope（推送範圍）中 **Edit Selections**（編輯選擇）。
2. 選取 **Device Groups**（裝置群組），選取您已新增的裝置群組，以及 **Include Device and Network Templates**（包括裝置和網路範本）。
3. 按一下 **Ok**（確定），以儲存您對 Push Scope（推送範圍）所做的變更。
4. **Commit and Push**（提交並推送）您的變更。

STEP 3 | 確認 Panorama 已套用範本和原則設定。

1. 在 Panorama 標頭中，將 **Context**（內容）設為防火牆以存取其網頁介面。
2. 檢閱範本和原則設定，以確保您的變更存在。

管理大規模防火牆部署

Panorama™ 提供多個選項，管理大規模防火牆部署。對於所有管理功能的彙總，Panorama 支援使用處於 Management Only（僅限管理）模式的 M-600 設備管理多至 5,000 個防火牆，或使用處於 Management Only（僅限管理）模式的 Panorama 虛擬設備管理多至 2,500 個防火牆。要簡化超過 5000 道防火牆的大規模防火牆部署和操作管理，Panorama Interconnect 外掛程式允許您從單 Panorama 控制器管理多個 Panorama 管理伺服器節點。

> 確定最佳大規模防火牆部署解決方案
> 為 M-600 和 Panorama 虛擬設備增加設備管理容量
> Panorama Interconnect

確定最佳大規模防火牆部署解決方案

為減輕大規模防火牆部署組態管理的操作負擔，Palo Alto Networks 會提供最適合您的部署案例的不同防火牆管理選項。

如果您的大規模防火牆部署由一個，或極少量的 Panorama 管理伺服器組成，您可以部署一台 M-600 設備，以管理多至 5000 個防火牆，或部署 Panorama 虛擬設備，以利用所有 Panorama 能力，從單個 Panorama 管理伺服器管理多至 2,500 個防火牆。為 M-600 和 Panorama 虛擬設備增加設備管理容量 是縱向調整部署的理想方案，您可以從單個 Panorama 管理伺服器管理大量防火牆，而不是部署多個 Panorama 管理伺服器以管理少量防火牆。

如果您的大規模防火牆部署由多個具有類似組態的 Panorama 管理伺服器組成，Panorama Interconnect 外掛程式將允許您從單個 Panorama 控制器管理多個 Panorama 節點。此外掛程式可簡化大規模防火牆部署的部署與作業管理，因為您可以透過 Panorama 控制器來集中管理原則和設定。從 Panorama 控制器，裝置群組和範本堆疊設定被同步至 Panorama 節點並推送至受管理的裝置。Panorama Interconnect 外掛程式是水平擴展防火牆部署的理想程式，並帶有多個散佈的 Panorama 管理伺服器。

© 2019 Palo Alto Networks, Inc.

為 M-600 和 Panorama 虛擬設備增加設備管理容量

處於 Management Only（僅限管理）模式的 M-600 設備可管理多至 5,000 個防火牆，處於 Management Only（僅限管理）模式的 Panorama 虛擬設備可管理多至 2,500 個防火牆，以降低大規模防火牆部署的管理使用量。

- 增加的設備管理容量需求
- 為增加的設備管理部署 Panorama

增加的設備管理容量需求

您可以使用處於 Management Only（僅限管理）模式的單一 M-600 設備管理多至 5,000 個防火牆，或使用處於 Management Only（僅限管理）模式的單一 Panorama 虛擬設備管理多至 2,500 個防火牆。從單一 Panorama 管理伺服器管理此類大型部署降低了組態管理的操作複雜性，並減少了管理多個 Panorama 管理伺服器的安全和合規性風險。

對於日誌收集，單一 Panorama 管理伺服器是最理想的解決方案，因為其提供了集中式位置，以檢視及和分析受管理裝置的日誌資料，而不要求您存取每個個別的 Panorama 管理伺服器。為了提供備援以防系統或網路失效，Palo Alto Networks 推薦在高可用性 (HA) 設定中部署兩個 Panorama™ 管理伺服器。

要產生預先定義的報告，您必須啟用 Panorama 以將 Panorama 資料用於預定義報告。其透過使用 Panorama 或專用日誌收集器收集的日誌資料產生預先定義的報告，減少產生報告時的資源使用率。務必啟用此設定，否則 Panorama 效能可能受到影響，且 Panorama 變得無回應。

要管理多至 5000 道防火牆，Panorama 管理伺服器必須滿足以下最低需求：

需求	M-Series 設備	Panorama 虛擬設備
Model	M-600	所有支援的 Panorama Hypervisor。如需詳細資訊，請參閱Panorama 型號。
Panorama 模式	僅限管理	僅限管理
受管理防火牆數目	5,000	2,500
系統磁碟	240GB SSD—用於儲存作業系統檔案和系統日誌。	• 81GB—用於儲存作業系統檔案和系統日誌。 • 至少 90GB 的額外磁碟容量。
核心	28（含超執行緒）	28（含超執行緒）
記憶體	256GB	250GB
日誌收集	不支援本機日誌收集。 參閱 部署具備專用日誌收集器的 Panorama 設置日誌收集。	不支援本機日誌收集。 參閱 部署具備專用日誌收集器的 Panorama 設置日誌收集。
記錄日誌與報告	啟用 **Use Panorama Data for Pre-Defined Reports**（使用預定義報告的	啟用 **Use Panorama Data for Pre-Defined Reports**（使用預定義報告的

© 2019 Palo Alto Networks, Inc.

需求	M-Series 設備	Panorama 虛擬設備
	Panorama 資料）設定（**Panorama** > **Setup**（設定）> **Management**（管理）> **Logging and Reporting Settings**（記錄日誌與報告設定）> **Log Export and Reporting**（日誌匯出與報告））	**Panorama** 資料）設定（**Panorama** > **Setup**（設定）> **Management**（管理）> **Logging and Reporting Settings**（記錄日誌與報告設定）> **Log Export and Reporting**（日誌匯出與報告））

為增加的設備管理部署 Panorama

若要為增加的裝置管理部署 Panorama，請確定您的部署案例並遵循下列程序：

- 為增加的設備管理容量安裝 Panorama
- 為增加的設備管理容量升級 Panorama

為增加的設備管理容量安裝 *Panorama*

啟動裝置管理授權以從單一 M-600 Panorama™ 管理伺服器或單一 Panorama 虛擬設備管理超過 1,000 個防火牆。

STEP 1 | 聯絡您的 Palo Alto Networks 銷售代表以獲得 Panorama 裝置管理授權，讓您可以管理多至 5000 道防火牆。

- 如果您在部署 M-600 裝置，獲得 `PAN-M-600-P-1K` 裝置管理授權。
- 如果您在部署 Panorama 虛擬裝置，請獲取 `PAN-PRA-1000` 裝置管理授權。

STEP 2 | 設定 Panorama 管理伺服器。

- （僅限 M-600 設備）設定 M-Series 設備。

或

- 設定 Panorama 虛擬設備。

STEP 3 | 變更 Panorama 管理伺服器至 Management Only（僅限管理）模式（如果 Panorama 未處於此模式下）。

- 從第 5 步開始 在僅管理模式下設定 M-Series 設備。
- 在僅管理模式下設定 Panorama 虛擬設備。

STEP 4 | 註冊您的 Panorama 管理伺服器並安裝授權。

1. 註冊 Panorama。
2. 啟動 Panorama 支援授權。
3. 啟用 Panorama 管理伺服器上的裝置管理授權。
   - 在 M-Series 設備上啟動/擷取防火牆管理授權。
   - 在 Panorama 虛擬設備並未與網際網路連線時，啟動/擷取防火牆管理授權。
   - 在 Panorama 虛擬設備與網際網路連線時，啟動/擷取防火牆管理授權。

STEP 5 | 選取 **Panorama** > **Licenses**（授權），確認已成功啟動裝置管理授權。

© 2019 Palo Alto Networks, Inc.

Device Management License	
Date Issued	January 22, 2020
Date Expires	Never
Description	Device management license to manage up to 1000 devices

如果您在 *Panorama* 上啟動新裝置管理授權，您可以用 *M-600* 設備管理多至 *5,000* 個防火牆，或用 *Panorama* 虛擬設備管理多至 *2,500* 個防火牆，但說明仍然顯示 `Device management license to manage up to 1000 devices or more`（裝置管理授權管理多至 `1000` 部裝置或更多）。

為增加的設備管理容量升級 *Panorama*

升級至 PAN-OS 9.1 或更高版本，以使用 M-600 設備上現有的裝置管理授權，管理多至 5,000 個防火牆，或使用 Panorama™ 虛擬設備管理多至 2,500 個防火牆。

STEP 1 | 如果 Panorama 虛擬設備已無法滿足所增加裝置管理的最低資源需求，在 Panorama 虛擬設備上增加 CPU 和記憶體。

請檢閱 增加的設備管理容量需求 以在升級前確認您現有的 Panorama 虛擬設備是否滿足最低資源需求。

STEP 2 | 登入 Panorama CLI。

STEP 3 | 變更 Panorama 管理伺服器至 Management Only（僅限管理）模式（如果 Panorama 未處於此模式下）。

- （僅適用於 M-600 設備）從步驟 5 開始以 在僅管理模式下設定 M-Series 設備。

或

- 在僅管理模式下設定 Panorama 虛擬設備。

STEP 4 | 登入 Panorama 網頁介面。

STEP 5 | 升級 Panorama 管理伺服器。

- 為有網際網路連線的 Panorama 安裝更新。
- 為沒有連線至網際網路的 Panorama 安裝更新。
- 在 HA 組態中為 Panorama 安裝更新。

STEP 6 | 選取 **Panorama** > **Licenses**（授權），確認已成功啟動裝置管理授權。

Device Management License	
Date Issued	January 22, 2020
Date Expires	Never
Description	Device management license to manage up to 1000 devices

如果您已啟動您的裝置管理授權并接著升級至 *PAN-OS 9.1* 或更高版本，您可以用 *M-600* 設備管理多至 *5,000* 個防火牆，或用 *Panorama* 虛擬設備管理多至 *2,500* 個防火牆，但說明仍然顯示 `Device management license to manage up to 1000 devices or more`（裝置管理授權管理多至 `1000` 部裝置或更多）。

© 2019 Palo Alto Networks, Inc.

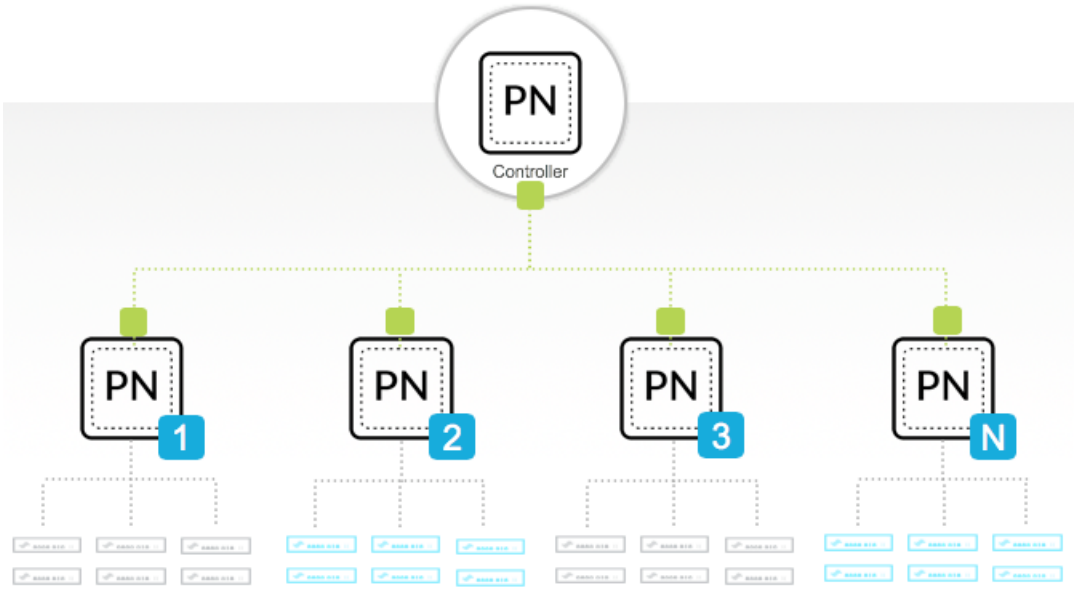
Panorama Interconnect

使用 Panorama™ Interconnect 管理您的大規模防火牆部署設定。當管理多個具有類似設定的 Panorama 管理伺服器設定時，Panorama Interconnect 是理想的解決方案。

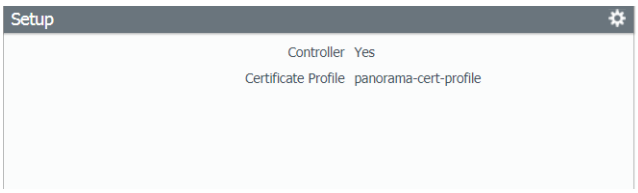
- Panorama Interconnect 概要
- Panorama Interconnect 需求
- 啟用 Panorama 控制器與節點間驗證
- 設定 Panorama Interconnect 外掛程式
- 同步 Panorama Interconnect
- 管理 Panorama Interconnect 的防火牆
- 升級 Panorama Interconnect 外掛程式

Panorama Interconnect 概要

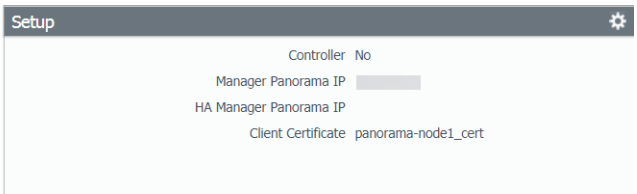
若大量防火牆具有同質設定，超出單一 Panorama 實例的管理容量，或者部署了多個 Panorama™ 管理伺服器，您可以使用 Panorama 上的 Interconnect 外掛程式來降低作業負擔。透過 Interconnect 外掛程式，您可以設定 Panorama 控制器管理多達 64 個 Panorama 節點，從而精簡 Panorama 設備與網路上的受管理防火牆間的通用組態和原則。例如，您可將 Panorama 控制器設定為中心點，管理 Panorama 的具體設定，例如 Panorama 節點上的管理員角色，以及所有您推送至 Panorama 節點用於管理所有防火牆的通用範本堆疊和裝置群組設定。下圖顯示了 Panorama Interconnect 階層，其中 Panorama 控制器管理多個 Panorama 節點，這些節點相應地管理多個裝置。



下圖顯示了成功設定 Panorama 控制器和 Panorama 節點後，其在 Panorama Interconnect 上的 **Setup**（設定）頁面範例。



Panorama Controller



Panorama Node

© 2019 Palo Alto Networks, Inc.

必須完成下列工作，才能設定 Panorama Interconnect 外掛程式：

工作	詳細資訊
檢閱 Panorama Interconnect 需求	Panorama 管理伺服器和防火牆必須滿足系統和作業需求，以便成功部署 Panorama Interconnect。 這包括安裝和啟動授權，以及註冊 Panorama 管理伺服器。
啟用 Panorama 控制器與節點間驗證	產生或匯入一個憑證授權單位並簽發節點憑證，以及設定憑證設定檔，從而保障 Panorama 控制器與 Panorama 節點間的安全通訊。
設定 Panorama Interconnect 外掛程式	在 Panorama 控制器和 Panorama 節點上下載、安裝和設定 Panorama Interconnect 外掛程式。
準備 Panorama 控制器，以推送設定至受管理防火牆	在 Panorama 控制器上，新增裝置群組 並 設定範本堆疊 來設定原則規則、物件和設定，從而使防火牆能夠在網路上運作。
同步 Panorama Interconnect	將 Panorama 特定設定以及範本堆疊和裝置群組設定，從 Panorama 控制器推送至 Panorama 節點。
管理 Panorama Interconnect 的防火牆	新增一個或多個防火牆，並將同步設定從 Panorama 節點推送至受管理裝置。

Panorama Interconnect 需求

規劃並檢閱在 Panorama 管理伺服器上成功部署 Panorama™ Interconnect 外掛程式的需求：

- 規劃 Panorama Interconnect 部署
- Panorama Interconnect 系統需求
- Panorama Interconnect 憑證需求

規劃 *Panorama Interconnect* 部署

若要在 Panorama 管理伺服器上成功部署 Panorama™ Interconnect 外掛程式：

- ❑ 檢閱 Panorama Interconnect 系統需求。

  確認您的 Panoramas 和受管理防火牆滿足最低資源需求且您的防火牆是單 vsys 防火牆。
- ❑ 為您的 Panorama 節點和受管理防火牆計劃裝置群組和範本堆疊設定。

  設定管理集中在 Panorama 控制器上，並複製到 Panorama 控制器管理的所有 Panorama 節點中。確保此設定簡單、緊湊，且在所有 Panorama 節點上基本相同。

  Interconnect 支援基於裝置群組和範本的集中設定，其中包括物件、原則、防火牆和網路設定。Interconnect 部署中不支援 Panorama 整合外掛程式（如 NSX、SD-WAN 和 Prisma Access）新增的增量功能。

  Panorama 節點設定只能從 *Panorama* 控制器進行管理。當將 Panorama 節點與 Panorama 控制器同步時，在 *Panorama* 節點上所做的設定變更將被覆寫。
- ❑ 將 Panorama 控制器和 Panorama 節點設定為僅管理模式。請參閱 在僅管理模式下設定 M-Series 設備 或 在僅管理模式下設定 Panorama 虛擬設備 瞭解有關變更 Panorama 管理伺服器模式詳細資訊。

© 2019 Palo Alto Networks, Inc.

以 *Panorama* 模式及本機日誌收集模式在 *Panorama* 控制器或 *Panorama* 節點上部署 *Panorama Interconnect*，可能由於管理程序和日誌收集程序需要大量資源而導致效能降低。

- 註冊 Panorama 與安裝授權 Panorama 控制器和 Panorama 節點。
- 部署一個或多個專用的日誌收集器用於日誌收集。請參閱 設定 Panorama 瞭解有關以日誌收集模式部署 Panorama 管理伺服器的日誌儲存空間需求和程序的詳細資訊。

  僅能從 Panorama 節點產生日誌和報告。
- 確定 Panorama 控制器和所有 Panorama 節點均處於作業模式再安裝外掛程式。Panorama Interconnect 外掛程式不支援 FIPS 模式的 Panorama 管理伺服器，且可能導致 Panorama 管理伺服器無法回應。
- 取得憑證授權單位 (Ca)，並產生由 Panorama 控制器 CA 簽署的 Panorama 節點憑證，以保障 Panorama 控制器與 Panorama 節點間安全通訊。如需詳細資訊，請參閱 啟用 Panorama 控制器與節點間驗證。
- 啟用 Panorama 控制器、Panorama 節點和受管理防火牆上的 HTTPS 存取權，從而能夠登入 Panorama 網頁介面 和防火牆 Web 介面。Panorama Interconnect 不支援存取 CLI 和 API。

Panorama Interconnect 系統需求

確定 Panorama™ 管理伺服器和防火牆滿足下列系統需求，以便成功安裝 Panorama Interconnect 外掛程式，並管理您的大規模防火牆部署：

- Panorama Interconnect 僅可管理單 VSYS 防火牆

需求	Panorama 控制器和節點	防火牆
模式	僅管理（建議）	不適用
CPU 和記憶體	16 個 CPU 和 32GB 記憶體	不適用
系統磁碟	81GB	不適用
支援的作業系統	PAN-OS 8.1.3 或更新版本	PAN-OS 7.1 或更新版本
支援的機型	• **M-Series** 設備—M-600 • **Panorama** 虛擬設備—請參閱 Panorama 型號 瞭解所有支援的 Panorama 虛擬設備機型。	• 物理防火牆—請參閱防火牆機型 瞭解所有支援的物理防火牆機型。 • **VM-Series** 防火牆—請參閱 VM-Series 機型 瞭解所有支援的 VM-Series 防火牆。

Panorama Interconnect 憑證需求

若要保障 Panorama™ 控制器與 Panorama 節點間的安全通訊，確保您使用的憑證符合下列需求：

- Panorama 控制器需要有負責簽發 Panorama 節點憑證的憑證授權單位 (CA)。您可以建立自我簽署根 CA 憑證或匯入憑證與私密金鑰以簽署憑證。請注意，您必須在 **Panorama** 標籤中設定 CA 憑證，以便設定 Interconnect 外掛程式。
- 為每個 Panorama 節點匯入一個憑證或產生唯一的憑證，Panorama 控制器上的 CA 憑證必須簽發您在節點上使用的憑證。
  - 如果您匯入一個憑證至 Panorama 節點，請確保憑證 **Common Name**（通用名稱）為 Panorama 節點的序號。
  - 憑證必須為 PKCS12 或 PEM 格式，且必須包含私密金鑰，以便 Panorama 節點能夠成功驗證。

© 2019 Palo Alto Networks, Inc.

啟用 Panorama 控制器與節點間驗證

建立用於保障 Panorama 控制器與 Panorama 節點間安全通訊的憑證設定檔。

- 取得 Panorama 控制器的 CA 憑證
- 產生 Panorama 節點憑證
- 建立驗證 Panorama 節點的憑證設定檔

取得 *Panorama* 控制器的 *CA* 憑證

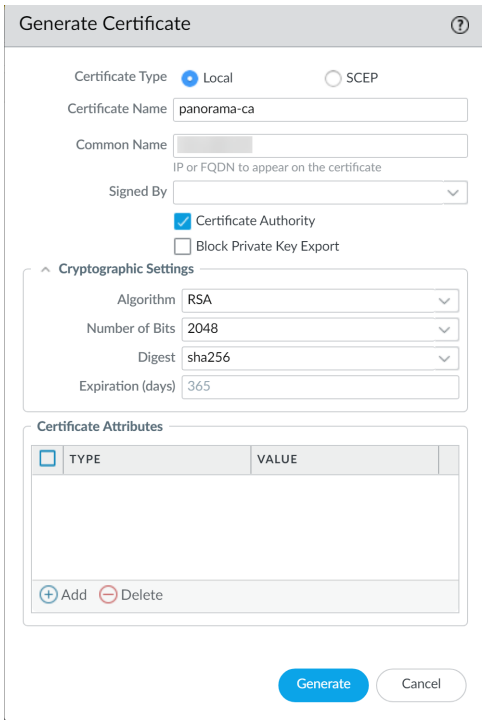
建立受信任的憑證授權單位 (CA)，負責簽發憑證給 Panorama™ 節點，以保障與網際網路間的安全連線。針對大規模防火牆部署設定 Panorama 時需要受信任的 CA。

STEP 1 | 登入 Panorama 網頁介面Panorama 控制器。

STEP 2 | 建立憑證授權單位憑證。

- 產生新的 **CA** 憑證

1. 選取 **Panorama** > **Certificate Management**（憑證管理）> **Certificates**（憑證），然後 **Generate**（產生）新的憑證。
2. 對於 **Certificate Type**（憑證類似），選取 **Local**（本機）。
3. 輸入 **Certificate Name**（憑證名稱），例如 **`panorama-CA`**。名稱區分大小寫，最長可達 31 個字元。名稱必須是唯一的，且只能使用字母、數字、連字號與底線。
4. 在 **Common Name**（通用名稱）欄位中，輸入 Panorama 控制器的 IP 位址或 FQDN。
5. 將**Signed By**（簽署者）欄位保留空白，以指定憑證為自我簽署。
6. 選取 **Certificate Authority**（憑證授權單位）核取方塊。
7. **Generate**（產生）CA 憑證。

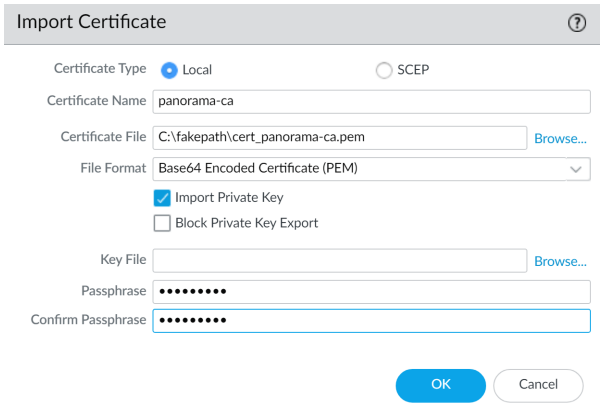


- 匯入現有 **CA** 憑證

1. 選取 **Panorama** > **Certificate Management**（憑證管理）> **Certificates**（憑證），然後 **Import**（匯入）CA 憑證。

© 2019 Palo Alto Networks, Inc.

2. 輸入 **Certificate Name**（憑證名稱），例如 **panorama-CA**。名稱區分大小寫，最長可達 31 個字元。名稱必須是唯一的，且只能使用字母、數字、連字號與底線。
3. **Browse**（瀏覽）以尋找 **Certificate File**（憑證檔案）。
4. 選取 **File Format**（檔案格式）：
   - **Base64 編碼憑證 (PEM)**—您必須將金鑰與憑證分開匯入。核取 **Import Private Key**（匯入私密金鑰）核取方塊，然後 **Browse**（瀏覽） **Key File**（金鑰檔案）。
   - **加密的私密金鑰與憑證 (PKCS12)**—常見格式，其中的金鑰與憑證是在單一容器內（**Certificate File**（憑證檔案））。
5. 輸入用於加密金鑰的 **Passphrase**（複雜密碼），並重新輸入進行確認。
6. 按一下 **OK**（確定）。憑證頁面即會顯示匯入的 CA 憑證。



STEP 3 | 按一下 **Commit**（提交）和 **Commit to Panorama**（提交至 **Panorama**）。

產生 *Panorama* 節點憑證

如需 Panorama™ 控制器驗證每個 Panorama 節點，則為每個 Panorama 節點建立唯一的憑證。Panorama 控制器和節點使用基於憑證的驗證，確保其相互之間安全通訊。產生唯一的 Panorama 節點憑證之前，取得 Panorama 控制器的 CA 憑證。

如果您的 Panorama 節點在高可用性 (HA) 組態中，您必須建立及匯入這兩個 Panorama 節點的 Panorama 節點憑證至 HA 組態中的每個 HA 對等。

STEP 1 | 登入 Panorama 網頁介面Panorama 控制器。

STEP 2 | 選取 **Panorama** > **Certificate Management**（憑證管理） > **Certificates**（憑證），然後 **Generate**（產生）新的憑證：

1. 對於 **Certificate Type**（憑證類似），選取 **Local**（本機）。

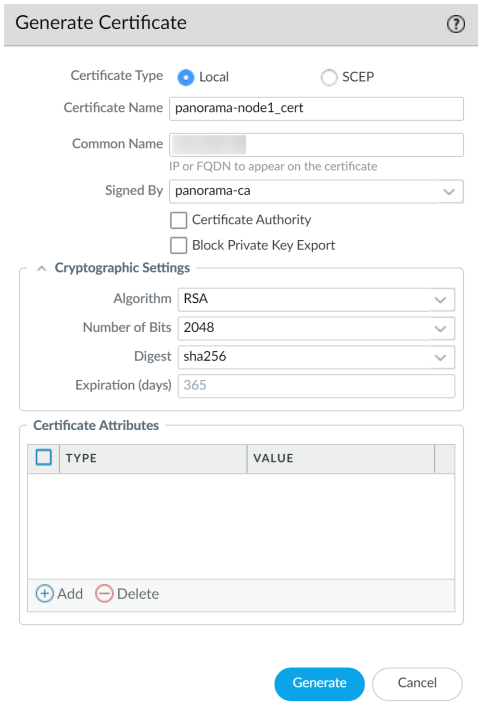
   SCEP 目前不受支援。

2. 輸入 **Certificate Name**（憑證名稱），例如 **panorama-node1_cert**。名稱區分大小寫，最長可達 31 個字元。名稱必須是唯一的，且只能使用字母、數字、連字號與底線。
3. 在 **Common Name**（通用名稱）欄位，輸入 Panorama 節點的序號。

   必須在 *Common Name*（通用名稱）欄位輸入序號，以便驗證 *Panorama* 控制器與 *Panorama* 節點間的連線。若未在此欄位輸入序號，*Panorama* 節點則無法連線至 *Panorama* 控制器。

4. 在 **Signed By**（簽署者）欄位中，選取 CA 憑證。
5. 產生憑證。

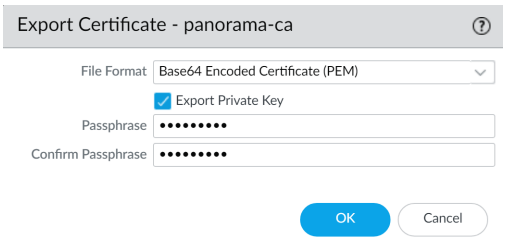
© 2019 Palo Alto Networks, Inc.



STEP 3 | 按一下 **Commit**（提交）和 **Commit to Panorama**（提交至 **Panorama**）。

STEP 4 | 匯出每個 Panorama 節點在步驟 2 中產生的憑證。

1. 選取 **Panorama** > **Certificate Management**（憑證管理）> **Certificates**（憑證），然後選取憑證並 **Export Certificate**（匯出憑證）。
2. 選取 **File Format**（檔案格式）：
   - **Base64 Encoded Certificate (PEM)**（**Base64** 編碼憑證 **(PEM)**）—允許您分別匯出憑證及私密金鑰。若您希望匯出的檔案包含私密金鑰，請選取 **Export Private Key**（匯出私密金鑰）核取方塊。
   - **Encrypted Private Key and Certificate (PKCS12)**（加密的私密金鑰與憑證 **(PKCS12)**）—在單一檔案中匯出憑證與私密金鑰。
3. 核取 **Export private key**（匯出私密金鑰）方塊。
4. 輸入 **Passphrase**（複雜密碼）和 **Confirm Passphrase**（確認複雜密碼），以對私密金鑰加密。匯入憑證金鑰至 Panorama 節點時需要此複雜密碼。
5. 按一下 **OK**（確定）並將憑證/金鑰檔案儲存至您的本機電腦。



6. 輸入憑證的描述性檔案名稱，以便您輕鬆識別需要匯入的 Panorama 節點，然後 **Save**（儲存）憑證。

STEP 5 | 匯入憑證至每個 Panorama 節點。

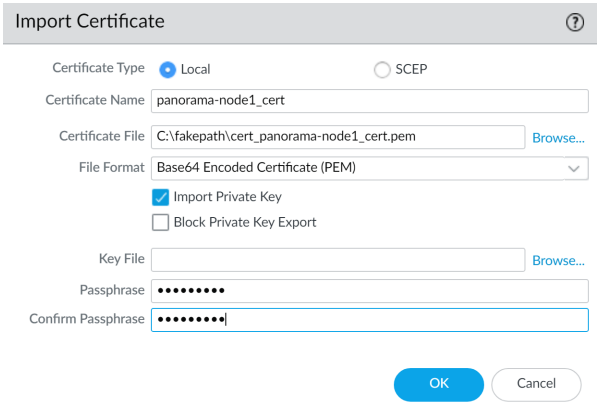
1. 登入 Panorama 網頁介面 Panorama 節點。
2. 選取 **Panorama** > **Certificate Management**（憑證管理）> **Certificates**（憑證），然後 **Import**（匯入）憑證：

© 2019 Palo Alto Networks, Inc.

1. 對於 **Certificate Type**（憑證類似），選取 **Local**（本機）。

   SCEP 目前不受支援。

2. 輸入相同的 **Certificate Name**（憑證名稱）。名稱區分大小寫，最長可達 31 個字元。名稱必須是唯一的，且只能使用字母、數字、連字號與底線。
3. **Browse**（瀏覽）您在步驟 4 中匯出的憑證。
4. 核取 **Import private key**（匯入私密金鑰）方塊。
5. 輸入用於對私密金鑰加密的 **Passphrase**（複雜密碼）和 **Confirm Passphrase**（確認複雜密碼）。
6. 按一下確定匯入憑證。



3. 按一下 **Commit**（提交）和 **Commit to Panorama**（提交至 **Panorama**）。

建立驗證 *Panorama* 節點的憑證設定檔

憑證設定檔定義要使用哪些憑證授權單位 (CA) 憑證，以確認用於保障 Panorama™ 控制器與 Panorama 節點之間安全通訊，及確認 Panorama 節點撤銷狀態。需要憑證設定檔，以設定適用於大規模防火牆部署的 Panorama。

STEP 1 | 登入 Panorama 網頁介面Panorama 控制器。

STEP 2 | 取得 Panorama 控制器的 CA 憑證。

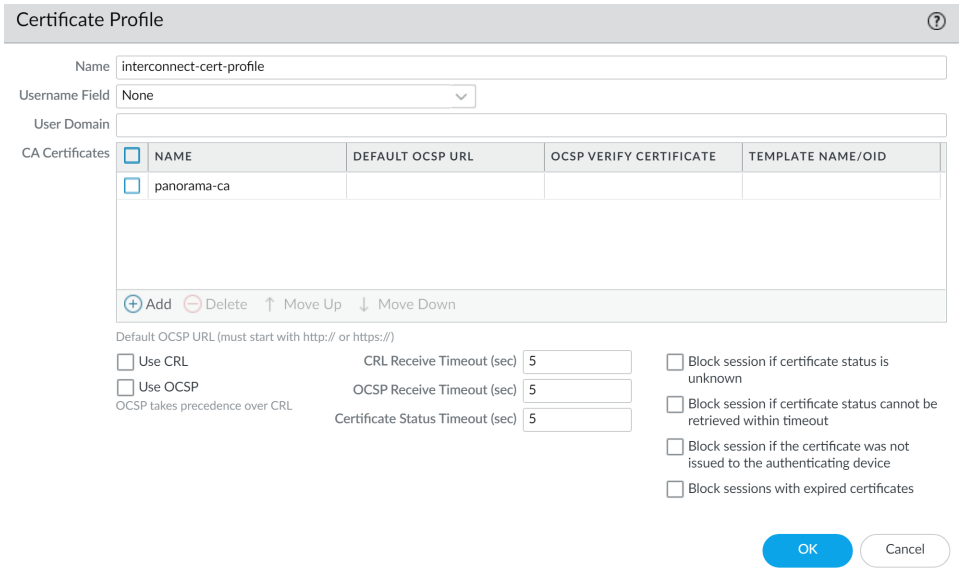
STEP 3 | 產生 Panorama 節點憑證 用於保障 Panorama 控制器與 Panorama 節點間的安全通訊。針對所有 Panorama 節點重複此步驟。

STEP 4 | 建立憑證設定檔。

CRL 和 *OCSP* 目前不受支援。

1. 選取 **Panorama** > **Certificate Management**（憑證管理）> **Certificate Profile**（憑證設定檔），然後 **Add**（新增）新的憑證設定檔。
2. 輸入憑證設定檔的 **Name**（名稱）。
3. **Add**（新增）步驟 2 中建立的 CA 憑證。
4. 按一下 **OK**（確定）來完成憑證設定檔新增。

© 2019 Palo Alto Networks, Inc.



STEP 5 | 按一下 **Commit**（提交）和 **Commit to Panorama**（提交至 **Panorama**）。

設定 Panorama Interconnect 外掛程式

使用 Panorama™ Interconnect 集中管理範本堆疊和裝置群組，以將複寫設定從 Panorama 控制器推送至 Panorama 節點，從而確保防火牆組態和安全性原則的一致性。Panorama Interconnect 可讓您建立 Panorama 控制器來管理 Panorama 節點，並透過節點來管理防火牆和推送設定。這讓您在一處即可管理大規模防火牆部署的設定，減少設定多個 Panorama 管理伺服器所需的時間，以及減少因設定錯誤導致的安全性弱點。在 Panorama 管理伺服器上設定 Panorama Interconnect 外掛程式之前，請檢閱 Panorama Interconnect 需求。

如果您的 Panorama 節點在高可用性 (HA) 組態中，您必須在這兩個 Panorama HA 對等上設定 Panorama Interconnect 外掛程式。

STEP 1 | 安裝 Panorama Interconnect 外掛程式。您必須在 Panorama 控制器和所有 Panorama 節點上安裝外掛程式。

1. 登入 Panorama 網頁介面。
2. 選取 **Panorama** > **Plugins**（外掛程式），然後搜尋 `Interconnect`。
3. **Download**（下載）並 **Install**（安裝）Panorama Interconnect 外掛程式。
4. 按一下 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），以完成 Panorama Interconnect 外掛程式安裝。

STEP 2 | 啟用 Panorama 控制器與節點間驗證 保障 Panorama 控制器與 Panorama 節點間的安全驗證。

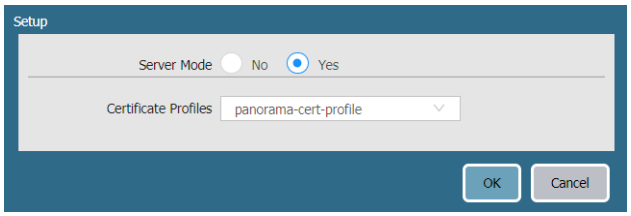
STEP 3 | 在 Panorama 控制器上設定外掛程式。若 Panorama 控制器為 HA 設定，則對高可用性對等重複此步驟。

> *Panorama* 設定為 *Panorama* 控制器後，無法再將 *Panorama* 控制器重新設定為 *Panorama* 模式。確定已將正確的 *Panorama* 管理伺服器設定為 *Panorama* 控制器後再繼續。

1. 選取 **Panorama** > **Interconnect** > **Setup**（設定），然後編輯 **Interconnect Plugin Setup**（**Interconnect** 外掛程式設定）：
2. 在 **Server Mode**（伺服器模式）欄位中，選取 **Yes**（是）。

© 2019 Palo Alto Networks, Inc.

3. 選取在步驟 2 中建立的 **Certificate Profile**（憑證設定檔）。
4. 按一下 **OK**（確定）以儲存設定。

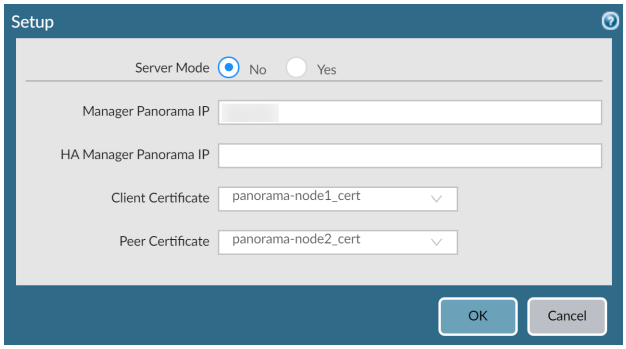


5. 按一下 **Commit**（提交）和 **Commit to Panorama**（提交至 **Panorama**）。

STEP 4 | 在 Panorama 節點上設定外掛程式。針對所有 Panorama 節點重複此步驟。

如果您的 *Panorama* 節點在高可用性 *(HA)* 組態中，在每個 *Panorama HA* 對等上設定 *Panorama Interconnect* 外掛程式時，您必須選取已匯入至每個 *Panorama* 節點 *HA* 對等上的 *Panorama* 節點憑證。

1. 選取 **Panorama** > **Interconnect** > **Setup**（設定），然後編輯 **Interconnect Plugin Setup**（**Interconnect** 外掛程式設定）：
   1. 在 **Server Mode**（伺服器模式）欄位中，選取 **No**（否）。
   2. **Manager Panorama IP**（管理 **Panorama Ip**）—輸入—輸入 Panorama 控制器的 IP 位址。
   3. **HA Manager IP**（**HA** 管理 **IP**）—若 Panorama 控制器為高可用性設定，則輸入 HA Panorama 控制器對等的 IP 位址。
   4. 選取您在步驟 2 中匯入的 Panorama 節點憑證。
   5. （僅限 HA）選取您在步驟 2 中匯入的對等 Panorama 節點憑證。
2. 按一下 **OK**（確定）以儲存設定。



3. 按一下 **Commit**（提交）和 **Commit to Panorama**（提交至 **Panorama**）以完成在 Panorama 節點上設定外掛程式。

STEP 5 | 新增 Panorama 節點至 Panorama 控制器。

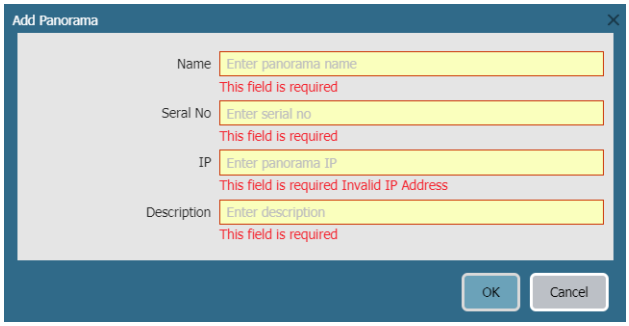
1. 選取 **Panorama** > **Interconnect** > **Panorama Nodes**（**Panorama** 節點），然後 **Add**（新增）Panorama 節點。
   1. 為 Panorama 節點輸入 **Name**（名稱）。這不需要與 Panorama 管理伺服器上設定的裝置名稱相符。

      Panorama Node Name（名稱）不支援句點 *(.)*。

   2. 輸入 Panorama 節點的 **Serial No**（序號）。
   3. 輸入 Panorama 節點的 **IP** 位址。Panorama 控制必須能夠存取該 IP 位址。
   4. 為 Panorama 節點輸入 **Description**（描述）。

© 2019 Palo Alto Networks, Inc.

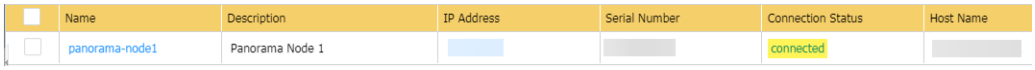
2. 按一下 **OK**（確定）來新增來新增 Panorama 節點。



3. 按一下 **Commit**（提交）和 **Commit to Panorama**（提交至 **Panorama**），以完成 Panorama 節點新增。

STEP 6 | 確認新增的 Panorama 節點為 `Connected`（已連線）。

1. 選取 **Panorama** > **Interconnect** > **Panorama Nodes**（**Panorama** 節點）。
2. 尋找您已新增的 Panorama 節點，確認 Connection Status（連線狀態）欄顯示 `Connected`（已連線）。



STEP 7 | 在 Panorama 控制器和 Panorama 節點上成功安裝外掛程式後，執行後續步驟以完成 Panorama Interconnect 設定：

1. 在 Panorama 控制器上，新增裝置群組。重複此步驟，建立所需裝置群組。
2. 在 Panorama 控制器上，設定範本堆疊。重複此步驟，建立所需範本堆疊。
3. 同步 Panorama Interconnect 將 Panorama 特定設定以及範本堆疊和裝置群組設定，從 Panorama 控制器推送至 Panorama 節點。
4. 在 Panorama 控制器上，新增一個或多個由 Panorama 節點管理的防火牆。
   - 新增防火牆至 Panorama 節點
   - 匯入多個防火牆至 Panorama 節點
5. 推送 Panorama 節點組態至受管理裝置。

同步 Panorama Interconnect

若要從 Panorama 控制器推送 Panorama™ 範本堆疊和裝置群組設定，需要同步 Panorama 節點設定與 Panorama 控制器，從而同步任何 Panorama 特定設定，並使 Panorama 節點將設定推送至受管理防火牆。

- 推送通用 Panorama 組態至 Panorama 節點
- 同步 Panorama 節點與 Panorama 控制器

推送通用 *Panorama* 組態至 *Panorama* 節點

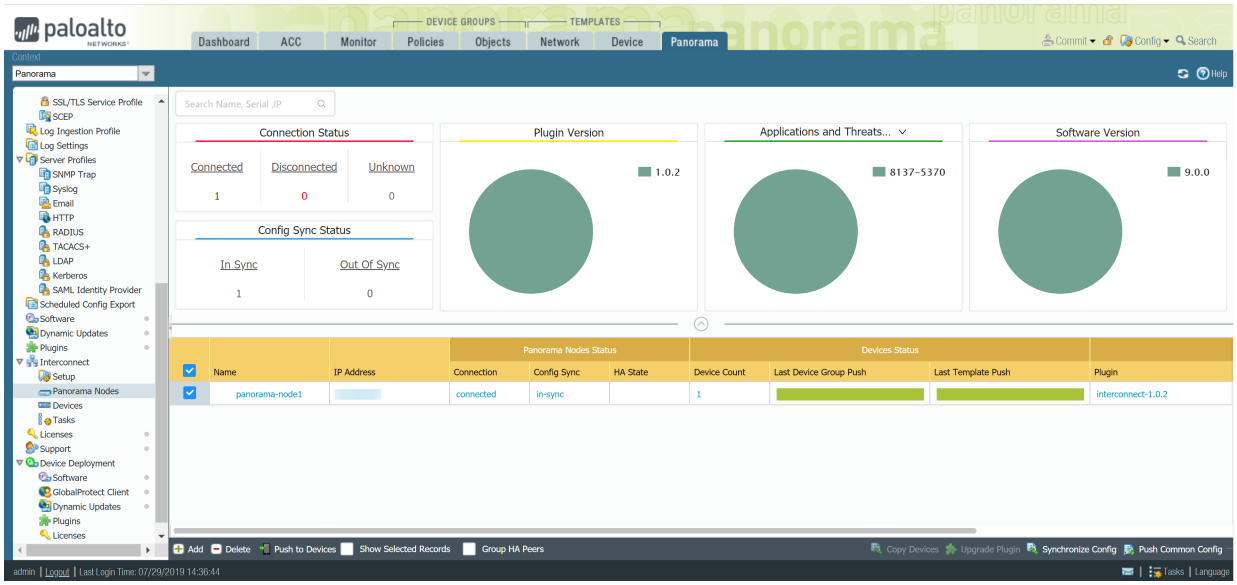
將 Panorama™ 控制器的通用設定推送至 Panorama 節點，以套用任何 Panorama 特定設定至 Panorama 節點。若要同步範本堆疊和裝置群組設定，以將其推送至受管理裝置，請參閱 同步 Panorama 節點與 Panorama 控制器。

STEP 1 | 登入 Panorama 網頁介面Panorama 控制器。

STEP 2 | 選取 **Panorama** > **Interconnect** > **Panorama Nodes**（**Panorama** 節點），然後選取 Panorama 節點，管理推送設定的目標防火牆。

STEP 3 | 選取 **Push Common Config**（推送通用設定），以推送 Panorama 特定設定至 Panorama 節點。

© 2019 Palo Alto Networks, Inc.



同步 *Panorama* 節點與 *Panorama* 控制器

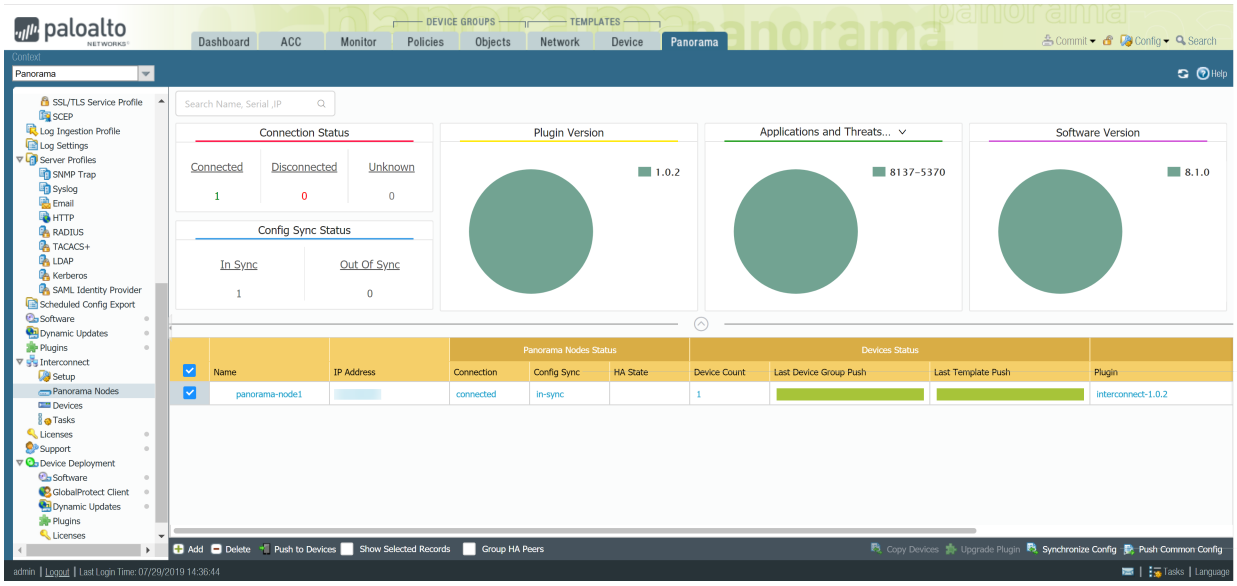
同步 Panorama™ 控制器設定與 Panorama 節點，以便 Panorama 節點可將任何範本堆疊或裝置群組設定推送至受管理裝置。

STEP 1 | 登入 Panorama 網頁介面Panorama 控制器。

STEP 2 | 選取 **Panorama** > **Interconnect** > **Panorama Nodes**（**Panorama** 節點），然後選取 Panorama 節點以同步 Panorama 控制器。

STEP 3 | **Synchronize Config**（同步設定）以將裝置群組和範本堆疊設定推送至 Panorama 節點。推送設定至受管理裝置需要執行此動作。

STEP 4 | 在 Sync Status（同步狀態）欄中，確認 Panorama 節點已 **in-sync**（同步）。



© 2019 Palo Alto Networks, Inc.

管理 Panorama Interconnect 的防火牆

新增單一防火牆或大量匯入由 Panorama™ 節點管理的多個裝置。

- 新增防火牆至 Panorama 節點
- 匯入多個防火牆至 Panorama 節點
- 匯入範本堆疊變數
- 透過 Panorama Interconnect 管理主要金鑰
- 推送 Panorama 節點組態至受管理裝置

新增防火牆至 *Panorama* 節點

新增由 Panorama™ 節點管理的單一防火牆，以便管理中央 Panorama 控制器的範本堆疊和裝置群組組態。若要大量匯入多個防火牆，請參閱 匯入多個防火牆至 Panorama 節點。

STEP 1 | 設定防火牆與 Panorama 節點進行通訊。

1. 在防火牆上執行初始設定，讓防火牆可供存取，並且能透過網路與 Panorama 通訊。
2. 將 Panorama 節點 IP 位址新增至防火牆。
    1. 選取 **Device**（裝置）> **Setup**（設定）> **Management**（管理），再編輯 [Panorama 設定]。
    2. 在第一個欄位中輸入 Panorama IP 位址。
    3. （選用）如果您已在 Panorama 中設定高可用性配對，請在第二個欄位中輸入次要 Panorama 的 IP 位址。
    4. 按一下 **OK**（確定）。
3. 選取 **Commit**（提交）並 **Commit**（提交）您的變更。

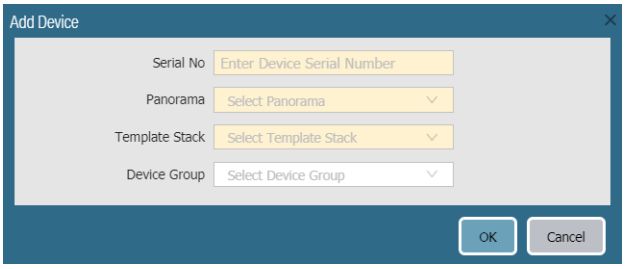
STEP 2 | 登入 Panorama 網頁介面Panorama 控制器。

STEP 3 | 選取 **Panorama** > **Interconnect** > **Devices**（裝置），然後 **Add**（新增）防火牆。

STEP 4 | 輸入防火牆資訊：

- 輸入防火牆的 **Serial No**（序號）。
- 選取 **Panorama** 節點以管理防火牆。
- 選取 **Template Stack**（範本堆疊），用以管理防火牆組態。
- 選取 **Device Group**（裝置群組），用以關聯防火牆。

STEP 5 | 按一下 **Ok**（確定）以新增防火牆作為受管理裝置。



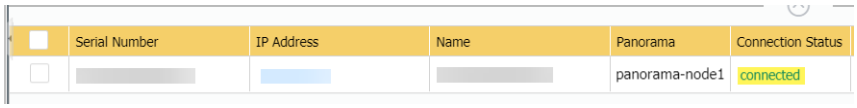
STEP 6 | 按一下 **Commit**（提交）和 **Commit to Panorama**（提交至 **Panorama**），以完成防火牆新增。

STEP 7 | 選取 **Panorama** > **Interconnect** > **Panorama Nodes**（**Panorama** 節點）和 **Synchronize Config**（同步組態）。

STEP 8 | 確認新增的防火牆為 `Connected`（已連線）。

© 2019 Palo Alto Networks, Inc.

1. 選取 **Panorama** > **Interconnect** > **Devices**（裝置）。
2. 尋找您已新增的防火牆，確認 Connection Status（連線狀態）欄顯示 `Connected`（已連線）。



匯入多個防火牆至 *Panorama* 節點

您可以使用匯入程序期間提供的 CSV 範本，匯入多個由 Panorama™ 節點管理的防火牆。同時匯入多個防火牆可讓您快速將多個防火牆新增至 Panorama 節點，並將其指派給範本堆疊和裝置群組，從而集中管理其設定。

匯入多個防火牆後，您可以將防火牆新增至不同的 Panorama 節點、不同的範本堆疊和裝置群組。例如，您已部署 Panorama 節點 A 和 Panorama 節點 B，各自均帶有兩個範本堆疊和兩個裝置樽俎。若您匯入 100 個防火牆，則可用下列方式匯入：

- 新增 50 個防火牆至 Panorama 節點 A：
  - 指派 25 個防火牆至範本堆疊 A1 和裝置群組 A1。
  - 指派 25 個防火牆至範本堆疊 A2 和裝置群組 A2。
- 新增 50 個防火牆至 Panorama 節點 B：
  - 指派 30 個防火牆至範本堆疊 B1 和裝置群組 B1。
  - 指派 20 個防火牆至範本堆疊 B2 和裝置群組 B2。

若要新增單一防火牆，請參閱 新增防火牆至 Panorama 節點。

STEP 1 | 設定防火牆與 Panorama 節點進行通訊。

針對由 Panorama 使用 Interconnect 外掛程式管理的所有防火牆重複此步驟。

1. 在防火牆上執行初始設定，讓防火牆可供存取，並且能透過網路與 Panorama 通訊。
2. 將 Panorama 節點 IP 位址新增至防火牆。
   1. 選取 **Device**（裝置）> **Setup**（設定）> **Management**（管理），再編輯 [Panorama 設定]。
   2. 在第一個欄位中輸入 Panorama IP 位址。
   3. （選用）如果您已在 Panorama 中設定高可用性配對，請在第二個欄位中輸入次要 Panorama 的 IP 位址。
   4. 按一下 **OK**（確定）。
3. 選取 **Commit**（提交）並 **Commit**（提交）您的變更。

STEP 2 | 登入 Panorama 網頁介面Panorama 控制器。

STEP 3 | 按一下 **Commit**（提交）和 **Commit to Panorama**（提交至 **Panorama**）Panorama 控制器的任何擱置設定變更。匯入多個防火牆需要 Panorama 控制器沒有任何擱置變更，否則匯入將失敗。

STEP 4 | 選取 **Panorama** > **Interconnect** > **Devices**（裝置），然後 **Import**（匯入）防火牆。

STEP 5 | 按一下 **Download Sample CSV**（下載樣本 **CSV**），下載正確格式的 CSV 檔案範本，以上傳多個防火牆。

STEP 6 | 填寫下載的 CSV。在 **serial**（序號）、**panorama**、**device-group**（裝置群組）和 **template-stack**（範本堆疊）欄位中輸入對應的值。Panorama 控制器必須已新增和建立 Panorama 節點、裝置群組和範本堆疊，再匯入防火牆，且需要成功新增防火牆。完成防火牆資訊輸入後，**Save**（儲存）該檔案。

© 2019 Palo Alto Networks, Inc.

您還能夠將防火牆指派給內容排程。匯入防火牆則不需要。

變更 *CSV* 欄順序不受支援。如果欄位重新排序，防火牆匯入將會失敗。

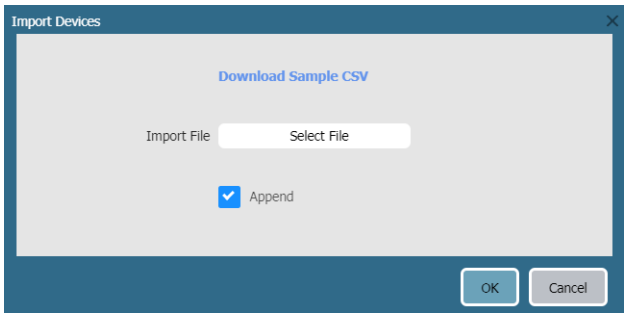
STEP 7 | 返回 Panorama Web 介面，按一下 **Select File**（選取檔案）瀏覽並選取包含防火牆資訊的 CSV 檔案。

防火牆在大量匯入過程中遺失必要資訊將會導致整個匯入失敗。如果遇到錯誤，系統將會提示錯誤訊息，指示匯入檔案出現問題的位置。

STEP 8 | **Append**（附加）新裝置，將其新增至 **Devices**（裝置）清單末尾。所有匯入的裝置必須是新裝置。如果任何正在匯入的裝置是 Panorama 控制器執行中設定的一部分，則匯入將會失敗。

如果您想要刪除清單中的現有裝置，且只新增您現在新增的新裝置，則取消核取 *Append*（附加）方塊。

STEP 9 | 按一下 **Ok**（確定）以新增防火牆作為受管理裝置。

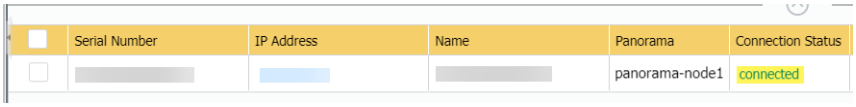


STEP 10 | 按一下 **Commit**（提交）和 **Commit to Panorama**（提交至 **Panorama**），以完成防火牆新增。

STEP 11 | 選取 **Panorama** > **Interconnect** > **Panorama Nodes**（**Panorama** 節點）和 **Synchronize Config**（同步組態）。

STEP 12 | 確認新匯入的防火牆為 `Connected`（已連線）。

1. 選取 **Panorama** > **Interconnect** > **Devices**（裝置）。
2. 尋找您已匯入的防火牆，確認 Connection Status（連線狀態）欄顯示 `Connected`（已連線）。



匯入範本堆疊變數

使用範本堆疊變數來取代 IP 位址、IP 範圍、FQDN、IKE 介面、VPN 和 HA 設定，以及防火牆組態中的群組 ID。變數讓您可以減少需要管理的範本和範本堆疊總數量，同時讓您可以保留任何防火牆特定值。

匯入範本堆疊變數可讓您覆寫多個現有變數的值，但匯入時您不能建立新的範本堆疊變數。如需更多有關如何建立新的範本或範本堆疊變數的資訊，請參閱設定範本或範本堆疊變數。

STEP 1 | 匯入現有範本堆疊變數。

1. 登入 Panorama 網頁介面（Panorama 控制器）。
2. 選取 **Panorama** > **Interconnect** > **Devices**（裝置）和 **Export Variables**（匯出變數）。
3. 從下拉式選單中，選取範本堆疊 **Name**（名稱）。

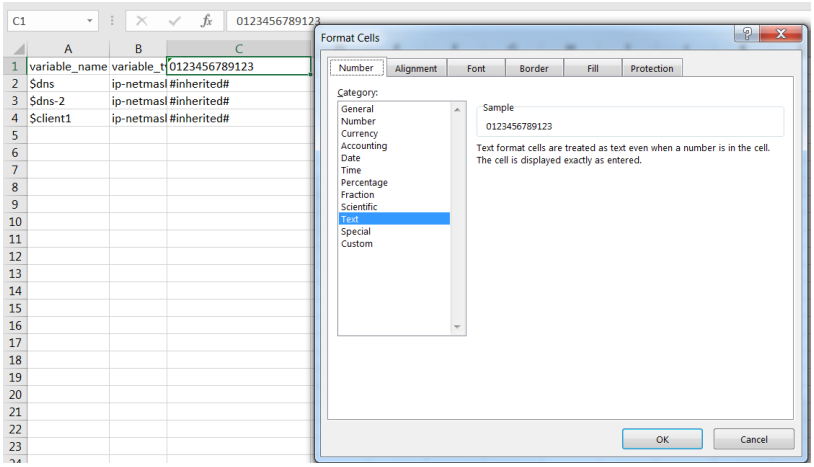
© 2019 Palo Alto Networks, Inc.

4. 按一下 **OK**（確定）並儲存 CSV 檔案。

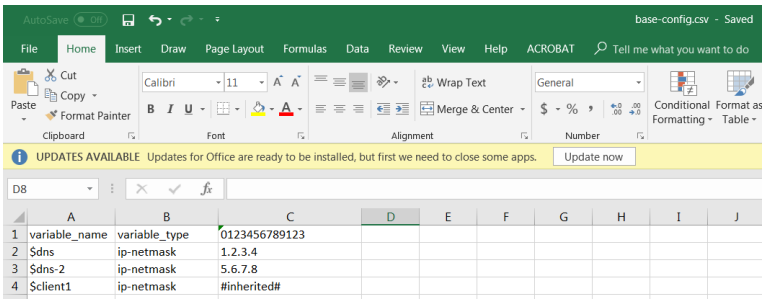
STEP 2 | 編輯包含範本堆疊變數的 CSV 檔案，以下列格式匯入 Panorama Interconnect：

顯示為 `#inherited#` 的值是範本堆疊中定義的值。

1. 更正包含防火牆序號的資料格編號。針對 CSV 檔案中的所有防火牆重複這些步驟。
   1. 在包含防火牆序號的資料格上按一下滑鼠右鍵，然後選取 **Format Cells**（格式資料格。
   2. 選取 **Number**（編號）> **Text**（文字），然後按一下 **OK**（確定）。
   3. 在序號開頭加上 0。

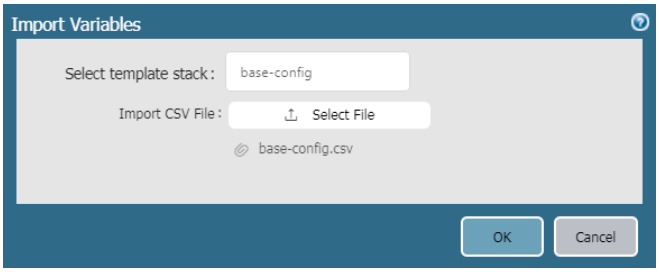


2. 輸入所需範本變數的新值。
3. 選取 **File**（檔案）> **Save As**（另存新檔），然後以 **CSV UTF-8** 格式儲存檔案。



STEP 3 | 匯入 CSV 檔案至範本堆疊。

1. 登入 Panorama 網頁介面（Panorama 控制器）。
2. 選取 **Panorama** > **Interconnect** > **Devices**（裝置）和 **Import Variables**（匯入變數）。
3. 在 **Select template stack**（選取範本堆疊）下拉式清單中，選取要匯入變數的範本堆疊。
4. 在 **Import CSV File**（匯入 **CSV** 檔案）中，按一下 **Select File**（選取檔案），然後選取包含範本堆疊變數的 CSV 檔案。
5. 按一下 **OK**（確定）來匯入範本堆疊變數。



© 2019 Palo Alto Networks, Inc.

6. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

STEP 4 | 同步 Panorama 節點與 Panorama 控制器。

STEP 5 | 推送 Panorama 節點組態至受管理裝置。

透過 *Panorama Interconnect* 管理主要金鑰

Panorama、防火牆、日誌收集器和 WF-500 設備使用主要金鑰加密設定內的敏感元素，並帶有預設主要金鑰用於加密密碼和設定元素。

作為標準安全做法的一部分，當您的主要金鑰過期時，您必須更新各單個防火牆、日誌收集器、WildFire 設備和 Panorama 上的金鑰。您的受管理裝置上部署的，Panorama 控制器、Panorama 節點和受管理裝置的主要金鑰必須一致，以成功推送組態。要確保統一的金鑰部署，從 Panorama 直接向多個防火牆、日誌收集器和 WF-500 設備部署一個新的主要金鑰或更新過期的金鑰。當使用 Panorama Interconnect 時，您必須在單個程序中，為 Panorama 控制器和所有的 Panorama 節點以及受管理的裝置設定和部署相同的主要金鑰。要部署主要金鑰至受管理的設備，您必須在各 Panorama 節點上設定主要金鑰，並將其部署至該節點管理的所有裝置。請參閱 設定主要金鑰 ，獲取更多資訊。

STEP 1 | 設定 Panorama 控制器上的主要金鑰。

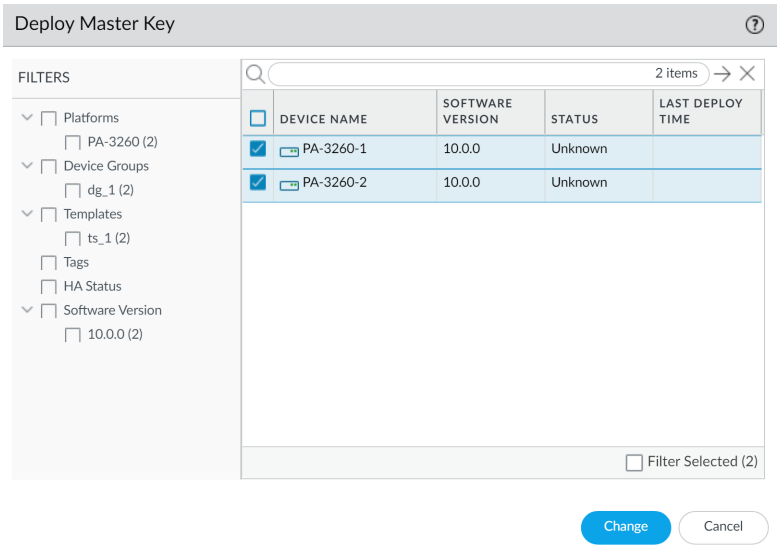
1. 登入 Panorama 網頁介面 在 Panorama 控制器上。
2. 選取 **Panorama** > **Master Key and Diagnostics**（主要金鑰與診斷），然後設定主要金鑰。
    1. 如果要更新主要金鑰，輸入 **Current Master Key**（當前主要金鑰）。如果您透過新的主要金鑰更換預設主要金鑰，不得指定 **Current Master Key**（當前主要金鑰）。
    2. 設定 **New Master Key**（新主要金鑰）並 **Confirm Master Key**（確認主要金鑰）。
    3. 設定主要金鑰 **Lifetime**（生命週期）與 **Time for Reminder**（提醒時間）。
    4. 設定 Panorama 控制器以在金鑰生命週期過期後指定的天數內 **Auto Renew with Same Master Key**（透過相同的主要金鑰自動更新）。
    5. 按一下 **OK**（確定）。
3. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

STEP 2 | 部署主要金鑰至 Panorama 節點管理的裝置。

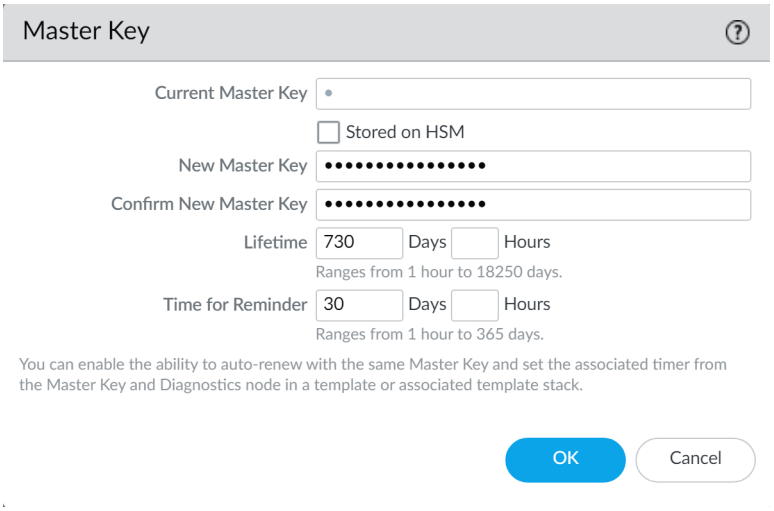
針對所有 Panorama 節點重複此步驟。

1. 登入 Panorama 網頁介面 在 Panorama 節點上。
2. 選取 **Panorama** > **Master Key and Diagnostics**（主要金鑰與中斷）並設定主要金鑰。新的主要金鑰必須與您在第 1 步中，於 Panorama 控制器上設定的金鑰一致
    1. 如果要更新主要金鑰，輸入 **Current Master Key**（當前主要金鑰）。如果您透過新的主要金鑰更換預設主要金鑰，不得指定 **Current Master Key**（當前主要金鑰）。
    2. 設定 **New Master Key**（新主要金鑰）並 **Confirm Master Key**（確認主要金鑰）。
    3. 設定主要金鑰 **Lifetime**（生命週期）與 **Time for Reminder**（提醒時間）。
    4. 設定 Panorama 控制器以在金鑰生命週期過期後指定的天數內 **Auto Renew with Same Master Key**（透過相同的主要金鑰自動更新）。
    5. 按一下 **OK**（確定）。
3. 選取 **Panorama** > **Managed Devices**（受管理的裝置）> **Summary**（摘要）並 **Deploy Master Key**（部署主要金鑰）。
4. 選取所有壯漢子並 **Change**（變更）主要金鑰。

© 2019 Palo Alto Networks, Inc.



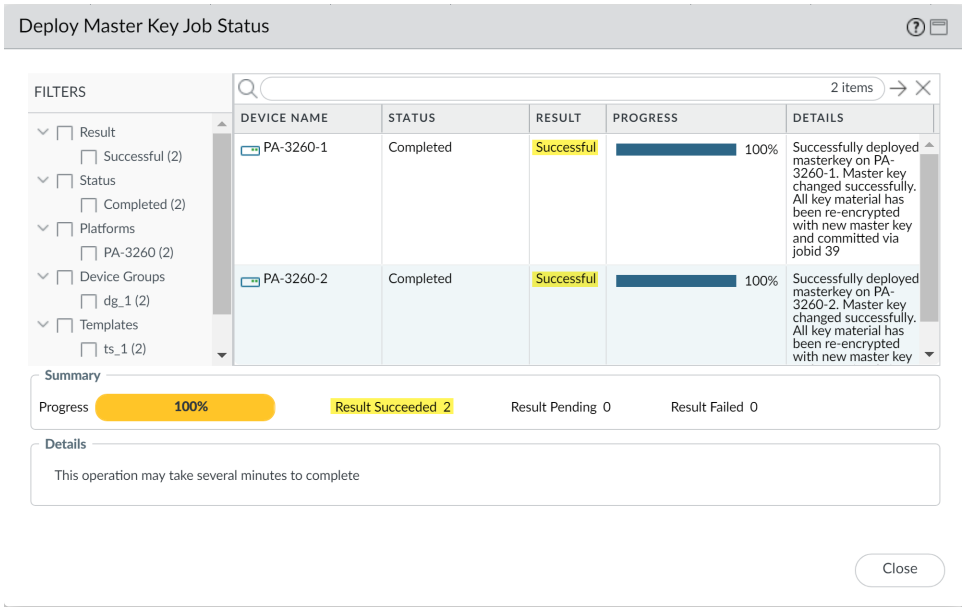
5. 設定主要金鑰。金鑰必須與您在第 1 步中設定的金鑰一致：
   1. 如果要更新主要金鑰，輸入 **Current Master Key**（當前主要金鑰）。如果您透過新的主要金鑰更換預設主要金鑰，不得指定 **Current Master Key**（當前主要金鑰）。
   2. 設定 **New Master Key**（新主要金鑰）並 **Confirm Master Key**（確認主要金鑰）。
   3. 設定主要金鑰 **Lifetime**（生命週期）與 **Time for Reminder**（提醒時間）。
   4. 按一下 **OK**（確定）。



6. 確認主要金鑰已成功部署至所有已選裝置。

   當您從 Panorama 部署新的主要金鑰時，系統日誌產生。

© 2019 Palo Alto Networks, Inc.



STEP 3 | 部署主要金鑰至日誌收集器。

針對所有 Panorama 節點重複此步驟。新的主要金鑰必須與您在第 1 步中設定的金鑰一致。

1. 選取 **Panorama** > **Managed Devices**（受管理的裝置）和 **Deploy Master Key**（部署主要金鑰）。
2. 選取所有壯漢子並 **Change**（變更）主要金鑰。
3. 設定主要金鑰：
    1. 如果要更新主要金鑰，輸入 **Current Master Key**（當前主要金鑰）。如果您透過新的主要金鑰更換預設主要金鑰，不得指定 **Current Master Key**（當前主要金鑰）。
    2. 指定 **New Master Key**（新主要金鑰）並 **Confirm Master Key**（確認主要金鑰）。
    3. 設定主要金鑰 **Lifetime**（生命週期）與 **Time for Reminder**（提醒時間）。
    4. 按一下 **OK**（確定）。
4. 確認主要金鑰已成功部署至所有已選裝置。

    當您從 Panorama 部署新的主要金鑰時，系統日誌產生。

STEP 4 | 部署主要金鑰至受管理的 WildFire 設備。

針對所有 Panorama 節點重複此步驟。新的主要金鑰必須與您在第 1 步中設定的金鑰一致。

1. 選取 **Panorama** > **Managed WildFire Appliances**（受管理的 **WildFire** 設備）和 **Deploy Master Key**（部署主要金鑰）。
2. 選取所有壯漢子並 **Change**（變更）主要金鑰。
3. 設定主要金鑰：
    1. 如果要更新主要金鑰，輸入 **Current Master Key**（當前主要金鑰）。如果您透過新的主要金鑰更換預設主要金鑰，不得指定 **Current Master Key**（當前主要金鑰）。
    2. 指定 **New Master Key**（新主要金鑰）並 **Confirm Master Key**（確認主要金鑰）。
    3. 設定主要金鑰 **Lifetime**（生命週期）與 **Time for Reminder**（提醒時間）。
    4. 按一下 **OK**（確定）。
4. 確認主要金鑰已成功部署至所有已選裝置。

    當您從 Panorama 部署新的主要金鑰時，系統日誌產生。

© 2019 Palo Alto Networks, Inc.

推送 *Panorama* 節點組態至受管理裝置

同步 Panorama 節點與 Panorama 控制器範本堆疊和裝置群組設定之後，將其推送至受管理裝置。

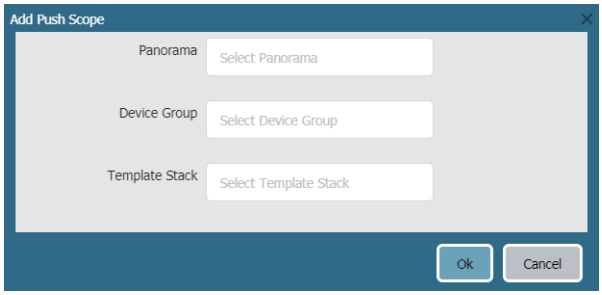
STEP 1 | 登入 Panorama 網頁介面Panorama 控制器。

STEP 2 | 選取 **Panorama** > **Interconnect** > **Devices**（裝置）。

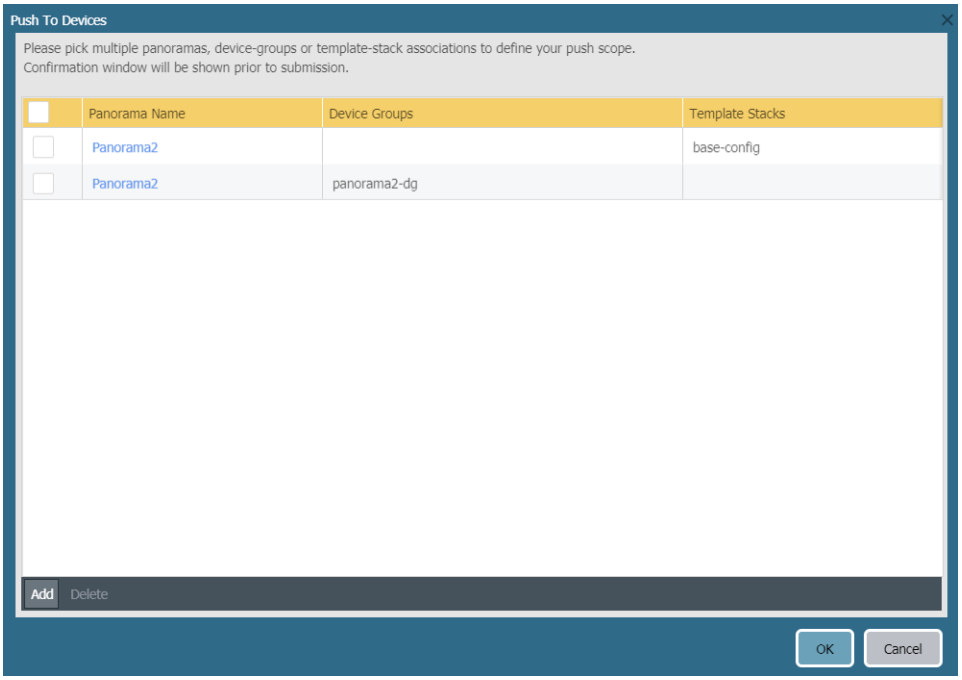
STEP 3 | 選取 **Push to Devices**（推送至裝置）以將同步設定從 Panorama 節點推送至受管理裝置。

STEP 4 | **Add**（新增）Panorama 節點，管理推送設定的目標裝置。重複此步驟，視需推送至多個 Panorama 節點、裝置群組或範本：

1. 選取 **Panorama** 節點。
2. 選取 **Device Group**（裝置群組）來推送裝置群組和範本堆疊，或選取 **Template Stack**（範本堆疊）僅推送範本堆疊設定。
3. 按一下 **OK**（確定）來完成推送範本界定。



STEP 5 | 按一下 **Ok**（確定）來推送設定至受管理裝置。



STEP 6 | 在 Device Group Push Status（裝置群組推送狀態）欄和 Template Stack Push Status（範本堆疊推送狀態）欄中，確認推送 `in-sync`（已同步）。

© 2019 Palo Alto Networks, Inc.

升級 Panorama Interconnect 外掛程式

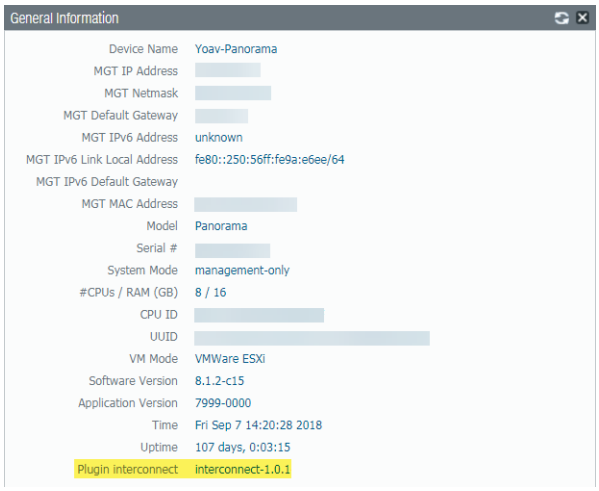
使用下列程序在 Panorama 控制器和 Panorama 節點上升級 Panorama™ Interconnect 外掛程式。升級 Panorama Interconnect 外掛程式時，您必須先升級 Panorama 控制器，再將 Panorama 節點升級至與控制器相同的外掛程式版本。您在 Panorama 節點上下載和安裝的新外掛程式版本必須與在 Panorama 控制器上安裝的版本相同，以確保 Panorama 控制器和選定 Panorama 節點上的外掛程式版本保持同步。

若這是首次安裝外掛程式版本，請參閱 設定 Panorama Interconnect 外掛程式。

STEP 1 | 登入 Panorama 網頁介面Panorama 控制器。

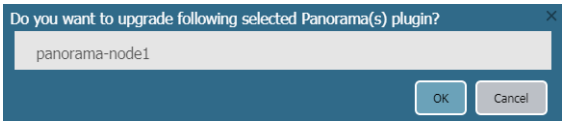
STEP 2 | 在 Panorama 控制器上升級 Panorama Interconnect 外掛程式。

1. 選取 **Panorama** > **Plugins**（外掛程式），然後搜尋 `Interconnect`。
2. **Download**（下載）並 **Install**（安裝）新的 Interconnect 外掛程式版本。提示即會顯示，通知您安裝已完成。
3. 確認 **Dashboard**（儀表板）顯示新安裝的 Interconnect 外掛程式版本。

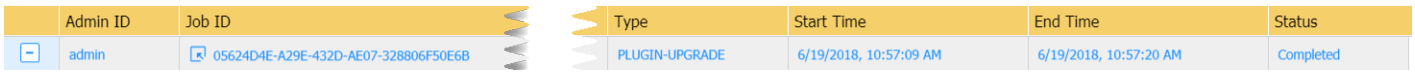


STEP 3 | 在 Panorama 節點上升級 Panorama Interconnect 外掛程式。

1. 選取 **Panorama** > **Interconnect** > **Panorama Nodes**（**Panorama** 節點），選取一個或多個 Panorama 節點，然後 **Upgrade Plugin**（升級外掛程式）。
2. 確認已選取 Panorama 節點，然後按一下 **OK**（確定），開始外掛程式升級。



3. 等待直至外掛程式升級工作 `Completed`（已完成）。按一下**Panorama** > **Interconnect** > **Tasks**（工作），檢視工作進度。



4. 升級成功完成後，選取 **Panorama** > **Interconnect** > **Panorama Nodes**（**Panorama** 節點），確認 **Plugin**（外掛程式）版本適用於選定的 Panorama 節點。



© 2019 Palo Alto Networks, Inc.

管理日誌收集

所有 Palo Alto Networks 防火牆都可產生日誌，以提供防火牆活動的稽核線索。對於集中化日誌記錄與回報，您必須轉送在防火牆生成的日誌到包含 Panorama™ 管理伺服器或日誌收集器的內部部署基礎設施中，或將日誌傳送到雲端式 Cortex Data Lake（Cortex 資料湖）。或者，您可以選擇設定 Panorama 將日誌轉送至外部的日誌記錄目的地（例如 syslog 伺服器）。

如果您將日誌轉送至傳統模式的 Panorama 虛擬設備，則不需要執行任何其他工作即可啟用日誌記錄。如果您將日誌轉送至日誌收集器，則必須設定為受管理的收集器，並指派給收集器群組。受管理的收集器可位於 M-Series 設備上，或 Panorama 模式下的 Panorama 虛擬設備上。此外，M-Series 設備或日誌收集器模式下的 Panorama 虛擬設備可以成為專用日誌收集器。若要決定是否部署受管理收集器的其中一種或兩種都部署，請參閱本機和分散式日誌收集。

若要管理 Panorama 在本機產生的系統與設定日誌，請參閱監控 Panorama。

> 設定受管理收集器
> 為專用日誌收集器設定驗證
> 管理收集器群組
> 設定日誌轉送至 Panorama
> 設定 Syslog 轉送至外部目的地
> 轉送日誌至 Cortex 資料湖
> 確認日誌轉送至 Panorama
> 修改日誌轉送及緩衝預設值
> 設定日誌從 Panorama 轉送至外部目的地
> 日誌收集部署

設定受管理收集器

為了讓 Panorama 管理伺服器能夠管理日誌收集器，您必須將其新增為受管理的收集器。您可以新增兩種受管理的收集器：

- 專用日誌收集器—若要設定新的 M-600、M-500、M-200 或 Panorama 虛擬設備作為日誌收集器，或將現有 M-Series 設備或 Panorama 虛擬設備從 Panorama 模式切換至日誌收集器模式，請參閱將 M-Series 設備設定為日誌收集器。記住，從 Panorama 模式切換至日誌收集器模式時，將會移除 Panorama 模式的 M-Series 設備上預先定義的本機日誌收集器。
- 本機日誌收集器—日誌收集器可以在 M-600、M-500、M-200 設備或 Panorama 模式的 Panorama 虛擬設備本機執行。在 M-Series 設備上，日誌收集器已預先定義；在虛擬設備上，您必須新增日誌收集器。如果 Panorama 管理伺服器採用高可用性 (HA) 設定，各 HA 端點都可以有本機日誌收集器。但是，相對於主要 Panorama，次要 Panorama 上的日誌收集器在遠端，而不是本機。因此，若要在次要 Panorama 上使用日誌收集器，您必須手動將其新增至主要 Panorama（詳細資訊，請參閱部署具備本機日誌收集器的 Panorama M-Series 設備或部署具備本機日誌收集器的 Panorama 虛擬設備）。如果您刪除本機日誌收集器，以後可以加回來。下列步驟說明如何新增本機日誌收集器。



最佳作法是在 *Panorama* 管理伺服器上保留本機日誌收集器和收集器群組，而無論其是否管理專用日誌收集器。



如果 *Panorama* 虛擬設備是傳統模式，您必須切換至 *Panorama* 模式才能建立日誌收集器。詳細資訊，請參閱設定具備本機日誌收集器的 Panorama 虛擬設備。

STEP 1 | 記錄日誌收集器的序號。

當您將新的日誌收集器新增為受管理的收集器時，您需要此序號。

1. 存取 Panorama Web 介面。
2. 選取 **Dashboard**（儀表板），然後記錄 General Information（一般資訊）部分中的 **Serial #**（序號）。

STEP 2 | 新增日誌收集器作為受管理的收集器。

1. 選取 **Panorama** > **Managed Collectors**（受管理的收集器），然後 **Add**（新增）新的日誌收集器。
2. 在 **General**（一般）設定中，輸入您記錄的收集器序號（**Collector S/N**（收集器序號））。
3. 按一下 **OK**（確定）儲存您的變更。
4. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**）。

STEP 3 | （選用）設定日誌收集器管理員驗證。

1. 選取 **Panorama** > **Managed Collectors**（受管理的收集器），然後按一下名稱來編輯日誌收集器。
2. 設定日誌收集器管理員密碼：
   1. 選取密碼 **Mode**（模式）。
   2. 如果您選取了 **Password**（密碼）模式，輸入純文字 **Password**（密碼）並 **Confirm Password**（確認密碼）。如果您選取了 **Password Hash**（密碼雜湊）模式，輸入最多 63 個字元的雜湊密碼字串。
3. 設定管理員登入安全需求：



如果您將 *Failed Attempts*（失敗的嘗試）數值設定為 *0* 以外的數字，但將 *Lockout Time*（鎖定時間）保留為 *0*，管理員使用者將被鎖定，直到另一位管理員手動解鎖該被鎖定的管理員為止。如果沒有建立其他管理員，您必須在 *Panorama* 上重新設定 *Failed Attempts*（失敗的嘗試）和 *Lockout Time*（鎖定時間）設定，並將組態變更

© 2019 Palo Alto Networks, Inc.

推送至日誌收集器。要確保管理員不會被鎖定，讓 *Failed Attempts*（失敗的嘗試）和 *Lockout Time*（鎖定時間）都使用預設值 *0*。

1. 輸入登入 **Failed Attempts**（失敗的嘗試）值數字。範圍為預設值 0 至最大值 10 之間的數字，數值 0 表示無限次登入嘗試。
2. 輸入預設值 0 至最大值 60 分鐘之間的 **Lockout Time**（鎖定時間）值。

4. 按一下 **OK**（確定）儲存您的變更。

STEP 4 | 啟用日誌記錄磁碟。

1. 選取 **Panorama** > **Managed Collectors**（受管理的收集器），然後按一下名稱來編輯日誌收集器。

   日誌收集器名稱的值與 Panorama 管理伺服器的主機名稱相同。
2. 選取 **Disks**（磁碟），然後 **Add**（新增）每一個磁碟配對。
3. 按一下 **OK**（確定）儲存您的變更。
4. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**）。

STEP 5 | （選用）如果您的部署使用自訂憑證在 Panorama 和受管理的裝置之間驗證，請部署自訂用戶端裝置憑證。如需詳細資訊，請參閱設定使用自訂憑證進行驗證。

1. 選取 **Panorama** > **Certificate Management**（憑證管理）> **Certificate Profile**（憑證設定檔），然後從下拉式清單中選擇憑證設定檔，或按一下 **New Certificate Profile**（新憑證設定檔）以建立憑證設定檔。
2. 選取 **Panorama** > **Managed Collectors**（受管理的收集器），然後 **Add**（新增）新的日誌收集器，或選取現有日誌收集器。選取 **Communication**（通訊）。
3. 從 Type（類型）下拉式清單中，選取裝置憑證的類型。
   - 如果您使用本機裝置憑證，請從 **Certificate**（憑證）和 **Certificate Profile**（憑證設定檔）各自的下拉式清單中選取。
   - 如果您使用 SCEP 作為裝置憑證，請從 **SCEPC Profile**（**SCEP** 設定檔）和 **Certificate Profile**（憑證設定檔）各自的下拉式清單中選取。
4. 按一下 **OK**（確定）。

STEP 6 | （選用）在日誌收集器上設定 Secure Server Communication（安全伺服器通訊）。如需詳細資訊，請參閱設定使用自訂憑證進行驗證。

1. 選取 **Panorama** > **Managed Collectors**（受管理的收集器），然後按一下 **Add**（新增）。選取 **Communication**（通訊）。
2. 確認未選取 **Custom Certificate Only**（僅限自訂憑證）核取方塊。這樣可讓您在移轉至自訂憑證期間繼續管理所有裝置。

   選取 *Custom Certificate Only*（僅限自訂憑證）核取方塊時，日誌收集器不會使用預先定義的憑證來驗證裝置，也無法使用這種憑證從裝置接收日誌。
3. 從 **SSL/TLS Service Profile**（**SSL/TLS** 服務設定檔）下拉式清單中，選取 SSL/TLS 服務設定檔。此 SSL/TLS 服務設定檔會套用至日誌收集器和送來日誌的裝置之間的所有 SSL 連線。
4. 從 **Certificate Profile**（憑證設定檔）下拉式清單中，選取憑證設定檔。
5. 選取 **Authorize Client Based on Serial Number**（根據序號來授權用戶端），讓伺服器根據受管理裝置的序號來檢查用戶端。用戶端憑證必須以特殊關鍵字 $UDID 來設定 CN，才能根據序號來驗證。
6. 在 **Disconnect Wait Time (min)**（中斷連線等候時間（分鐘））中，輸入 Panorama 在中斷並重新建立與受管理裝置間的連線之前應該等候的時間量。依預設，此欄位是空白，範圍是 0 至 44,640 分鐘。

   直到您提交新設定，中斷連線等候時間才會開始倒數計時。
7. （選用）設定授權清單。
   1. 按一下 Authorization List（授權清單）下的 **Add**（新增）。

© 2019 Palo Alto Networks, Inc.

2. 選取 **Subject**（主體）或 **Subject Alt Name**（主體別名）作為識別項類型。
3. 輸入所選類型的識別項。
4. 按一下 **OK**（確定）。
5. 選取 **Check Authorization List**（檢查授權清單）以強制執行授權清單。

8. 按一下 **OK**（確定）。
9. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**）。

STEP 7 | 確認變更。

1. 在 **Panorama** > **Managed Collectors**（受管理收集器）頁面中，列出您已新增的日誌收集器。Connected（已連線）欄中會顯示核取標記，表示日誌收集器已連線至 Panorama。您可能需要等待幾分鐘，然後頁面才會顯示更新後的連線狀態。

   在您 設定收集器群組 並將組態變更推送至收集器群組之前，*Configuration Status*（組態狀態）欄會顯示 *Out of Sync*（不同步），*Run Time Status*（執行階段狀態）欄會顯示 *disconnected*（已中斷連線），*CLI* 命令 **`show interface all`** 會顯示介面為 `down`（關閉）。
2. 按一下最後一欄中的 **Statistics**（統計資料），確認日誌記錄磁碟已啟用。

STEP 8 | 接下來的步驟...

在日誌收集器可以接收防火牆日誌之前，您必須：

1. 設定日誌轉送至 Panorama。
2. 設定收集器群組—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。在這兩種型號上，將防火牆指派給本機日誌收集器以轉送日誌。

© 2019 Palo Alto Networks, Inc.

為專用日誌收集器設定驗證

透過設定具有精確驗證參數的本機管理使用者，以及利用 RADIUS、TACAS+ 或 LDAP 進行授權和驗證，為您的專用日誌收集器建立和設定增強的驗證。

當您在 Panorama 上設定管理員並進行推送時，您在 Panorama 上設定的管理員將覆寫專用日誌收集器中的現有管理員。

- 為專用日誌收集器設定管理帳戶
- 為專用日誌收集器設定 RADIUS 驗證
- 為專用日誌收集器設定 TACACS+ 驗證
- 為專用日誌收集器設定 LDAP 驗證

為專用日誌收集器設定管理帳戶

為您的專用日誌收集器建立一個或多個具有精確驗證參數的管理員，以便從 Panorama™ 管理伺服器進行管理。此外，您還可以從 Panorama 設定本機管理員，這可以從專用日誌收集器的 CLI 直接進行設定。但是，向專用日誌收集器推送新設定變更後，為專用日誌收集器設定的管理員會覆寫現有本機管理員。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 設定受管理收集器。

STEP 3 | （選用）設定驗證設定檔以定義驗證服務，用於對存取專用日誌收集器 CLI 之管理員的登入認證進行驗證。

STEP 4 | 根據需要設定一個或多個管理員帳戶。

在 Panorama 上建立的管理員帳戶之後會匯入到專用日誌收集器並從 Panorama 進行管理。

STEP 5 | 為專用日誌收集器設定驗證。

1. 選取 **Panorama** > **Managed Collectors**（受管理的收集器），然後選取您之前新增的專用日誌收集器。
2. （選用）選取您在上一步中設定的 **Authentication Profile**（驗證設定檔）。
3. 為專用日誌收集器設定驗證 **Timeout Configuration**（逾時設定）。
    1. 輸入 **Failed Attempt**（失敗嘗試）次數，在達到此次數之後使用者將被鎖定在專用日誌收集器 CLI 之外。
    2. 輸入 **Lockout Time**（鎖定時間）（以分鐘為單位），在使用者達到設定的 **Failed Attempts**（失敗嘗試）次數後專用日誌收集器鎖定使用者帳戶的時間。
    3. 輸入 **Idle Timeout**（閒置逾時）（以分鐘為單位），在此時間之後使用者會因為處於非作用狀態而自動登出。
    4. 輸入 **Max Session Count**（最大工作階段計數），設定多少使用者帳戶可以同時存取專用日誌收集器。
    5. 輸入管理員在自動登出之前可登入的 **Max Session Time**（最長工作階段時間）。
4. 新增專用日誌收集器管理員。

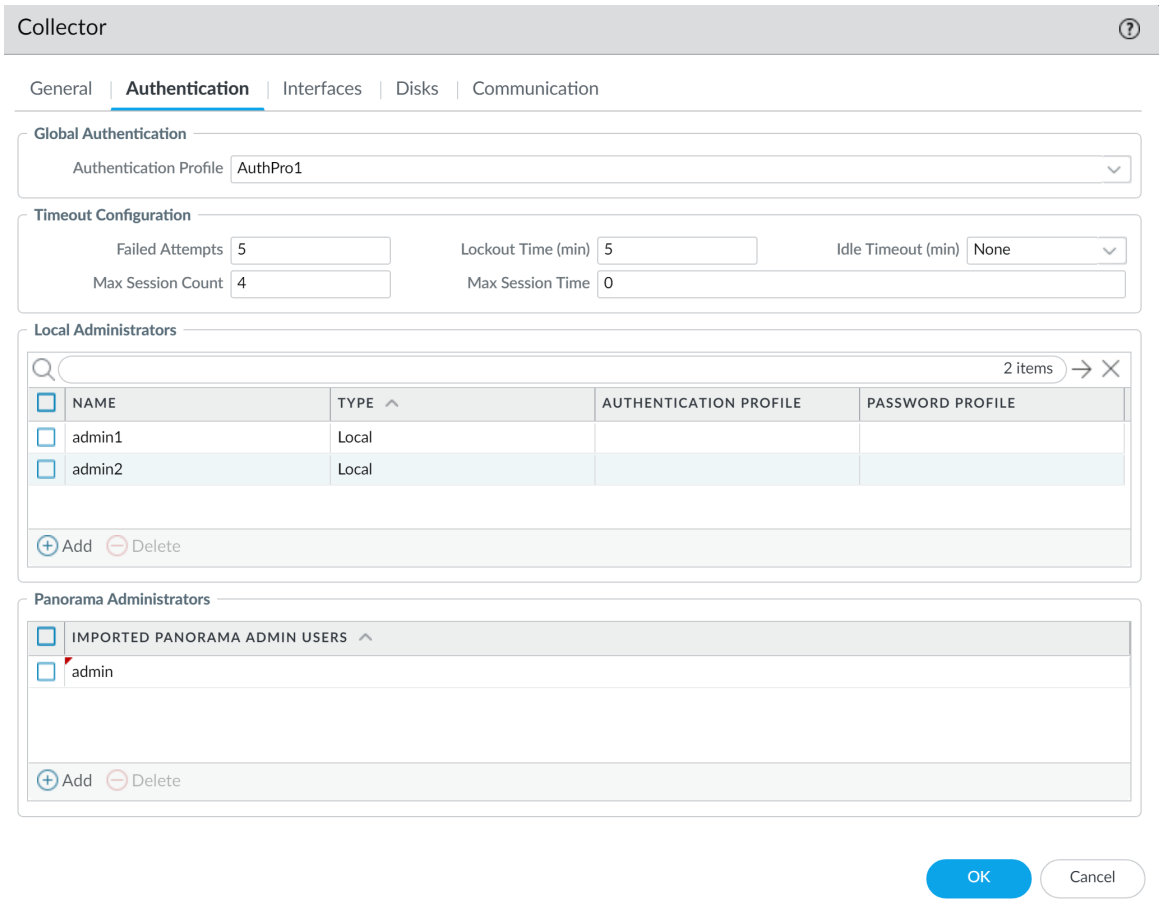
    管理員可以新增為本機管理員或作為匯入的 Panorama 管理員—但不能同時為二者。不支援將同一管理員同時新增為本機管理員和作為匯入的 Panorama 管理員，這會導致 Panorama 提交失敗。例如，如果您將 `admin1` 同時新增為本機和 Panorama 管理員，到 Panorama 的提交將會失敗。

    1. **Add**（新增）並設定專屬於專用日誌收集器的新管理員。這些管理員特定於為其建立的專用日誌收集器，您可以從此表格管理這些管理員。

© 2019 Palo Alto Networks, Inc.

2. **Add**（新增）在 Panorama 上設定的任何管理員。這些管理員在 Panorama 上建立，並匯入至專用日誌收集器。

5. 按一下 **OK**（確定）以儲存專用日誌收集器驗證設定。



STEP 6 | **Commit**（提交），然後 **Commit and Push**（提交並推送）設定變更。

STEP 7 | 使用本地管理員使用者 登入 Panorama CLI 專用日誌收集器以驗證您能夠成功存取專用日誌收集器。

為專用日誌收集器設定 RADIUS 驗證

使用 RADIUS 伺服器來驗證對專用日誌收集器 CLI 的管理存取。您也可以在 RADIUS 伺服器上定義廠商特定屬性 (VSA) 來進行管理員授權管理。使用 VSA 可讓您透過目錄服務快速變更管理員的角色、存取網域和使用者群組，這通常比在 Panorama™ 管理伺服器上重新設定更加簡單。

您可以將 Palo Alto 網路 RADIUS 詞典 匯入 *RADIUS* 伺服器，以定義 *Panorama* 和 *RADIUS* 伺服器之間通訊所需的驗證屬性。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 設定受管理收集器。

STEP 3 | 設定 RADIUS 驗證。

1. 新增 RADIUS 伺服器設定檔。

© 2019 Palo Alto Networks, Inc.

設定檔定義了專用日誌收集器將採用何種方式連線 RADIUS 伺服器。

1. 選取 **Panorama** > **Server Profiles**（伺服器設定檔）> **RADIUS**，然後 **Add**（新增）設定檔。
2. 輸入用來識別伺服器設定檔的 **Profile Name**（設定檔名稱）。
3. 輸入 **Timeout**（逾時）間隔時間（單位為秒），超過此時間後，驗證要求將逾時（預設值為 3；範圍為 1-20）。
4. 選取專用日誌收集器用於向 RADIUS 伺服器驗證的 **Authentication Protocol**（驗證通訊協定）（預設值為 **CHAP**）。

   選取 *CHAP*（如果 *RADIUS* 伺服器支援此通訊協定）；它比 *PAP* 更安全。

5. **Add**（新增）每個 RADIUS 伺服器，然後輸入下列資訊：
   1. 用來識別伺服器的 **Name**（名稱）。
   2. **RADIUS Server**（**RADIUS** 伺服器）IP 位址或 FQDN。
   3. **Secret**（密碼）/**Confirm Secret**（確認密碼）（用於加密使用者名稱和密碼的金鑰）。
   4. 用於驗證要求的伺服器 **Port**（連接埠）（預設值為 1812）。
6. 按一下 **OK**（確定）來儲存伺服器設定檔。

2. 將 RADIUS 伺服器設定檔指派給驗證設定檔。

   驗證設定檔中定義一群管理員通用的驗證設定。

   1. 選取 **Panorama** > **Authentication Profile**（驗證設定檔），然後 **Add**（新增）設定檔。
   2. 輸入用來識別驗證設定檔的 **Name**（名稱）。
   3. 將 **Type**（類型）設為 **RADIUS**。
   4. 選取您設定的 **Server Profile**（伺服器設定檔）。
   5. 選取 **Retrieve user group from RADIUS**（從 **RADIUS** 擷取使用者群組），以從 RADIUS 伺服器上定義的 VSA 收集使用者群組資訊。

      Panorama 會比對群組資訊與您在驗證設定檔「允許清單」中指定的群組。
   6. 選取 **Advanced**（進階），然後在 Allow List（允許清單）中，**Add**（新增）允許使用此驗證設定檔進行驗證的管理員。
   7. 按一下 **OK**（確定）來儲存驗證設定檔。

STEP 4 | 為專用日誌收集器設定驗證。

1. 選取 **Panorama** > **Managed Collectors**（受管理的收集器），然後選取您之前新增的專用日誌收集器。
2. 選取您在上一步中設定的 **Authentication Profile**（驗證設定檔）。

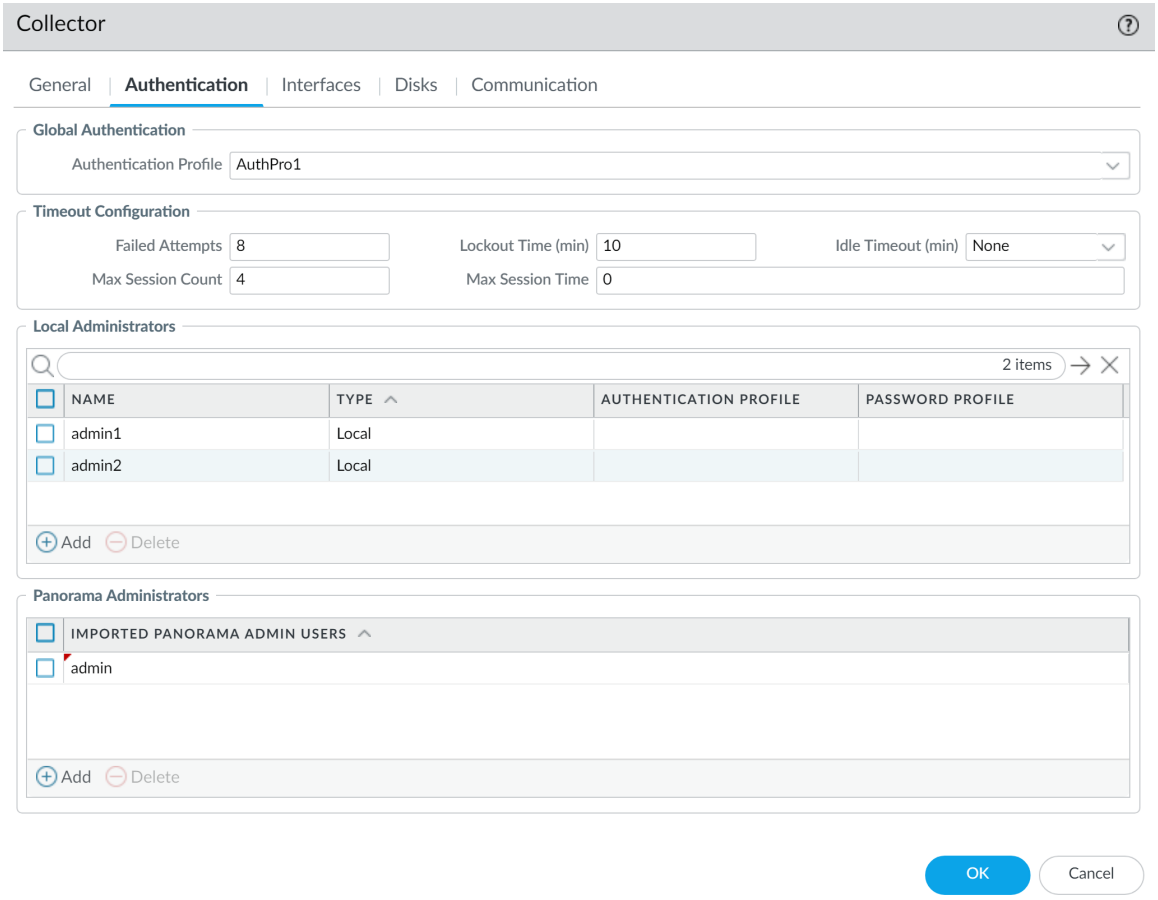
   如果沒有指派全域驗證設定檔，您必須指派一個驗證設定檔到單獨每個本機管理員才可利用遠端驗證。
3. 為專用日誌收集器設定驗證 **Timeout Configuration**（逾時設定）。
   1. 輸入 **Failed Attempt**（失敗嘗試）次數，在達到此次數之後使用者將被鎖定在專用日誌收集器 CLI 之外。
   2. 輸入 **Lockout Time**（鎖定時間）（以分鐘為單位），在使用者達到設定的 **Failed Attempts**（失敗嘗試）次數後專用日誌收集器鎖定使用者帳戶的時間。
   3. 輸入 **Idle Timeout**（閒置逾時）（以分鐘為單位），在此時間之後使用者會因為處於非作用狀態而自動登出。
   4. 輸入 **Max Session Count**（最大工作階段計數），設定多少使用者帳戶可以同時存取專用日誌收集器。
   5. 輸入管理員在自動登出之前可登入的 **Max Session Time**（最長工作階段時間）。
4. 新增專用日誌收集器管理員。

© 2019 Palo Alto Networks, Inc.

管理員可以新增為本機管理員或作為匯入的 Panorama 管理員—但不能同時為二者。不支援將同一管理員同時新增為本機管理員和作為匯入的 Panorama 管理員，這會導致 Panorama 提交失敗。例如，如果您將 **admin1** 同時新增為本機和 Panorama 管理員，到 Panorama 的提交將會失敗。

1. **Add**（新增）並設定專屬於專用日誌收集器的新管理員。這些管理員特定於為其建立的專用日誌收集器，您可以從此表格管理這些管理員。
2. **Add**（新增）在 Panorama 上設定的任何管理員。這些管理員在 Panorama 上建立，並匯入至專用日誌收集器。

5. 按一下 **OK**（確定）以儲存專用日誌收集器驗證設定。



STEP 5 | **Commit**（提交），然後 **Commit and Push**（提交並推送）設定變更。

STEP 6 | 使用本地管理員使用者 登入 Panorama CLI 專用日誌收集器以驗證您能夠成功存取專用日誌收集器。

為專用日誌收集器設定 TACACS+ 驗證

您可以使用 TACACS+ 伺服器來驗證對專用日誌收集器 CLI 的管理存取。您也可以在 TACACS+ 伺服器上定義廠商特定屬性 (VSA) 來進行管理員授權管理。使用 VSA 可讓您透過目錄服務快速變更管理員的角色、存取網域和使用者群組，這通常比在 Panorama 上重新設定更加簡單。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 設定受管理收集器。

© 2019 Palo Alto Networks, Inc.

STEP 3 | 設定 TACACS+ 驗證。

1. 新增 TACACS+ 伺服器設定檔。

   設定檔定義了專用日誌收集器將採用何種方式連線 TACACS+ 伺服器。

   1. 選取 **Panorama** > **Server Profiles**（伺服器設定檔）> **TACACS+**，然後 **Add**（新增）設定檔。
   2. 輸入用來識別伺服器設定檔的 **Profile Name**（設定檔名稱）。
   3. 輸入 **Timeout**（逾時）間隔時間（單位為秒），超過此時間後，驗證要求將逾時（預設值為 3；範圍為 1-20）。
   4. 選取 Panorama 用於向 TACACS+ 伺服器驗證的 **Authentication Protocol**（驗證通訊協定）（預設值為 **CHAP**）。
   5. 選取 **CHAP**（如果 TACACS+ 伺服器支援此通訊協定）；它比 **PAP** 更安全。
   6. **Add**（新增）每個 TACACS+ 伺服器，然後輸入下列資訊：

      1. 用來識別伺服器的 **Name**（名稱）。
      2. **TACACS+ Server**（**TACACS+** 伺服器）IP 位址或 FQDN。
      3. **Secret**（密碼）/**Confirm Secret**（確認密碼）（用於加密使用者名稱和密碼的金鑰）。
      4. 用於驗證要求的伺服器 **Port**（連接埠）（預設值為 49）。

   7. 按一下 **OK**（確定）來儲存伺服器設定檔。

2. 將 TACACS+ 伺服器設定檔指派給驗證設定檔。

   驗證設定檔中定義一群管理員通用的驗證設定。

   1. 選取 **Panorama** > **Authentication Profile**（驗證設定檔），然後 **Add**（新增）設定檔。
   2. 輸入用來識別設定檔的 **Name**（名稱）。
   3. 將 **Type**（類型）設為 **TACACS+**。
   4. 選取您設定的 **Server Profile**（伺服器設定檔）。
   5. 選取 **Retrieve user group from TACACS+**（從 **TACACS+** 擷取使用者群組），以從 TACACS+ 伺服器上定義的 VSA 收集使用者群組資訊。

      Panorama 會比對群組資訊與您在驗證設定檔「允許清單」中指定的群組。

   6. 選取 **Advanced**（進階），然後在 Allow List（允許清單）中，**Add**（新增）允許使用此驗證設定檔進行驗證的管理員。
   7. 按一下 **OK**（確定）來儲存驗證設定檔。

STEP 4 | 為專用日誌收集器設定驗證。

1. 選取 **Panorama** > **Managed Collectors**（受管理的收集器），然後選取您之前新增的專用日誌收集器。
2. 選取您在上一步中設定的 **Authentication Profile**（驗證設定檔）。

   如果沒有指派全域驗證設定檔，您必須指派一個驗證設定檔到單獨每個本機管理員才可利用遠端驗證。

3. 為專用日誌收集器設定驗證 **Timeout Configuration**（逾時設定）。

   1. 輸入 **Failed Attempt**（失敗嘗試）次數，在達到此次數之後使用者將被鎖定在專用日誌收集器 CLI 之外。
   2. 輸入 **Lockout Time**（鎖定時間）（以分鐘為單位），在使用者達到設定的 **Failed Attempts**（失敗嘗試）次數後專用日誌收集器鎖定使用者帳戶的時間。
   3. 輸入 **Idle Timeout**（閒置逾時）（以分鐘為單位），在此時間之後使用者會因為處於非作用狀態而自動登出。
   4. 輸入 **Max Session Count**（最大工作階段計數），設定多少使用者帳戶可以同時存取專用日誌收集器。
   5. 輸入管理員在自動登出之前可登入的 **Max Session Time**（最長工作階段時間）。

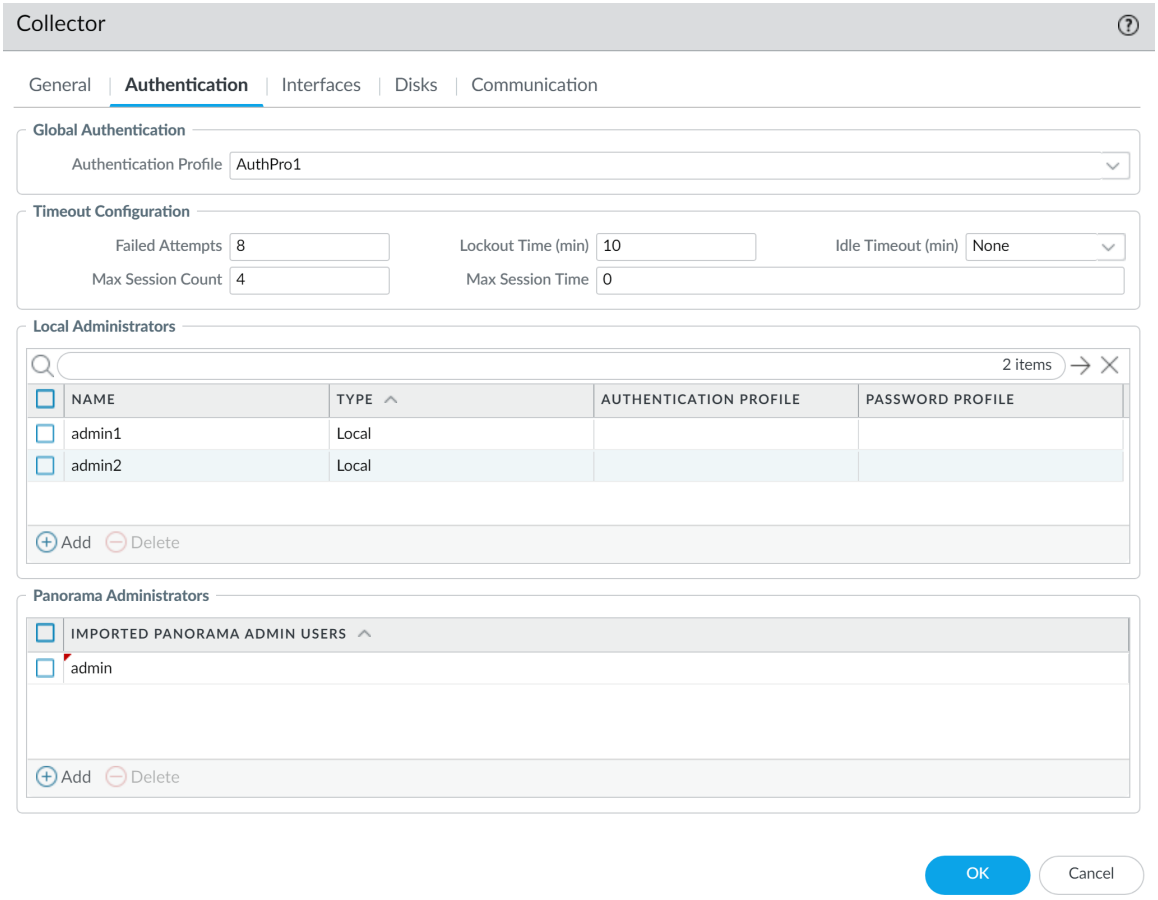
4. 新增專用日誌收集器管理員。

© 2019 Palo Alto Networks, Inc.

管理員可以新增為本機管理員或作為匯入的 Panorama 管理員—但不能同時為二者。不支援將同一管理員同時新增為本機管理員和作為匯入的 Panorama 管理員，這會導致 Panorama 提交失敗。例如，如果您將 **admin1** 同時新增為本機和 Panorama 管理員，到 Panorama 的提交將會失敗。

1. **Add**（新增）並設定專屬於專用日誌收集器的新管理員。這些管理員特定於為其建立的專用日誌收集器，您可以從此表格管理這些管理員。
2. **Add**（新增）在 Panorama 上設定的任何管理員。這些管理員在 Panorama 上建立，並匯入至專用日誌收集器。

5. 按一下 **OK**（確定）以儲存專用日誌收集器驗證設定。



STEP 5 | **Commit**（提交），然後 **Commit and Push**（提交並推送）設定變更。

STEP 6 | 使用本地管理員使用者 登入 Panorama CLI 專用日誌收集器以驗證您能夠成功存取專用日誌收集器。

為專用日誌收集器設定 LDAP 驗證

您可以使用 LDAP 驗證存取專用日誌收集器 Web 介面的一般使用者。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 設定受管理收集器。

STEP 3 | 新增 LDAP 伺服器設定檔。

設定檔定義了專用日誌收集器將採用何種方式連線 LDAP 伺服器。

© 2019 Palo Alto Networks, Inc.

1. 選取 **Panorama** > **Server Profiles**（伺服器設定檔）> **LDAP**，然後 **Add**（新增）伺服器設定檔。
2. 輸入用來識別伺服器設定檔的 **Profile Name**（設定檔名稱）。
3. **Add**（新增）LDAP 伺服器（最多可新增四個）。對於每個伺服器，輸入 **Name**（名稱）（用於識別伺服器）、**LDAP Server**（**LDAP** 伺服器）IP 位址或 FQDN，以及伺服器 **Port**（連接埠）（預設值為 389）。

   
   如果您使用 *FQDN* 位址物件識別伺服器並隨後變更了位址，則必須要提交變更，以便新伺服器位址生效。
4. 選取伺服器 **Type**（類型）。
5. 選取 **Base DN**（基礎 **DN**）。

   識別您目錄 Base DN，打開**Active Directory Domains and Trusts**（主動式目錄網域與信任）Microsoft 管理控制台管理單元，並使用頂級網域名稱。
6. 輸入 **Bind DN**（繫結 **DN**）與 **Password**（密碼）以讓驗證服務能驗證防火牆。

   
   繫結 *DN* 賬號須具有讀取 *LDAP* 目錄的權限。
7. 輸入 **Bind Timeout**（繫結逾時）和**Search Timeout**（搜尋逾時），單位為秒（預設值均為 30）。
8. 輸入 **Retry Interval**（重試間隔）（秒）（預設值為 60）。
9. （選用）如果您希望端點使用 SSL 或 TLS 更安全的連線目錄伺服器，請啟用 **Require SSL/TLS secured connection**（需要 **SSL/TLS** 安全連線）選項（預設為已啟用）。端點使用的協定視乎伺服器連接埠而定：
   - 389（預設）—TLS（特別是專用日誌收集器會使用 StartTLS 操作，用來升級連線至 TLS 的初始純文字連線。）
   - 636—SSL
   - 任何其他連接埠—專用日誌收集器首先會嘗試使用 TLS。若目錄伺服器不支援 TLS，則專用日誌收集器會回復使用 SSL。
10. （選用）為了獲得額外的安全，請啟用 **Verify Server Certificate for SSL sessions**（確認 **SSL** 工作階段的伺服器憑證）選項，讓端點確認目錄伺服器為 SSL/TLS 連線所呈現的憑證。若要啟用驗證，您也必須啟用 **Require SSL/TLS secured connection**（要求 **SSL/TLS** 安全連線）選項。為了順利確認，憑證必須滿足以下條件之一：
    - 位於 Panorama 憑證清單內：**Panorama** > **Certificate Management**（憑證管理）> **Certificates**（憑證）> **Device Certificates**（設備憑證）。若有必要，將憑證匯入至 Panorama。
    - 憑證簽署者位於受信任的憑證授權單位清單中：**Panorama** > **Certificate Management**（憑證管理）> **Certificates**（憑證）。
11. 按一下 **OK**（確定）來儲存伺服器設定檔。

STEP 4 | 為專用日誌收集器設定驗證。

1. 選取 **Panorama** > **Managed Collectors**（受管理的收集器），然後選取您之前新增的專用日誌收集器。
2. 為專用日誌收集器設定驗證 **Timeout Configuration**（逾時設定）。
    1. 輸入 **Failed Attempt**（失敗嘗試）次數，在達到此次數之後使用者將被鎖定在專用日誌收集器 CLI 之外。
    2. 輸入 **Lockout Time**（鎖定時間）（以分鐘為單位），在使用者達到設定的 **Failed Attempts**（失敗嘗試）次數後專用日誌收集器鎖定使用者帳戶的時間。
    3. 輸入 **Idle Timeout**（閒置逾時）（以分鐘為單位），在此時間之後使用者會因為處於非作用狀態而自動登出。
    4. 輸入 **Max Session Count**（最大工作階段計數），設定多少使用者帳戶可以同時存取專用日誌收集器。
    5. 輸入管理員在自動登出之前可登入的 **Max Session Time**（最長工作階段時間）。

© 2019 Palo Alto Networks, Inc.

3. 新增專用日誌收集器管理員。

   管理員可以新增為本機管理員或作為匯入的 Panorama 管理員—但不能同時為二者。不支援將同一管理員同時新增為本機管理員和作為匯入的 Panorama 管理員，這會導致 Panorama 提交失敗。例如，如果您將 **admin1** 同時新增為本機和 Panorama 管理員，到 Panorama 的提交將會失敗。

   - 設定本機管理員。

     設定專屬於專用日誌收集器的新管理員。這些管理員特定於為其建立的專用日誌收集器，您可以從此表格管理這些管理員。

     1. **Add**（新增）一個或多個新本機管理員。
     2. 輸入本機管理員的 **Name**（名稱）。
     3. 指派您之前建立的 **Authentication Profile**（驗證設定檔）。

        LDAP 驗證設定檔僅支援個別本地管理員。

     4. 啟用（核取）**Use Public Key Authentication (SSH)**（使用公開金鑰驗證 **(SSH)**）以匯入公開金鑰檔案進行驗證。
     5. 選取 **Password Profile**（密碼設定檔）以設定到期參數。
   - 匯入現有 Panorama 管理員

     匯入 Panorama 上的現有管理員。這些管理員在 Panorama 上設定和管理，並匯入至專用日誌收集器。

     1. **Add**（新增）現有 Panorama 管理員
4. 按一下 **OK**（確定）以儲存專用日誌收集器驗證設定。

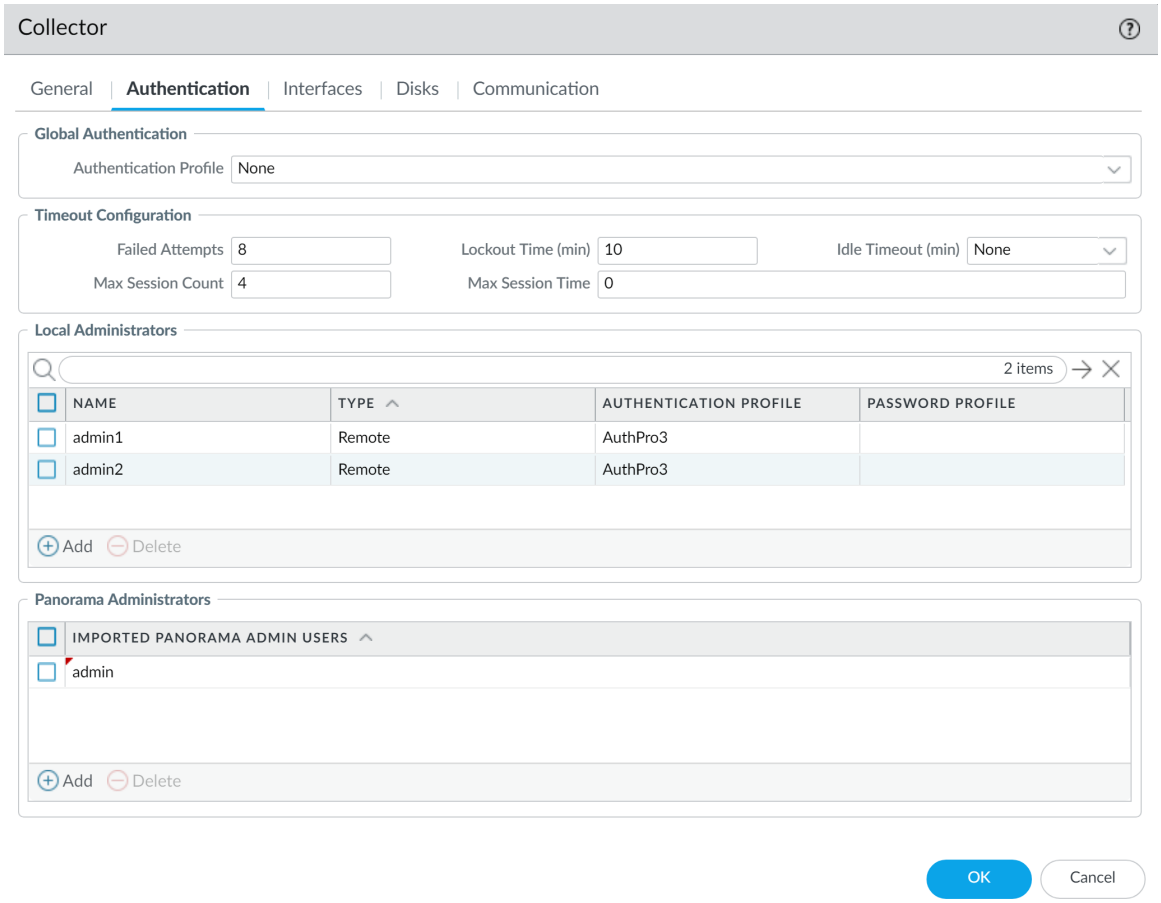
STEP 5 | 為專用日誌收集器設定驗證。

1. 選取 **Panorama** > **Managed Collectors**（受管理的收集器），然後選取您之前新增的專用日誌收集器。
2. 選取您在上一步中設定的 **Authentication Profile**（驗證設定檔）。
3. 為專用日誌收集器設定驗證 **Timeout Configuration**（逾時設定）。
   1. 輸入 **Failed Attempt**（失敗嘗試）次數，在達到此次數之後使用者將被鎖定在專用日誌收集器 CLI 之外。
   2. 輸入 **Lockout Time**（鎖定時間）（以分鐘為單位），在使用者達到設定的 **Failed Attempts**（失敗嘗試）次數後專用日誌收集器鎖定使用者帳戶的時間。
   3. 輸入 **Idle Timeout**（閒置逾時）（以分鐘為單位），在此時間之後使用者會因為處於非作用狀態而自動登出。
   4. 輸入 **Max Session Count**（最大工作階段計數），設定多少使用者帳戶可以同時存取專用日誌收集器。
   5. 輸入管理員在自動登出之前可登入的 **Max Session Time**（最長工作階段時間）。
4. 新增專用日誌收集器管理員。

   您必須將管理員 (**admin**) 新增為本機管理員或作為匯入的 Panorama 管理員—但不能同時為二者。如果沒有新增管理員，或者管理員被同時新增為本機管理員和匯入的 Panorama 管理員，則會導致推送到受管理收集器失敗。

   1. **Add**（新增）並設定專屬於專用日誌收集器的新管理員。這些管理員特定於為其建立的專用日誌收集器，您可以從此表格管理這些管理員。
   2. **Add**（新增）在 Panorama 上設定的任何管理員。這些管理員在 Panorama 上建立，並匯入至專用日誌收集器。
5. 按一下 **OK**（確定）以儲存專用日誌收集器驗證設定。

© 2019 Palo Alto Networks, Inc.



STEP 6 | **Commit（提交），然後 Commit and Push（提交並推送）設定變更。**

STEP 7 | **使用本地管理員使用者 登入 Panorama CLI 專用日誌收集器以驗證您能夠成功存取專用日誌收集器。**

© 2019 Palo Alto Networks, Inc.

管理收集器群組

收集器群組是 1 至 16 個日誌收集器，以單一邏輯單元運作來收集日誌。您必須指派至少一個日誌收集器給收集器群組，防火牆才能成功將日誌傳送至日誌收集器。如果未設定收集器群組，或未指派日誌收集器給收集器群組，則會丟棄防火牆日誌。您可以設定具有多個日誌收集器的收集器群組，確保日誌備援或支援超出單一日誌收集器能力的日誌記錄速率（請參閱 Panorama 型號）。若要瞭解相關風險及建議的減輕方式，請參閱警告有收集器群組擁有多個日誌收集器。

Panorama 模式的 M-600、M-500 和 M-200 設備具有預先定義的收集器群組，其中包含預先定義的本機日誌收集器。您可以編輯預先定義的收集器群組的所有設定，但名稱除外（預設值）。

如果您刪除收集器群組，則會失去日誌。

Palo Alto Networks 建議在 *Panorama* 管理伺服器上保留預先定義的日誌收集器和收集器群組，而無論 *Panorama* 是否也管理專用日誌收集器。

如果您將 *M-Series* 設備從 *Panorama* 模式切換至日誌收集器模式，裝置會失去其預先定義的收集器群組和日誌收集器。於是，您必須將 M-Series 設備設定為日誌收集器，當作受管理的收集器新增至 *Panorama*，然後設定收集器群組來包含這個受管理的收集器。

- 設定收集器群組
- 以日誌收集器間的自訂憑證，來設定驗證
- 移動日誌收集器至不同的收集器群組
- 從收集器群組移除防火牆

設定收集器群組

在設定收集器群組之前，請決定每個群組只有單一日誌收集器，還是有多個日誌收集器（最多 16 個）。具有多個日誌收集器的收集器群組支援較高的日誌記錄速率和日誌備援，但有下列需求：

- 在任何單一收集器群組中，所有日誌收集器都必須在相同 Panorama 型號上執行：全部是 M-600 設備、全部都是 M-500 設備、全部都是 M-200，或全部是 Panorama 虛擬設備。
- 只有當每一個日誌收集器都具有相同數量的日誌磁碟時，日誌備援才可用。若要將磁碟新增至日誌收集器，請參閱增加 M-Series 設備的儲存容量。
- （最佳做法）相同收集器群組內的所有日誌收集器應位於相同的區域網路中 (LAN)。避免在相同或不同廣域網路 (WAN) 內，為相同收集器群組新增日誌收集器，因為這樣更容易發生網路中斷，並導致日誌資料丟失。此外，建議相同收集器群組內的日誌收集器在物理位置上相互緊挨，以便讓 Panorama 在需要時可迅速進行查詢。

STEP 1 | 在設定收集器群組前，執行下列工作。

1. 對於您將指派至收集器群組的各防火牆，將防火牆新增為受管理的設備。
2. 對於您將指派至收集器群組的各日誌收集器，設定受管理收集器。

STEP 2 | 新增收集器群組。

1. 存取 Panorama web 介面，選取**Panorama** > **Collector Groups**（收集器群組），並 **Add**（新增）收集器群組或編輯現有群組。
2. 如果是新增收集器群組，請輸入其 **Name**（名稱）。

   您無法重新命名現有的收集器群組。
3. 輸入收集器群組保留防火牆日誌的 **Minimum Retention Period**（最短保留週期）天數（1 至 2,000）。

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

© 2019 Palo Alto Networks, Inc.

5. （建議）如果您要將多個日誌收集器新增至單一收集器群組，請 **Enable log redundancy across collectors**（啟用跨收集器的日誌備援）。

   如果有任何一個日誌收集器群組無法使用，備援可確保不會遺失日誌。每個日誌將有兩個副本，每個副本都將保留在不同的日誌收集器上。例如，如果您在收集器群組中有兩個日誌收集器，則日誌會寫入至這兩個日誌收集器。

   啟用備援會建立更多日誌，因此此設定需要更多儲存容量，而使儲存能力減少一半。收集器群組空間用盡時，其會刪除較舊的日誌。由於每個日誌收集器都必須散佈每個接收的日誌複本，因此備援會讓收集器群組中的日誌處理流量加倍，並讓最大日誌記錄速率減半。

STEP 3 | 將日誌收集器和防火牆指派給收集器群組。

1. 選取 **Device Log Forwarding**（裝置日誌轉竑），**Add**（新增）防火牆的日誌轉送偏好設定清單。

   透過單獨的 TCP 通道轉送日誌資料。藉由新增日誌轉送偏好設定清單，您可以建立單獨的 TCP 連線以轉送日誌資料。

   偏好設定清單決定日誌收集器從防火牆接收日誌的順序。如果未指派日誌轉送偏好設定清單，您可能會遇到下列狀況：

   - 如果 *Panorama* 處於僅管理模式，*Panorama* 會捨棄所有傳入日誌。
   - 如果 *Panorama* 處於 *Panorama* 模式時，且本機日誌收集器未設定為受管理的收集器，則 *Panorama* 會捨棄所有傳入日誌。
   - 如果 *Panorama* 處於 *Panorama* 模式，且本機日誌收集器已設定為受管理的收集器，則會接收傳入日誌，但 *Panorama* 會成為瓶頸，因為在日誌重新散佈至其他可用的日誌收集器之前，所有受管理的防火牆會先將日誌轉送至本機日誌收集器。

   1. 在 Devices（裝置）部分中，**Modify**（修改）防火牆清單，然後按一下 **OK**（確定）。
   2. 在 Collectors（收集器）部分中，將日誌收集器 **Add**（新增）至偏好設定清單。

      如果您在步驟 2 中啟用備援，建議新增至少兩個日誌收集器。如果您指派多個日誌收集器，則第一個會是主要；當主要日誌收集器無法使用時，防火牆會將日誌轉送到清單中的下一個日誌收集器。若要變更日誌收集器的優先順序，請選取該收集器，然後 **Move Up**（上移）（提高優先順序）或 **Move Down**（下移）（降低優先順序）。
   3. 按一下 **OK**（確定）。

STEP 4 | 定義各日誌類型的儲存容量（日誌配額）和到期日期。

1. 返回 **General**（一般）頁籤，然後按一下 **Log Storage**（日誌儲存）值。

   如果此欄位顯示成 *0MB*，請確認您已啟用磁碟配對以記錄日誌與提交變更（請參閱設定受管理收集器，*Disks*（磁碟）頁籤）。
2. 輸入每個日誌類型的日誌儲存 **Quota**（配額）(%)。
3. 輸入各日誌類型的 **Max Days**（最大天數）（到期時間）（1 至 2,000）。

   依預設，欄位為空，意味著日誌從不過期。

STEP 5 | 認可並驗證變更。

1. 選取 **Commit**（提交）> **Commit and Push**（提交並推送），然後將您的變更 **Commit and Push**（提交並推送）至 Panorama 和您設定的收集器群組。
2. 選取 **Panorama** > **Managed Collectors**（受管理的收集器），以驗證收集器群組中的日誌收集器為下列狀態：

   - 已連線至 **Panorama** - Connected（已連線）欄顯示核取標記圖示，表示日誌收集器已連線至 Panorama。
   - 已與 **Panorama** 同步—Configuration Status（組態狀態）欄指出日誌收集器與 Panorama `In Sync`（同步）（綠色圖示）還是 `Out of Sync`（不同步）（紅色圖示）。

© 2019 Palo Alto Networks, Inc.

STEP 6 | 疑難排解網路資源連線 確認您的防火牆是否成功連線至日誌收集器。

STEP 7 | 接下來的步驟...

1. 設定日誌轉送至 Panorama。

   在您設定防火牆轉送至 Panorama 之前，收集器群組不會接收防火牆日誌。
2. （選用）設定日誌從 Panorama 轉送至外部目的地。

   您可以設定各收集器群組將日誌轉送至不同目的地（例如 syslog 伺服器）。

以日誌收集器間的自訂憑證，來設定驗證

完成以下程序以設定日誌收集器間通訊的自訂憑證。您必須在收集器群組內的每個日誌收集器中設定安全伺服器通訊與安全用戶端通訊，因為伺服器和用戶端角色是動態選定的。使用自訂憑證以建立唯一信任鏈，確保您日誌記錄器群組成員間的相互驗證。

對於使用自訂憑證的詳細內容，請參閱 SSL/TLS 連線如何相互驗證？

STEP 1 | 取得 每個日誌記錄器的金鑰配對與憑證授權單位 (CA)。

STEP 2 | 匯入 CA 憑證以驗證用戶端日誌收集器、伺服器金鑰配對和記錄器群組內每個日誌記錄器的身份。

1. 選取 **Panorama** > **Certificate Management**（憑證管理）> **Certificates**（憑證）> **Import**（匯入）。
2. 匯入 CA 憑證、伺服器金鑰配對和用戶端金鑰配對。
3. 每個日誌收集器皆重覆此 步驟。

STEP 3 | 設定包含 root CA 和中繼 CA 的憑證設定檔以保護伺服器通訊。此憑證設定檔定義日誌收集器間的驗證。

1. 選取 **Panorama** > **Certificates Management**（憑證管理）> **Certificate Profile**（憑證設定檔）。
2. 設定憑證設定檔。

   如果您在憑證設定檔中設定中繼 CA，則必須也包含 root CA。

STEP 4 | 設定憑證設定檔以保護用戶端通訊。您可以在每個用戶端日誌收集器個別地設定此設定檔，或您可以從 Panorama™ 推送設定到受管理的日誌收集器。



如果您使用 *SCEP* 傳送用戶端憑證，請設定 SCEP 設定檔而非憑證設定檔。

1. 選取 **Panorama** > **Certificates Management**（憑證管理）> **Certificate Profile**（憑證設定檔）。
2. 設定憑證設定檔。

STEP 5 | 設定 SSL/TLS 服務設定檔。

1. 選取 **Panorama** > **Certificate Management**（憑證管理）> **SSL/TLS Service Profile**（**SSL/TLS** 服務設定檔）。
2. 設定 SSL/TLS 服務設定檔，以定義憑證和通訊協定供用於 SSL/TLS 服務的日誌收集器。

STEP 6 | 在所有受管理的日誌收集器上部署自訂憑證後，強制執行自訂憑證驗證。

1. 選取 **Panorama** > **Collector Groups**（收集器群組），再選取收集器群組。
2. 在 General（一般）頁籤上，**Enable secure inter LC Communication**（啟用安全性 **Inter LC** 通訊）。

   若您啟用安全性 Inter LC 通訊且您的收集器群組包含本機收集器，則因顯示說明在本機 **Panorama** 上的日誌收集器正使用來自 **Panorama** 的安全用戶端設定 > 安全性通訊設定的連結。您可以按一下此連結以開啟安全性通訊對話，並為來自該處的本機日誌收集器設定安全伺服器和安全用戶端設定。

© 2019 Palo Alto Networks, Inc.

3. 按一下 **OK**（確定）。
4. **Commit**（提交）您的變更。

STEP 7 | 在每個日誌收集器上設定安全伺服器通訊。

1. 對專用日誌收集器，選取 **Panorama** > **Managed Collectors**（受管理的收集器），或對本機日誌收集器，選取 **Panorama** > **Setup**（設定） > **Management**（管理） 並 **Edit**（編輯） 安全通訊設定。
2. 對於專用日誌收集器，請按一下日誌收集器並選取 **Communications**（通訊）。
3. 啟用 **Customize Secure Server Communication**（自訂安全伺服器通訊）功能。
4. 從 **SSL/TLS Service Profile**（**SSL/TLS** 服務設定檔）下拉式清單中，選取 SSL/TLS 服務設定檔。此 SSL/TLS 服務設定檔會套用日誌收集器之間的所有 SSL 連線。
5. 從下拉式清單選取**Certificate Profile**（憑證設定檔）。
6. 確認 **Custom Certificates Only**（僅限自訂憑證）為停用（已清除）。這能讓 Inter 日誌收集器設定自訂憑證同時，繼續使用預定義憑證通訊。
7. 設定斷線等候時間—在斷開與其他日誌收集器連線並重新建立前的日誌記錄器等候分鐘數。依預設，此欄位是空白（範圍是 0 至 44,640 分鐘）。
8. （選用）設定授權清單。授權清單可在憑證驗證之外多加一層安全性。授權清單會檢查用戶端憑證「主體」或「主體別名」。如果伴隨用戶端憑證一起出現的主體或主體別名不符合授權清單內的識別項，則會拒絕驗證。
   1. **Add**（新增）授權清單。
   2. 在憑證設定檔中，選取 **Subject**（主體）或 **Subject Alt Name**（主體別名）作為識別項類型。
   3. 如果識別項是`Subject`（主體），請輸入Common Name（通用名稱），如果識別項是 `Subject Alt Name`（主體別名），請輸入 IP 位址、主機名稱或電子郵件。
   4. 按一下 **OK**（確定）。
   5. 啟用 **Check Authorization List**（檢查授權清單）選項以設定 Panorama 強制執行授權清單。
9. 按一下 **OK**（確定）。
10. **Commit**（提交）您的變更。

在提交這些變更後，連線斷開等候時間開始倒數。在等候時間結束時，在收集器群組內的日誌收集器無法在沒有訂定憑證的情況下連線。

STEP 8 | 在每個日誌收集器上設定安全用戶端。

1. 對專用日誌收集器，選取 **Panorama** > **Managed Collectors**（受管理的收集器），或對本機日誌收集器，選取 **Panorama** > **Setup**（設定） > **Management**（管理） 並 **Edit**（編輯） 安全通訊設定。
2. 對於專用日誌收集器，請按一下日誌收集器並選取 **Communications**（通訊）。
3. 在安全用戶端通訊下，選取來自各別下拉式選單的 **Certificate Type**（憑證類型）、**Certificate**（憑證）與 **Certificate Profile**（憑證設定檔）。
4. 按一下 **OK**（確定）。
5. **Commit**（提交）您的變更。

移動日誌收集器至不同的收集器群組

M-600、M-500、M-200 和 Panorama 虛擬設備在每個收集器群組中可以有一個或多個日誌收集器。您需要根據收集器群組的日誌記錄速率和日誌儲存需求，將日誌收集器指派給收集器群組。如果收集器群組的速率和所需儲存空間增大，最佳的作法是增加 M-Series 日誌儲存容量）或利用額外的日誌收集器設定收集器群組。但是，在某些部署中，在收集器群組之間移動日誌收集器可能更加節省成本。

當日誌收集器是 *Panorama* 模式下設備的本機收集器時，僅在 *M-600*、*M-500* 或 *M-200* 設備是採用高可用性 *(HA)* 設定的被動對等時，方可對其進行移動。*HA* 同步適用於新收集器群組相關的設定。切勿移動主動 *HA* 對等本機的日誌收集器。

在任何單一收集器群組中，所有日誌收集器都必須在相同 *Panorama* 型號上執行：全部是 *M-600* 設備、全部都是 *M-500* 設備、全部都是 *M-200*，或全部是 *Panorama* 虛擬設備。

© 2019 Palo Alto Networks, Inc.

只有當每一個日誌收集器都具有相同數量的日誌磁碟時，日誌備援才可用。若要將磁碟新增至日誌收集器，請參閱增加 M-Series 設備的儲存容量。

STEP 1 | 從 Panorama 管理移除日誌收集器。

1. 選取 **Panorama** > **Collector Groups**（收集器群組），編輯包含您將移動的日誌收集器的收集器群組。
2. 在 Collector Group Members（收集器群組成員）部分中，**Add**（新增）日誌收集器。
3. 選取 **Device Log Forwarding**（裝置日誌轉送），在 Log Forwarding Preferences（日誌轉送偏好設定）清單中，針對指派給您將移動的日誌收集器的各組防火牆，執行下列步驟：
   1. 在設備欄中，按一下指派至日誌收集器的防火牆連結。
   2. 在 Collectors（收集器）部分中，選取並 **Delete**（刪除）日誌收集器。

      若要重新指派防火牆，*Add*（新增）將轉送日誌的新日誌收集器。
   3. 按兩下 **OK**（確定）儲存您的變更。
4. 選取 **Panorama** > **Managed Collectors**（受管理的收集器），然後選取並 **Delete**（刪除）您將移動的日誌收集器。

STEP 2 | 設定收集器群組。

新增日誌收集器至其新收集器群組並指派防火牆至日誌收集器。

當您將變更推送至收集器群組設定時，*Panorama* 會開始將日誌重新散佈至日誌收集器。每 *TB* 日誌的此程序均需要數小時。重新分配程序期間會降低最大日誌記錄速率。在 *Panorama* > *Collector Groups*（收集器群組）頁面中，*Log Redistribution State*（日誌重新散佈狀態）欄會以百分比指出程序的完成狀態。

STEP 3 | 設定日誌轉送至 Panorama 您設定的新收集器群組。

STEP 4 | 選取 **Commit**（提交）> **Commit and Push**（提交並推送），將您的變更提交至 Panorama，並將變更推送至裝置群組、範本和收集器群組。

從收集器群組移除防火牆

如果您使用傳統模式的 Panorama 虛擬設備來管理專用日誌收集器，您可以選擇將防火牆日誌轉送至 Panorama，而非轉送至日誌收集器。在此情況下，您必須從收集器群組中移除防火牆；防火牆將會自動將其日誌轉送至 Panorama。

若要在防火牆上暫時移除日誌轉送偏好設定清單，您可以在防火牆上使用 *CLI* 刪除它。然而，您必須在 *Panorama* 的收集器群組設定中，移除指定的防火牆。否則，您下一次將變更推送至收集器群組時，防火牆會重新設定為將日誌傳送至指派的日誌收集器。

STEP 1 | 選取 **Panorama** > **Collector Groups**（收集器群組），然後編輯收集器群組。

STEP 2 | 選取 **Device Log Forwarding**（裝置日誌轉送），在 Devices（裝置）清單中按一下防火牆，**Modify**（修改）Devices（裝置）清單，清除防火牆的核取方塊，然後按一下 **OK**（確定）三次。

STEP 3 | 選取 **Commit**（提交）> **Commit and Push**（提交並推送），然後將您的變更 **Commit and Push**（提交並推送）至 Panorama 和您從中移除防火牆的收集器群組。

© 2019 Palo Alto Networks, Inc.

設定日誌轉送至 Panorama

依預設，每個防火牆會將日誌檔儲存在本機，且無法顯示其他防火牆上的日誌。因此，若要在所有防火牆監控的網路活動上達到全域可見度，您必須將所有防火牆日誌轉送至 Panorama，並使用 Panorama 增強可見度。如果組織中的某些團隊能夠透過僅監控與其業務相關的日誌提高效率，您可以根據任何日誌屬性（例如威脅類型或來源使用者）建立轉送篩選器。例如，負責調查惡意軟體攻擊的安全性操作分析員可能僅對屬性設定為 wildfire-virus 的威脅日誌感興趣。

下列步驟說明如何使用 Panorama 範本和裝置群組，以設定多個防火牆來轉送日誌。

如果 *Panorama* 要管理 *PAN-OS 7.0* 之前的防火牆執行軟體版，指定一個 *WildFire*® 伺服器，從該伺服器中，*Panorama* 可以收集那些防火牆提交的 *WildFire* 樣本分析資訊。*Panorama* 使用該資訊完成 *WildFire* 提交日誌，該日誌是 *PAN-OS 7.0* 中引入的缺失欄位值。執行早期版本的防火牆不會填入這些欄位。若要指定伺服器，選取 *Panorama* > *Setup*（設定）> *WildFire*，編輯一般設定，然後輸入 *WildFire Server*（*WildFire* 伺服器）名稱。預設為 *wildfire-public-cloud*，這是位於美國的 *WildFire* 雲。

您還可以將防火牆日誌轉送至外部服務（例如 *syslog* 伺服器）。詳細資訊，請參閱日誌轉送選項。

STEP 1 | 為將要轉送日誌的防火牆新增裝置群組。

Panorama 需要一個裝置群組來向防火牆推送日誌轉送設定檔。建立新裝置群組或將防火牆指派至現有裝置群組。

STEP 2 | 為將要轉送日誌的防火牆新增範本。

Panorama 需要一個範本來向防火牆推送日誌設定。建立新範本或將防火牆指派至現有範本。

STEP 3 | 建立日誌轉送設定檔。

設定檔中定義了流量、威脅、WildFire 提交、URL 篩選、資料篩選、通道及驗證日誌的目的地。

1. 選取 **Objects**（物件）> **Log Forwarding**（日誌轉送）並選取會轉送日誌的防火牆 **Device Group**（設備群組），然後 **Add**（新增）設定檔。
2. 輸入用來識別日誌轉送設定檔的 **Name**（名稱）。
3. **Add**（新增）一個或多個比對清單設定檔。

   這些設定檔指定了日誌查詢篩選器、轉送目的地以及標記等自動動作。對於每個比對清單設定檔：

   1. 輸入用來識別設定檔的 **Name**（名稱）。
   2. 選取 **Log Type**（日誌類型）。
   3. 在 **Filter**（篩選器）下拉式清單中選取 **Filter Builder**（篩選器產生器）。指定下列選項，然後 **Add**（篩選器產生器）每項查詢：

      Connector（連接器）邏輯（And/Or）

      日誌 **Attribute**（屬性）

      Operator（運算子），用於定義包含或排除邏輯

      用於比對的查詢屬性 **Value**（值）
   4. 選取 **Panorama**。
4. 按一下 **OK**（新增）以儲存日誌轉送設定檔。

STEP 4 | 將日誌轉送設定檔指派給原則規則和網路區域。

安全性、嚴重和 DoS 保護規則支援日誌轉送。在此範例中，將設定檔指派給安全性規則。

© 2019 Palo Alto Networks, Inc.

針對將觸發日誌轉送的每個規則執行下列步驟：

1. 選取規則庫（例如，**Policies**（原則）> **Security**（安全性）> **Pre Rules**（預先規則）），並選取將轉送日誌的防火牆的 **Device Group**（裝置群組），然後編輯規則。
2. 選取 **Actions**（動作）頁籤，然後選取所建立的 **Log Forwarding**（日誌轉送）設定檔。
3. 將 **Profile Type**（設定檔類型）設定為 **Profiles**（設定檔）或 **Group**（群組），然後選取相應的安全性設定檔或 **Group Profile**（群組設定檔）以觸發日誌產生和轉送：
   - 威脅日誌—流量必須符合指派給規則的任何安全性設定檔。
   - WildFire 日誌—流量必須符合指派給規則的 WildFire 分析設定檔。
4. 對於流量日誌，選取 **Log At Session Start**（開始時的日誌）及/或 **Log At Session End**（結束時的日誌）。
5. 按一下 **OK**（確定）來儲存規則。

STEP 5 | 設定系統日誌、設定日誌、User-ID™ 日誌和 HIP 比對日誌的目的地。



Panorama 會根據其收到的防火牆日誌而非彙總來自防火牆的關聯日誌，來產生關聯日誌。

1. 選取 **Device**（設備）> **Log Settings**（日誌設定）並選取會轉送日誌的防火牆 **Template**（範本）。
2. 對於防火牆將轉送的每種日誌類型，請參閱步驟新增一個或多個比對清單設定檔。

STEP 6 | （僅限 PA-7000 Series 防火牆）設定日誌卡介面以執行日誌轉送。

當您將其中一個 PA-7000 Series Network Processing Card（網路處理卡 - NPC）上的資料連接埠設定為日誌卡介面時，防火牆會自動開始使用此介面，將日誌轉送至您設定的日誌記錄目的地，並轉送檔案供 WildFire 分析。確保您設定的介面可以到達日誌轉送目的地，以及 WildFire 雲端、WildFire 設備或兩者。



因為 *PA-7000 Series* 防火牆現在可以將日誌轉送至 *Panorama*，*Panorama* 不會再將其管理的 *PA-7000 Series* 防火牆視為日誌收集器。如果您尚未設定 *PA-7000 Series* 防火牆將日誌轉送至 *Panorama*，則受管理的 *PA-7000 Series* 防火牆產生的所有日誌，只有從本機防火牆才能看見，從 *Panorama* 看不到。如果您尚無日誌轉送基礎結構能夠處理來自 *PA-7000 Series* 防火牆的日誌記錄速率和數量，從 *PAN-OS 8.0.8* 開始，您可以讓 *Panorama* 在監控日誌時直接查詢 *PA-7000 Series* 防火牆。若要使用此功能，*Panorama* 和 *PA-7000 Series* 防火牆都必須執行 *PAN-OS 8.0.8* 或更新版本。請從 *Panorama CLI* 輸入下列命令，讓 *Panorama* 能夠直接查詢 *PA-7000 Series* 防火牆：

```
> debug reportd send-request-to-7k yes
```

執行此命令之後，您就能夠在 *Panorama Monitor*（監控）頁籤上檢視受管理 *PA-7000 Series* 防火牆的日誌。此外，對於所有受管理的裝置，您還可以選取 *Remote Device Data*（遠端裝置資料）作為 *Data Source*（資料來源），以產生包含 *PA-7000 Series* 日誌資料的報告。如果您後來決定讓 *PA-7000 Series* 防火牆將日誌轉送至 *Panorama*，則必須先使用 ***debug reportd send-request-to-7k no*** 命令來停用此選項。

1. 選取 **Network**（網路）> **Interfaces**（介面）> **Ethernet**（乙太網路），並選取將轉送日誌的防火牆的 **Template**（範本），然後 **Add Interface**（新增介面）。
2. 選取 **Slot**（插槽）和 **Interface Name**（介面名稱）。
3. 將 **Interface Type**（介面名稱）設定為 **Log Card**（日誌卡）。
4. 輸入 **IP Address**（IP 位址）、**Default Gateway**（預設閘道）和（僅適用於 IPv4）**Netmask**（網路遮罩）。
5. 選取 **Advanced**（進階），然後指定 **Link Speed**（連結速度）、**Link Duplex**（連結雙工）與 **Link State**（連結狀態）。

© 2019 Palo Alto Networks, Inc.

這些欄位預設為 *auto*，其指定防火牆根據連接自動決定值。但是，任何連接的最小建議 *Link Speed*（連結速度）為 *1000 (Mbps)*。

6. 按一下 **OK**（確定）儲存您的變更。

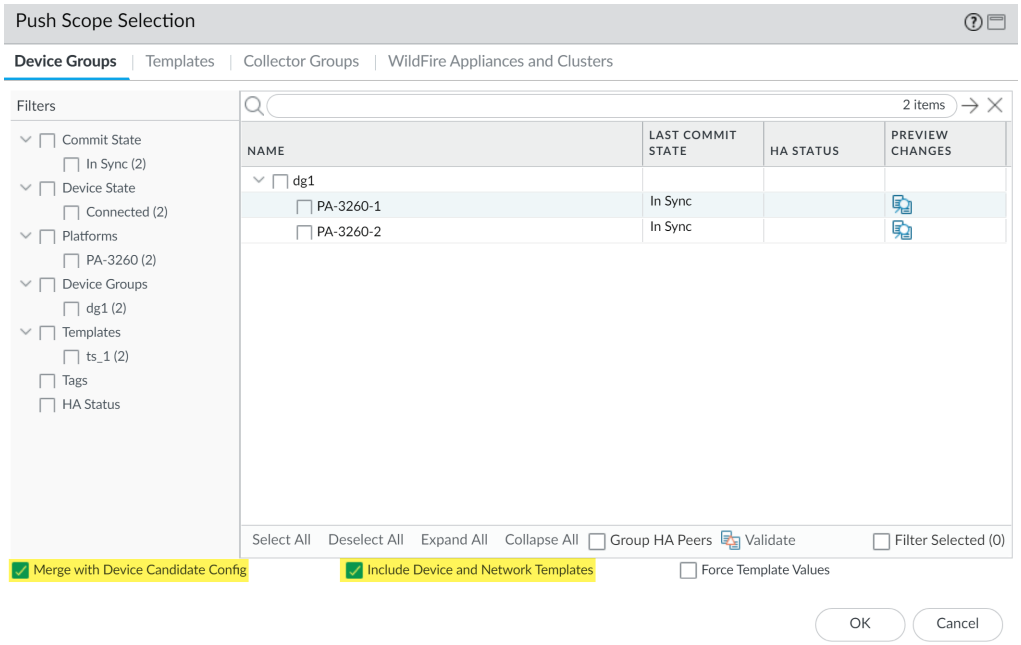
STEP 7 | 設定 Panorama 接收日誌。

如果要將日誌轉送至傳統模式的 *Panorama* 虛擬設備，您可以跳過此步驟。

1. 對於將接收日誌的各日誌收集器，設定受管理收集器。
2. 設定收集器群組，將防火牆指派給特定日誌收集器來轉送日誌。

STEP 8 | 提交組態變更。

1. 選取 **Commit**（提交）> **Commit and Push**（提交並推送），然後 **Edit Selections**（編輯選擇）。
2. 選取 **Merge with Device Candidate Config**（與裝置候選設定合併）、**Include Device and Network Templates**（包含裝置與網路範本）並按一下 **OK**（確定）。



3. **Commit and Push**（提交並推送），將您的變更提交至 Panorama，並將變更推送至裝置群組、範本和收集器群組。
4. 確認日誌轉送至 Panorama以確認設定成功。

若要變更防火牆將日誌傳送至 *Panorama* 時所使用的日誌轉送模式，您可以修改日誌轉送及緩衝預設值。您還可以管理日誌和報告儲存配額和到期日期。

© 2019 Palo Alto Networks, Inc.

設定 Syslog 轉送至外部目的地

如果是具有高日誌產生率的部署，則可以透過乙太網路介面轉送 syslog，以防止日誌丟失並減少管理介面上的負載，從而最佳化管理操作。

僅使用 Panorama 模式或日誌收集器模式的 Panorama™ 管理伺服器才支援使用乙太網路介面進行 syslog 轉送。此外，無論 Panorama 處於 Panorama 模式還是日誌收集器模式，您都只能在一個介面上啟用 syslog 轉送。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 設定受管理收集器。

STEP 3 | 設定收集器群組。

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。但是，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。對於這兩種設定，您都需要指派防火牆到日誌收集器以用於日誌轉送。

STEP 4 | 設定系統日誌伺服器設定檔。

1. 選取 **Panorama** > **Server Profiles**（伺服器設定檔）> **Syslog**，並 **Add**（新增）新的 syslog 伺服器設定檔。
2. 輸入 syslog 伺服器設定檔的 **Name**（名稱）。
3. 對於每個 syslog 伺服器，**Add**（新增）Panorama 或專用日誌收集器與之連線所需的資訊：
   - 名稱—syslog 伺服器的唯一名稱。
   - **Syslog** 伺服器—系Syslog 伺服器的 IP 位址或完全合格網域名稱 (FQDN)。
   - 傳輸—選取 **UDP**、**TCP** 或 **SSL** 作為與 syslog 伺服器的通訊方法。
   - 連接埠— 轉送 syslog 訊息時使用的連接埠號碼（預設為連接埠 514 上的 UDP）；您必須在 Panorama 和專用日誌收集器上使用相同的連接埠號碼。
   - 格式—選取要使用的 syslog 訊息格式：**BSD**（預設值）或 **IETF**。傳統上，UDP 上為 **BSD** 格式，TCP 或 SSL 上則為 **IETF** 格式。
   - 裝置—選取 syslog 標準值（預設值是 **LOG_USER**），以在 syslog 伺服器實作中計算優先順序 (PRI) 欄位。選取對應如何將 PRI 欄位用於管理 syslog 的值。
4. （選用）要自訂 Panorama 或專用日誌收集器傳送的 syslog 訊息的格式，請選取 **Custom Log Format**（自訂日誌格式）。如需為各種日誌類型建立自訂格式的詳細資訊，請參閱《常見事件格式組態指南》。
5. 按一下 **OK**（確定）以儲存 syslog 伺服器設定檔。

STEP 5 | 設定乙太網路介面用於轉送 syslog。

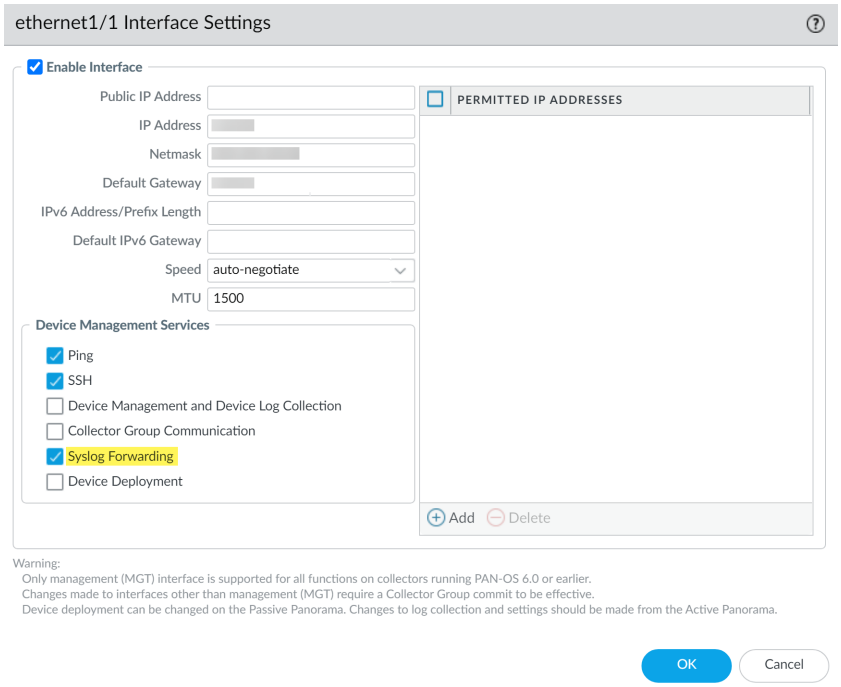
依預設，syslog 轉送在管理介面上啟用，且一次僅在一個介面上受支援。

- 在 Panorama Web 介面的本機日誌收集器上設定乙太網路介面。
  1. 選取 **Panorama** > **Setup**（設定）> **Interfaces**（介面），然後選取乙太網路介面。
  2. 啟用介面。
  3. 根據需要設定乙太網路介面。
  4. 在「裝置管理服務」區段中，啟用 **Syslog Forwarding**（**Syslog** 轉送）。
  5. 選取 **Yes**（是）以確認您的 syslog 轉送變更。

     只能在本機日誌收集器的一個乙太網路介面上進行轉送。
  6. 按一下 **OK**（確定）儲存您的變更。

© 2019 Palo Alto Networks, Inc.

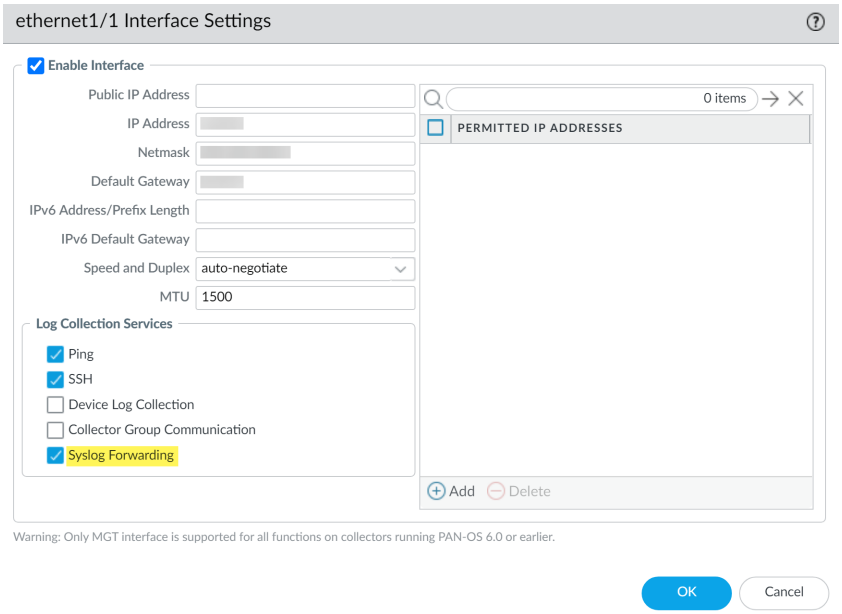
7. **Commit**（提交），然後 **Commit and Push**（提交並推送）設定變更。



- 在專用日誌收集器上設定乙太網路介面。
  1. 選取 **Panorama** > **Managed Collectors**（受管理的收集器），然後選取專用日誌收集器。
  2. 啟用介面。
  3. 根據需要設定乙太網路介面。
  4. 在「日誌收集服務」區段中，啟用 **Syslog Forwarding**（**Syslog** 轉送）。
  5. 選取 **Yes**（是）以確認您的 syslog 轉送變更。

     只能在專用日誌收集器的一個乙太網路介面上進行轉送。
  6. 按一下 **OK**（確定）儲存您的變更。
  7. **Commit**（提交），然後 **Commit and Push**（提交並推送）設定變更。

© 2019 Palo Alto Networks, Inc.



- 在 Panorama CLI 的本機日誌收集器或專用日誌收集器上設定乙太網路介面。

  要成功設定透過 CLI 的乙太網路介面進行 syslog 轉送，必須首先在管理介面上停用 syslog 轉送，然後在 CLI 的乙太網路介面上啟用 syslog 轉送。Panorama 不會自動停用透過管理介面進行的 syslog 轉送，如果您同時在管理和乙太網路介面上啟用了 syslog 轉送，syslog 轉送將會繼續透過管理介面進行。

  1. 登入 Panorama CLI
  2. 在管理介面上停用 syslog 轉送：

     ```
     admin@Panorama> configure
     ```

     ```
     admin@Panorama> set log-collector <Log Collector Serial Number>
      deviceconfig system service disable-syslog-forwarding yes
     ```

  3. 在乙太網路介面上啟用 syslog 轉送：

     ```
     admin@Panorama> configure
     ```

     ```
     admin@Panorama> set log-collector <Log Collector Serial Number>
      deviceconfig system eth<Interface Number>  service disable-syslog-
     forwarding no
     ```

     ```
     admin@Panorama> commit
     ```

  4. 提交設定變更：

     ```
     admin@Panorama> run commit-all log-collector-config log-collector-
     group <Collector Group name>
     ```

STEP 6 | 設定日誌轉送至 Panorama。

STEP 7 | 設定從 Panorama 到 syslog 伺服器的 syslog 轉送。

© 2019 Palo Alto Networks, Inc.

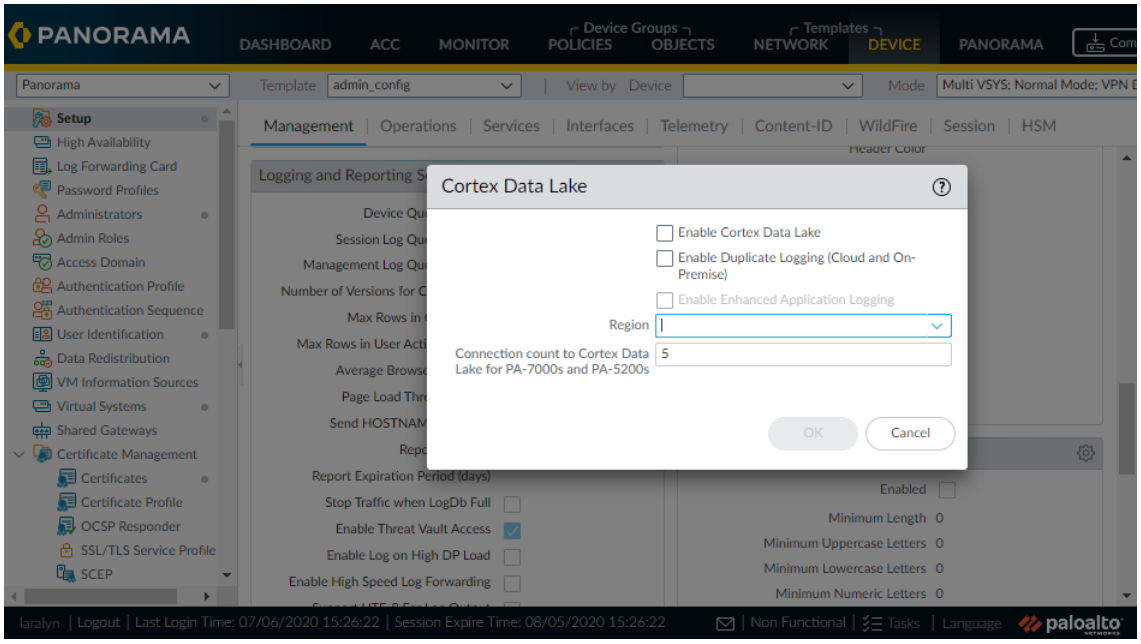
轉送日誌至 Cortex 資料湖

Cortex Data Lake（Cortex 資料湖）是 Palo Alto Networks 的雲端日誌記錄基礎設施。在您可以設定受管理的防火牆，以傳送日誌到 Cortex Data Lake（Cortex 資料湖，以前稱為日誌記錄服務）之前，您需要為部署中的日誌數量購買授權，並安裝雲端服務外掛程式。如果已經擁有內部部署日誌收集器，則可使用 Cortex Data Lake（Cortex 資料湖）以補充及增強已有的設定。

STEP 1 | 安裝 Panorama 外掛程式。

STEP 2 | 設定防火牆以傳送日誌到 Cortex Data Lake（Cortex 資料湖）。

對於執行 PAN-OS 8.1 或更新版本的防火牆，您可以選擇傳送日誌到 Cortex Data Lake（Cortex 資料湖）與 Panaroma 上，並在您選取 **Enable Duplicate Logging (Cloud and On-Premise)**（啟用複製日誌記錄（雲端與內部部署））時，傳送到內部部署日誌收集設定上。在啟用時，屬於選定範本的防火牆將在這兩個地方都儲存一份日誌複本。您可以選取 **Enable Duplicate Logging (Cloud and On-Premise)**（啟用複製日誌記錄（雲端與內部部署））或 **Enable Cortex Data Lake**（啟用 **Cortex** 資料湖），但不能兩者皆選取。



© 2019 Palo Alto Networks, Inc.

確認日誌轉送至 Panorama

一旦設定將日誌轉送至 Panorama 或 Cortex Data Lake（Cortex 資料湖）後，確認日誌轉送至 Panorama，以測試您的設定是否成功。

在設定日誌轉送至日誌收集器後，受管理的防火牆打開至所有設定日誌收集器的 TCP 連線。這些連線每六十 (60) 秒即超時，並表示防火牆失去與日誌收集器的連線。當您在 受支援的乙太網路介面 設定日誌轉送至本機或專用日誌收集器時，防火牆流量日誌顯示 `incomplete`（不完整）工作階段，儘管防火牆已成功連線至日誌收集器。如果您在管理連接埠上設定日誌轉發，產生顯示 `incomplete`（不完整）工作階段的無流量日誌。顯示 `incomplete`（不完整）工作階段的流量日誌由 PA-5200 和 PA-7000 系列防火牆以外的所有防火牆產生。

STEP 1 | 存取防火牆 CLI。

STEP 2 | 如果您設定日誌收集器，確認每道防火牆具有日誌轉送偏好設定清單。

```
> show log-collector preference-list
```

如果收集器群組只有一個日誌收集器，則將會有類似於以下的輸出：

```
Forward to all: No
Log collector Preference List
Serial Number: 003001000024
IP Address: 10.2.133.48
IPV6 Address: unknown
```

STEP 3 | 確認各防火牆正在轉送日誌。

```
> show logging-status
```

對於成功轉送，輸出表示日誌轉送代理程式使用中。

- 若為 Panorama 虛擬設備，代理程式為 `Panorama`。
- 對於 M 系列設備，代理程式為 `Log Collector`（日誌收集器）。
- 若為 Cortex Data Lake（Cortex 資料湖），代理程式為 `Log Collection Service`（日誌收集服務）。還有

```
'Log Collection log forwarding agent' is active and connected
 to <IP_address>.
```

STEP 4 | 檢視平均日誌記錄速率。顯示的速率為最後五分鐘的平均日誌數/秒。

- 如果日誌收集器接收日誌，存取 Panorama web 介面，選取 **Panorama** > **Managed Collectors**（受管理的收集器）並按一下最右欄的 **Statistics**（統計資料）連結。
- 如果傳統模式的 Panorama 虛擬設備接收日誌，請存取 Panorama CLI 並執行下列命令：**debug log-collector log-collection-stats show incoming-logs**ts show incoming-logs



此命令也可用於 *M-Series* 設備。

© 2019 Palo Alto Networks, Inc.

修改日誌轉送及緩衝預設值

您可以定義防火牆將日誌傳送至 Panorama 時所使用的日誌轉送模式，並且在高可用性 (HA) 設定中設定時，指定哪個 Panorama 端點可接收日誌。若要存取這些選項，請選取 **Panorama** > **Setup**（設定）> **Management**（管理），編輯記錄日誌與報告設定，然後選取 **Log Export and Reporting**（日誌匯出與報告）。

- 在防火牆上定義日誌轉送模式：防火牆可在緩衝的日誌轉送模式或即時模式日誌轉送模式中，將日誌轉送給 Panorama（專屬於 M-Series 設備和 Panorama 虛擬設備）。

日誌記錄選項	說明
（最佳做法）從裝置轉送的已緩衝記錄 預設值：已啟用	允許每一個受管理防火牆緩衝日誌，並以 30 秒間隔將日誌傳送至 Panorama（使用者無法設定）。 當防火牆失去與 Panorama 的連線時，緩衝的日誌轉送非常有用。防火牆會將日誌項目緩衝至其本機硬碟，並保留指標來記錄傳送給 Panorama 的最後一個日誌項目。還原連線後，防火牆將繼續從離開處轉送日誌。 緩衝可用的磁碟空間取決於防火牆型號的日誌儲存配額，以及擱置延緩的日誌量。如果防火牆長期中斷連線，且最後一個轉送的日誌待處理的狀況中，會在重新連線時，將其本機硬碟的所有日誌轉送至 Panorama。如果耗盡防火牆本機硬碟的可用空間，則將刪除最早的項目以允許新事件的日誌記錄。
設備的即時模式日誌轉送 清除 **Buffered Log Forwarding from Device**（從裝置轉送已緩衝的記錄）核取方塊時會啟用此選項。	在即時模式中，受管理防火牆會在防火牆上記錄每個日誌交易的同時，將該交易傳送至 Panorama。

- 在部署於高可用性 (HA) 設定中的傳統模式 Panorama 虛擬設備上，定義日誌轉送偏好設定：
  - 將日誌記錄至虛擬磁碟時，只允許將日誌記錄至主要 Panorama 對等上的本機磁碟。依預設，HA 設定中的兩個 Panorama 端點都會接收日誌。

    對於 *5200* 和 *7000* 系列防火牆，僅主動端點接收日誌。
  - 將日誌記錄至 NFS 時（僅限 ESXi 伺服器），允許防火牆僅將最近產生的日誌傳送至次要 Panorama 對等（容錯移轉後會升級為主要）。

日誌記錄選項	專屬於	說明
僅限本地磁碟的使用中主要日誌 預設值：已停用	傳統模式 Panorama 虛擬設備，此設備將日誌記錄至虛擬磁碟且部署於高可用性 (HA) 設定中。	只允許您設定主要 Panorama 對等將日誌儲存至本機磁碟。
轉換為主要時僅取得新記錄 預設值：已停用	傳統模式的 Panorama 虛擬設備，此設備掛載至 Network File System（網路檔案系統 -	藉助 NFS 日誌記錄，當您在高可用性設定中設定 Panorama 伺服器配對時，只有主要 Panorama 端點會安裝 NFS 資料

© 2019 Palo Alto Networks, Inc.

日誌記錄選項	專屬於	說明
	NFS）資料存放、在 VMware ESXi 伺服器上執行，且部署於 HA 設定中	存放。因此，防火牆只能將日誌傳送至主要 Panorama 端點，從而寫入 NFS 資料存放。 HA 故障復原發生時，管理員可使用**Get Only New Logs on Convert to Primary**（轉換為主要時僅取得新記錄）選項來設定受管理防火牆，僅將最近產生的日誌傳送至 Panorama。向主要提示主動次要 Panorama 的優先順序時會觸發此事件，而且它會開始將日誌記錄至 NFS。之所以會啟用此行為，通常是為了在經過一段長時間後還原 Panorama 連線時，防止防火牆傳送大量的緩衝日誌。

© 2019 Palo Alto Networks, Inc.

設定日誌從 Panorama 轉送至外部目的地

Panorama 可讓您將日誌轉送至外部服務，包括 syslog、電子郵件、SNMP 設陷和基於 HTTP 的服務。使用外部服務可讓您收到重要事件的警示、透過專用的長期儲存空間封存系統上的監控資訊，以及與第三方安全性監控工具整合。除了轉送防火牆日誌，您還可以轉送 Panorama 管理伺服器和日誌收集器所產生的日誌。轉送日誌的 Panorama 管理伺服器或日誌收集器會將日誌轉換成適合目的地的格式（syslog 訊息、電子郵件通知、SNMP 設陷或 HTTP 承載）。



如果 *Panorama* 管理伺服器是傳統模式的 *Panorama* 虛擬設備，則會將日誌轉換並轉送至外部服務，而不會使用日誌收集器。

您也可以將日誌直接從防火牆轉送至外部服務：請參閱日誌轉送選項。

在運行 *Panorama 5.1* 或之前版本的 *Panorama* 虛擬設備上，您可以使用來自 CLI 安全複製 (SCP) 命令以匯出整個日誌資料庫至 *SCP* 伺服器，並將其匯入至另一個 *Panorama* 虛擬設備。執行 *Panorama 6.0* 或更新版本的 *Panorama* 虛擬設備，以及執行任何版本的 *M-Series* 設備，都不支援這些選項，因為這些型號上的日誌資料庫太大，難以匯出或匯入。

若要將日誌轉送至外部服務，首先，請設定防火牆將日誌轉送至 Panorama。接著，您必須設定伺服器設定檔，以定義 Panorama 和日誌收集器如何連接至服務。最後，再將伺服器設定檔指派給 Panorama 的日誌設定和收集器群組。

STEP 1 | 設定防火牆以轉送日誌至 Panorama。

設定日誌轉送至 Panorama。

STEP 2 | 針對每個將收到日誌資訊的外部服務設定伺服器設定檔。

1. 選取 **Panorama** > **Server Profiles**（伺服器設定檔）並選取接收日誌資料的伺服器類型：**SNMP Trap**（**SNMP** 設陷）、**Syslog** 或 **Email**（電子郵件）或 **HTTP**。
2. 設定伺服器設定檔：
   - 設定 SNMP 設陷伺服器設定檔。關於 SNMP 如何用於 Panorama 和日誌收集器的詳細資訊，請參閱 SNMP 支援。
   - 設定系統日誌伺服器設定檔。如果系統日誌伺服器要求用戶端驗證，使用**Panorama** > **Certificate Management**（憑證管理）> **Certificates**（憑證）頁面以建立 SSL 上系統日誌安全通訊的憑證。
   - 設定電子郵件伺服器設定檔。
   - 設定 HTTP 伺服器設定檔。

STEP 3 | 設定下列項目的目的地：

- Panorama 管理伺服器和日誌收集器產生的日誌。
- 傳統模式的 Panorama 虛擬設備所收集的防火牆日誌。

1. 選取**Panorama** > **Log Settings**（日誌設定）。
2. 為每種日誌類型 **Add**（新增）一個或多個比對清單設定檔。

   這些設定檔指定了日誌查詢篩選器、轉送目的地以及標記等自動動作。對於每個比對清單設定檔：

   1. 輸入用來識別設定檔的 **Name**（名稱）。
   2. 選取 **Log Type**（日誌類型）。
   3. 在 **Filter**（篩選器）下拉式清單中選取 **Filter Builder**（篩選器產生器）。指定下列選項，然後 **Add**（篩選器產生器）每項查詢：

      Connector（連接器）邏輯（And/Or）

      日誌 **Attribute**（屬性）

© 2019 Palo Alto Networks, Inc.

Operator（運算子），用於定義包含或排除邏輯

用於比對的查詢屬性 **Value**（值）

4. **Add**（新增）您為每個外部服務設定的伺服器設定檔。
5. 按一下 **OK**（確定）來儲存設定檔。

STEP 4 | 為日誌收集器接收的防火牆日誌設定目的地。



各收集器群組可轉送日誌至不同的目的地。如果日誌收集器位於高可用性 *(HA)* 配對的 *Panorama* 管理伺服器本機，您必須登入各 *HA* 對等，以設定其收集器群組的日誌轉送。

1. 選取 **Panorama** > **Collector Groups**（收集器群組），並編輯接收防火牆日誌的收集器群組。
2. （選用，僅限 SNMP 設陷轉送）選取 **Monitoring**（監控）並進行 SNMP 設定。
3. 選取 **Collector Log Forwarding**（收集器日誌轉送）並在必要時 **Add**（新增）設定的比對清單設定檔。
4. 按一下 **OK**（確定）以儲存對收集器群組所做的變更。

STEP 5 | （僅限 syslog 轉送）如果 syslog 伺服器需要用戶端驗證，且防火牆會將日誌轉送至專用日誌收集器，請指派憑證來透過 SSL 保護 syslog 通訊。

針對每個專用日誌收集器執行下列步驟：

1. 選取 **Panorama** > **Managed Collectors**（受管理的收集器），再編輯日誌收集器。
2. 選取 **Certificate for Secure Syslog**（安全 **Syslog** 的憑證），然後按一下 **OK**（確定）。

STEP 6 | （僅限 SNMP 設陷轉送）讓您的 SNMP 管理程式可以解譯設陷。

載入支援的 MIB，如有必要就編譯。如需特定步驟，請參閱 SNMP 管理員文件。

STEP 7 | 提交並驗證您的設定變更。

1. 選取 **Commit**（提交）> **Commit and Push**（提交並推送），將您的變更提交至 Panorama，並將變更推送至裝置群組、範本和收集器群組。
2. 確認外部服務正在接收日誌資訊：
   - 電子郵件伺服器—確認指定的收件者已透過電子郵件通知收到日誌。
   - **Syslog** 伺服器—請參閱 syslog 伺服器的文件，以確認其已透過 syslog 訊息收到日誌。
   - **SNMP** 管理程式—請參閱 SNMP 設陷的文件，以確認其已透過 SNMP 設陷收到日誌。
   - **HTTP** 伺服器—確認基於 HTTP 的伺服器收到正確承載格式的日誌。

© 2019 Palo Alto Networks, Inc.

日誌收集部署

下列主題說明如何在大多數的一般部署中設定日誌收集。開始之前，請根據目前和未來的記錄日誌需求，以規劃 Panorama 部署。

在這些主題中的部署全都描述高可用性 *(HA)* 設定中的 *Panorama*。*Palo Alto Networks* 建議使用 *HA*，因為其允許未作為設定備份儲存的部分元件自動恢復（當伺服器發生故障時）。在 *HA* 部署中，*Panorama* 管理伺服器只支援主動/被動設定。

- 部署具備專用日誌收集器的 Panorama
- 部署具備本機日誌收集器的 Panorama M-Series 設備
- 部署具備本機日誌收集器的 Panorama 虛擬設備
- 部署具備本機日誌收集的傳統模式 Panorama 虛擬設備

部署具備專用日誌收集器的 Panorama

下圖說明分散式日誌收集部署中的 Panorama。在這些範例中，Panorama 管理伺服器包含兩個 Panorama 模式的 M-Series 或 Panorama 虛擬設備，被部署在主動/被動高可用性 (HA) 組態中。防火牆會將日誌傳送至專用日誌收集器（日誌收集器模式中的 M-Series 或 Panorama 虛擬設備）。如果防火牆以超過 10,000 個日誌/秒的速率產生日誌，則此為建議的設定。

如果您要將一個以上的日誌收集器指派給收集器群組，請參閱警告有收集器群組擁有多個日誌收集器，瞭解需求、風險和建議的緩和措施。

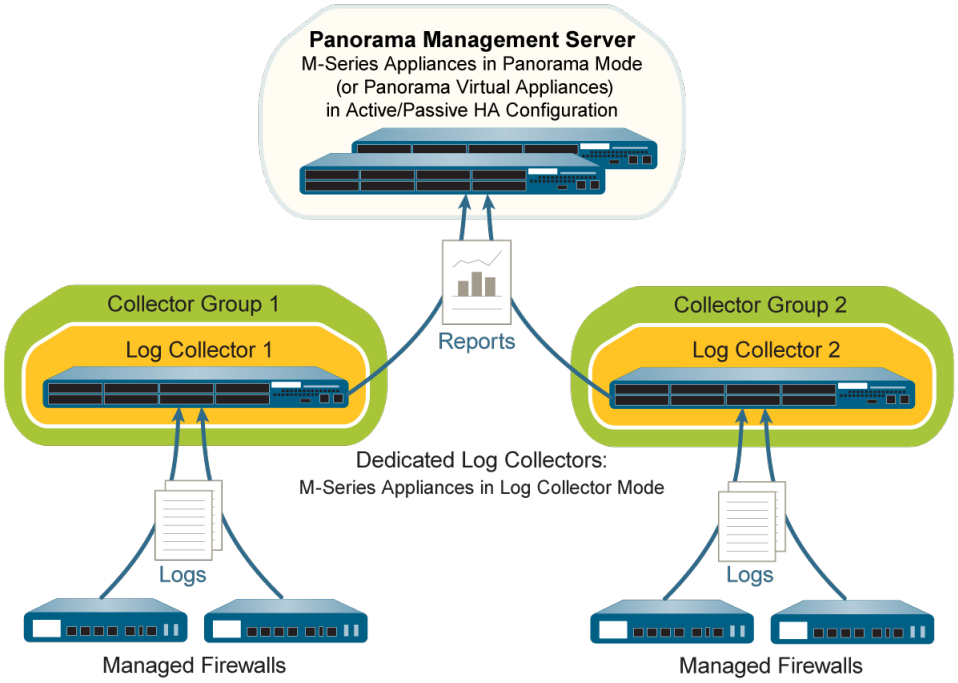


圖 17: 每個收集器群組一個專用日誌收集器

© 2019 Palo Alto Networks, Inc.

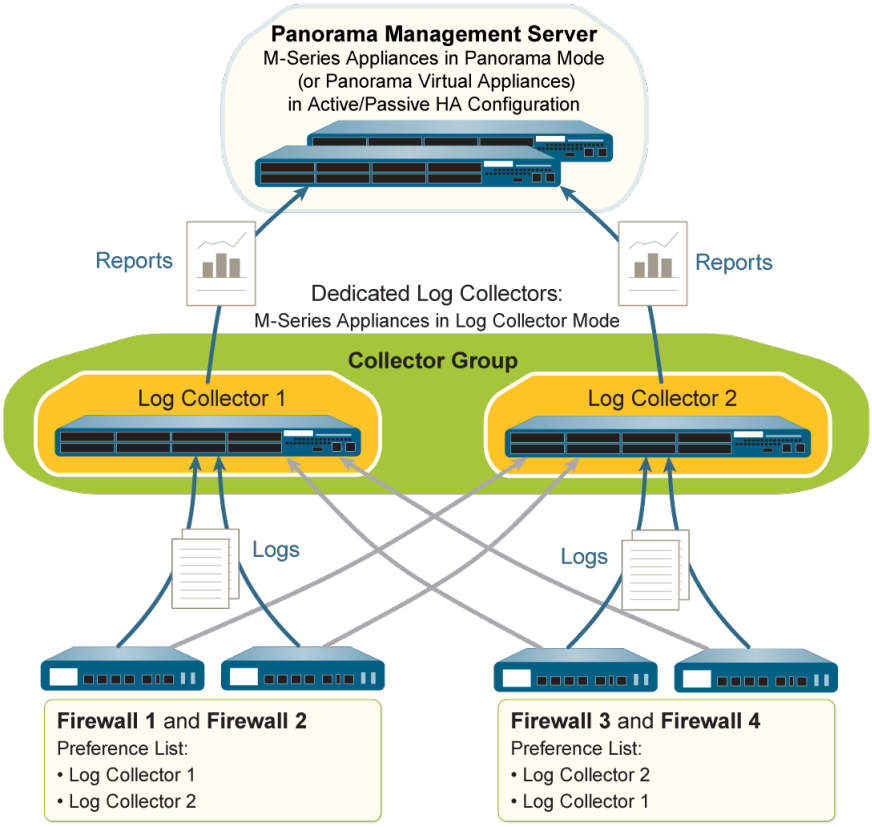


圖 18: 每個收集器群組多個專用日誌收集器

執行下列步驟可部署具備專用日誌收集器的 Panorama。略過任何您已執行的步驟（例如初始設定）。

STEP 1 | 執行 Panorama 管理伺服器（虛擬設備或 M-Series 設備）與專用日誌收集器的初始設定。

對於各 M-Series 設備：

1. 在機架中安裝 M-Series 設備。請參閱 M-Series 硬體參考指南的指示。
2. 執行 M-Series 設備的初始設定。

Palo Alto Networks 建議將管理 *(MGT)* 介面保留為 *Panorama* 的管理存取，並準備獨立的 M-Series 設備介面專供其他 *Panorama* 服務使用。

3. 設定每個陣列。為了使 RAID 磁碟可用於記錄日誌，需要完成此工作。您也可以選擇新增磁碟以增加 M-Series 設備的儲存容量。
4. 註冊 Panorama 並安裝授權。
5. 安裝 Panorama 的內容與軟體更新。

對於每個虛擬設備（若有的話）：

1. 安裝 Panorama 虛擬設備。
2. 執行 Panorama 虛擬設備的初始設定。
3. 註冊 Panorama 並安裝授權。
4. 安裝 Panorama 的內容與軟體更新。

對於 Panorama 管理伺服器（虛擬設備或 M-Series 設備），您還必須在 Panorama 上設定 HA。

STEP 2 | 在每個用作專用日誌收集器的 Panorama 管理伺服器上，從 Panorama 模式切換至日誌收集器模式。

© 2019 Palo Alto Networks, Inc.

切換 *M-Series* 或 *Panorama* 虛擬設備模式，刪除任何現有日誌資料並刪除除管理存取設定外的所有組態。切換後，*M-Series* 或 *Panorama* 虛擬設備仍保有 *CLI* 存取權，但會失去 *Web* 介面存取權。

1. 以下列其中一種方式連線至 Panorama：
   - （僅限 M-Series 設備）將序列纜線從電腦連接至 M-Series 設備的主控台連接埠。然後使用終端機模擬軟體 (9600-8-N-1) 進行連線。
   - 使用終端機模擬軟體（例如 PuTTY），針對在初始組態期間指定給 Panorama 管理伺服器的 MGT 介面的 IP 位址開啟 SSH 工作階段。
2. 按照提示登入 CLI。使用預設的管理員帳戶，及在初始設定期間指定的密碼。
3. 輸入下列命令，切換至日誌收集器模式：

```
> request system system-mode logger
```

4. 輸入 **Y** 以確認模式變更。Panorama 管理伺服器重新啟動。如果重新啟動程序終止終端機模擬軟體的工作階段，請重新連線至 Panorama 以顯示 Panorama 登入提示。

   如果您看到 ***CMS Login***（*CMS* 登入）提示，則表示日誌收集器未完成重新啟動。在提示框中按 *Enter*，而不輸入使用者名稱或密碼。
5. 重新登入 CLI。
6. 確認已成功切換至日誌收集器模式：

```
> show system info | match system-mode
```

如果模式變更成功，則輸出顯示為：

```
system-mode: logger
```

STEP 3 | 啟用日誌收集器和 Panorama 管理伺服器之間的連線。

需要先完成此步驟，才能在啟用日誌收集器上的日誌記錄磁碟。

在每個日誌收集器的 CLI 上輸入下列命令：*<IPaddress1>* 用於主動 Panorama 的 MGT 介面 以及 *<IPaddress2>* 用於被動 Panorama 的 MGT 介面。

```
> configure
# set deviceconfig system panorama-server <IPaddress1> panorama-server-2
 <IPaddress2>
# commit
# exit
```

STEP 4 | 記錄日誌收集器的序號。

您需要這些序號以便在 Panorama 管理伺服器上將日誌收集器新增為受管理的收集器。

1. 在每個日誌收集器的 CLI 上，輸入以下命令以顯示器序號。

```
> show system info | match serial
```

2. 記錄序號。

STEP 5 | 將各日誌收集器新增為受管理的收集器。

© 2019 Palo Alto Networks, Inc.

使用主要 Panorama 管理伺服器對等的網頁介面設定受管理的收集器：

1. 選取 **Panorama** > **Managed Collectors**（受管理的收集器），再 **Add**（新增）受管理的收集器。
2. 在 **General**（一般）頁籤中，輸入您記錄的收集器序號（**Collector S/N**（收集器序號））。
3. 分別在 **Panorama Server IP**（**Panorama** 伺服器 **IP**）欄位和 **Panorama Server IP 2**（**Panorama** 伺服器 **IP 2**）欄位中輸入主動和被動 Panorama HA 端點的 IP 位址或 FQDN。*以下欄目必須填寫。
4. 選取**Interfaces**（介面），按一下**Management**（管理），然後根據網路的 IP 通訊協定而定，為 MGT 介面設定下列其中一個或兩個欄位集。
   - IPv4—**IP Address**（**IP** 位址）、**Netmask**（網路遮罩）及 **Default Gateway**（預設閘道）
   - IPv6—**IPv6 Address/Prefix Length**（**IPv6** 位址/首碼長度）及 **Default IPv6 Gateway**（預設的 **IPv6** 閘道）
5. （選用）如果您將使用 SNMP 管理員來監控日誌收集器的統計資料，請選取 **SNMP**。

   使用 SNMP 除了要設定日誌收集器，還需要額外的步驟（請參閱透過 SNMP 監控 Panorama 和日誌收集器統計資料）。
6. 按一下 **OK**（確定）儲存您的變更。
7. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

   需要先完成此步驟，才能在啟用日誌收集器上的日誌記錄磁碟。
8. 在 **Panorama** > **Managed Collectors**（受管理收集器）頁面中，列出您已新增的日誌收集器。Connected（已連線）欄中會顯示核取標記，表示日誌收集器已連線至 Panorama。您可能需要等待幾分鐘，然後頁面才會顯示更新後的連線狀態。



此時，*Configuration Status*（組態狀態）欄會顯示 *Out of Sync*（不同步），*Run Time Status*（執行階段狀態）欄會顯示 *disconnected*（已中斷連線）。設定收集器群組之後（步驟 9），狀態將變更為 *In Sync*（同步）和 *connected*（已連線）。

STEP 6 | 在每個日誌收集器上啟用日誌記錄磁碟。

使用主要 Panorama 管理伺服器對等的網頁介面執行下列步驟：

1. 選取 **Panorama** > **Managed Collectors**（受管理的收集器），再編輯日誌收集器。
2. 選取 **Disks**（磁碟），**Add**（新增）每一個磁碟配對，然後按一下 **OK**（確定）。
3. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

STEP 7 | （建議）如果日誌收集器會將 **Ethernet1**、**Ethernet2**、**Ethernet3**、**Ethernet4** 和 **Ethernet5** 介面用於 **Device Log Collection**（裝置日誌收集）（從防火牆接收日誌）和 **Collector Group Communication**（收集器群組通訊），請設定這些介面。

依預設，日誌收集器會將 MGT 介面用於日誌收集和收集器群組通訊。將其他介面指派給這些功能，可讓您保留 MGT 介面給管理流量。在日誌流量很大的環境中，請考慮將 M-500 設備上的 10Gbps 介面（**Ethernet4** 和 **Ethernet5**）用於日誌收集和收集器群組通訊。若要平衡介面之間日誌記錄流量的負載，您可以在多個介面上啟用 **Device Log Collection**（裝置日誌收集）。

針對每個日誌收集器，使用主要 Panorama 管理伺服器對等的網頁介面執行下列步驟：

1. 選取 **Panorama** > **Managed Collectors**（受管理的收集器），編輯日誌收集器，然後選取 **Interfaces**（介面）。
2. 為每個介面執行下列步驟：
   1. 按一下介面名稱以編輯介面。
   2. 選取 **<interface-name>** 以啟用介面。
   3. 視您網路的 IP 通訊協定而定，完成下列其中一個或兩個欄位集：

© 2019 Palo Alto Networks, Inc.

IPv4—IP Address（**IP** 位址）、**Netmask**（網路遮罩）及 **Default Gateway**（預設閘道）

IPv6—IPv6 Address/Prefix Length（**IPv6** 位址/首碼長度）及 **Default IPv6 Gateway**（預設的 **IPv6** 閘道）

4. 選取介面支援的裝置管理服務：

   Device Log Collection（裝置日誌收集）—您可以指派一個或多個介面。

   Collector Group Communication（收集器群組通訊）—您只能指派一個介面。

5. 按一下 **OK**（確定）以儲存對介面所做的變更。

3. 按一下 **OK**（確定），以儲存對日誌收集器所做的變更。
4. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後將您的變更 **Commit**（提交）至 Panorama 組態。

STEP 8 | 將防火牆新增為受管理的裝置。

針對會將日誌轉送至日誌收集器的每個防火牆，使用主要 Panorama 管理伺服器對等的網頁介面執行此工作。

STEP 9 | 設定收集器群組。

如果每個收集器群組有一個日誌收集器，繼續操作之前，請先為每個收集器群組重複此步驟。

如果您要指派所有日誌收集器至一個收集器群組，請僅執行此步驟一次。

使用主要 Panorama 管理伺服器對等的網頁介面設定收集器群組：

1. 選取 **Panorama** > **Collector Groups**（收集器群組），再 **Add**（新增）收集器群組。
2. 輸入用來識別收集器群組的 **Name**（名稱）。
3. 將一個或多個日誌收集器 **Add**（新增）至 Collector Group Members（收集器群組成員）清單。

   在任何單一收集器群組中，所有日誌收集器都必須在相同 *Panorama* 型號上執行：全部是 *M-600* 設備、全部都是 *M-500* 設備、全部都是 *M-200*，或全部是 *Panorama* 虛擬設備。

4. （最佳作法）如果您將多個日誌收集器新增至單一收集器群組，請 **Enable log redundancy across collectors**（啟用跨收集器的日誌備援）。使用此選項時，每個日誌收集器必須有相同數目的日誌記錄磁碟。
5. （選用）如果您使用 SNMP 來監控日誌收集器統計資料和陷阱，請選取 **Monitoring**（監控）並進行設定。
6. 選取 **Device Log Forwarding**（裝置日誌轉送），並設定 Log Forwarding Preferences（日誌轉送偏好設定）清單。此清單定義哪些防火牆將日誌轉送至哪些日誌收集器。根據此收集器群組中的日誌收集器數目指派防火牆：
   - 單一—將轉送日誌的防火牆指派給該日誌收集器，如每個收集器群組一個專用日誌收集器所示。
   - 多個—將每個防火牆指派給兩個日誌收集器當作備援。設定偏好設定時，讓日誌收集器 1 成為一半防火牆的第一優先，讓日誌收集器 2 成為另一半防火牆的第一優先，如每個收集器群組多個專用日誌收集器所示。
7. 按一下 **OK**（確定）以儲存對收集器群組所做的變更。
8. 選取 **Commit**（提交）> **Commit and Push**（提交並推送），然後將您的變更 **Commit and Push**（提交並推送）至 Panorama 和您新增的收集器群組。
9. 選取 **Panorama** > **Managed Collectors**（受管理的收集器），確認日誌收集器設定已與 Panorama 同步。

   Configuration Status（組態狀態）欄應該顯示 In Sync（同步），Run Time Status（執行階段狀態）欄應該顯示 connected（已連線）。

STEP 10 | 設定將日誌從防火牆轉送至 Panorama。

© 2019 Palo Alto Networks, Inc.

使用主要 Panorama 管理伺服器對等的網頁介面：

1. 設定日誌轉送至 Panorama。
2. 確認日誌轉送至 Panorama。
3. （選用）設定日誌從 Panorama 轉送至外部目的地。

部署具備本機日誌收集器的 Panorama M-Series 設備

下圖說明集中式日誌收集部署中的 Panorama。在這些範例中，Panorama 管理伺服器包含兩個 Panorama 模式的 M-Series 設備，被部署在主動/被動高可用性 (HA) 設定中。防火牆會將日誌傳送到每個 Panorama M-Series 設備上的預先定義（預設）本機日誌收集器。如果防火牆以最高 10,000 個日誌/秒的速率產生日誌，則此為建議的部署。

如果您要將一個以上的日誌收集器指派給收集器群組，請參閱警告有收集器群組擁有多個日誌收集器，瞭解需求、風險和建議的緩和措施。

實施此部署後，如果日誌記錄速率增加到超過每秒 *10,000* 個日誌，*Palo Alto Networks* 建議您新增專用日誌收集器（日誌收集器模式的 *M-Series* 設備），如部署具備專用日誌收集器的 Panorama 中所述。如此擴充可能需要將防火牆從本機日誌收集器，改派給專用日誌收集器。

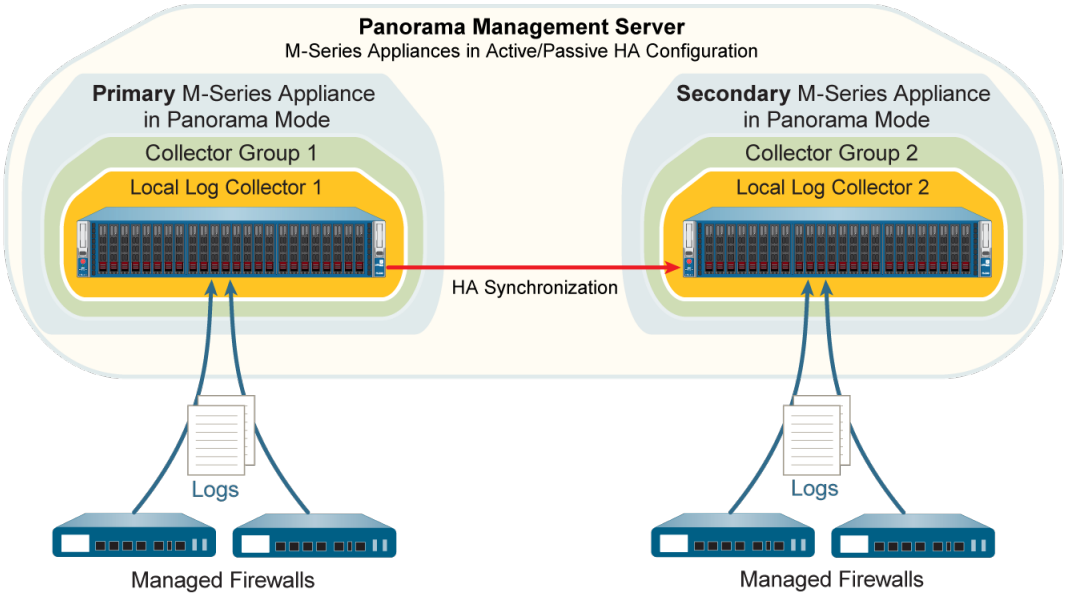


圖 19: 每個收集器群組一個本機日誌收集器

© 2019 Palo Alto Networks, Inc.

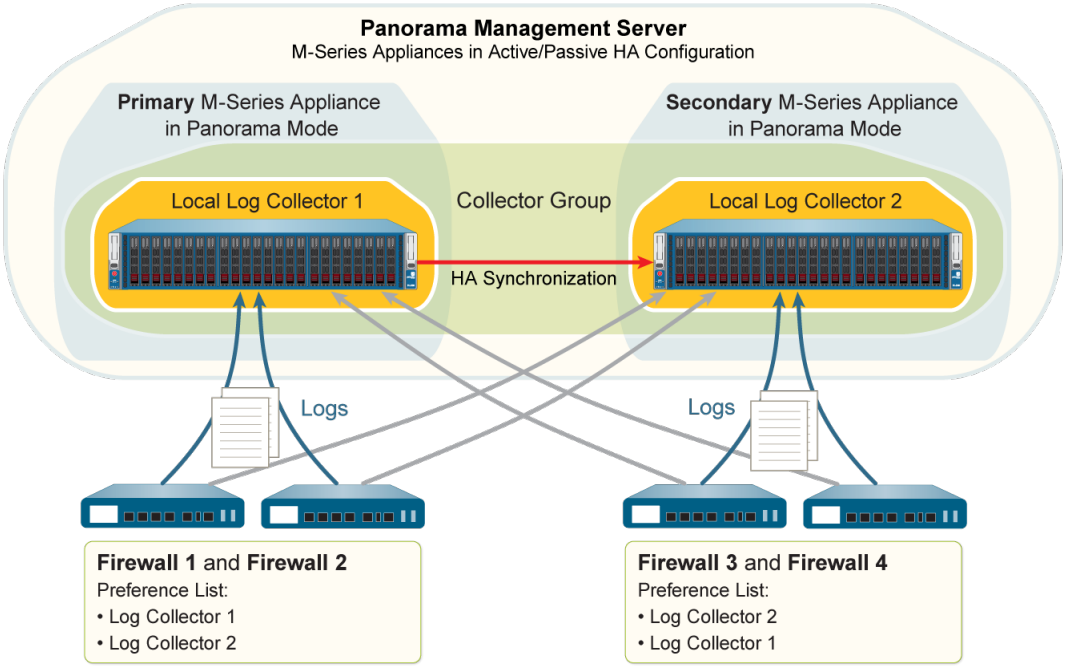


圖 20: 每個收集器群組多個本機日誌收集器

執行下列步驟可部署具備本機日誌收集器的 Panorama。略過任何您已執行的步驟（例如初始設定）。

STEP 1 | 執行每個 M-Series 設備的初始設定。

1. 在機架中安裝 M-Series 設備。請參閱 M-Series 硬體參考指南的指示。
2. 執行 M-Series 設備的初始設定。

   Palo Alto Networks 建議將管理 *(MGT)* 介面保留為 *Panorama* 的管理存取，並準備獨立的 M-Series 設備介面專供其他 *Panorama* 服務使用。
3. 設定每個陣列。為了使 RAID 磁碟可用於記錄日誌，需要完成此工作。您也可以選擇新增磁碟以增加 M-Series 設備的儲存容量。
4. 註冊 Panorama 並安裝授權。
5. 安裝 Panorama 的內容與軟體更新。
6. 在 Panorama 上設定 HA。

STEP 2 | 執行下列步驟，為日誌收集做好準備。

1. 以下列其中一種方式連線主要 Panorama：
   - 將序列纜線從電腦連線至主要 Panorama 的主控台連接埠。然後使用終端機模擬軟體 (9600-8-N-1) 進行連線。
   - 使用終端機模擬軟體（例如 PuTTY），針對在初始設定期間指定給主要 Panorama 的 MGT 介面的 IP 位址開啟 SSH 工作階段。
2. 按照提示登入 CLI。使用預設的管理員帳戶，及在初始設定期間指定的密碼。
3. 輸入下列命令，啟用主要 Panorama 以連線至次要 Panorama，其中 *<IPaddress2>* 代表次要 Panorama 的管理介面：

```
> configure
# set deviceconfig system panorama-server <IPaddress2>
# commit
```

4. 登入次要 Panorama 的 CLI。

© 2019 Palo Alto Networks, Inc.

5. 輸入下列命令，啟用次要 Panorama 以連線至主要 Panorama，其中 *<IPaddress1>* 代表主要 Panorama 的管理介面：

```
> configure
# set deviceconfig system panorama-server <IPaddress1>
# commit
# exit
```

6. 在次要 Panorama 的 CLI 中，輸入下列命令以顯示序號，然後記錄序號：

```
> show system info | match serial
```

您需要序號才能將次要 Panorama 的日誌收集器作為受管理的收集器新增至主要 Panorama。

STEP 3 | 編輯主要 Panorama 的本機日誌收集器。

使用主要 Panorama 的網頁介面執行以下步驟：

1. 選取 **Panorama** > **Managed Collectors**（受管理的收集器），然後選取預設（本機）日誌收集器。
2. 選取 **Disks**（磁碟），然後 **Add**（新增）每一個日誌記錄磁碟配對。
3. 按一下 **OK**（確定）儲存您的變更。

STEP 4 | 設定次要 Panorama 本機的日誌收集器。



由於此日誌收集器非主要 *Panorama* 的本機收集器，因此 *Panorama* 將其視為遠端收集器。因此您必須在主要 *Panorama* 上手動新增它。

使用主要 Panorama 的網頁介面設定受管理的收集器：

1. 選取 **Panorama** > **Managed Collectors**（受管理的收集器），再 **Add**（新增）日誌收集器。
2. 輸入您記錄的次要 Panorama 日誌收集器的序號（**Collector S/N**（收集器序號））。
3. 分別輸入 **Panorama Server IP**（**Panorama** 伺服器 **IP**）欄位和 **Panorama Server IP 2**（**Panorama** 伺服器 **IP 2**）欄位中主要和次要 Panorama HA 端點的 IP 位址或 FQDN。

   以下兩個欄位均為必填欄位。
4. 選取 **Interfaces**（介面），設定日誌收集器將使用的每個介面。**Management**（管理）介面為必要。為每個介面執行下列步驟：
   1. 按一下介面名稱。
   2. 視網路的 IP 通訊協定而定，設定下列其中一個或兩個欄位集。

      IPv4—IP Address（**IP** 位址）、**Netmask**（網路遮罩）及 **Default Gateway**（預設閘道）

      IPv6—IPv6 Address/Prefix Length（**IPv6** 位址/首碼長度）及 **Default IPv6 Gateway**（預設的 **IPv6** 閘道）
   3. （僅限管理介面）如果您將使用 SNMP 管理員來監控日誌收集器的統計資料，請選取 **SNMP**。

      使用 SNMP 除了要設定日誌收集器，還需要額外的步驟（請參閱透過 SNMP 監控 Panorama 和日誌收集器統計資料）。
   4. 按一下 **OK**（確定）以儲存對介面所做的變更。
5. 按一下 **OK**（確定），以儲存對日誌收集器所做的變更。
6. 選取 **Commit**（提交） > **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

   需要先完成此步驟，才能啟用日誌記錄磁碟。
7. 按一下名稱以編輯日誌收集器。
8. 選取 **Disks**（磁碟），**Add**（新增）每一個 RAID 磁碟配對，然後按一下 **OK**（確定）。

© 2019 Palo Alto Networks, Inc.

9. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

STEP 5 | 將防火牆新增為受管理的裝置。

針對會將日誌轉送至日誌收集器的每個防火牆，使用主要 Panorama 的網頁介面執行此工作。

STEP 6 | 編輯主要 Panorama 預先定義的預設收集器群組。

使用主要 Panorama 的網頁介面設定收集器群組：

1. 選取 **Panorama** > **Collector Groups**（收集器群組），編輯 **default**（預設）收集器群組。
2. 如果您要將多個日誌收集器新增至單一收集器群組，請將次要 Panorama 的本機日誌收集器 **Add**（新增）至 Collector Group Members（收集器群組成員）清單。依預設，此清單會顯示主要 Panorama 的本機日誌收集器，因為此收集器已預先指派給預設收集器群組。

   在任何單一收集器群組中，所有日誌收集器都必須在相同 *Panorama* 型號上執行：全部是 *M-600* 設備、全部都是 *M-500* 設備、全部都是 *M-200*，或全部是 *Panorama* 虛擬設備。
3. （最佳作法）如果您將多個日誌收集器新增至單一收集器群組，請 **Enable log redundancy across collectors**（啟用跨收集器的日誌備援）。使用此選項時，每個日誌收集器必須有相同數目的日誌記錄磁碟。
4. （選用）如果您使用 SNMP 來監控日誌收集器統計資料和陷阱，請選取 **Monitoring**（監控）並進行設定。
5. 選取 **Device Log Forwarding**（裝置日誌轉送），並設定 Log Forwarding Preferences（日誌轉送偏好設定）清單。此清單定義哪些防火牆將日誌轉送至哪些日誌收集器。根據此收集器群組中的日誌收集器數目指派防火牆：
   - 單一—將轉送日誌的防火牆指派給主要 Panorama 的本機日誌收集器，如每個收集器群組一個本機日誌收集器所示。
   - 多個—將每個防火牆指派給兩個日誌收集器當作備援。設定偏好設定時，讓日誌收集器 1 成為一半防火牆的第一優先，讓日誌收集器 2 成為另一半防火牆的第一優先，如每個收集器群組多個本機日誌收集器所示。
6. 按一下 **OK**（確定）儲存您的變更。

STEP 7 | 設定收集器群組來包含次要 Panorama 的日誌收集器。

如果各收集器群組僅有一個日誌收集器則必須執行此步驟。

使用主要 Panorama 的網頁介面設定收集器群組：

1. 選取 **Panorama** > **Collector Groups**（收集器群組），再 **Add**（新增）收集器群組。
2. 輸入用來識別收集器群組的 **Name**（名稱）。
3. 將次要 Panorama 的本機日誌收集器 **Add**（新增）至 Collector Group Members（收集器群組成員）清單。
4. （選用）如果您要使用 SNMP 管理員來監控日誌收集器統計資料和陷阱，請選取 **Monitoring**（監控）並進行設定。
5. 選取 **Device Log Forwarding**（裝置日誌轉送），在 Log Forwarding Preferences（日誌轉送偏好設定）清單中 **Add**（新增）項目：
   1. **Modify**（修改）Devices（裝置）清單，選取會將日誌轉送至次要 Panorama 本機日誌收集器的防火牆（請參閱每個收集器群組一個本機日誌收集器），然後按一下 **OK**（確定）。
   2. 將次要 Panorama 的本機日誌收集器 **Add**（新增）至 Collectors（收集器）清單，然後按一下 **OK**（確定）。
6. 按一下 **OK**（確定）儲存您的變更。

STEP 8 | 將您的變更提交並推送至 Panorama 組態和收集器群組。

© 2019 Palo Alto Networks, Inc.

在主要 Panorama 的網頁介面中，選取 **Commit**（提交）> **Commit and Push**（提交並推送），然後將您的變更 **Commit and Push**（提交並推送）至 Panorama 和您新增的收集器群組。

STEP 9 | 手動故障復原，讓次要 Panorama 成為作用中。

使用主要 Panorama 的 Web 介面執行下列步驟：

1. 選取 **Panorama** > **High Availability**（高可用性）。
2. 按一下操作命令區段內的 **Suspend local Panorama**（暫停本機 **Panorama**）。

STEP 10 | 在次要 Panorama 上，設定主要 Panorama 本機上日誌收集器的網路設定。

使用次要 Panorama 的 Web 介面執行下列步驟：

1. 在 Panorama Web 介面中，選取 **Panorama** > **Managed Collectors**（受管理的收集器），然後選取主要 Panorama 本機上的日誌收集器。
2. 分別輸入 **Panorama Server IP**（**Panorama** 伺服器 **IP**）欄位和 **Panorama Server IP 2**（**Panorama** 伺服器 **IP 2**）欄位中主要和次要 Panorama HA 端點的 IP 位址或 FQDN。

   以下兩個欄位均為必填欄位。
3. 選取 **Interfaces**（介面），按一下 **Management**（管理），並將主要 Panorama 的 MGT 介面值填入下列其中一個或兩個欄位集（根據網路的 IP 通訊協定而定）：
   - **IPv4—IP Address**（**IP** 位址）、**Netmask**（網路遮罩）及 **Default Gateway**（預設閘道）
   - **IPv6—IPv6 Address/Prefix Length**（**IPv6** 位址/首碼長度）及 **Default IPv6 Gateway**（預設的 **IPv6** 閘道）
4. 按一下 **OK**（確定）儲存您的變更。
5. 選取 **Commit**（提交）> **Commit and Push**（提交並推送），然後將您的變更 **Commit and Push**（提交並推送）至 Panorama 和您新增的收集器群組。

STEP 11 | 手動進行故障復原，讓主要 Panorama 重新作用。

使用次要 Panorama 的 Web 介面執行下列步驟：

1. 選取 **Panorama** > **High Availability**（高可用性）。
2. 按一下操作命令區段內的 **Suspend local Panorama**（暫停本機 **Panorama**）。

STEP 12 | 設定將日誌從防火牆轉送至 Panorama。

使用主要 Panorama 的網頁介面：

1. 設定日誌轉送至 Panorama。
2. 確認日誌轉送至 Panorama。
3. （選用）設定日誌從 Panorama 轉送至外部目的地。



您可以將個別的外部伺服器設定檔指派給每個 *Panorama HA* 對等。例如，您可能需要各端點轉送日誌至不同的系統日誌伺服器。如果您想要各 *Panorama* 端點轉送日誌至不同的外部服務，則選取 *Panorama* > *Collector Groups*（收集器群組），選取相關收集器群組，再選取 *Collector Log Forwarding*（收集器群組轉送），指派伺服器設定檔，然後按一下 *OK*（確定）。

部署具備本機日誌收集器的 Panorama 虛擬設備

您可以設定防火牆將日誌傳送至 Panorama 模式的 Panorama 虛擬設備上執行的日誌收集器。在高可用性 (HA) 設定中，每個 Panorama 對等都可以有本機日誌收集器。您可以將 HA 對等上的本機日誌收集器，指派給相同的收集器群組或不同的收集器群組，如下圖所示。當在 VMware 虛擬基礎結構內部署具備本機日誌收集器的 Panorama 虛擬設備時，請參閱 設定 Panorama 虛擬設備的先決條件 以查看支援的每秒日誌數。

© 2019 Palo Alto Networks, Inc.

如果您要將一個以上的日誌收集器指派給收集器群組，請參閱警告有收集器群組擁有多個日誌收集器，瞭解需求、風險和建議的緩和措施。

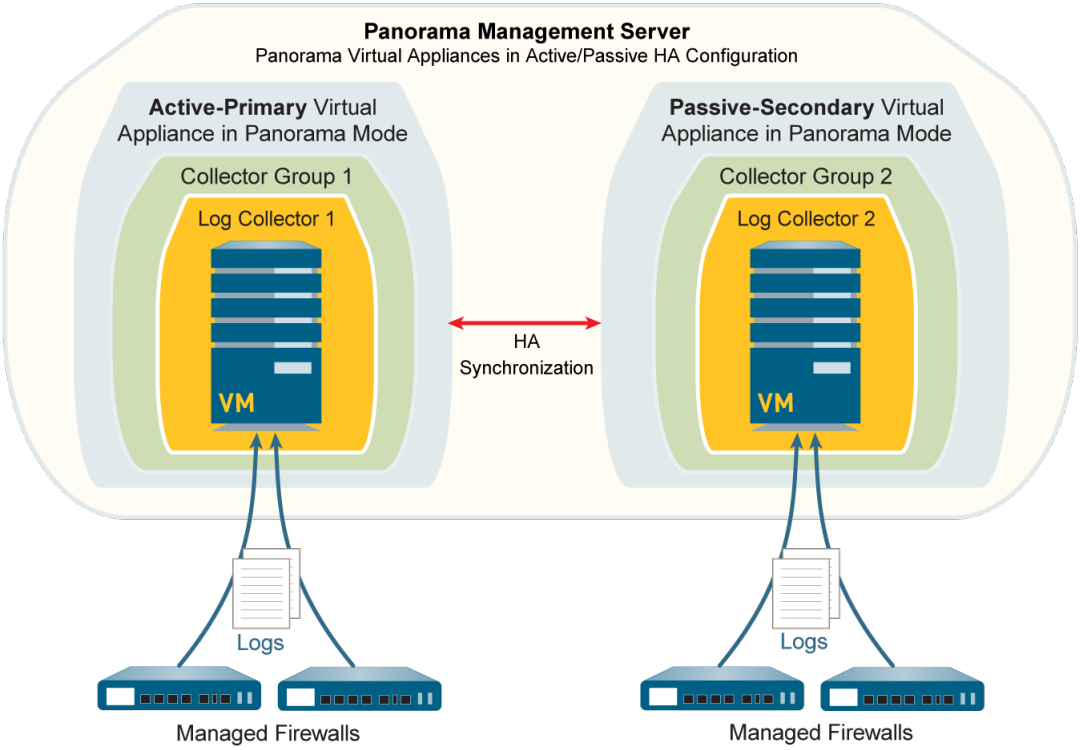


圖 21: 每個收集器群組一個日誌收集器

© 2019 Palo Alto Networks, Inc.

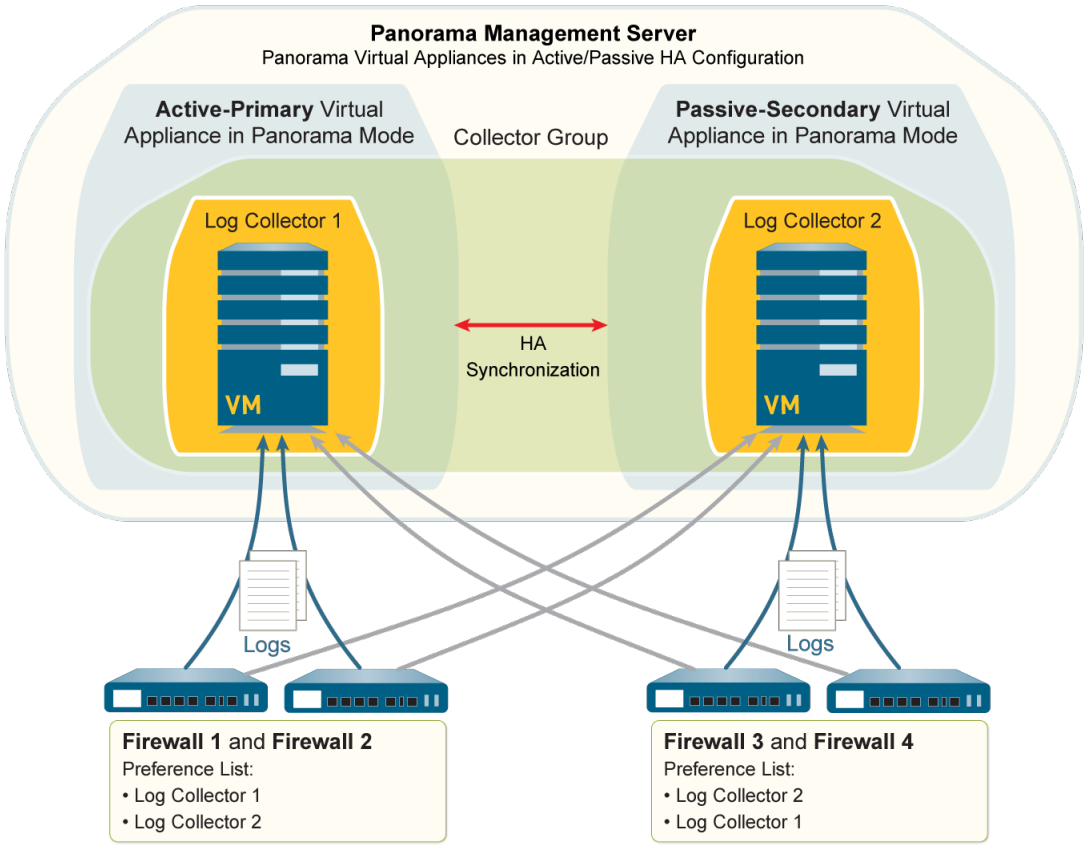


圖 22: 每個收集器群組多個日誌收集器

執行下列步驟可部署具備本機日誌收集器的 Panorama。略過任何您已執行的步驟（例如初始設定）。

STEP 1 | 執行每個 Panorama 虛擬設備的初始設定。

1. 安裝 Panorama 虛擬設備。您必須設定下列資源，以確保虛擬設備以 Panorama 模式啟動：
   - 儲存空間剛好為 81GB 的系統磁碟。
   - CPU 和記憶體必須足夠處理 Panorama 接收和儲存的日誌數量。
   - 儲存空間為 2–24TB 的虛擬日誌記錄磁碟。

   Panorama 會自動將新磁碟分割成 *2TB* 分割區，各成為獨立的虛擬磁碟。
2. 執行 Panorama 虛擬設備的初始設定。
3. 註冊 Panorama 並安裝授權。
4. 安裝 Panorama 的內容與軟體更新。

STEP 2 | 在 HA 組態中設定 Panorama 虛擬設備。

1. 在 Panorama 上設定 HA。
2. 測試 Panorama HA 容錯移轉。

STEP 3 | 新增主要 Panorama 本機的日誌收集器。

在主要 Panorama 上：

1. 記錄 Panorama 序號。
   1. 存取 Panorama Web 介面。

© 2019 Palo Alto Networks, Inc.

2. 選取 **Dashboard**（儀表板），然後記錄 General Information（一般資訊）部分中的 **Serial #**（序號）。

2. 新增日誌收集器作為受管理的收集器。
   1. 選取 **Panorama** > **Managed Collectors**（受管理的收集器），然後 **Add**（新增）新的日誌收集器。
   2. 在 **General**（一般）設定中，輸入您為 Panorama 記錄的序號（**Collector S/N**（收集器序號））。
   3. 按一下 **OK**（確定）儲存您的變更。
   4. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**）。

      需要先完成此步驟，才能新增虛擬日誌記錄磁碟。
3. 新增虛擬日誌記錄磁碟。
   1. 選取 **Panorama** > **Managed Collectors**（受管理的收集器），然後按一下名稱來編輯日誌收集器。

      日誌收集器名稱的值與主要 Panorama 的主機名稱相同。
   2. 選取 **Disks**（磁碟），然後 **Add**（新增）虛擬日誌記錄磁碟。
   3. 按一下 **OK**（確定）儲存您的變更。
   4. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**）。

STEP 4 | 新增次要 Panorama 本機的日誌收集器。



由於此日誌收集器不是在主要 *Panorama* 本機執行，因此 *Panorama* 將其視為遠端收集器。

1. 記錄次要 Panorama 的序號。
   1. 存取次要 Panorama 的網頁介面。
   2. 選取 **Dashboard**（儀表板），然後記錄 General Information（一般資訊）部分中的 **Serial #**（序號）。
2. 存取主要 Panorama 的網頁介面。
3. 選取 **Panorama** > **Managed Collectors**（受管理的收集器），再 **Add**（新增）日誌收集器。
4. 在 **General**（一般）設定中，輸入您為次要 Panorama 記錄的序號（**Collector S/N**（收集器序號））。
5. 分別輸入 **Panorama Server IP**（**Panorama** 伺服器 **IP**）欄位和 **Panorama Server IP 2**（**Panorama** 伺服器 **IP 2**）欄位中主要和次要 Panorama HA 端點的 IP 位址或 FQDN。

   以下兩個欄位均為必填欄位。
6. 按一下 **OK**（確定），以儲存對日誌收集器所做的變更。
7. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

   需要先完成此步驟，才能新增虛擬日誌記錄磁碟。
8. 按一下名稱以編輯日誌收集器。

   日誌收集器名稱的值與次要 Panorama 的主機名稱相同。
9. 選取 **Disks**（磁碟），**Add**（新增）虛擬日誌記錄磁碟，然後按一下 **OK**（確定）。
10. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

STEP 5 | 將防火牆新增為受管理的裝置。

針對會將日誌轉送至日誌收集器的每個防火牆，使用主要 Panorama 執行此工作。

STEP 6 | 設定收集器群組。

如果您要將兩個日誌收集器都指派給相同的收集器群組，請執行一次此步驟。否則，請為每個日誌收集器設定收集器群組。

© 2019 Palo Alto Networks, Inc.

在主要 Panorama 上：

1. 選取 **Panorama** > **Collector Groups**（收集器群組），然後 **Add**（新增）收集器群組。
2. 將一個或兩個日誌收集器 **Add**（新增）為收集器群組成員。

   在任何單一收集器群組中，所有日誌收集器都必須在相同 *Panorama* 型號上執行：全部是 *M-600* 設備、全部都是 *M-500* 設備、全部都是 *M-200*，或全部是 *Panorama* 虛擬設備。
3. （最佳作法）如果您將多個日誌收集器新增至單一收集器群組，請 **Enable log redundancy across collectors**（啟用跨收集器的日誌備援）。使用此選項時，每個日誌收集器必須有相同數目的虛擬日誌記錄磁碟。

   啟用備援會使收集器群組中的日誌數量和日誌處理流量增加一倍。若有必要，擴展 Panorama 虛擬設備的日誌儲存容量。
4. 選取 **Device Log Forwarding**（裝置日誌轉送），並設定 Log Forwarding Preferences（日誌轉送偏好設定）清單。此清單定義哪些防火牆將日誌轉送至哪些日誌收集器。根據此收集器群組中的日誌收集器數目指派防火牆：
   - **Single**（單一）—將轉送日誌的防火牆指派給位於主要 Panorama 的日誌收集器，如每個收集器群組一個日誌收集器所示。
   - 多個—將每個防火牆指派給兩個日誌收集器當作備援。設定偏好清單時，讓日誌收集器 1 成為一半防火牆的第一優先，讓日誌收集器 2 成為另一半防火牆的第一優先，如每個收集器群組多個日誌收集器所示。
5. 按一下 **OK**（確定）儲存您的變更。
6. 選取 **Commit**（提交）> **Commit and Push**（提交並推送），然後將您的變更 **Commit and Push**（提交並推送）至 Panorama 和您新增的收集器群組。

STEP 7 | 在主要 Panorama 上觸發容錯移轉，讓次要 Panorama 變成主動。

在主要 Panorama 上：

1. 選取 **Panorama** > **High Availability**（高可用性）。
2. 按一下操作命令區段內的 **Suspend local Panorama**（暫停本機 **Panorama**）。

STEP 8 | 設定從次要 Panorama 到主要 Panorama 本機的日誌收集器之間的連線。

在次要 Panorama 上：

1. 在 Panorama Web 介面中，選取 **Panorama** > **Managed Collectors**（受管理的收集器），然後選取主要 Panorama 本機上的日誌收集器。
2. 分別輸入 **Panorama Server IP**（**Panorama** 伺服器 **IP**）欄位和 **Panorama Server IP 2**（**Panorama** 伺服器 **IP 2**）欄位中主要和次要 Panorama HA 端點的 IP 位址或 FQDN。

   以下兩個欄位均為必填欄位。
3. 按一下 **OK**（確定）儲存您的變更。
4. 選取 **Commit**（提交）> **Commit and Push**（提交並推送），然後將您的變更 **Commit and Push**（提交並推送）至 Panorama 和收集器群組。

STEP 9 | 在次要 Panorama 上觸發容錯回復，讓主要 Panorama 變成主動。

在次要 Panorama 上：

1. 選取 **Panorama** > **High Availability**（高可用性）。
2. 按一下操作命令區段內的 **Suspend local Panorama**（暫停本機 **Panorama**）。

STEP 10 | 設定將日誌從防火牆轉送至 Panorama。

© 2019 Palo Alto Networks, Inc.

在主要 Panorama 上：

1. 從防火牆設定日誌轉送至 Panorama。
2. 確認日誌轉送至 Panorama。

部署具備本機日誌收集的傳統模式 Panorama 虛擬設備

下圖說明集中式日誌收集部署中的 Panorama。在此範例中，Panorama 管理伺服器包含兩個部署在主動/被動高可用性 (HA) 設定中的傳統模式 Panorama 虛擬設備。此設定適用於在 Panorama 可處理 10,000 個日誌/秒的 VMware 虛擬基礎結構內防火牆管理。防火牆會將日誌傳送至 Panorama 管理伺服器上的 NFS 資料存放（僅限 ESXi 伺服器）或虛擬磁碟。依預設，主動和被動端點都會接收日誌，雖然您可以修改日誌轉送及緩衝預設值從而僅主動端點可實現。對於 5200 和 7000 系列防火牆，僅主動端點接收日誌。依預設，傳統模式的 Panorama 虛擬設備在其內部磁碟分割區上大約使用 11GB 來儲存日誌，但您可以根據需要擴展 Panorama 虛擬設備的日誌儲存容量。



如果日誌記錄速率增加到超過每秒 *10,000* 個日誌，建議您部署具備專用日誌收集器的 Panorama。

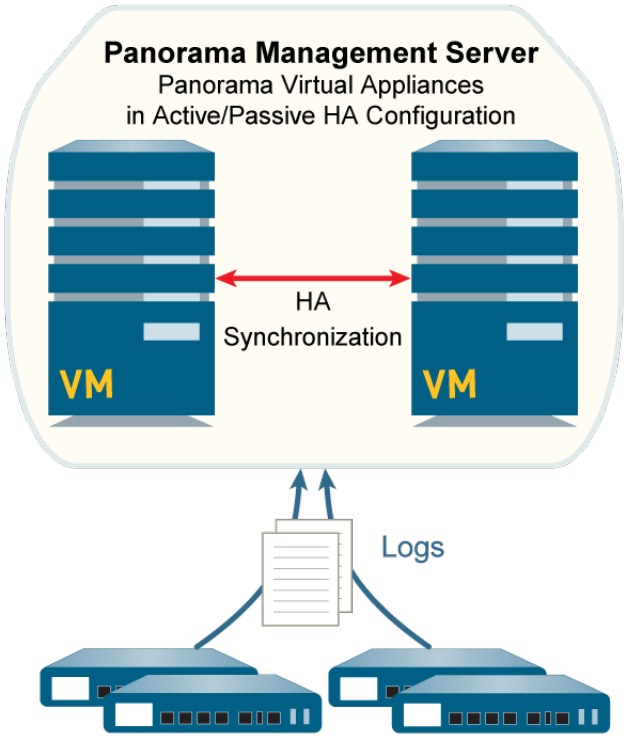


圖 23: 具備本機日誌收集的傳統模式 Panorama 虛擬設備

執行下列步驟可部署具備本機日誌收集的 Panorama 虛擬設備。略過任何您已執行的步驟（例如初始設定）。

STEP 1 | 執行每個 Panorama 虛擬設備的初始設定。

1. 安裝 Panorama 虛擬設備。為了確保虛擬設備以 Panorama 模式啟動，請勿在安裝期間新增虛擬日誌記錄磁碟。

   依預設，*Panorama* 在其系統磁碟上會使用 *11GB* 分割區來儲存日誌。如果想要有更多儲存空間，您可以在安裝之後新增專用的虛擬日誌記錄磁碟，最大為 *8TB*。
2. 執行 Panorama 虛擬設備的初始設定。

© 2019 Palo Alto Networks, Inc.

3. 註冊 Panorama 並安裝授權。
4. 安裝 Panorama 的內容與軟體更新。

STEP 2 | 在 HA 組態中設定 Panorama 虛擬設備。

1. 在 Panorama 上設定 HA。
2. 測試 Panorama HA 容錯移轉。

STEP 3 | 執行下列步驟，為日誌收集做好準備。

1. 對於將向 Panorama 轉送日誌的各防火牆，將防火牆新增為受管理的裝置。
2. 設定日誌轉送至 Panorama。

STEP 4 | Commit（提交）您的變更。

選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

管理 *WildFire* 設備

您可以使用 Panorama M-Series 或虛擬設備，以集中管理最多 200 個獨立 WildFire 設備和 WildFire 設備叢集節點。相較於使用本機 CLI 來個別管理 WildFire 設備和設備叢集，使用 Panorama 可集中管理和監控多個設備和設備叢集。集中管理可讓您將通用設定、設定更新和軟體更新，推送至所有或一部分受管理的 WildFire 設備，較容易確保 WildFire 設備和設備叢集有一致的設定。

當您使用 Panorama 以管理 WildFire 設備叢集時，Panorama 必須執行與受管理的 WildFire 設備相同或更新的版本。

> 新增獨立 WildFire 設備給 Panorama 管理
> 在 Panorama 上進行 WildFire 設備基本設定
> 使用 WildFire 設備和叢集上的自訂憑證進行驗證
> 移除 WildFire 設備不要由 Panorama 管理
> 管理 WildFire 叢集

新增獨立 WildFire 設備給 Panorama 管理

您可以使用 Panorama M-Series 或虛擬設備來管理最多 200 個 WildFire 設備。200 WildFire 設備限制等於獨立設備加 WildFire 設備叢集節點（如果您還在 Panorama 上設定叢集和新增節點）的合計。

請確定 Panorama 至少執行 8.0.1 版，且您新增至 Panorama 的任何 WildFire 設備也至少執行 8.0.1 版。

STEP 1 | 使用本機 CLI，確認您要以 Panorama 管理的每個 WildFire 設備都執行 PAN-OS 8.0.1 或更新版本。

```
admin@qa16> show system info | match version
sw-version: 8.0.1-c45
wf-content-version: 702-283
logdb-version: 8.0.15
```

STEP 2 | 在您要用來管理 WildFire 設備的每個 Panorama 設備上，確認 Panorama 執行 8.0.1 版或更新版本：

Dashboard（儀表板）> **General Information**（一般資訊）> **Software Version**（軟體版本）可顯示執行中的軟體版本。

STEP 3 | 如果您在本機 WildFire 設備 CLI 上不確定 WildFire 設備是否屬於 WildFire 設備叢集，或是否為獨立設備，請檢查 **Node mode** 以確定狀態為 **stand_alone**，並檢查 **Application status** 以確定 **global-db-service** 和 **global-queue-service** 指出 **ReadyStandalone**。

```
admin@WF-500> show cluster membership
Service Summary:  wfpc signature
Cluster name:
Address:          10.10.10.100
Host name:        WF-500
Node name:        wfpc-012345678901-internal
Serial number:    012345678901
Node mode:     stand_alone
Server role:      True
HA priority:
Last changed:     Mon, 06 Mar 2017 16:34:25 -0800
Services:         wfcore signature wfpc infra
Monitor status:
                  Serf Health Status: passing
                      Agent alive and reachable
Application status:
                  global-db-service: ReadyStandalone
        wildfire-apps-service: Ready
       global-queue-service: ReadyStandalone
        wildfire-management-service: Done
        siggen-db: ReadyMaster
Diag report:
                  10.10.10.100: reported leader '10.10.10.100', age 0.
                  10.10.10.100: local node passed sanity check.
```

STEP 4 | 如果您要以 Panorama 管理的 WildFire 設備是新的，請查看開始使用 WildFire，以確保您完成基本步驟，例如確認 WildFire 授權有效、啟用日誌記錄、將防火牆連接至 WildFire 設備，以及設定基本 WildFire 功能。

© 2019 Palo Alto Networks, Inc.

STEP 5 | 在 Panorama 伺服器將管理的每個 WildFire 設備上的本機 CLI，設定 Panorama 伺服器的 IP 位址。

將獨立 WildFire 設備註冊到 Panorama 設備之前，您必須先在每個 WildFire 設備上設定 Panorama IP 位址或 FQDN。這樣每個 WildFire 設備才知道它是由哪個 Panorama 設備所管理。

1. 設定主要 Panorama 設備管理介面的 IP 位址或 FQDN：

```
admin@WF-500# set deviceconfig system panorama-server <ip-address | FQDN>
```

2. 如果您使用備份 Panorama 設備來支援高可用性（建議），請設定備份 Panorama 設備管理介面的 IP 位址或 FQDN：

```
admin@WF-500# set deviceconfig system panorama-server-2 <ip-address |
 FQDN>
```

STEP 6 | 在主要 Panorama 設備上註冊 WildFire 設備。

1. 從 Panorama 網頁介面，選取 **Panorama** > **Managed WildFire Appliances**（受管理的 **WildFire** 設備）和 **Add Appliance**（新增設備）。
2. 將每個 WildFire 設備的序號輸入成各自一行。如果您沒有序號清單，請在每個 WildFire 設備上執行：

```
admin@WF-500> show system info | match serial
serial: 012345678901
```

有幾個本機 CLI 命令可顯示 WildFire 設備序號，包括 **show cluster membership**。

3. 按一下 **OK**（確定）。

將會顯示 WildFire 設備上已提交的設定相關資訊（若有的話），例如 IP 位址和軟體版本。

STEP 7 | （選用）將 WildFire 設備組態匯入至 Panorama 設備。

1. 從受管理的 WildFire 設備清單中選取設備，這些設備有您要匯入的設定。
2. **Import Config**（匯入設定）。
3. 選取 **Yes**（是）。

匯入設定會更新顯示的資訊，並使匯入的設定成為 Panorama 設備候選設定的一部分。

4. **Commit to Panorama**（提交至 **Panorama**），使匯入的 WildFire 設備組態成為 Panorama 執行中設定的一部分。

STEP 8 | 設定或確認 WildFire 設備介面的組態。

每個 WildFire 設備有四個介面：**Management**（管理）(Ethernet0)、**Analysis Network Environment**（分析網路環境）(Ethernet1)、**Ethernet2** 和 **Ethernet3**。

1. 選取 **Panorama** > **Managed WildFire Appliances**（受管理的 **WildFire** 設備），然後選取 WildFire 設備。
2. 選取 **Interfaces**（介面）。
3. 選取介面來設定或編輯。您可以啟用介面、設定每個介面的速度和雙工、IP 位址和網路遮罩、預設閘道、MTU、DNS 伺服器、連結狀態，以及 **Management Services**（管理服務）。您也可以 **Add**（新增）許可 IP 位址，使介面僅接受來自指定位址的流量。

Analysis Network Environment（分析網路環境）、**Ethernet2** 和 **Ethernet3** 介面僅支援 **Ping** 作為 **Management Services**（管理服務）選項。

© 2019 Palo Alto Networks, Inc.

Management（管理）介面支援 **Ping**、**SSH** 和 **SNMP** 作為 **Management Services**（管理服務）選項。此外，在無法直接連接至網際網路的情況下，**Management**（管理）介面支援 Proxy 伺服器設定。

4. 進行設定或確認設定之後，按一下 **OK**（確定）。

STEP 9 | 在 Panorama 設備上提交設定，然後推送至一或多個設備。

1. **Commit and Push**（提交並推送）。
2. 如果 Panorama 設備上有您不想推送的設定，請 **Edit Selections**（編輯選擇），以選取將設定推送至哪些設備。推送的設定會覆寫 WildFire 設備上執行中的設定。

STEP 10 | 確認組態。

1. 選取 **Panorama** > **Managed WildFire Appliances**（受管理的 **WildFire** 設備）。
2. 檢查下列欄位：
   - **Connected**（已連線）—狀態為 **Connected**（已連線）。
   - **Role**（角色）—每個 WildFire 設備的角色為 **Standalone**（獨立）。
   - **Config Status**（設定狀態）—狀態為 `In Sync`（同步）。
   - **Last Commit State**（上次提交狀態）—`Commit succeeded`（提交成功）。

© 2019 Palo Alto Networks, Inc.

在 Panorama 上進行 WildFire 設備基本設定

設定基本設定，例如內容更新和 WildFire 雲端伺服器、WildFire 雲端服務、日誌記錄、驗證等，就類似於如何在 Panorama 上進行一般叢集設定。並不是選取叢集，然後在叢集上進行設定，而是選取 WildFire 設備，再針對該設備進行個別設定。選取並設定您新增至 Panorama 的每個 WildFire 設備。

設定 WildFire 設備說明如何將 WildFire 設備整合至網域，然後使用 CLI 執行基本設定，但概念同於使用 Panorama 執行基本設定。

許多設定中都已預先填入預設值、*WildFire* 設備上先前既有設定的資訊，或您將 *WildFire* 設備新增至 *Panorama* 時所進行的設定。

- 為 WildFire 設備設定驗證

為 WildFire 設備設定驗證

透過設定具有精確驗證參數的本機管理使用者，以及利用 RADIUS、TACAS+ 或 LDAP 進行授權和驗證，為您的 WildFire 設備建立和設定增強的驗證。

當您在 Panorama 上設定管理員並進行推送時，您在 Panorama 上設定的管理員將覆寫 WildFire 設備中的現有管理員。

- 為 WildFire 設備設定管理帳戶
- 為 WildFire 設備設定 RADIUS 驗證
- 為 WildFire 設備設定 TACACS+ 驗證
- 為 WildFire 設備設定 LDAP 驗證

為 *WildFire* 設備設定管理帳戶

為您的 WildFire 設備建立一個或多個具有精確驗證參數的管理員，以便從 Panorama™ 管理伺服器進行管理。此外，您還可以從 Panorama 設定本機管理員，這可以從 WildFire 設備的 CLI 直接進行設定。但是，向 WildFire 設備推送新設定變更後，為 WildFire 設備設定的管理員會覆寫本機管理員。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 新增獨立 WildFire 設備給 Panorama 管理。

STEP 3 | （選用）設定驗證設定檔以定義驗證服務，用於對存取 WildFire 設備 CLI 之管理員的登入認證進行驗證。

STEP 4 | 根據需要設定一個或多個管理員帳戶。

在 Panorama 上建立的管理員帳戶之後會匯入到 WildFire 設備並從 Panorama 進行管理。

STEP 5 | 為 WildFire 設備設定驗證。

1. 選取 **Panorama** > **Managed WildFire Appliances**（受管理的 **WildFire** 設備），然後選取您之前新增的 WildFire 設備。
2. （選用）選取您在上一步中設定的 **Authentication Profile**（驗證設定檔）。
3. 為 WildFire 設備設定驗證 **Timeout Configuration**（逾時設定）。
    1. 輸入 **Failed Attempt**（失敗嘗試）次數，在達到此次數之後使用者將被鎖定在 WildFire 設備 CLI 之外。
    2. 輸入 **Lockout Time**（鎖定時間）（以分鐘為單位），在使用者達到設定的 **Failed Attempts**（失敗嘗試）次數後 WildFire 設備鎖定使用者帳戶的時間。

© 2019 Palo Alto Networks, Inc.

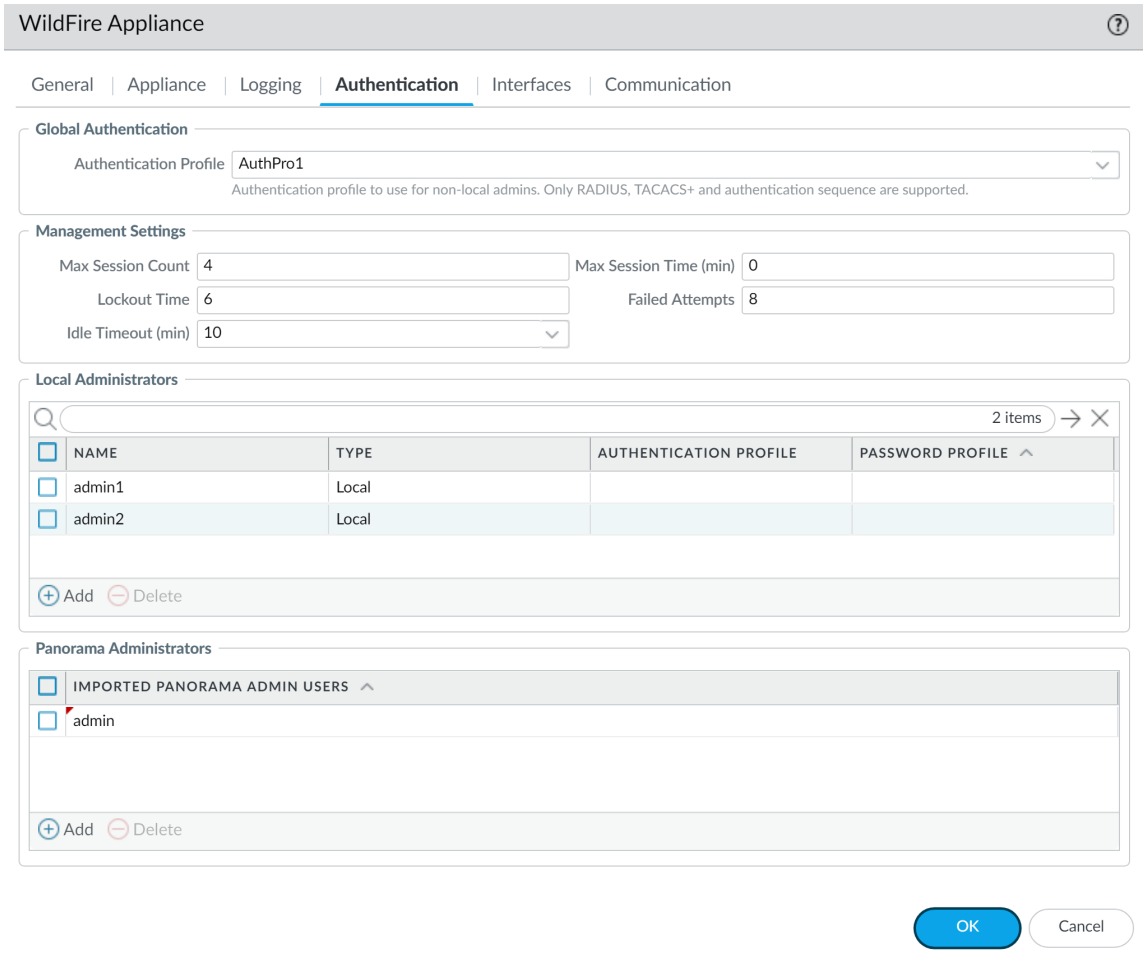
3. 輸入 **Idle Timeout**（閒置逾時）（以分鐘為單位），在此時間之後使用者會因為處於非作用狀態而自動登出。
4. 輸入 **Max Session Count**（最大工作階段計數），設定多少使用者帳戶可以同時存取 WildFire 設備。
5. 輸入管理員在自動登出之前可登入的 **Max Session Time**（最長工作階段時間）。

4. 新增 WildFire 設備管理員。

   管理員可以新增為本機管理員或作為匯入的 Panorama 管理員—但不能同時為二者。不支援將同一管理員同時新增為本機管理員和作為匯入的 Panorama 管理員，這會導致 Panorama 提交失敗。例如，如果您將 `admin1` 同時新增為本機和 Panorama 管理員，到 Panorama 的提交將會失敗。

   1. **Add**（新增）並設定專屬於 WildFire 設備的新管理員。這些管理員特定於為其建立的 WildFire 設備，您可以從此表格管理這些管理員。
   2. **Add**（新增）在 Panorama 上設定的任何管理員。這些管理員在 Panorama 上建立，並匯入至 WildFire 設備。

5. 按一下 **OK**（確定）以儲存 WildFire 設備驗證設定。



STEP 6 | **Commit**（提交），然後 **Commit and Push**（提交並推送）設定變更。

STEP 7 | 使用本機管理員使用者存取 WildFire 設備 CLI 以驗證您能夠成功存取 WildFire 設備。

© 2019 Palo Alto Networks, Inc.

為 *WildFire* 設備設定 *RADIUS* 驗證

使用 RADIUS 伺服器來驗證對 WildFire 設備 CLI 的管理存取。您也可以在 RADIUS 伺服器上定義廠商特定屬性 (VSA) 來進行管理員授權管理。使用 VSA 可讓您透過目錄服務快速變更管理員的角色、存取網域和使用者群組，這通常比在 Panorama™ 管理伺服器上重新設定更加簡單。



您可以將 Palo Alto 網路 RADIUS 詞典 匯入 *RADIUS* 伺服器，以定義 *Panorama* 和 *RADIUS* 伺服器之間通訊所需的驗證屬性。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 新增獨立 WildFire 設備給 Panorama 管理。

STEP 3 | 設定 RADIUS 驗證。

1. 新增 RADIUS 伺服器設定檔。

   設定檔定義了 WildFire 設備將採用何種方式連線 RADIUS 伺服器。

   1. 選取 **Panorama** > **Server Profiles**（伺服器設定檔）> **RADIUS**，然後 **Add**（新增）設定檔。
   2. 輸入用來識別伺服器設定檔的 **Profile Name**（設定檔名稱）。
   3. 輸入 **Timeout**（逾時）間隔時間（單位為秒），超過此時間後，驗證要求將逾時（預設值為 3；範圍為 1-20）。
   4. 選取 WildFire 設備用於向 RADIUS 伺服器驗證的 **Authentication Protocol**（驗證通訊協定）（預設值為 **CHAP**）。

      選取 *CHAP*（如果 *RADIUS* 伺服器支援此通訊協定）；它比 *PAP* 更安全。

   5. **Add**（新增）每個 RADIUS 伺服器，然後輸入下列資訊：

      1. 用來識別伺服器的 **Name**（名稱）。
      2. **RADIUS Server**（**RADIUS** 伺服器）IP 位址或 FQDN。
      3. **Secret**（密碼）/**Confirm Secret**（確認密碼）（用於加密使用者名稱和密碼的金鑰）。
      4. 用於驗證要求的伺服器 **Port**（連接埠）（預設值為 1812）。

   6. 按一下 **OK**（確定）來儲存伺服器設定檔。
2. 將 RADIUS 伺服器設定檔指派給驗證設定檔。

   驗證設定檔中定義一群管理員通用的驗證設定。

   1. 選取 **Panorama** > **Authentication Profile**（驗證設定檔），然後 **Add**（新增）設定檔。
   2. 輸入用來識別驗證設定檔的 **Name**（名稱）。
   3. 將 **Type**（類型）設為 **RADIUS**。
   4. 選取您設定的 **Server Profile**（伺服器設定檔）。
   5. 選取 **Retrieve user group from RADIUS**（從 **RADIUS** 擷取使用者群組），以從 RADIUS 伺服器上定義的 VSA 收集使用者群組資訊。

      Panorama 會比對群組資訊與您在驗證設定檔「允許清單」中指定的群組。

   6. 選取 **Advanced**（進階），然後在 Allow List（允許清單）中，**Add**（新增）允許使用此驗證設定檔進行驗證的管理員。
   7. 按一下 **OK**（確定）來儲存驗證設定檔。

STEP 4 | 為 WildFire 設備設定驗證。

1. 選取 **Panorama** > **Managed WildFire Appliances**（受管理的 **WildFire** 設備），然後選取您之前新增的 WildFire 設備。
2. 選取您在上一步中設定的 **Authentication Profile**（驗證設定檔）。

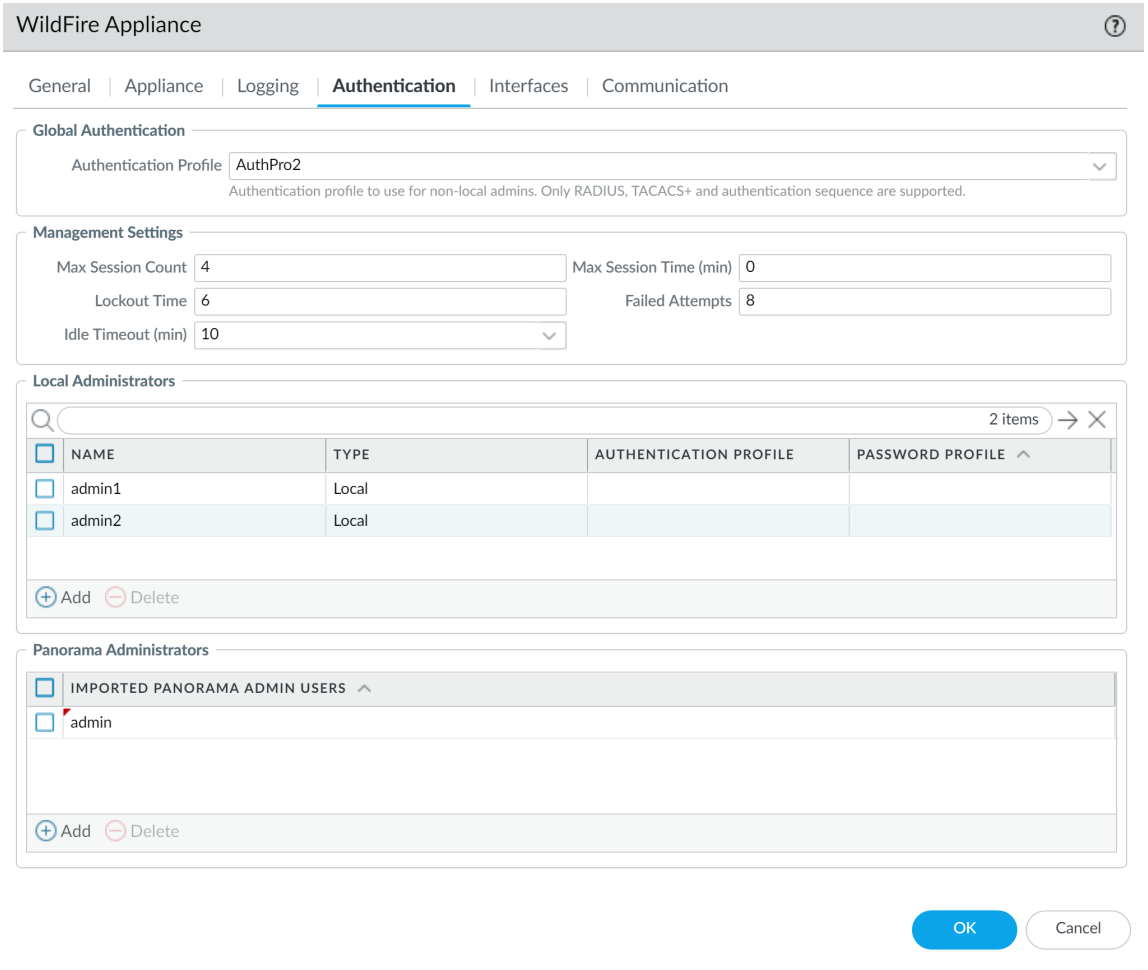
© 2019 Palo Alto Networks, Inc.

如果沒有指派全域驗證設定檔，您必須指派一個驗證設定檔到單獨每個本機管理員才可利用遠端驗證。

3. 為 WildFire 設備設定驗證 **Timeout Configuration**（逾時設定）。
   1. 輸入 **Failed Attempt**（失敗嘗試）次數，在達到此次數之後使用者將被鎖定在 WildFire 設備 CLI 之外。
   2. 輸入 **Lockout Time**（鎖定時間）（以分鐘為單位），在使用者達到設定的 **Failed Attempts**（失敗嘗試）次數後 WildFire 設備鎖定使用者帳戶的時間。
   3. 輸入 **Idle Timeout**（閒置逾時）（以分鐘為單位），在此時間之後使用者會因為處於非作用狀態而自動登出。
   4. 輸入 **Max Session Count**（最大工作階段計數），設定多少使用者帳戶可以同時存取 WildFire 設備。
   5. 輸入管理員在自動登出之前可登入的 **Max Session Time**（最長工作階段時間）。
4. 新增 WildFire 設備管理員。

   管理員可以新增為本機管理員或作為匯入的 Panorama 管理員—但不能同時為二者。不支援將同一管理員同時新增為本機管理員和作為匯入的 Panorama 管理員，這會導致 Panorama 提交失敗。例如，如果您將 **`admin1`** 同時新增為本機和 Panorama 管理員，到 Panorama 的提交將會失敗。

   1. **Add**（新增）並設定專屬於 WildFire 設備的新管理員。這些管理員特定於為其建立的 WildFire 設備，您可以從此表格管理這些管理員。
   2. **Add**（新增）在 Panorama 上設定的任何管理員。這些管理員在 Panorama 上建立，並匯入至 WildFire 設備。
5. 按一下 **OK**（確定）以儲存 WildFire 設備驗證設定。



© 2019 Palo Alto Networks, Inc.

STEP 5 | **Commit**（提交），然後 **Commit and Push**（提交並推送）設定變更。

STEP 6 | 使用本機管理員使用者存取 WildFire 設備 CLI 以驗證您能夠成功存取 WildFire 設備。

為 *WildFire* 設備設定 *TACACS+* 驗證

您可以使用 TACACS+ 伺服器來驗證對 WildFire 設備 CLI 的管理存取。您也可以在 TACACS+ 伺服器上定義廠商特定屬性 (VSA) 來進行管理員授權管理。使用 VSA 可讓您透過目錄服務快速變更管理員的角色、存取網域和使用者群組，這通常比在 Panorama 上重新設定更加簡單。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 新增獨立 WildFire 設備給 Panorama 管理。

STEP 3 | 設定 TACACS+ 驗證。

1. 新增 TACACS+ 伺服器設定檔。

   設定檔定義了 WildFire 設備將採用何種方式連線 TACACS+ 伺服器。

   1. 選取 **Panorama** > **Server Profiles**（伺服器設定檔）> **TACACS+**，然後 **Add**（新增）設定檔。
   2. 輸入用來識別伺服器設定檔的 **Profile Name**（設定檔名稱）。
   3. 輸入 **Timeout**（逾時）間隔時間（單位為秒），超過此時間後，驗證要求將逾時（預設值為 3；範圍為 1-20）。
   4. 選取 Panorama 用於向 TACACS+ 伺服器驗證的 **Authentication Protocol**（驗證通訊協定）（預設值為 **CHAP**）。
   5. 選取 **CHAP**（如果 TACACS+ 伺服器支援此通訊協定）；它比 **PAP** 更安全。
   6. **Add**（新增）每個 TACACS+ 伺服器，然後輸入下列資訊：
      1. 用來識別伺服器的 **Name**（名稱）。
      2. **TACACS+ Server**（**TACACS+** 伺服器）IP 位址或 FQDN。
      3. **Secret**（密碼）/**Confirm Secret**（確認密碼）（用於加密使用者名稱和密碼的金鑰）。
      4. 用於驗證要求的伺服器 **Port**（連接埠）（預設值為 49）。
   7. 按一下 **OK**（確定）來儲存伺服器設定檔。
2. 將 TACACS+ 伺服器設定檔指派給驗證設定檔。

   驗證設定檔中定義一群管理員通用的驗證設定。

   1. 選取 **Panorama** > **Authentication Profile**（驗證設定檔），然後 **Add**（新增）設定檔。
   2. 輸入用來識別設定檔的 **Name**（名稱）。
   3. 將 **Type**（類型）設為 **TACACS+**。
   4. 選取您設定的 **Server Profile**（伺服器設定檔）。
   5. 選取 **Retrieve user group from TACACS+**（從 **TACACS+** 擷取使用者群組），以從 TACACS+ 伺服器上定義的 VSA 收集使用者群組資訊。

      Panorama 會比對群組資訊與您在驗證設定檔「允許清單」中指定的群組。
   6. 選取 **Advanced**（進階），然後在 Allow List（允許清單）中，**Add**（新增）允許使用此驗證設定檔進行驗證的管理員。
   7. 按一下 **OK**（確定）來儲存驗證設定檔。

STEP 4 | 為 WildFire 設備設定驗證。

1. 選取 **Panorama** > **Managed WildFire Appliances**（受管理的 **WildFire** 設備），然後選取您之前新增的 WildFire 設備。
2. 選取您在上一步中設定的 **Authentication Profile**（驗證設定檔）。

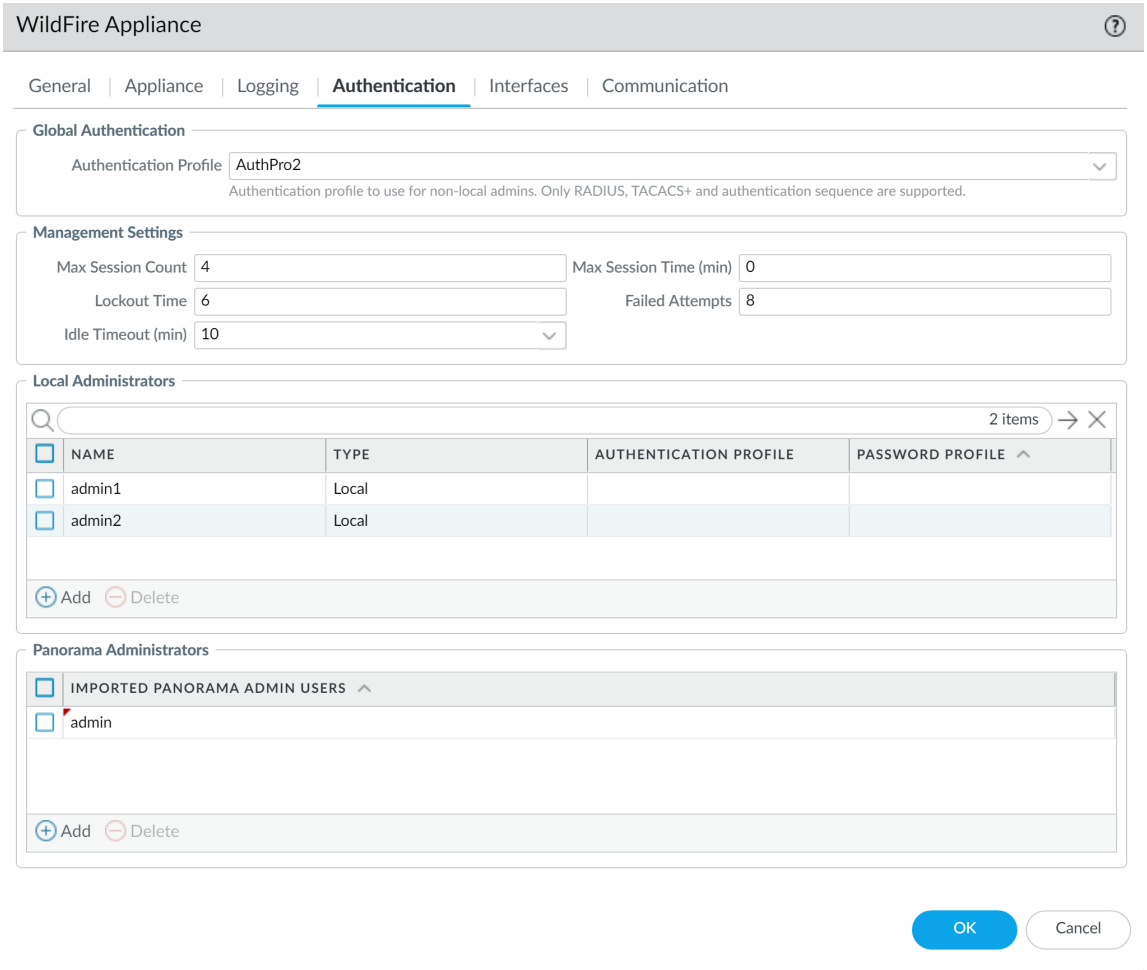
© 2019 Palo Alto Networks, Inc.

如果沒有指派全域驗證設定檔，您必須指派一個驗證設定檔到單獨每個本機管理員才可利用遠端驗證。

3. 為 WildFire 設備設定驗證 **Timeout Configuration**（逾時設定）。
   1. 輸入 **Failed Attempt**（失敗嘗試）次數，在達到此次數之後使用者將被鎖定在 WildFire 設備 CLI 之外。
   2. 輸入 **Lockout Time**（鎖定時間）（以分鐘為單位），在使用者達到設定的 **Failed Attempts**（失敗嘗試）次數後 WildFire 設備鎖定使用者帳戶的時間。
   3. 輸入 **Idle Timeout**（閒置逾時）（以分鐘為單位），在此時間之後使用者會因為處於非作用狀態而自動登出。
   4. 輸入 **Max Session Count**（最大工作階段計數），設定多少使用者帳戶可以同時存取 WildFire 設備。
   5. 輸入管理員在自動登出之前可登入的 **Max Session Time**（最長工作階段時間）。
4. 新增 WildFire 設備管理員。

   管理員可以新增為本機管理員或作為匯入的 Panorama 管理員—但不能同時為二者。不支援將同一管理員同時新增為本機管理員和作為匯入的 Panorama 管理員，這會導致 Panorama 提交失敗。例如，如果您將 **admin1** 同時新增為本機和 Panorama 管理員，到 Panorama 的提交將會失敗。

   1. **Add**（新增）並設定專屬於 WildFire 設備的新管理員。這些管理員特定於為其建立的 WildFire 設備，您可以從此表格管理這些管理員。
   2. **Add**（新增）在 Panorama 上設定的任何管理員。這些管理員在 Panorama 上建立，並匯入至 WildFire 設備。
5. 按一下 **OK**（確定）以儲存 WildFire 設備驗證設定。



© 2019 Palo Alto Networks, Inc.

STEP 5 | **Commit**（提交），然後 **Commit and Push**（提交並推送）設定變更。

STEP 6 | 使用本機管理員使用者存取 WildFire 設備 CLI 以驗證您能夠成功存取 WildFire 設備。

為 *WildFire* 設備設定 *LDAP* 驗證

您可以使用 LDAP 對存取 WildFire 設備 CLI 的一般使用者進行驗證。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 新增獨立 WildFire 設備給 Panorama 管理。

STEP 3 | 新增 LDAP 伺服器設定檔。

設定檔定義了 WildFire 設備將採用何種方式連線 LDAP 伺服器。

1. 選取 **Panorama** > **Server Profiles**（伺服器設定檔）> **LDAP**，然後 **Add**（新增）伺服器設定檔。
2. 輸入用來識別伺服器設定檔的 **Profile Name**（設定檔名稱）。
3. **Add**（新增）LDAP 伺服器（最多可新增四個）。對於每個伺服器，輸入 **Name**（名稱）（用於識別伺服器）、**LDAP Server**（**LDAP** 伺服器）IP 位址或 FQDN，以及伺服器 **Port**（連接埠）（預設值為 389）。

   如果您使用 *FQDN* 位址物件識別伺服器並隨後變更了位址，則必須要提交變更，以便新伺服器位址生效。
4. 選取伺服器 **Type**（類型）。
5. 選取 **Base DN**（基礎 **DN**）。

   識別您目錄 Base DN，打開**Active Directory Domains and Trusts**（主動式目錄網域與信任）Microsoft 管理控制台管理單元，並使用頂級網域名稱。
6. 輸入 **Bind DN**（繫結 **DN**）與 **Password**（密碼）以讓驗證服務能驗證防火牆。

   繫結 *DN* 賬號須具有讀取 *LDAP* 目錄的權限。
7. 輸入 **Bind Timeout**（繫結逾時）和**Search Timeout**（搜尋逾時），單位為秒（預設值均為 30）。
8. 輸入 **Retry Interval**（重試間隔）（秒）（預設值為 60）。
9. （選用）如果您希望端點使用 SSL 或 TLS 更安全的連線目錄伺服器，請啟用 **Require SSL/TLS secured connection**（需要 **SSL/TLS** 安全連線）選項（預設為已啟用）。端點使用的協定視乎伺服器連接埠而定：
   - 389（預設）—TLS（特別是 WildFire 設備會使用 StartTLS 操作，用來升級連接至 TLS 的初始純文字連線。）
   - 636—SSL
   - 任何其他連接埠—WildFire 設備首先會嘗試使用 TLS。若目錄伺服器不支援 TLS，則 WildFire 設備會回復使用 SSL。
10. （選用）為了獲得額外的安全，請啟用 **Verify Server Certificate for SSL sessions**（確認 **SSL** 工作階段的伺服器憑證）選項，讓端點確認目錄伺服器為 SSL/TLS 連線所呈現的憑證。若要啟用驗證，您也必須啟用 **Require SSL/TLS secured connection**（要求 **SSL/TLS** 安全連線）選項。為了順利確認，憑證必須滿足以下條件之一：
    - 位於 Panorama 憑證清單內：**Panorama** > **Certificate Management**（憑證管理）> **Certificates**（憑證）> **Device Certificates**（設備憑證）。若有必要，將憑證匯入至 Panorama。
    - 憑證簽署者位於受信任的憑證授權單位清單中：**Panorama** > **Certificate Management**（憑證管理）> **Certificates**（憑證）。
11. 按一下 **OK**（確定）來儲存伺服器設定檔。

© 2019 Palo Alto Networks, Inc.

STEP 4 | 為 WildFire 設備設定驗證。

1. 選取 **Panorama** > **Managed WildFire Appliances**（受管理的 **WildFire** 設備），然後選取您之前新增的 WildFire 設備。
2. 為 WildFire 設備設定驗證 **Timeout Configuration**（逾時設定）。
   1. 輸入 **Failed Attempt**（失敗嘗試）次數，在達到此次數之後使用者將被鎖定在 WildFire 設備 CLI 之外。
   2. 輸入 **Lockout Time**（鎖定時間）（以分鐘為單位），在使用者達到設定的 **Failed Attempts**（失敗嘗試）次數後 WildFire 設備鎖定使用者帳戶的時間。
   3. 輸入 **Idle Timeout**（閒置逾時）（以分鐘為單位），在此時間之後使用者會因為處於非作用狀態而自動登出。
   4. 輸入 **Max Session Count**（最大工作階段計數），設定多少使用者帳戶可以同時存取 WildFire 設備。
   5. 輸入管理員在自動登出之前可登入的 **Max Session Time**（最長工作階段時間）。
3. 新增 WildFire 設備管理員。

   管理員可以新增為本機管理員或作為匯入的 Panorama 管理員—但不能同時為二者。不支援將同一管理員同時新增為本機管理員和作為匯入的 Panorama 管理員，這會導致 Panorama 提交失敗。例如，如果您將 **admin1** 同時新增為本機和 Panorama 管理員，到 Panorama 的提交將會失敗。

   - 設定本機管理員。

     設定專屬於 WildFire 設備的新管理員。這些管理員特定於為其建立的 WildFire 設備，您可以從此表格管理這些管理員。

     1. **Add**（新增）一個或多個新本機管理員。
     2. 輸入本機管理員的 **Name**（名稱）。
     3. 指派您之前建立的 **Authentication Profile**（驗證設定檔）。

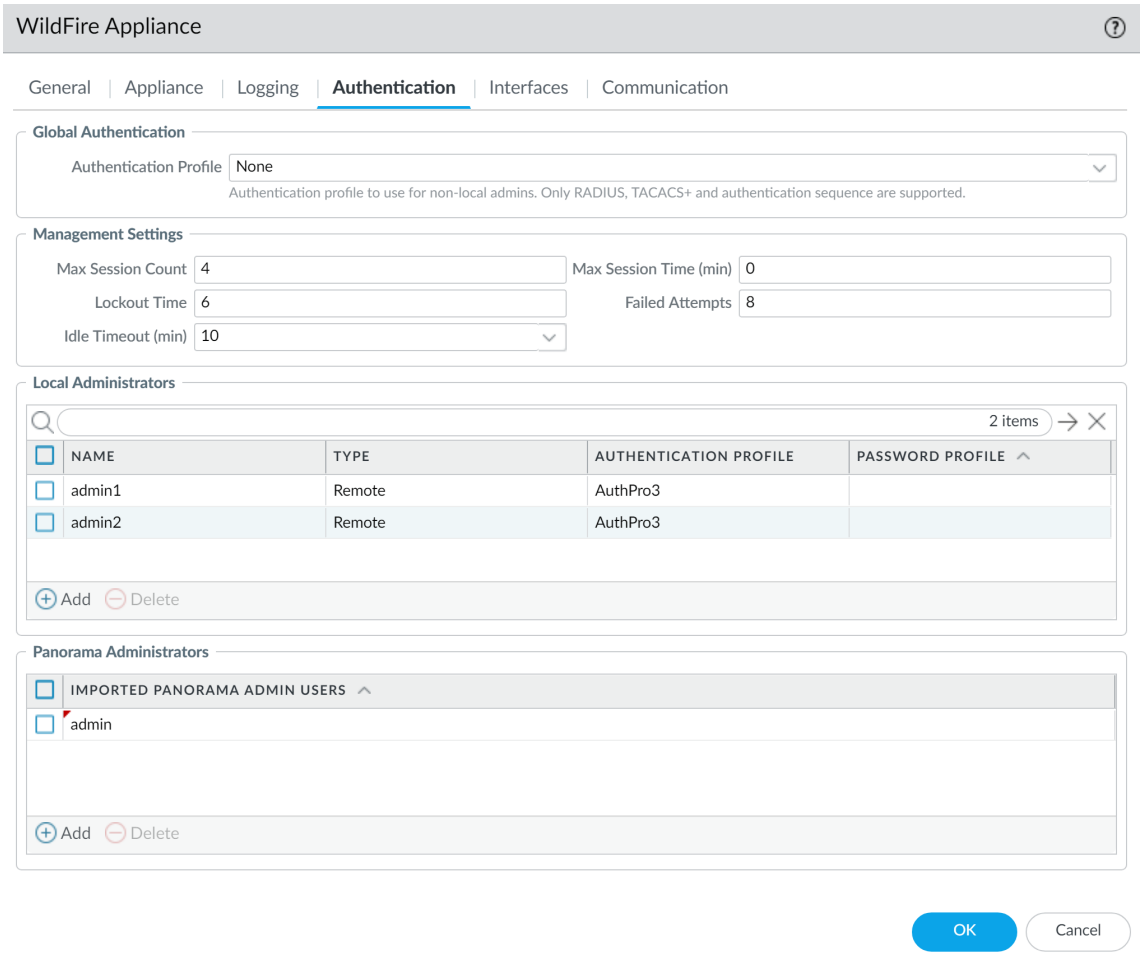
        LDAP 驗證設定檔僅支援個別本地管理員。

     4. 啟用（核取）**Use Public Key Authentication (SSH)**（使用公開金鑰驗證 **(SSH)**）以匯入公開金鑰檔案進行驗證。
     5. 選取 **Password Profile**（密碼設定檔）以設定到期參數。
   - 匯入現有 Panorama 管理員

     匯入 Panorama 上的現有管理員。這些管理員在 Panorama 上設定和管理，並匯入至 WildFire 設備。

     1. **Add**（新增）現有 Panorama 管理員
4. 按一下 **OK**（確定）以儲存 WildFire 設備驗證設定。

© 2019 Palo Alto Networks, Inc.



STEP 5 | **Commit**（提交），然後 **Commit and Push**（提交並推送）設定變更。

STEP 6 | 使用本機管理員使用者存取 WildFire 設備 CLI 以驗證您能夠成功存取 WildFire 設備。

© 2019 Palo Alto Networks, Inc.

使用 WildFire 設備和叢集上的自訂憑證進行驗證

依預設，WildFire® 設備會使用預先定義的憑證，以讓其他 PaloAltoNetworks® 防火牆和設備相互驗證，以建立 SSL 連線來用於管理存取和裝置間通訊。不過，您可以設定改用自訂憑證進行驗證。自訂憑證可讓您建立唯一的信任鏈，以確保 Panorama™ 和防火牆所管理的 WildFire 設備與 WildFire 叢集之間的相互驗證。您可以在 Panorama 或防火牆上本機生成這些憑證、從受信任的第三方憑證授權單位（CA）獲得它們，或從企業私有關鍵基礎設施（PKI）獲得憑證。

對於使用自訂憑證的詳細內容，請參閱 SSL/TLS 連線如何相互驗證？

- 設定 Panorama 管理的 WildFire 設備的自訂憑證
- 以單一自訂憑證設定 WildFire 叢集驗證
- 將自訂憑證套用在透過 Panorama 設定的 WildFire 設備

設定 Panorama 管理的 WildFire 設備的自訂憑證

若您使用 Panorama™ 管理您的 WildFire® 設備或 WildFire 叢集，則可以透過 Panorama 網頁介面而非使用 WildFire 設備 CLI 來設定自訂憑證驗證。使用此連線以轉送樣本到 WildFire 作為分析使用的防火牆或 Panorama。

此程序說明如何在單一 WildFire 設備安裝唯一的憑證。如果 WildFire 設備為叢集的一部分，則該裝置與每一個叢集成員都會有唯一的用戶端憑證。若要將單一憑證部署到所有叢集的 WildFire 設備中，請參閱以單一自訂憑證設定 WildFire 叢集驗證。

STEP 1 | 取得關鍵配對與憑證授權單位 (CA)，以授予 WildFire 設備和防火牆憑證。

STEP 2 | 輸入 CA 憑證以驗證防火牆身份以及 WildFire 金鑰配對。

1. 選取 **Panorama** > **Certificate Management**（憑證管理）> **Certificates**（憑證）> **Import**（匯入）。
2. 輸入 CA 憑證與 Panorama 金鑰配對。

STEP 3 | 設定包含 root CA 和中繼 CA 的憑證設定檔。此憑證設定檔定義 WildFire 設備與防火牆如何手動驗證。

1. 選取 **Panorama** > **Certificates Management**（憑證管理）> **Certificate Profile**（憑證設定檔）。
2. 設定憑證設定檔。

   如果您在憑證設定檔中設定中繼 CA，則必須也包含 root CA。

STEP 4 | 設定 WildFire 設備的 SSL/TLS 設定檔。

PAN-OS 8.0 和更新版本僅支援 *TLS 1.2* 和更高級版本，因此 你必須設定最高版本為 *TLS 1.2* 或 *max*（最高）。

1. 選取 **Panorama** > **Certificate Management**（憑證管理）> **SSL/TLS Service Profile**（**SSL/TLS** 服務設定檔）。
2. 設定 SSL/TLS 服務設定檔，以定義憑證和通訊協定供 WildFire 設備其防火牆與用於 SSL/TLS 服務。

STEP 5 | 在 WildFire 上設定安全伺服器通訊。

1. 選取 **Panorama** > **Managed WildFire Clusters**（受管理的 **WildFire** 叢集）或 **Panorama** > **Managed WildFire Appliances**（受管理的 **WildFire** 設備）並選取一個叢集或設備。
2. 選取 **Communication**（通訊）。

© 2019 Palo Alto Networks, Inc.

3. 啟用 **Customize Secure Server Communication**（自訂安全伺服器通訊）功能。
4. 選取 **SSL/TLS Service Profile**（**SSL/TLS** 服務設定檔）。此 SSL/TLS 服務設定檔會套用至 WildFire 設備和防火牆或 Panorama 之間的所有 SSL 連線。
5. 選取您設定作為 WildFire 設備和防火牆或 Panorama 通訊使用的 **Certificate Profile**（憑證設定檔）。
6. 確認 **Custom Certificates Only**（僅限自訂憑證）為停用（已清除）。這能讓 WildFire 設備在移轉至自訂憑證同時，繼續使用預定義憑證與防火牆通訊。
7. （選用）設定授權清單。
   1. **Add**（新增）授權清單。
   2. 在憑證設定檔中，選取 **Subject**（主體）或 **Subject Alt Name**（主體別名）作為識別項類型。
   3. 如果識別項是 Subject（主體），請輸入 Common Name（通用名稱），如果識別項是 Subject Alt Name（主體別名），請輸入 IP 位址、主機名稱或電子郵件。
   4. 按一下 **OK**（確定）。
   5. 啟用 **Check Authorization List**（檢查授權清單）以強制執行授權清單。
8. 按一下 **OK**（確定）。
9. **Commit**（提交）您的變更。

STEP 6 | 輸入 CA 憑證以驗證 WildFire 設備憑證。

1. 登入防火牆 Web 介面。
2. 匯入 CA 憑證。

STEP 7 | 設定防火牆本機或 SCEP 憑證。

- 若您使用本機憑證，請 輸入防火牆金鑰配對。
- 如果您使用 SCEP 傳送防火牆憑證，請設定 SCEP 設定檔。

STEP 8 | 為防火牆或 Panorama 設定憑證設定檔。您可以在每個用戶端防火牆或 Panorama 設備上個別地設定此設定檔，或者您可以使用範本從 Panorama 推送設定到受管理的防火牆。

1. 對於防火牆，請選取 **Device**（裝置）> **Certificate Management**（憑證管理）> **Certificate Profile**（憑證設定檔），或者對於 Panorama，則選取 **Panorama** > **Certificate Management**（憑證管理）> **Certificate Profile**（憑證設定檔）。
2. 設定憑證設定檔。

STEP 9 | 將自訂憑證部署在每個防火牆或 Panorama 設備。

1. 登入防火牆 Web 介面。
2. 防火牆請選取 **Device**（裝置）> **Setup**（設定）> **Management**（管理）或 Panorama 請選取 **Panorama** > **Setup**（設定）> **Management**（管理）並 **Edit**（編輯）安全通訊設定。
3. 選取 **Certificate Type**（憑證類型）、**Certificate**（憑證）與 **Certificate Profile**（憑證設定檔）。
4. 在自訂通訊設定中，選取 **WildFire Communication**（**WildFire** 通訊）。
5. 按一下 **OK**（確定）。
6. **Commit**（提交）您的變更。

STEP 10 | 在所有受管理的裝置上部署自訂憑證後，強制執行自訂憑證驗證。

1. 登入 Panorama。
2. 選取 **Panorama** > **Managed WildFire Clusters**（受管理的 **WildFire** 叢集）或 **Panorama** > **Managed WildFire Appliances**（受管理的 **WildFire** 設備）並選取一個叢集或設備。
3. 選取 **Communication**（通訊）。
4. 選取 **Custom Certificate Only**（僅限自訂憑證）。
5. 按一下 **OK**（確定）。
6. **Commit**（提交）您的變更。

在提交此變更後，WildFire 會立即開始強制執行自訂憑證。

© 2019 Palo Alto Networks, Inc.

以單一自訂憑證設定 WildFire 叢集驗證

與為每個在叢集中的 WildFire® 設備指派唯一憑證相反，您可以指派單一、共享的用戶端憑證給整個 WildFire 叢集，因此，也允許您推送單一憑證到所有叢集中的 WildFire 應用程式，而非為每個叢集成員設定單獨的憑證。因為個別 WildFire 設備共享一個用戶端憑證，因此您必須為每個 WildFire 設備設定唯一的主機名稱（DNS 名稱）。接著您可以將所有主機名稱新增到共享的憑證中作為憑證屬性，或使用匹配所有在此叢集中 WildFire 設備上自訂主機名稱的一個通配符字串。

若要設定 WildFire 叢集的單一自訂憑證，以在與 Panorama™ 通訊時使用，請完成以下程序。

STEP 1 | 獲得伺服器金鑰配對與 CA 憑證（Panorama）。

STEP 2 | 設定包含 root 憑證授權單位（CA）和中繼 CA 的憑證設定檔。憑證設定檔定義 WildFire 叢集（用戶端）與 Panorama 設服（主機端）的驗證。

1. 選取 **Panorama** > **Certificates Management**（憑證管理）> **Certificate Profile**（憑證設定檔）。
2. 設定憑證設定檔。

   如果您在憑證設定檔中設定中繼 CA，則必須也包含 root CA。

STEP 3 | 設定 SSL/TLS 服務設定檔。

1. 選取 **Panorama** > **Certificate Management**（憑證管理）> **SSL/TLS Service Profile**（**SSL/TLS** 服務設定檔）。
2. 設定 SSL/TLS 服務設定檔，以定義憑證和通訊協定供 WildFire 叢集及用於 SSL/TLS 服務的 Panorama 設備。

STEP 4 | 連接每個在 Panorama 叢集的節點。

STEP 5 | 在叢集的每個節點上設定唯一主機名稱（DNS 名稱）或使用匹配所有叢集中 WildFire 設備上設定的自訂 DNS 名稱。

若使用單一通配符字串，請參閱 RFC-6125，章節 6.4.3 以瞭解通配符字串值的需求及限制。在設定自訂 DNS 名稱時，請確定您瞭解這些需求與限制。

1. 登入節點上的 WildFire CLI。
2. 使用以下命令以指派唯一自訂 DNS 名稱給節點。

```
admin@WF-500> configure
```

```
admin@WF-500# set deviceconfig setting wildfire custom-dns-name <dns-name>
```

3. **Commit**（提交）您的變更。
4. 對於叢集中的每個節點，重覆此程序。

STEP 6 | 在 Panorama 上，為所有叢集中的節點生成用戶端憑證。在憑證屬性下，為每個您指派給叢集節點的自訂 DNS 名稱新增一個主機名稱項目，或用匹配所有節點主機名稱的一個通配符字串新增一個主機名稱項目，如 *.example.com；您僅能在每個自訂 DNS 名稱共享一個通用字串時才能這麼做。

STEP 7 | 在 Panorama 設定叢集用戶端憑證的憑證設定檔。

1. 選取 Panorama 的 **Panorama** > **Certificates Management**（憑證管理）> **Certificate Profile**（憑證設定檔）。
2. 設定憑證設定檔。

STEP 8 | 在每個節點上部署自訂憑證。此憑證設定檔必須包含簽訂 Panorama 伺服器憑證的 CA 憑證。

© 2019 Palo Alto Networks, Inc.

1. 選取 **Panorama** > **Managed WildFire Clusters**（受管理的 **WildFire** 叢集），然後按一下業集名稱。
2. 選取 **Communication**（通訊）。
3. 在安全用戶端通訊下，選取 **Certificate Type**（憑證類型）、**Certificate**（憑證）與 **Certificate Profile**（憑證設定檔）。
4. 按一下 **OK**（確定）。
5. **Commit**（提交）您的變更。

STEP 9 | 在 Panorama 上設定安全伺服器通訊。

1. 選取 **Panorama** > **Setup**（設定） > **Management**（管理） 和 **Edit**（編輯） 以選取 **Customize Secure Server Communication**（自訂安全伺服器通訊）。
2. 啟用 **Customize Secure Server Communication**（自訂安全伺服器通訊）。
3. 選取 **SSL/TLS Service Profile**（**SSL/TLS** 服務設定檔）。此 SSL/TLS 服務設定檔會套用至 WildFire 和 Panorama 之間的所有 SSL 連線。
4. 選取 Panorama **Certificate Profile**（憑證設定檔）。
5. 啟用 **Custom Certificate Only**（僅限自訂憑證）。
6. 按一下 **OK**（確定）。
7. **Commit**（提交）您的變更。

將自訂憑證套用在透過 Panorama 設定的 WildFire 設備

依預設，Panorama™ 在與 WildFire® 設備通訊時使用預定義的憑證以推送設定。您可以或者設定自訂憑證為 Panorama 用來推送設定到受管理的 WildFire 設備或叢集的連線建立相互驗證。完成以下程序以設定 Panorama 上的伺服器憑證以及 WildFire 設備上的用戶端憑證。

STEP 1 | 取得 關鍵配對與憑證授權單位 (CA)，以授予 Panorama 和 WildFire 設備憑證。

STEP 2 | 輸入 CA 憑證以驗證 WildFire 設備身份以及 Panorama 金鑰配對。

1. 選取 **Panorama** > **Certificate Management**（憑證管理） > **Certificates**（憑證） > **Import**（匯入）。
2. 輸入 CA 憑證與 Panorama 金鑰配對。

STEP 3 | 設定包含 root CA 和中繼 CA 的憑證設定檔。憑證設定檔定義 WildFire 設備（用戶端）與 Panorama 虛擬或 M-Series 設備（主機端）的驗證。

1. 選取 **Panorama** > **Certificates Management**（憑證管理） > **Certificate Profile**（憑證設定檔）。
2. 設定憑證設定檔。

   如果您在憑證設定檔中設定中繼 CA，則必須也包含 root CA。

STEP 4 | 設定 SSL/TLS 服務設定檔。

1. 選取 **Panorama** > **Certificate Management**（憑證管理） > **SSL/TLS Service Profile**（**SSL/TLS** 服務設定檔）。
2. 設定 SSL/TLS 服務設定檔，以定義憑證和通訊協定供 WildFire 及用於 SSL/TLS 服務的 Panorama 設備。

STEP 5 | 在 Panorama 設備上設定安全伺服器通訊。

1. 選取 **Panorama** > **Setup**（設定） > **Management**（管理） 和 **Edit**（編輯） 以選取 **Customize Secure Server Communication**（自訂安全伺服器通訊）。
2. 啟用 **Customize Secure Server Communication**（自訂安全伺服器通訊）功能。
3. 選取 **SSL/TLS Service Profile**（**SSL/TLS** 服務設定檔）。
4. 從 **Certificate Profile**（憑證設定檔）下拉式清單中，選取憑證設定檔。
5. 確認 **Custom Certificates Only**（僅限自訂憑證）為停用（已清除）。這能讓 Panorama 在移轉至自訂憑證同時，繼續使用預定義憑證與 WildFire 通訊。

© 2019 Palo Alto Networks, Inc.

6. （選用）設定授權清單。
   1. **Add**（新增）授權清單。
   2. 在憑證設定檔中，選取 **Subject**（主體）或 **Subject Alt Name**（主體別名）作為識別項類型。
   3. 如果識別項是`Subject`（主體），請輸入**Common Name**（通用名稱），如果識別項是 `Subject Alt Name`（主體別名），請輸入 **IP** 位址、主機名稱或電子郵件。
   4. 按一下 **OK**（確定）。
   5. 啟用 **Check Authorization List**（檢查授權清單）選項以設定 Panorama 強制執行授權清單。
7. 按一下 **OK**（確定）。
8. **Commit**（提交）您的變更。

STEP 6 | 輸入 CA 憑證以驗證 Panorama 憑證。

1. 登入 Panorama 使用者介面。
2. 匯入 CA 憑證。

STEP 7 | 設定 WildFire 設備的本機或 SCEP 憑證。

1. 若您使用本機憑證，請 輸入 WF-500 設備金鑰配對。
2. 如果您為 WildFire 設備憑證使用 SCEP，請設定 SCEP 設定檔。

STEP 8 | 為 WildFire 設備設定憑證設定檔。

1. 選取 **Panorama** > **Certificates Management**（憑證管理）> **Certificate Profile**（憑證設定檔）。
2. 設定憑證設定檔。

STEP 9 | 在每個受管理的 WildFire 設備上部署自訂憑證。

1. 登入 Panorama。
2. 選取 **Panorama** > **Managed WildFire Appliance**（受管理的 **WildFire** 設備），然後按一下叢集或設備名稱。
3. 選取 **Communication**（通訊）。
4. 在安全用戶端通訊下，選取來自各別下拉式選單的 **Certificate Type**（憑證類型）、**Certificate**（憑證）與 **Certificate Profile**（憑證設定檔）。
5. 按一下 **OK**（確定）。
6. **Commit**（提交）您的變更。

STEP 10 | 在所有受管理的 WildFire 設備上部署自訂憑證後，強制執行自訂憑證驗證。

1. 選取 **Panorama** > **Setup**（設定）> **Management**（管理），然後 **Edit**（編輯）安全通訊設定。
2. **Allow Custom Certificate Only**（僅允許自訂憑證）。
3. 按一下 **OK**（確定）。
4. **Commit**（提交）您的變更。

在提交此變更後，連線斷開等候時間開始倒數。在等候時間結束時，Panorama 與其受管理的 WildFire 設備無法在沒有訂定憑證的情況下連線。

© 2019 Palo Alto Networks, Inc.

移除 WildFire 設備不要由 Panorama 管理

您可以從 Panorama 管理移除 WildFire 獨立設備。當您移除獨立 WildFire 設備不要由 Panorama 管理時，就無法再享有集中管理的好處，而必須使用其本機 CLI 和指令碼來管理設備。

STEP 1 | 選取 **Panorama** > **Managed WildFire Appliances**（受管理的 **WildFire** 設備）。

STEP 2 | 選取每個設備旁的核取方塊，或按一下設備的那一列，以選取您想移除不要由 Panorama 管理的一個或多個 WildFire 設備。

STEP 3 | **Remove**（移除）選取的 WildFire 設備不要由 Panorama 管理。

© 2019 Palo Alto Networks, Inc.

管理 WildFire 叢集

WildFire 設備叢集是一組互連的 WildFire 設備，可彙集資源以提升分析與儲存能力、為更多防火牆提供支援，及簡化多個 WildFire 設備的設定和管理。若要增加安全性並維持轉移內容的保密性，則您也可以加密叢集中 WildFire 設備間的通訊。若需要 WildFire 叢集與部署流程的詳細資料，請參考 WildFire 設備叢集。

以下任務可以使用 Panorama 執行以管理您的 WildFire 叢集。

- 在 Panorama 上集中設定叢集
- 使用 Panorama 檢視 WildFire 叢集狀態
- 在有網際網路連線的情況下在 Panorama 上集中升級叢集
- 在沒有網際網路連線的情況下在 Panorama 上集中升級叢集
- 使用集中於 Panorama 的預定義憑證，設定設備對設備的加密
- 使用集中於 Panorama 的自訂憑證設定設備對設備的加密

在 Panorama 上集中設定叢集

在 Panorama M-Series 或虛擬設備上設定 WildFire 設備之前，使兩個 WildFire 設備可以作為一個高可用性控制器節點對進行設定，並用所需的任何其他 WildFire 設備作為工作節點，提升叢集的分析、儲存及復原能力。

如果 WildFire 設備是新設備，請查看開始使用 WildFire，以確保您完成設定的基本步驟，例如確認您的 WildFire 授權為主動、啟用日誌記錄、將防火牆連接至 WildFire 設備，以及設定基本 WildFire 功能。

若要建立 *WildFire* 設備叢集，必須將您想要放入叢集的所有 WildFire 設備升級至 *PAN-OS 8.0.1* 或更新版本。如果您使用 *Panorama* 來管理 *WildFire* 設備叢集，*Panorama* 也必須運行 *PAN-OS 8.0.1* 或更新版本。在您想要新增至叢集的每個 *WildFire* 設備上，在 *WildFire* 設備 *CLI* 上運行 ***show system info | match version*** 以確保設備運行的是 *PAN-OS 8.0.1* 或更新版本。在您用於管理叢集（ 或獨立設備 ）的每個 *Panorama* 設備上，*Dashboard*（儀表板）> *General Information*（一般資訊）> *Software Version*（軟體版本）會顯示運行的軟體版本。

當 WildFire 設備可用時，請執行適當的工作：

- 在 Panorama 上設定叢集並新增節點
- 在 Panorama 上設定一般叢集設定
- 為 WildFire 叢集設定驗證
- 從 Panorama 管理中移除叢集

不支援使用 *Panorama* 從叢集中移除節點。而要使用本機 *WildFire CLI* 從本機叢集移除節點。

在 *Panorama* 上設定叢集並新增節點

使用 Panorama 設定 WildFire 設備之前，您必須將 Panorama 升級至 8.0.1 或更新版本，並將您打算新增至叢集的所有 WildFire 設備升級 8.0.1 或更新版本。所有 WildFire 設備必須執行相同版本的 PAN-OS。

您可以使用 Panorama M-Series 或虛擬設備來管理最多 200 個 WildFire 設備。這 200 個 WildFire 設備包括獨立設備和 WildFire 設備叢集節點（如果您也新增了 WildFire 設備以使用 Panorama 管理）。除非特別說明，設定在 Panorama 上進行。

每個 *WildFire* 設備叢集節點在相同子網路中必須具有靜態 *IP* 地址及低延遲連線。

© 2019 Palo Alto Networks, Inc.

STEP 1 | 使用本機 CLI，設定將管理 WildFire 設備叢集的 Panorama 伺服器的 IP 地址。

註冊叢集或獨立 WildFire 設備至 Panorama 設備之前，您首先必須使用本機 WildFire CLI 在每個 WildFire 設備上設定 Panorama IP 地址或 FQDN。這樣每個 WildFire 設備才知道它是由哪個 Panorama 設備所管理。

1. 在每個 WildFire 設備上，設定主要 Panorama 設備管理介面的 IP 地址或 FQDN：

```
admin@WF-500# set deviceconfig system panorama-server <ip-address | FQDN>
```

2. 如果您使用備份 Panorama 設備以實現高可用性（建議），在每個 WildFire 設備上，設定備份 Panorama 設備管理介面的 IP 地址或 FQDN：

```
admin@WF-500# set deviceconfig system panorama-server-2 <ip-address |
 FQDN>
```

3. 提交每個 WildFire 設備上的設定：

```
admin@WF-500# commit
```

STEP 2 | 在主要 Panorama 設備上，註冊 WildFire 設備。

除非由於本機叢集設定，設備已屬於叢集，否則新註冊的設備將處於獨立模式。

1. 選取 **Panorama** > **Managed WildFire Appliances**（受管理的 **WildFire** 設備）與 **Add Appliance**（新增設備）。
2. 將每個 WildFire 設備的序號輸入成各自一行。如果您沒有 WildFire 設備序號清單，使用本機 CLI，在每個 WildFire 設備上執行 **show system info**，以取得序號。
3. 按一下 **OK**（確定）。

   將會顯示 WildFire 設備上已提交的設定相關資訊（若有的話），例如 IP 位址和軟體版本。已屬於叢集的 WildFire 設備（例如，由於本機叢集設定）會顯示其叢集資訊和連線狀態。

STEP 3 | （選用）將 WildFire 設備組態匯入至 Panorama 設備。

匯入設定可以節省時間，因為您能夠在 Panorama 上重新使用或編輯設定，然後將其推送至一個或多個 WildFire 設備叢集或獨立 WildFire 設備中。如果沒有您要匯入的設定，則略過此步驟。當您推送 Panorama 的設定時，推送的設定會覆寫本機設定。

1. 選取 **Panorama** > **Managed WildFire Appliances**（受管理的 **WildFire** 設備），然後從受管理的 WildFire 設備清單中選取具有您想要匯入的設定的設備。
2. **Import Config**（匯入設定）。
3. 選取 **Yes**（是）。

   匯入設定會更新顯示的資訊，並使匯入的設定成為 Panorama 設備候選設定的一部分。
4. **Commit to Panorama**（提交至 **Panorama**），使匯入的 WildFire 設備組態成為 Panorama 執行中設定的一部分。

STEP 4 | 建立新 WildFire 設備叢集。

1. 選取 **Managed WildFire Clusters**（受管理的 **WildFire** 叢集）。

   Appliance（設備）> **No Cluster Assigned**（未指定叢集）顯示獨立 WildFire 設備（節點）並表明有多少個可用節點未指定給叢集。
2. **Create Cluster**（建立叢集）。
3. 輸入英數字元叢集 **Name**（名稱），最多 63 個字元。**Name**（名稱）可以包含小寫字元和數字，如果不是第一個或最後一個字元，還可使用連字號與句點。不允許使用空格或其他字元。
4. 按一下 **OK**（確定）。

© 2019 Palo Alto Networks, Inc.

新叢集名稱會顯示，但沒有指定的 WildFire 節點。

STEP 5 | 新增 WildFire 設備至新叢集。

新增至叢集的第一個 WildFire 設備將自動變成控制器節點，新增至叢集的第二個 WildFire 設備將自動變成控制器備份節點。新增至叢集的所有後續 WildFire 設備將自動變成工作節點。工作節點會使用控制器節點設定，以使叢集的設定一致。

1. 選取新叢集。
2. 選取 **Clustering**（叢集）。
3. **Browse**（瀏覽）不屬於叢集的 WildFire 設備清單。
4. 新增（⊕）您想要包含在叢集中的每個 WildFire 設備。您最多可新增二十個節點至一個叢集。您新增至叢集的每個 WildFire 設備及其自動指定的角色將顯示。
5. 按一下 **OK**（確定）。

STEP 6 | 設定 **Management**（管理）、**Analysis Environment Network**（分析環境網路）、HA 及叢集管理介面。

如果尚未設定，則在每個叢集成員（控制器和工作節點）上設定 **Management**（管理）、**Analysis Environment Network**（分析環網路）及叢集管理介面。叢集管理介面為在叢集內進行管理與通訊的專用介面，和管理介面不同。

在控制器節點和控制器備份節點上個別設定 HA 介面。HA 介面連線主要和備份控制器節點，使其保持同步，並可回應故障轉移。

叢集節點需要這四個 *WildFire* 設備介面的 *IP* 地址。您無法在工作節點上設定 *HA* 服務。

1. 選取新叢集。
2. 選取 **Clustering**（叢集）。
3. 如果管理介面未在叢集節點上設定，則選取 **Interface Name**（介面名稱）> **Management**（管理），並輸入介面的 IP 地址、網路遮罩、服務及其他資訊。
4. 如果分析環境網路的介面未在叢集節點上設定，則選取 **Interface Name**（介面名稱）> **Analysis Environment Network**（分析環境網路），並輸入介面的 IP 地址、網路遮罩、服務及其他資訊。
5. 在控制器節點和控制器備份節點上，選取介面以用於 HA 控制連結。您必須在兩個控制器節點上設定 HA 服務的相同介面。例如，在控制器節點和控制器備份節點上，選取 **Ethernet3**。
6. 對於每個控制器節點，選取 **Clustering Services**（叢集服務）> **HA**。（**HA** 選項不適用於工作節點。）如果您也想能夠偵測介面，可選取 **Management Services**（管理服務）> **Ping**（偵測）。
7. 按一下 **OK**（確定）。
8. （建議）選取介面以在控制器節點和控制器備份節點之間作為備份 HA 控制連結使用。您必須在兩個節點上使用 HA 備份服務的相同介面。例如，在兩個節點上，選取 **Management**（管理）。

   選取兩個節點的 **Clustering Services**（叢集服務）> **HA Backup**（**HA** 備份）。如果您想要這些 **Management Services**（管理服務）在介面上 ，也可選取 **Ping**（偵測）、**SSH** 及 **SNMP**。

   Analysis Environment Network（分析環境網路）介面不能是 *HA* 或 *HA* 備份介面或叢集管理介面。
9. 選取專用介面以用於在叢集內進行管理和通訊。您必須在兩個節點上使用相同介面，例如，**Ethernet2**。
10. 選取兩個節點的 **Clustering Services**（叢集服務）> **Cluster Management**（叢集管理）。如果您也想能夠偵測介面，可選取 **Management Services**（管理服務）> **Ping**（偵測）。

    叢集中的工作節點會自動繼承專用管理和通訊介面的控制器節點設定。

© 2019 Palo Alto Networks, Inc.

STEP 7 | 提交 Panorama 設備上的設定並將其推送至叢集。

1. **Commit and Push**（提交並推送）。
2. 如果 Panorama 設備上有您不想推送的設定，請 **Edit Selections**（編輯選擇），以選取將設定推送至哪些設備。推送的設定會覆寫叢集節點上正在執行的設定，因此所有叢集節點將執行相同設定。

STEP 8 | 確認組態。

1. 選取 **Panorama** > **Managed WildFire Clusters**（受管理的 **WildFire** 叢集）。
2. 檢查下列欄位：
   - **Appliance**（設備）—新增至叢集的 WildFire 節點會顯示在叢集名稱下方，而不是顯示為獨立設備。
   - **Cluster Name**（叢集名稱）—顯示的叢集名稱針對每個節點。
   - **Role**（角色）—顯示的適當角色（**Controller**（控制器）、**Controller Backup**（控制器備份）或 **Worker**（工作））針對每個節點。
   - **Config Status**（設定狀態）—狀態為 `In Sync`（同步）。
   - **Last Commit State**（上次提交狀態）—`Commit succeeded`（提交成功）。

STEP 9 | 使用主要控制器節點（不是 Panorama Web 介面）上的本機 CLI，檢查以確保設定已同步。

如果其未同步，可在控制器節點上手動同步高可用性設定，並提交設定。

雖然可以在 Panorama 上執行大部分其他設定，但同步控制器節點高可用性設定必須在主要控制器節點的 CLI 上進行。

1. 在主要控制器節點上，檢查以確保設定已同步：

```
admin@WF-500(active-controller)> show high-availability all
```

在輸出末尾，尋找 `Configuration Synchronization` 輸出：

```
Configuration Synchronization:
    Enabled: yes
    Running Configuration: synchronized
```

如果正在執行的設定已同步，您無需手動同步設定。但是，如果設定未同步，您需要手動同步設定。

2. 如果設定未同步，在主要控制器節點上，將高可用性設定同步至遠端對等控制器節點：

```
admin@WF-500(active-controller)> request high-availability sync-to-remote
 running-config
```

如果主要控制器節點與控制器備份節點上的設定不符，主要控制器節點上的設定會覆寫控制器備份節點上的設定。

3. 提交設定：

```
admin@WF-500# commit
```

在 *Panorama* 上設定一般叢集設定

部分一般設定為選用設定，而其他一般設定則已預先填入預設值。最好檢查一下這些設定以確保叢集設定符合您的需要。一般設定包括：

- 連線至 WildFire 公共雲端並提交樣本至公共雲端。
- 設定資料保留原則。

© 2019 Palo Alto Networks, Inc.

- 設定日誌記錄。
- 設定分析環境（最適合您環境的虛擬電腦影像檔）並自訂分析環境，以最好地服務於防火牆提交至 WildFire 的各種樣本。
- 設定 DNS 伺服器、NTP 伺服器等的 IP 地址。

STEP 1 | 設定 WildFire 設備叢集節點的設定。

許多設定預先填入了預設值、控制器節點上之前存在設定的資訊，或您剛剛設定的設定。

1. 選取叢集。
2. 選取 **Appliance**（設備）。
3. 輸入新資訊，保留預先填入的叢集控制器節點中的資訊，或編輯預先填入的資訊，包括：
   - **Domain**（網域）名稱。
   - **Primary DNS Server**（主要 **DNS** 伺服器）和 **Secondary DNS Server**（次要 **DNS** 伺服器）的 IP 位址。
   - **Primary NTP Server**（主要 **NTP** 伺服器）和 **Secondary NTP Server**（次要 **NTP** 伺服器）的 **NTP Server Address**（**NTP** 伺服器地址）和 **Authentication Type**（驗證類型）。**Authentication Type**（驗證類型）選項為 **None**（無）、**Symmetric Key**（對稱金鑰）和 **AutoKey**。

STEP 2 | 設定一般叢集設定。

許多設定預先填入了預設值、控制器節點上之前存在設定的資訊，或您剛剛設定的設定。

1. 選取新叢集 > **General**（一般）。
2. （選用）**Enable DNS**（啟用 **DNS**），以便控制器節點使用 DNS 協定公告服務狀態。叢集控制器在管理 (MGT) 介面連接埠提供 DNS 服務。
3. **Register Firewall To**（註冊防火牆至）可使用叢集控制器公告的服務。Palo Alto Networks 建議將兩個控制器均新增為授權伺服器，以實現高可用性。使用以下格式：

   ```
   wfpc.service.<cluster-name>.<domain>
   ```

   例如，*paloaltonetworks.com* 網域中名稱為 *mycluster* 的叢集的域名為：

   ```
   wfpc.service.mycluster.paloaltonetworks.com
   ```

4. 輸入叢集的 **Content Update Server**（內容更新伺服器）。使用預設 `updates.paloaltonetworks.com` FQDN 連線至最近的伺服器。**Check Server Identity**（檢查伺服器識別）可透過比對憑證中的通用名稱 (CN) 與伺服器的 IP 位址或 FQDN，確認更新伺服器的身分識別（預設情況下此選項為選中狀態）。
5. （選用）輸入公共 **WildFire Cloud Server**（**WildFire** 雲端伺服器）位置或使用預設 `wildfire.paloaltonetworks.com`，讓叢集（或 Panorama 管理的獨立設備）可以將資訊傳送到最接近的伺服器。如果您將此欄位留空，且不連線至 WildFire 雲端伺服器，叢集將無法直接從 WildFire 公共雲端接收特徵碼更新，並無法傳送樣本進行分析或向公共雲端提供資料。
6. 如果您將叢集連線至公共 WildFire 雲端，選取您想要啟用的雲端服務：
   - **Send Analysis Data**（傳送分析資料）—傳送關於本機惡意軟體分析的 XML 報告。如果您傳送實際樣本，叢集不會傳送報告。
   - **Send Malicious Samples**（傳送惡意樣本）—傳送惡意樣本。
   - **Send Diagnostics**（傳送診斷資料）—傳送診斷資料。
   - **Verdict Lookup**（裁定查找）—在執行本機分析前自動查詢 WildFire 公共雲端進行裁定，以減少本機 WildFire 設備叢集上的負載。
7. 根據叢集將分析的樣本類型，選取要使用的 **Sample Analysis Image**（樣本分析影像檔）。

© 2019 Palo Alto Networks, Inc.

8. 設定叢集保留 **Benign/Grayware**（良性/灰色）樣本資料和 **Malicious**（惡意）樣本資料的時間。前者的時間範圍為 1 到 90 天，預設值為 14 天；後者的最小值為 1 天，無最大值（無限），預設值為無限。惡意樣本資料包括網路釣魚裁定。
9. （選用）視環境而定，選取 **Preferred Analysis Environment**（偏好的分析環境）以對**Executables**（可執行檔）或**Documents**（文件）配置更多資源。**Default**（預設值）配置會在 **Executables**（可執行檔）和 **Documents**（文件）之間取得平衡。可用資源數量取決於叢集中 WildFire 節點的數量。

STEP 3 | 檢查以確保主要和備份 Panorama 伺服器均已設定。

如果您未設定備份 Panorama 伺服器並想設定，可以新增備份 Panorama 伺服器。

1. 選取叢集。
2. 選取 **Appliance**（設備）。
3. 核取（或輸入）主要 **Panorama Server**（**Panorama** 伺服器）和備份 **Panorama Server 2**（**Panorama** 伺服器 **2**）（如果您使用高可用性設定進行集中叢集管理）的 IP 地址或 FQDN。

STEP 4 | （選用）設定叢集的系統和設定日誌設定，包括日誌轉送。

1. 選取叢集。
2. 選取 **Logging**（日誌記錄）。
3. 選取 **System**（系統）或 **Configuration**（組態）以分別設定系統或設定日誌。設定兩者的程序非常類似。
4. **Add**（新增）（⊕）日誌轉送執行個體並為其 **Name**（命名），選取 **Filter**（篩選器），並設定 **Forward Method**（轉送方法）（**SNMP**、**Email**（電子郵件）、**Syslog**（系統日誌）或 **HTTP**）。

STEP 5 | 設定管理員驗證。

1. 選取叢集。
2. 選取 **Authentication**（驗證）。
3. 選取 **Authentication Profile**（驗證設定檔），為 **None**（無）或 **radius**。RADIUS 是唯一支援的外部驗證方法。
4. 將管理員使用者的 **Local Authentication**（本機驗證）模式設定為 **Password**（密碼）或 **Password Hash**（密碼雜湊），並輸入 **Password**（密碼）。

STEP 6 | 提交 Panorama 設備上的設定並將其推送至叢集。

1. **Commit and Push**（提交並推送）。
2. 如果 Panorama 設備上有您不想推送的設定，請 **Edit Selections**（編輯選擇），以選取將設定推送至哪些設備。推送的設定會覆寫叢集節點上正在執行的設定，因此所有叢集節點將執行相同設定。

為 *WildFire* 叢集設定驗證

透過設定具有精確驗證參數的本機管理使用者，以及利用 RADIUS、TACAS+ 或 LDAP 進行授權和驗證，為 WildFire 叢集中的所有 WildFire 設備建立和設定增強的驗證。

當您在 Panorama 上設定管理員並進行推送時，您在 Panorama 上設定的管理員將覆寫 WildFire 叢集中所有 WildFire 設備的現有管理員。

- 為 WildFire 叢集設定管理帳戶
- 為 WildFire 叢集設定 RADIUS 驗證
- 為 WildFire 叢集設定 TACACS+ 驗證
- 為 WildFire 叢集設定 LDAP 驗證

© 2019 Palo Alto Networks, Inc.

為 WildFire 叢集設定管理帳戶

為 WildFire 叢集中的所有 WildFire 設備建立一個或多個具有精確驗證參數的管理員，以便從 Panorama™ 管理伺服器進行管理。此外，您還可以從 Panorama 設定本機管理員，這可以從 WildFire 設備的 CLI 直接進行設定。但是，向 WildFire 設備推送新設定變更後，為 WildFire 設備設定的管理員會覆寫本機管理員。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 在 Panorama 上集中設定叢集。

STEP 3 | （選用）設定驗證設定檔以定義驗證服務，用於對存取 WildFire 設備 CLI 之管理員的登入認證進行驗證。

STEP 4 | 根據需要設定一個或多個管理員帳戶。

在 Panorama 上建立的管理員帳戶之後會匯入到 WildFire 叢集中的 WildFire 設備並從 Panorama 進行管理。

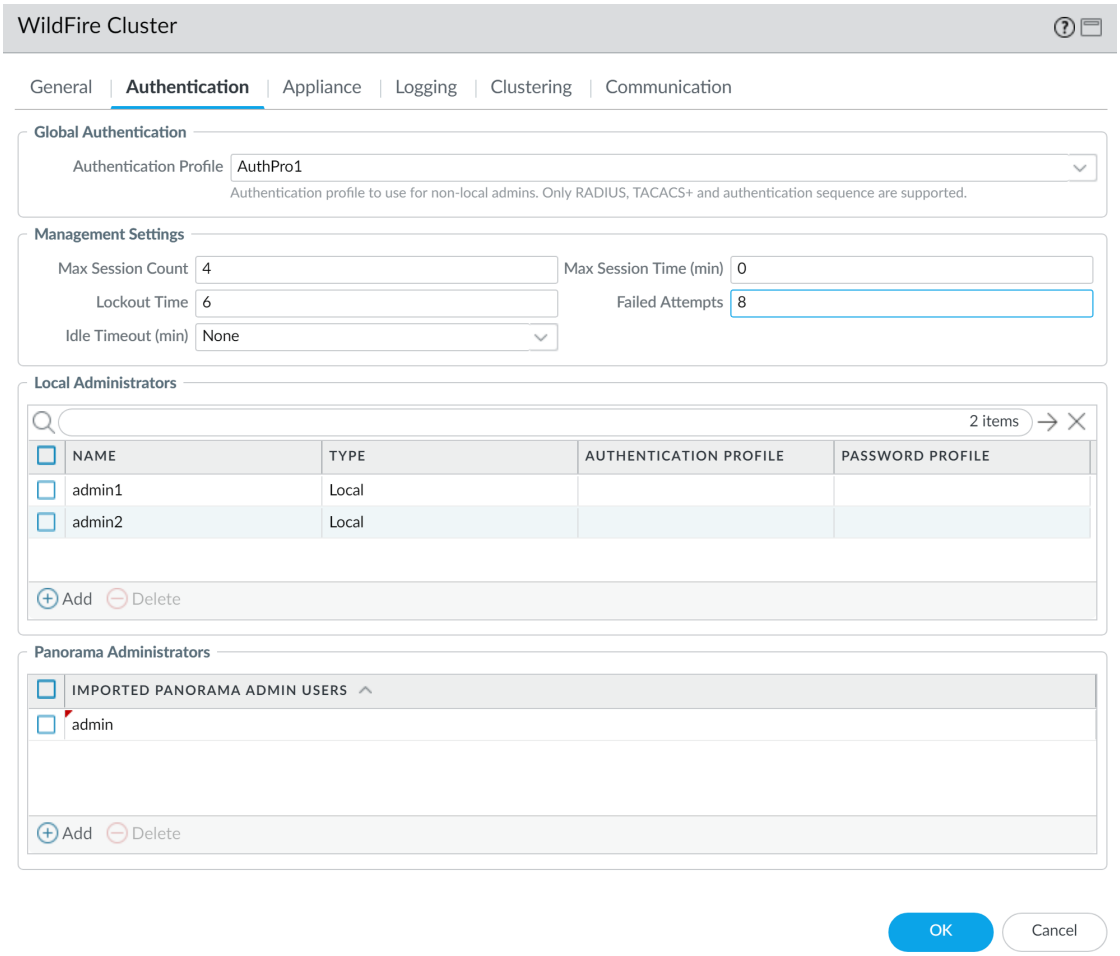
STEP 5 | 為 WildFire 叢集中的 WildFire 設備設定驗證。

1. 選取 **Panorama** > **Managed WildFire Clusters**（受管理的 **WildFire** 叢集），然後選取您之前設定的 WildFire 叢集。
2. （選用）選取您在上一步中設定的 **Authentication Profile**（驗證設定檔）。
3. 為 WildFire 設備設定驗證 **Timeout Configuration**（逾時設定）。
   1. 輸入 **Failed Attempt**（失敗嘗試）次數，在達到此次數之後使用者將被鎖定在 WildFire 設備 CLI 之外。
   2. 輸入 **Lockout Time**（鎖定時間）（以分鐘為單位），在使用者達到設定的 **Failed Attempts**（失敗嘗試）次數後 WildFire 設備鎖定使用者帳戶的時間。
   3. 輸入 **Idle Timeout**（閒置逾時）（以分鐘為單位），在此時間之後使用者會因為處於非作用狀態而自動登出。
   4. 輸入 **Max Session Count**（最大工作階段計數），設定多少使用者帳戶可以同時存取 WildFire 設備。
   5. 輸入管理員在自動登出之前可登入的 **Max Session Time**（最長工作階段時間）。
4. 新增 WildFire 設備管理員。

   管理員可以新增為本機管理員或作為匯入的 Panorama 管理員—但不能同時為二者。不支援將同一管理員同時新增為本機管理員和作為匯入的 Panorama 管理員，這會導致 Panorama 提交失敗。例如，如果您將 `admin1` 同時新增為本機和 Panorama 管理員，到 Panorama 的提交將會失敗。

   1. **Add**（新增）並設定專屬於 WildFire 叢集中 WildFire 設備的新管理員。這些管理員特定於為其建立的 WildFire 叢集中的 WildFire 設備，您可以從此表格管理這些管理員。
   2. **Add**（新增）在 Panorama 上設定的任何管理員。這些管理員在 Panorama 上建立，並匯入至 WildFire 叢集中的 WildFire 設備。
5. 按一下 **OK**（確定）以儲存 WildFire 叢集驗證設定。

© 2019 Palo Alto Networks, Inc.



STEP 6 | **Commit**（提交），然後 **Commit and Push**（提交並推送）設定變更。

STEP 7 | 使用本機管理員使用者存取 WildFire 設備 CLI 以驗證您能夠成功存取 WildFire 設備。

為 WildFire 叢集設定 RADIUS 驗證

使用 RADIUS 伺服器來驗證對 WildFire 叢集中 WildFire 設備 CLI 的管理存取。您也可以在 RADIUS 伺服器上定義廠商特定屬性 (VSA) 來進行管理員授權管理。使用 VSA 可讓您透過目錄服務快速變更管理員的角色、存取網域和使用者群組，這通常比在 Panorama™ 管理伺服器上重新設定更加簡單。

您可以將 Palo Alto 網路 RADIUS 詞典 匯入 *RADIUS* 伺服器，以定義 *Panorama* 和 *RADIUS* 伺服器之間通訊所需的驗證屬性。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 在 Panorama 上集中設定叢集。

STEP 3 | 設定 RADIUS 驗證。

1. 新增 RADIUS 伺服器設定檔。

   設定檔定義了 WildFire 叢集中的 WildFire 設備將採用何種方式連線 RADIUS 伺服器。

   1. 選取 **Panorama** > **Server Profiles**（伺服器設定檔）> **RADIUS**，然後 **Add**（新增）設定檔。

© 2019 Palo Alto Networks, Inc.

2. 輸入用來識別伺服器設定檔的 **Profile Name**（設定檔名稱）。
3. 輸入 **Timeout**（逾時）間隔時間（單位為秒），超過此時間後，驗證要求將逾時（預設值為 3；範圍為 1-20）。
4. 選取 WildFire 設備用於向 RADIUS 伺服器驗證的 **Authentication Protocol**（驗證通訊協定）（預設值為 **CHAP**）。

   選取 *CHAP*（如果 *RADIUS* 伺服器支援此通訊協定）；它比 *PAP* 更安全。
5. **Add**（新增）每個 RADIUS 伺服器，然後輸入下列資訊：
   1. 用來識別伺服器的 **Name**（名稱）。
   2. **RADIUS Server**（**RADIUS** 伺服器）IP 位址或 FQDN。
   3. **Secret**（密碼）/**Confirm Secret**（確認密碼）（用於加密使用者名稱和密碼的金鑰）。
   4. 用於驗證要求的伺服器 **Port**（連接埠）（預設值為 1812）。
6. 按一下 **OK**（確定）來儲存伺服器設定檔。

2. 將 RADIUS 伺服器設定檔指派給驗證設定檔。

   驗證設定檔中定義一群管理員通用的驗證設定。
   1. 選取 **Panorama** > **Authentication Profile**（驗證設定檔），然後 **Add**（新增）設定檔。
   2. 輸入用來識別驗證設定檔的 **Name**（名稱）。
   3. 將 **Type**（類型）設為 **RADIUS**。
   4. 選取您設定的 **Server Profile**（伺服器設定檔）。
   5. 選取 **Retrieve user group from RADIUS**（從 **RADIUS** 擷取使用者群組），以從 RADIUS 伺服器上定義的 VSA 收集使用者群組資訊。

      Panorama 會比對群組資訊與您在驗證設定檔「允許清單」中指定的群組。
   6. 選取 **Advanced**（進階），然後在 Allow List（允許清單）中，**Add**（新增）允許使用此驗證設定檔進行驗證的管理員。
   7. 按一下 **OK**（確定）來儲存驗證設定檔。

STEP 4 | 為 WildFire 叢集設定驗證。

1. 選取 **Panorama** > **Managed WildFire Clusters**（受管理的 **WildFire** 叢集），然後選取您之前新增的 WildFire 叢集。
2. 選取您在上一步中設定的 **Authentication Profile**（驗證設定檔）。

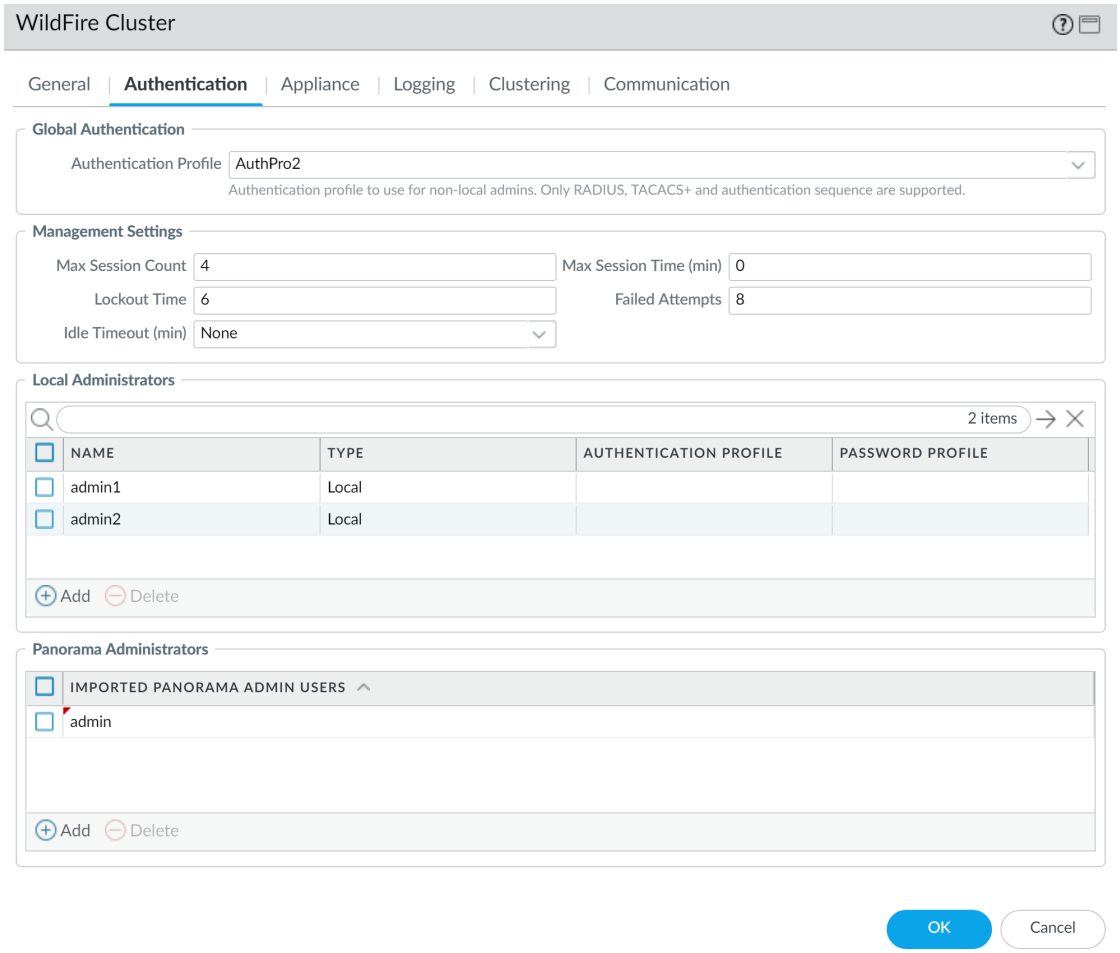
   如果沒有指派全域驗證設定檔，您必須指派一個驗證設定檔到單獨每個本機管理員才可利用遠端驗證。
3. 為 WildFire 設備設定驗證 **Timeout Configuration**（逾時設定）。
   1. 輸入 **Failed Attempt**（失敗嘗試）次數，在達到此次數之後使用者將被鎖定在 WildFire 設備 CLI 之外。
   2. 輸入 **Lockout Time**（鎖定時間）（以分鐘為單位），在使用者達到設定的 **Failed Attempts**（失敗嘗試）次數後 WildFire 設備鎖定使用者帳戶的時間。
   3. 輸入 **Idle Timeout**（閒置逾時）（以分鐘為單位），在此時間之後使用者會因為處於非作用狀態而自動登出。
   4. 輸入 **Max Session Count**（最大工作階段計數），設定多少使用者帳戶可以同時存取 WildFire 設備。
   5. 輸入管理員在自動登出之前可登入的 **Max Session Time**（最長工作階段時間）。
4. 新增 WildFire 設備管理員。

   管理員可以新增為本機管理員或作為匯入的 Panorama 管理員—但不能同時為二者。不支援將同一管理員同時新增為本機管理員和作為匯入的 Panorama 管理員，這會導致 Panorama 提交失敗。例如，如果您將 **admin1** 同時新增為本機和 Panorama 管理員，到 Panorama 的提交將會失敗。

© 2019 Palo Alto Networks, Inc.

1. **Add**（新增）並設定專屬於 WildFire 叢集中 WildFire 設備的新管理員。這些管理員特定於為其建立的 WildFire 叢集中的 WildFire 設備，您可以從此表格管理這些管理員。
2. **Add**（新增）在 Panorama 上設定的任何管理員。這些管理員在 Panorama 上建立，並匯入至 WildFire 叢集中的 WildFire 設備。

5. 按一下 **OK**（確定）以儲存 WildFire 叢集驗證設定。



STEP 5 | **Commit**（提交），然後 **Commit and Push**（提交並推送）設定變更。

STEP 6 | 使用本機管理員使用者存取 WildFire 設備 CLI 以驗證您能夠成功存取 WildFire 設備。

為 WildFire 叢集設定 TACACS+ 驗證

您可以使用 TACACS+ 伺服器來驗證對 WildFire 叢集中 WildFire 設備 CLI 的管理存取。您也可以在 TACACS+ 伺服器上定義廠商特定屬性 (VSA) 來進行管理員授權管理。使用 VSA 可讓您透過目錄服務快速變更管理員的角色、存取網域和使用者群組，這通常比在 Panorama 上重新設定更加簡單。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 在 Panorama 上集中設定叢集。

STEP 3 | 設定 TACACS+ 驗證。

1. 新增 TACACS+ 伺服器設定檔。

   設定檔定義了 WildFire 設備將採用何種方式連線 TACACS+ 伺服器。

© 2019 Palo Alto Networks, Inc.

1. 選取 **Panorama** > **Server Profiles**（伺服器設定檔）> **TACACS+**，然後 **Add**（新增）設定檔。
2. 輸入用來識別伺服器設定檔的 **Profile Name**（設定檔名稱）。
3. 輸入 **Timeout**（逾時）間隔時間（單位為秒），超過此時間後，驗證要求將逾時（預設值為 3；範圍為 1-20）。
4. 選取 Panorama 用於向 TACACS+ 伺服器驗證的 **Authentication Protocol**（驗證通訊協定）（預設值為 **CHAP**）。
5. 選取 **CHAP**（如果 TACACS+ 伺服器支援此通訊協定）；它比 **PAP** 更安全。
6. **Add**（新增）每個 TACACS+ 伺服器，然後輸入下列資訊：
    1. 用來識別伺服器的 **Name**（名稱）。
    2. **TACACS+ Server**（**TACACS+** 伺服器）IP 位址或 FQDN。
    3. **Secret**（密碼）/**Confirm Secret**（確認密碼）（用於加密使用者名稱和密碼的金鑰）。
    4. 用於驗證要求的伺服器 **Port**（連接埠）（預設值為 49）。
7. 按一下 **OK**（確定）來儲存伺服器設定檔。

2. 將 TACACS+ 伺服器設定檔指派給驗證設定檔。

    驗證設定檔中定義一群管理員通用的驗證設定。

    1. 選取 **Panorama** > **Authentication Profile**（驗證設定檔），然後 **Add**（新增）設定檔。
    2. 輸入用來識別設定檔的 **Name**（名稱）。
    3. 將 **Type**（類型）設為 **TACACS+**。
    4. 選取您設定的 **Server Profile**（伺服器設定檔）。
    5. 選取 **Retrieve user group from TACACS+**（從 **TACACS+** 擷取使用者群組），以從 TACACS+ 伺服器上定義的 VSA 收集使用者群組資訊。

        Panorama 會比對群組資訊與您在驗證設定檔「允許清單」中指定的群組。
    6. 選取 **Advanced**（進階），然後在 Allow List（允許清單）中，**Add**（新增）允許使用此驗證設定檔進行驗證的管理員。
    7. 按一下 **OK**（確定）來儲存驗證設定檔。

STEP 4 | 為 WildFire 叢集設定驗證。

1. 選取 **Panorama** > **Managed WildFire Clusters**（受管理的 **WildFire** 叢集），然後選取您之前新增的 WildFire 叢集。
2. 選取您在上一步中設定的 **Authentication Profile**（驗證設定檔）。

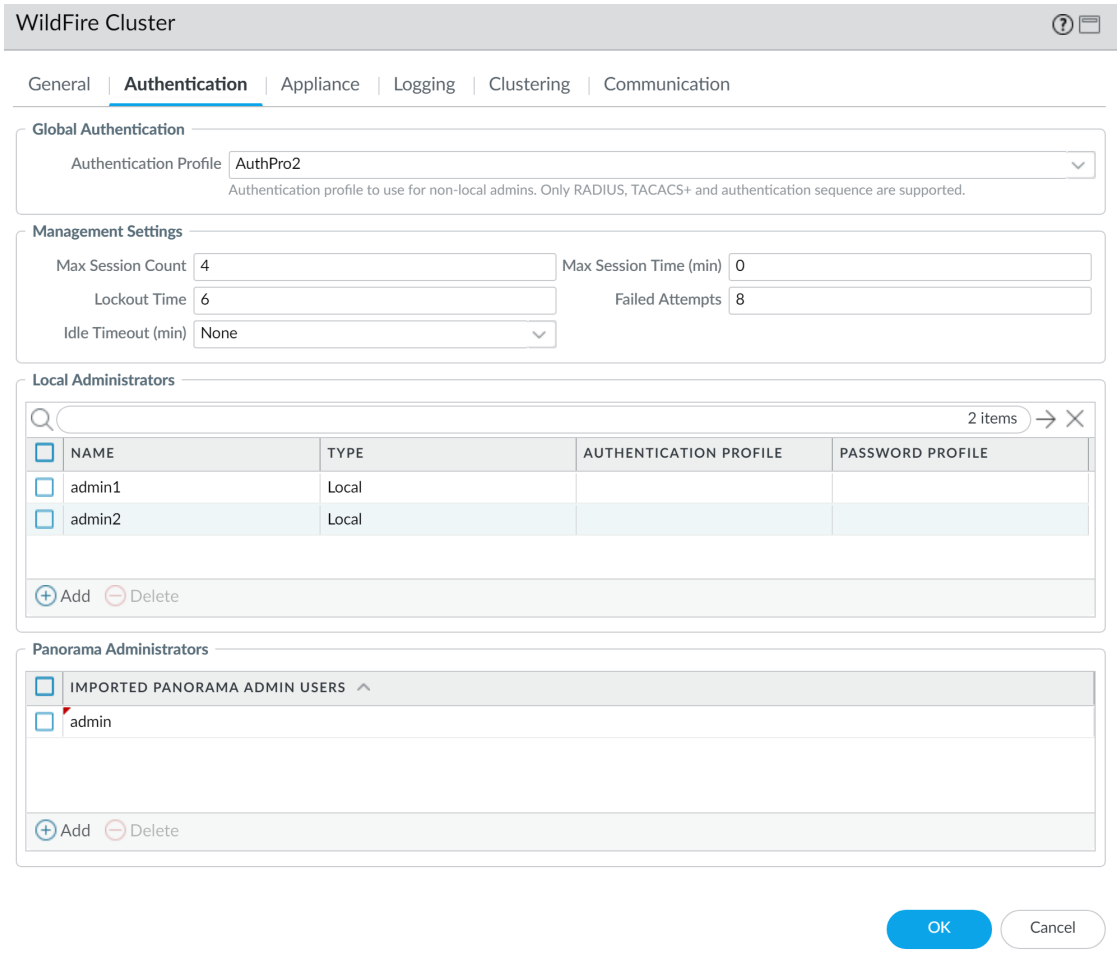
    如果沒有指派全域驗證設定檔，您必須指派一個驗證設定檔到單獨每個本機管理員才可利用遠端驗證。
3. 為 WildFire 設備設定驗證 **Timeout Configuration**（逾時設定）。
    1. 輸入 **Failed Attempt**（失敗嘗試）次數，在達到此次數之後使用者將被鎖定在 WildFire 設備 CLI 之外。
    2. 輸入 **Lockout Time**（鎖定時間）（以分鐘為單位），在使用者達到設定的 **Failed Attempts**（失敗嘗試）次數後 WildFire 設備鎖定使用者帳戶的時間。
    3. 輸入 **Idle Timeout**（閒置逾時）（以分鐘為單位），在此時間之後使用者會因為處於非作用狀態而自動登出。
    4. 輸入 **Max Session Count**（最大工作階段計數），設定多少使用者帳戶可以同時存取 WildFire 設備。
    5. 輸入管理員在自動登出之前可登入的 **Max Session Time**（最長工作階段時間）。
4. 新增 WildFire 設備管理員。

    管理員可以新增為本機管理員或作為匯入的 Panorama 管理員—但不能同時為二者。不支援將同一管理員同時新增為本機管理員和作為匯入的 Panorama 管理員，這會導致 Panorama 提交失敗。例如，如果您將 `admin1` 同時新增為本機和 Panorama 管理員，到 Panorama 的提交將會失敗。

© 2019 Palo Alto Networks, Inc.

1. **Add**（新增）並設定專屬於 WildFire 叢集中 WildFire 設備的新管理員。這些管理員特定於為其建立的 WildFire 叢集中的 WildFire 設備，您可以從此表格管理這些管理員。
2. **Add**（新增）在 Panorama 上設定的任何管理員。這些管理員在 Panorama 上建立，並匯入至 WildFire 叢集中的 WildFire 設備。

5. 按一下 **OK**（確定）以儲存 WildFire 叢集驗證設定。



STEP 5 | **Commit**（提交），然後 **Commit and Push**（提交並推送）設定變更。

STEP 6 | 使用本機管理員使用者存取 WildFire 設備 CLI 以驗證您能夠成功存取 WildFire 設備。

為 WildFire 叢集設定 LDAP 驗證

您可以使用 LDAP 對存取 WildFire 叢集中 WildFire 設備 CLI 的一般使用者進行驗證。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 在 Panorama 上集中設定叢集。

STEP 3 | 新增 LDAP 伺服器設定檔。

設定檔定義了 WildFire 設備將採用何種方式連線 LDAP 伺服器。

1. 選取 **Panorama** > **Server Profiles**（伺服器設定檔）> **LDAP**，然後 **Add**（新增）伺服器設定檔。
2. 輸入用來識別伺服器設定檔的 **Profile Name**（設定檔名稱）。

© 2019 Palo Alto Networks, Inc.

3. **Add**（新增）LDAP 伺服器（最多可新增四個）。對於每個伺服器，輸入 **Name**（名稱）（用於識別伺服器）、**LDAP Server**（**LDAP** 伺服器）IP 位址或 FQDN，以及伺服器 **Port**（連接埠）（預設值為 389）。

   如果您使用 *FQDN* 位址物件識別伺服器並隨後變更了位址，則必須要提交變更，以便新伺服器位址生效。
4. 選取伺服器 **Type**（類型）。
5. 選取 **Base DN**（基礎 **DN**）。

   識別您目錄 Base DN，打開**Active Directory Domains and Trusts**（主動式目錄網域與信任）Microsoft 管理控制台管理單元，並使用頂級網域名稱。
6. 輸入 **Bind DN**（繫結 **DN**）與 **Password**（密碼）以讓驗證服務能驗證防火牆。

   繫結 *DN* 賬號須具有讀取 *LDAP* 目錄的權限。
7. 輸入 **Bind Timeout**（繫結逾時）和**Search Timeout**（搜尋逾時），單位為秒（預設值均為 30）。
8. 輸入 **Retry Interval**（重試間隔）（秒）（預設值為 60）。
9. （選用）如果您希望端點使用 SSL 或 TLS 更安全的連線目錄伺服器，請啟用 **Require SSL/TLS secured connection**（需要 **SSL/TLS** 安全連線）選項（預設為已啟用）。端點使用的協定視乎伺服器連接埠而定：
   - 389（預設）—TLS（特別是 WildFire 設備會使用 StartTLS 操作，用來升級連接至 TLS 的初始純文字連線。）
   - 636—SSL
   - 任何其他連接埠—WildFire 設備首先會嘗試使用 TLS。若目錄伺服器不支援 TLS，則 WildFire 設備會回復使用 SSL。
10. （選用）為了獲得額外的安全，請啟用 **Verify Server Certificate for SSL sessions**（確認 **SSL** 工作階段的伺服器憑證）選項，讓端點確認目錄伺服器為 SSL/TLS 連線所呈現的憑證。若要啟用驗證，您也必須啟用 **Require SSL/TLS secured connection**（要求 **SSL/TLS** 安全連線）選項。為了順利確認，憑證必須滿足以下條件之一：
    - 位於 Panorama 憑證清單內：**Panorama** > **Certificate Management**（憑證管理）> **Certificates**（憑證）> **Device Certificates**（設備憑證）。若有必要，將憑證匯入至 Panorama。
    - 憑證簽署者位於受信任的憑證授權單位清單中：**Panorama** > **Certificate Management**（憑證管理）> **Certificates**（憑證）。
11. 按一下 **OK**（確定）來儲存伺服器設定檔。

STEP 4 | 為 WildFire 叢集設定驗證。

1. 選取 **Panorama** > **Managed WildFire Clusters**（受管理的 **WildFire** 叢集），然後選取您之前新增的 WildFire 叢集。
2. 為 WildFire 設備設定驗證 **Timeout Configuration**（逾時設定）。
    1. 輸入 **Failed Attempt**（失敗嘗試）次數，在達到此次數之後使用者將被鎖定在 WildFire 設備 CLI 之外。
    2. 輸入 **Lockout Time**（鎖定時間）（以分鐘為單位），在使用者達到設定的 **Failed Attempts**（失敗嘗試）次數後 WildFire 設備鎖定使用者帳戶的時間。
    3. 輸入 **Idle Timeout**（閒置逾時）（以分鐘為單位），在此時間之後使用者會因為處於非作用狀態而自動登出。
    4. 輸入 **Max Session Count**（最大工作階段計數），設定多少使用者帳戶可以同時存取 WildFire 設備。
    5. 輸入管理員在自動登出之前可登入的 **Max Session Time**（最長工作階段時間）。
3. 新增 WildFire 設備管理員。

© 2019 Palo Alto Networks, Inc.

管理員可以新增為本機管理員或作為匯入的 Panorama 管理員—但不能同時為二者。不支援將同一管理員同時新增為本機管理員和作為匯入的 Panorama 管理員，這會導致 Panorama 提交失敗。例如，如果您將 **admin1** 同時新增為本機和 Panorama 管理員，到 Panorama 的提交將會失敗。

- 設定本機管理員。

  設定專屬於 WildFire 叢集中 WildFire 設備的新管理員。這些管理員特定於為其建立的 WildFire 叢集中的 WildFire 設備，您可以從此表格管理這些管理員。

  1. **Add**（新增）一個或多個新本機管理員。
  2. 輸入本機管理員的 **Name**（名稱）。
  3. 指派您之前建立的 **Authentication Profile**（驗證設定檔）。

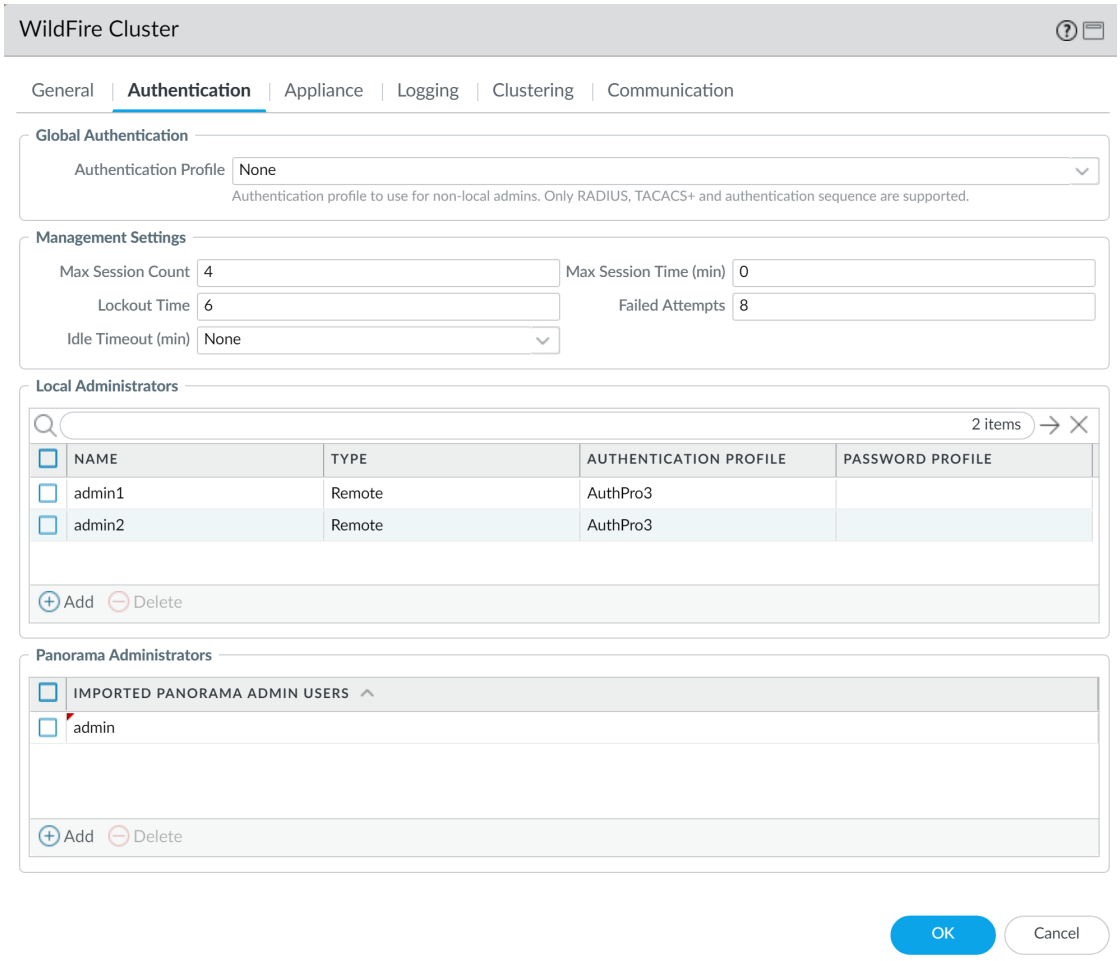
     LDAP 驗證設定檔僅支援個別本地管理員。

  4. 啟用（核取）**Use Public Key Authentication (SSH)**（使用公開金鑰驗證 **(SSH)**）以匯入公開金鑰檔案進行驗證。
  5. 選取 **Password Profile**（密碼設定檔）以設定到期參數。
- 匯入現有 Panorama 管理員

  匯入 Panorama 上的現有管理員。這些管理員在 Panorama 上設定和管理，並匯入至 WildFire 叢集中的所有 WildFire 設備。

  1. **Add**（新增）現有 Panorama 管理員

4. 按一下 **OK**（確定）以儲存 WildFire 叢集驗證設定。



© 2019 Palo Alto Networks, Inc.

STEP 5 | **Commit**（提交），然後 **Commit and Push**（提交並推送）設定變更。

STEP 6 | 使用本機管理員使用者存取 WildFire 設備 CLI 以驗證您能夠成功存取 WildFire 設備。

從 *Panorama* 管理中移除叢集

若要從 Panorama 管理移除叢集，選取 **Panorama** > **Managed WildFire Clusters**（受管理的 **WildFire** 叢集），並選取您想要移除的叢集行（不要按一下叢集名稱），然後 **Remove From Panorama**（從 **Panorama** 移除）。

如果您從 Panorama 管理中移除 WildFire 設備，Panorama Web 介面會使該叢集中的 WildFire 設備處於唯讀模式。雖然已移除叢集中的 WildFire 設備顯示在 Panorama Web 介面，但在唯讀模式中，您無法推送設定至 WildFire 設備或使用 Panorama 管理。從 Panorama 管理中移除後，WildFire 設備叢集成員會使用本機叢集設定，而且您可以使用本機 CLI 管理叢集。

從 Panorama 管理中移除叢集後，若要使用 Panorama 管理該叢集中的 WildFire 設備，請將叢集重新匯入至 Panorama（**Panorama** > **Managed WildFire Clusters**（受管理的 **WildFire** 叢集）> **Import Cluster Config**（匯入叢集設定））。

STEP 1 | 選取叢集的控制器節點。叢集名稱會自動填入 **Cluster**（叢集）。

STEP 2 | 按一下 **OK**（確定）。叢集備份控制器節點和工作節點會自動填入。

STEP 3 | 按一下 **OK**（確定）匯入叢集。

STEP 4 | **Commit**（提交）變更。

使用集中於 *Panorama* 的預定義憑證，設定設備對設備的加密

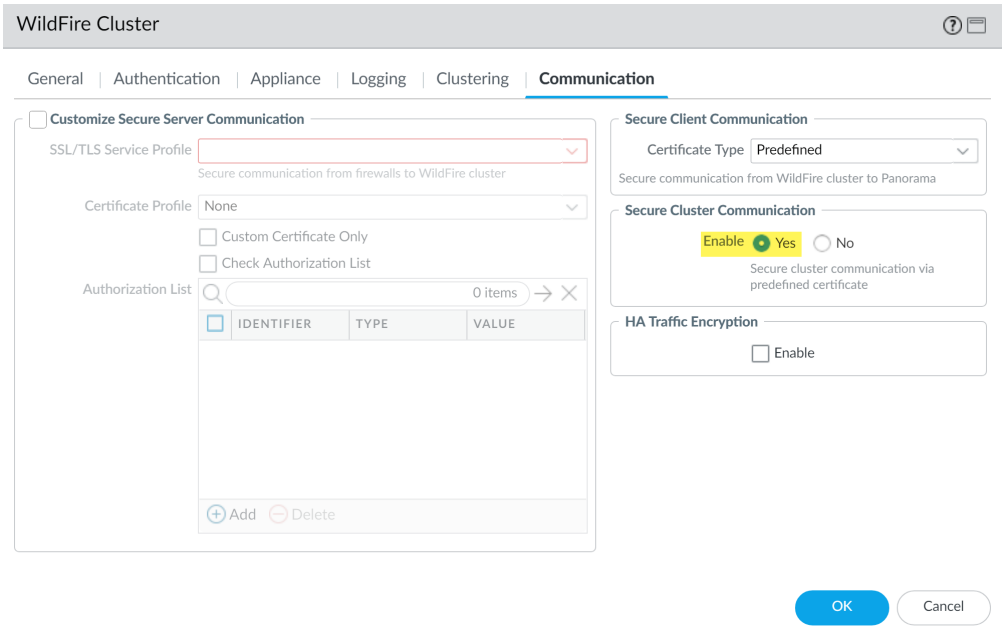
STEP 1 | 將每個受管理的 WildFire 設備升級至 PAN-OS 8.1.x。所有受管理的設備必須執行 PAN-OS 8.1 或更新版本，才能啟用設備至設備加密。

STEP 2 | 確認 WildFire 設備叢集已正確設定，且在健康狀態下執行。

STEP 3 | 在 Panorama 上，選取 **Panorama> Managed WildFire Clusters**（受管理的 **WildFire** 叢集）> *WF_cluster_name*（*WF* 彙集名稱）**> Communication**（通訊）。

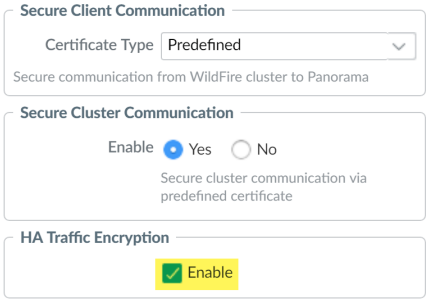
STEP 4 | **Enable**（啟用）安全性叢集通訊。

© 2019 Palo Alto Networks, Inc.



STEP 5 | （建議）**Enable**（啟用）HA 流量加密。這項選用設定可以加密 HA 配對之間的 HA 流量，是 Palo Alto Networks 建議的最佳做法。

在 *FIPS/CC* 模式下執行時，*HA* 流量加密無法停用。



STEP 6 | 按一下 **OK**（確定）來儲存 **WildFire Cluster**（**WildFire** 叢集）。

STEP 7 | **Commit**（提交）您的變更。

使用集中於 *Panorama* 的自訂憑證設定設備對設備的加密

STEP 1 | 將每個受管理的 WildFire 設備升級至 PAN-OS 8.1.x。所有受管理的設備必須執行 PAN-OS 8.1 或更新版本，才能啟用設備至設備加密。

STEP 2 | 確認 WildFire 設備叢集已正確設定，且在健康狀態下執行。

STEP 3 | 檢閱您現有的 WildFIRE 安全通訊設定。記住，如果您之前已使用自訂憑證設定 WildFire 設備和防火牆以確保通訊安全，則也可使用該自訂憑證確保 WildFire 設備之間的通訊安全。

1. 選取 **Panorama >Managed WildFire Clusters**（受管理的 **WildFire** 叢集）> *WF_cluster_name*（*WF* 叢集名稱）> **Communication**（通訊）。

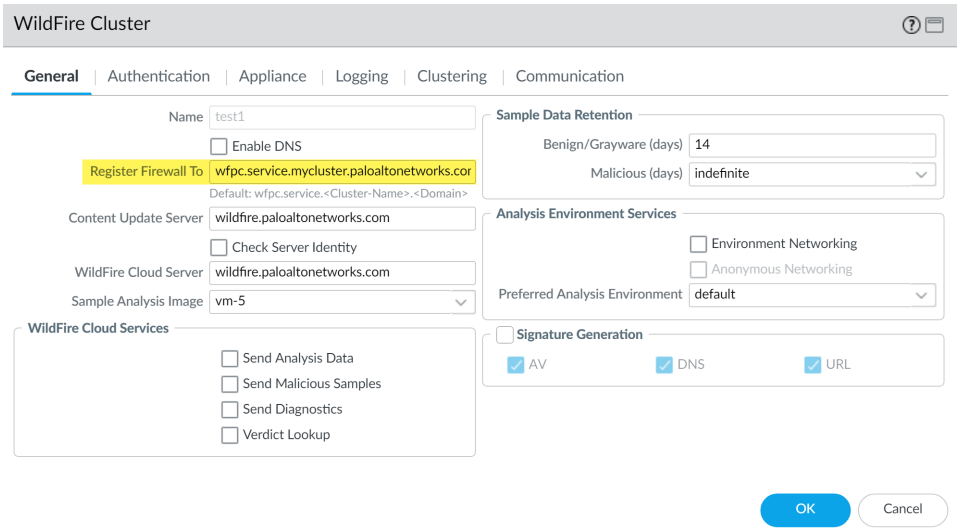
© 2019 Palo Alto Networks, Inc.

2. 若已啟用 **Customize Secure Server Communication**（自訂安全伺服器通訊），則您應使用該憑證來識別已用自訂憑證的詳細資料。否則，請進行步驟 5 以開啟安裝新自訂憑證的程序。
3. 確定將用來定義在步驟 4 中防火牆註冊位址的自訂憑證 FQDN（DNS 名稱）。

務必備註自訂憑證名稱以及相關聯的 *FQDN*。這些在設定流程期間會引用好幾次。

STEP 4 | 設定 Panorama 上的防火牆註冊位址。

1. 在 Panorama 上，選取 **Panorama >Managed WildFire Clusters**（受管理的 **WildFire** 叢集）> *WF_cluster_name*（*WF* 叢集名稱）> **General**（一般）。
2. 在 **Register Firewall To**（將防火牆註冊至）欄位內，指定在自訂憑證內用來驗證的 DNS 名稱（一般而言為 SubjectName 或 SubjectAltName）。例如，預設網域名稱是 **`wfpc.service.mycluster.paloaltonetworks.com`**



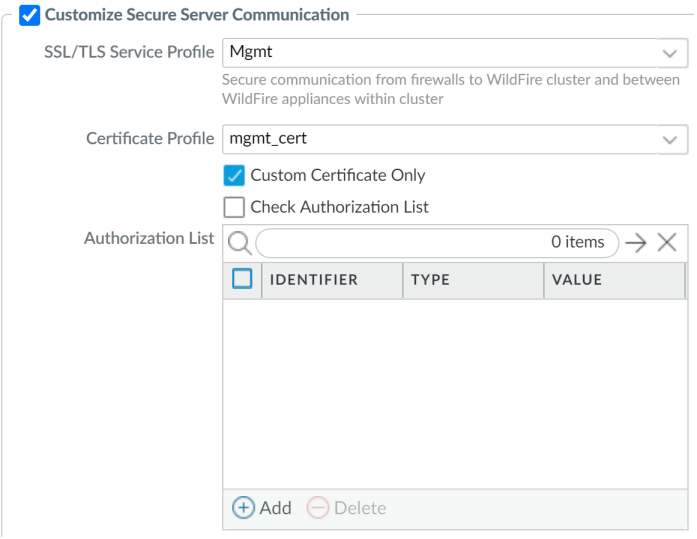
STEP 5 | 在 Panorama 上設定 WildFire **Secure Server Communication**（安全伺服器通訊）設定。若您已設定防火牆和 WildFire 設備間的安全通訊，並使用現有自訂憑證，請直接前往下面的步驟 4。

1. 在 Panorama 上，選取 **Panorama> Managed WildFire Clusters**（受管理的 **WildFire** 叢集）> *WF_cluster_name*（*WF* 叢集名稱）> **Communication**（通訊）。
2. 按一下 **Customize Secure Server Communication**（自訂安全伺服器通訊）。
3. 設定並部署 WildFire 設備及其相關聯防火牆所使用的自訂憑證。SSL/TLS 服務設定檔定義 WildFire 設備用來與 WildFire 設備端點和防火牆通訊的自訂憑證。您必須在與 WildFire 設備叢集相關的防火牆上設定自訂憑證設定。這會在稍後的步驟 9中設定。
   1. 開啟 SSL/TLS 服務設定檔下拉式清單，並按一下 SSL/TLS 服務設定檔。以您想要使用的自訂憑證設定 SSL/TLS 服務設定檔。在您設定 SSL/TLS 服務設定檔之後，按一下 OK（確定）以選取新建的 SSL/TLS 服務設定檔。
   2. 開啟憑證設定檔下拉式清單並按一下憑證設定檔。設定可識別用來建立防火牆和 WildFire 設備間安全連線的自訂憑證的憑證設定檔。在您設定憑證設定檔之後，按一下 OK（確定）並選取新建的設定檔。
4. 選取 **Custom Certificate**（自訂憑證）核取方塊。這讓您能夠使用設定的自訂憑證，而非預設的預設定憑證。
5. （選用）設定授權清單。此授權清單會檢查自訂憑證主體或主體別名；若與自訂憑證一同出現的 **Subject**（主體）或 **Subject Alt Name**（主體別名）不符合授權清單中的識別項，則會拒絕驗證。
   1. **Add**（新增）授權清單。

© 2019 Palo Alto Networks, Inc.

2. 在自訂憑證設定檔中，選取 **Subject**（主體）或 **Subject Alt Name**（主體別名）作為識別項類型。
3. 如果識別項是主體，請輸入通用名稱，如果識別項是主體別名，請輸入 IP 位址、主機名稱或電子郵件。
4. 按一下 **OK**（確定）。
5. 選取 **Check Authorization List**（檢查授權清單）以強制執行授權清單。

6. 按一下 **OK**（確定）。



STEP 6 | **Enable**（啟用）安全性叢集通訊。

STEP 7 | （建議）**Enable**（啟用）HA 流量加密。這項選用設定可以加密 HA 配對之間的 HA 流量，是 Palo Alto Networks 建議的最佳做法。

在 *FIPS/CC* 模式下執行時，*HA* 流量加密無法停用。

STEP 8 | 按一下 **OK**（確定）來儲存 **WildFire Cluster**（**WildFire** 叢集）。

STEP 9 | 在 Panorama 上進行防火牆安全通訊設定以將 WildFire 設備叢集與防火牆自訂憑證相關聯。這提供了防火牆與 WildFire 設備叢集之間的安全通訊通道。如果您已經設定了防火牆與 WildFire 設備叢集之間的安全通訊，並在使用現有自訂憑證，則執行下一步。

1. 選取 **Device**（裝置）> **Setup**（設定）> **Management** > **Secure Communication Settings**（管理 > 安全通訊設定），並在 **Secure Communication Settings**（安全通訊設定）中按一下**Edit**（編輯）圖示以進行防火牆自訂憑證設定。
2. 從各別下拉式清單選取 **Certificate Type**、**Certificate** 與 **Certificate Profile** 並設定它們使用自訂憑證。
3. 在自訂通訊下，選取 **WildFire Communication**（**WildFire** 通訊）。
4. 按一下 **OK**（確定）。

STEP 10 | **Commit**（提交）您的變更。

使用 Panorama 檢視 WildFire 叢集狀態

若要確認已設定的 WildFire 設備叢集是否在正常執行，您可以使用 Panorama 設備檢視目前狀態。

© 2019 Palo Alto Networks, Inc.

Palo Alto Networks 建議使用 *WildFire* 設備 *CLI* 確認 *WildFire* 叢集的狀態。*Panorama* 中不可見的其他狀態詳細資訊會在命令輸出中顯示。

STEP 1 | 在主要 Panorama 設備上，選取 **Panorama > Managed WildFire Clusters**（受管理的 **WildFire** 叢集）。

STEP 2 | 在 **Cluster Status**（叢集狀態）列，確認：

1. wfpc 和特徵碼服務正在執行。
2. 沒有其他操作。異常操作及其狀態情況包括：
   - 解除 [已要求 / 進行中 / 已拒絕 / 成功 / 失敗]
   - 暫停 [已要求 / 進行中 / 已拒絕 / 成功 / 失敗]
   - 重新啟動 [已要求 / 進行中 / 已拒絕 / 成功 / 失敗]
   - 叢集 [離線 / 腦分裂 / 未就緒]
   - 服務 [暫停 / 無]
   - HA [對等節點離線 / 設定未同步 / 設定同步關閉]

STEP 3 | 在 **Config Status**（設定狀態）列，確認：

1. 設備設定與 Panorama 設備上儲存的設定 **In Sync**（同步）。
2. 沒有其他狀態。異常狀態情況包括：
   - **Out of Sync**（不同步）[設備設定和其在 Panorama 上所儲存的設定不同步。可以使滑鼠停留在放大鏡上來顯示同步失敗原因]。

STEP 4 | 在 **Connected**（已連線）列，確認已設定的 WildFire 設備顯示狀態 **Connected**（已連線）。

在有網際網路連線的情況下在 Panorama 上集中升級叢集

如果一個叢集中的 WildFire 設備由 Panorama 管理，其升級可並行。如果 Panorama 直接連線至網際網路，您可直接從 Panorama 查看並下載新版本。

Panorama 只能管理執行相同軟體版本或更新軟體版本的 *WildFire* 設備和設備叢集。

STEP 1 | 將 Panorama 升級至與您想要在 WildFire 叢集上安裝的目標軟體版本相同或更新。

有關升級 Panorama 的詳細資料，請參閱安裝 Panorama 的內容與軟體更新。

STEP 2 | 暫停樣本分析。

1. 使防火牆停止轉送任何新樣本至 WildFire 設備。
   1. 登入防火牆 Web 介面。
   2. 選取 **Device**（設備）> **Setup**（設定）> **WildFire**，然後編輯**General Setting**（一般設定）。
   3. 清除 **WildFire Private Cloud**（**WildFire** 私人雲端）欄位。
   4. 按一下 **OK**（確定）與 **Commit**（提交）。
2. 確認防火牆已提交至設備的樣本分析已完成：
   1. 登入 Panorama 網頁介面。
   2. 選取 **Panorama > Managed WildFire Clusters**（受管理的 **WildFire** 叢集）並 **View**（檢視）叢集分析環境 **Utilization**（使用率）。
   3. 確認 **Virtual Machine Usage**（虛擬電腦使用率）未顯示任何進行中的樣本分析。

   如果您不想等待 *WildFire* 設備完成分析最近提交的樣本，可以繼續下一步。但是，要假定 *WildFire* 設備之後會從分析佇列捨棄擱置樣本。

© 2019 Palo Alto Networks, Inc.

STEP 3 | 安裝最新 WildFire 設備內容更新。

這些更新為設備提供了最新的威脅資訊以準確偵測惡意軟體。



您必須先安裝內容更新，再安裝軟體更新。參考版本資訊，瞭解您必須為 *Panorama* 版本安裝的最低內容版本。

1. 下載 WildFire 內容更新：
   1. 選取 **Panorama > Device Deployment > Dynamic Updates. (Panorama > 設備部署 > 動態更新。).**
   2. 選取 WildFire 內容更新套件版本並按一下 **Download**（下載）。
2. 按一下 **Install (安裝)**。
3. 選取您想要升級的 WildFire 叢集或個別設備。
4. 按一下 **OK**（確定）以啟動安裝。

STEP 4 | 下載 PAN-OS 軟體版本至 WildFire 設備。

升級 WildFire 設備時，您不能略過任何主要發行版本。例如，如果您想要從 PAN-OS 6.1 版升級至 PAN-OS 7.1 版，您首先必須下載並安裝 PAN-OS 7.0 版。

1. 下載 WildFire 軟體升級：
   1. 選取 **Panorama > Device Deployment**（設備部署） **> Software**（軟體）。
   2. 按一下 **Check Now**（立即檢查）以擷取已更新的版本清單。
   3. 選取要安裝的 WildFire 版本，並按一下 **Download**（下載）。
   4. 按一下 **Close**（關閉）以離開 **Download Software**（下載軟體）視窗
2. 按一下 **Install (安裝)**。
3. 選取您想要升級的 WildFire 叢集。
4. 選取安裝模式：
   - （8.0.2 及更新版本）**Select Reboot device after install**（安裝後選取重新啟動裝置）。
   - （8.0.1 及更新版本）選取 **Upload only**（僅上載）。
5. 按一下 **OK**（確定）以啟動安裝。
6. （選用）在 Panorama 上監控安裝程序。
7. （僅限 8.0.1）升級套件完成上載後，在每個節點上安裝升級：
   1. ```
      admin@WF-500 (passive-controller)> request system software install
       version 8.0.2
      ```
   2. 確認升級完成。執行下列命令並尋找 **Install** 工作類型及 **FIN** 狀態：

      ```
      admin@WF-500(passive-controller)> show jobs all

      Enqueued Dequeued ID Type Status Result Completed
      ---------------------------------------------------
      14:53:15 14:53:15 5 Install FIN    OK   14:53:19
      ```
   3. 慢慢地重新啟動設備：

      ```
      admin@WF-500(passive-controller)> request cluster reboot-local-node
      ```

      視乎 *WildFire* 設備上儲存的樣本數量，升級程序可能需要 *10* 分鐘或超過 *1* 小時。
   4. 對於叢集中的每個 WildFire 工作節點，重複此步驟。

© 2019 Palo Alto Networks, Inc.
      ```

STEP 5 | （選用）在 WildFire 控制器節點上檢視重新啟動工作的狀態。

在 WildFire 叢集控制器上，執行下列命令並尋找 **Install**（安裝）工作類型及 **FIN**（完成）狀態：

```
admin@WF-500(active-controller)> show cluster task pending
```

STEP 6 | 確認 WildFire 設備已可以繼續進行樣本分析。

1. 確認 sw-version 欄位顯示 8.0.1：

```
admin@WF-500(passive-controller)> show system info | match sw-version
```

2. 確認所有程序都在執行：

```
admin@WF-500(passive-controller)> show system software status
```

3. 確認自動提交（**AutoCom**（自動提交））工作已完成：

```
admin@WF-500(passive-controller)> show jobs all
```

在沒有網際網路連線的情況下在 Panorama 上集中升級叢集

如果一個叢集中的 WildFire 設備由 Panorama 管理，其升級可並行。如果 Panorama 沒有直接連線至網際網路，您必須從 Palo Alto Networks 支援網站下載軟體內容和更新，並將其在內部伺服器託管，然後由 Panorama 散佈。

Panorama 只能管理執行相同軟體版本或更新軟體版本的 *WildFire* 設備和設備叢集。

STEP 1 | 將 Panorama 升級至與您想要在 WildFire 叢集上安裝的目標軟體版本相同或更新。

有關升級 Panorama 的詳細資料，請參閱安裝 Panorama 的內容與軟體更新。

STEP 2 | 暫停樣本分析。

1. 使防火牆停止轉送任何新樣本至 WildFire 設備。
   1. 登入防火牆 Web 介面。
   2. 選取 **Device**（設備）> **Setup**（設定）> **WildFire**，然後編輯**General Setting**（一般設定）。
   3. 清除 **WildFire Private Cloud**（**WildFire** 私人雲端）欄位。
   4. 按一下 **OK**（確定）與 **Commit**（提交）。
2. 確認防火牆已提交至設備的樣本分析已完成：
   1. 登入 Panorama 網頁介面。
   2. 選取 **Panorama** > **Managed WildFire Clusters**（受管理的 **WildFire** 叢集）並 **View**（檢視）叢集分析環境 **Utilization**（使用率）。
   3. 確認 **Virtual Machine Usage**（虛擬電腦使用率）未顯示任何進行中的樣本分析。

   如果您不想等待 *WildFire* 設備完成分析最近提交的樣本，可以繼續下一步。但是，要假定 *WildFire* 設備之後會從分析佇列捨棄擱置樣本。

STEP 3 | 將 WildFire 內容與軟體更新下載至有網際網路存取權的主機。Panorama 必須具有主機的存取權。

1. 使用可存取網際網路的主機登入 Palo Alto Networks 客戶支援網站。

© 2019 Palo Alto Networks, Inc.

2. 下載內容更新：
    1. 在 [工具] 部分中按一下 **Dynamic Updates**（動態更新）。
    2. **Download**（下載）所需內容更新，然後將檔案儲存至主機。為您要更新的各內容類型執行此步驟。
3. 下載軟體更新：
    1. 返回 Palo Alto Networks 客戶支援網站的主頁面，然後在 [工具] 部分中按一下 **Software Updates**（軟體更新）。
    2. 檢閱 Download（下載）欄以決定您要安裝的版本。更新套件的檔案名稱表示升級的型號和版本：WildFire_<版本>。
    3. 按一下檔名，並將檔案儲存至主機。

STEP 4 | 安裝最新 WildFire 設備內容更新。

這些更新為設備提供了最新的威脅資訊以準確偵測惡意軟體。



您必須先安裝內容更新，再安裝軟體更新。參考版本資訊，瞭解您必須為 *Panorama* 版本安裝的最低內容版本。

1. 下載 WildFire 內容更新：
    1. 選取 **Panorama > Device Deployment > Dynamic Updates. (Panorama > 設備部署 > 動態更新。).**
    2. 按一下 **Upload**（上載），選取內容 **Type**（類型），**Browse**（瀏覽）至 WildFire 內容更新檔案，並按一下 **OK**（確定）。
    3. 按一下 **Install From File**（從檔案安裝），選取套件 **Type**（類型）、**File Name**（檔案名稱），以及叢集中您想要升級的 WildFire 設備，然後按一下 **OK**（確定）。
2. 按一下 **OK**（確定）以啟動安裝。

STEP 5 | 下載 PAN-OS 軟體版本至 WildFire 設備。

升級 WildFire 設備時，您不能略過任何主要發行版本。例如，如果您想要從 PAN-OS 6.1 版升級至 PAN-OS 7.1 版，您首先必須下載並安裝 PAN-OS 7.0 版。

1. 下載 WildFire 軟體升級：
    1. 選取 **Panorama > Device Deployment**（設備部署）**> Software**（軟體）。
    2. 按一下 **Check Now**（立即檢查）以擷取已更新的版本清單。
    3. 選取要安裝的 WildFire 版本，並按一下 **Download**（下載）。
    4. 按一下 **Close**（關閉）以離開 **Download Software**（下載軟體）視窗
2. 按一下 **Install (安裝)**。
3. 選取您想要升級的 WildFire 叢集。
4. 選取安裝模式：
    - （8.0.2 及更新版本）**Select Reboot device after install**（安裝後選取重新啟動裝置）。
    - （8.0.1 及更新版本）選取 **Upload only**（僅上載）。
5. 按一下 **OK**（確定）以啟動安裝。
6. （選用）在 Panorama 上監控安裝程序。
7. （僅限 8.0.1）升級套件完成上載後，在每個節點上安裝升級：
    1. ```
       admin@WF-500 (passive-controller)> request system software install
        version 8.0.2
       ```
    2. 確認升級完成。執行下列命令並尋找 **Install** 工作類型及 **FIN** 狀態：

       ```
       admin@WF-500(passive-controller)> show jobs all
       ```


© 2019 Palo Alto Networks, Inc.
       ```

```
Enqueued Dequeued ID Type Status Result Completed
---------------------------------------------------
14:53:15 14:53:15 5 Install FIN    OK   14:53:19
```

3. 慢慢地重新啟動設備：

```
admin@WF-500(passive-controller)> request cluster reboot-local-node
```



視乎 *WildFire* 設備上儲存的樣本數量，升級程序可能需要 *10* 分鐘或超過 *1* 小時。

4. 對於叢集中的每個 WildFire 工作節點，重複第 7 步。

STEP 6 | （選用）在 WildFire 控制器節點上檢視重新啟動工作的狀態。

在 WildFire 叢集控制器上，執行下列命令並尋找 **Install**（安裝）工作類型及 **FIN**（完成）狀態：

```
admin@WF-500(active-controller)> show cluster task pending
```

STEP 7 | 確認 WildFire 設備已可以繼續進行樣本分析。

1. 確認 sw-version 欄位顯示 8.0.1：

```
admin@WF-500(passive-controller)> show system info | match sw-version
```

2. 確認所有程序都在執行：
   admin@WF-500(passive-controller)> **show system software status**
3. 確認自動提交（**AutoCom**（自動提交））工作已完成：

```
admin@WF-500(passive-controller)> show jobs all
```

管理授權與更新

您可以使用 Panorama™ 管理伺服器，以集中管理防火牆和專用日誌收集器上的授權、軟體更新和內容更新。當您部署授權或更新時，Panorama 會簽入 Palo Alto Networks® 授權伺服器或更新伺服器，驗證要求的有效性，然後允許擷取和安裝授權或更新。此功能可幫助您部署，因為您不需要在每個防火牆或專用日誌收集器上重複執行相同的工作。此功能尤其適合管理無法直接存取網際網路的防火牆，或管理沒有網頁介面的專用日誌收集器。

在部署更新之前，請參閱 Panorama、日誌收集器、防火牆和 WildFire 版本相容性，瞭解關於更新版本相容性的重要資訊。

您必須直接在每個防火牆上啟動支援使用授權；您無法使用 Panorama 部署支援使用授權。

若要在 Panorama 管理伺服器上啟動授權或安裝更新，請參閱註冊 Panorama 並安裝授權和安裝 Panorama 的內容與軟體更新。

> 使用 Panorama 管理防火牆上的授權
> 使用 Panorama 將升級部署至防火牆、日誌收集器和 WildFire 設備

使用 Panorama 管理防火牆上的授權

下列步驟說明如何使用驗證碼擷取新授權，並將授權金鑰推送至受管理的防火牆。此外也說明如何手動更新（重新整理）無法直接存取網際網路的防火牆的授權狀態。對於無法直接存取網際網路的防火牆，Panorama™ 會自動對授權伺服器執行每日簽入，擷取授權更新與續約，並推送至防火牆。簽入固定於上午 1 點與 2 點進行；您無法變更此排程。



您無法使用 *Panorama* 來啟動防火牆的支援授權。您必須個別存取防火牆，才能啟動其支援授權。

若要為 *Panorama* 啟動授權，請參閱註冊 Panorama 並安裝授權。

- 啟動新購買的授權。
  1. 選取 **Panorama** > **Device Deployment**（裝置部署）> **Licenses**（授權），然後 **Activate**（啟動）。
  2. 輸入 Palo Alto Networks provided 為每個擁有新授權的防火牆提供的 **Auth Code**（驗證碼）。
  3. **Activate**（啟動）授權。
  4. （僅限 WildFire® 訂閱）在每個擁有新 WildFire 訂閱的防火牆上執行提交，以完成啟動：
     - **Commit**（提交）任何擱置中的變更。您必須存取防火牆的 Web 介面來完成此操作。
     - 如果沒有任何設定變更擱置中，請微幅變更，然後 **Commit**（提交）。例如，更新規則說明然後認可變更。如果防火牆屬於相同的裝置群組，您可以從 Panorama 推送規則變更以便在所有這些防火牆上執行認可，而不用單獨存取每一個防火牆。

     檢查 WildFire 分析設定檔規則是否包含 *WildFire* 使用授權支援的進階檔案類型。

- 更新防火牆的授權狀態。
  1. 選取 **Panorama** > **Device Deployment**（設備部署）> **Licenses**（授權）。

     頁面上的每一個項目可指出授權為使用中或非現用，並顯示使用中授權的到期日。
  2. 如果您先前在防火牆上直接啟動支援訂閱的驗證碼，請按一下 **Refresh**（重新整理），再從清單中選取防火牆。Panorama 可擷取授權，將授權部署到防火牆，並在 Panorama Web 介面上更新授權狀態。
  3. （僅限企業資料遺失防護 (DLP) 授權）將更新後的授權推送到利用企業 DLP 的受管理防火牆。
     1. 選取 **Commit**（提交）和 **Commit to Panorama**（提交到 **Panorama**）。
     2. 選取 **Commit**（提交）> **Push to Devices**（推送至裝置）和 **Edit Selections**（編輯選擇）。
     3. 選取 **Templates**（範本），然後選取與利用企業 DLP 的受管理防火牆關聯的範本堆疊。

        按一下 **OK**（確定）繼續。
     4. **Push**（推送）範本設定以成功更新企業 DLP 授權。

© 2019 Palo Alto Networks, Inc.

使用 Panorama 將升級部署至防火牆、日誌收集器和 WildFire 設備

您可以先將軟體和內容更新部署到一部分的防火牆、專用日誌收集器或 WildFire® 裝置和設備叢集，並使用 Panorama™ 來證明這些更新有用，然後才更新安裝在其餘的受管理的設備上。Panorama 需要直接的網際網路連線，您才能為定期的內容更新進行排程。若要依需求（非排程）部署軟體或內容更新，程序會根據 Panorama 是否連線至網際網路而有所不同。如果您在排程更新程序已開始或排程在五分鐘內開始時手動部署內容更新，Panorama 會顯示警告。

部署更新時，Panorama 會向受管理的設備（防火牆、日誌收集器和 WildFire 設備）通知有更新可用，裝置就會從 Panorama 擷取更新套件。依預設，受管理的設備會透過 Panorama 上的管理 (MGT) 介面擷取更新。不過，如果您要讓裝置使用另一個介面擷取更新，以降低 MGT 介面的流量負載，您可以設定 Panorama 來使用多個介面。

您可以使用 Panorama 快速將一個或多個防火牆的內容版本還原為之前安裝的內容版本。在新內容版本安裝於防火牆之後，如果新安裝的內容版本不穩定或甚至干擾了網路運作，您可以還原回之前安裝的版本。



依預設，您最多可將每個類型的兩個軟體或內容更新下載至 *Panorama*。當您開始任何超過該上限的下載時，*Panorama* 會刪除所選類型最舊的更新。若要變更該上限，請參閱 管理 Panorama 儲存軟體與內容更新。

- 支援的更新
- 使用 Panorama 排程內容更新
- 當 Panorama 連線至網際網路時升級日誌收集器
- 當 Panorama 未連線至網際網路時升級日誌收集器
- 當 Panorama 連線至網際網路時升級防火牆
- 當 Panorama 未連線至網際網路時升級防火牆
- 升級 ZTP 防火牆
- 從 Panorama 復原內容更新

支援的更新

您可以安裝的軟體與內容更新，根據各防火牆、日誌收集器及 WildFire® 設備和設備叢集上有哪些作用中的訂閱而異：

設備類型	軟體更新	內容更新
日誌收集器	Panorama™	應用程式（日誌收集器不需要威脅簽章） 防毒軟體 BrightCloud URL 篩選 WildFire®
防火牆	PAN-OS® GlobalProtect™ 代理程式/應用程式	應用程式 應用程式與威脅 防毒軟體 BrightCloud URL 篩選

© 2019 Palo Alto Networks, Inc.

設備類型	軟體更新	內容更新
		WildFire
WildFire	PAN-OS VM 映像	WildFire

使用 Panorama 排程內容更新

Panorama™ 需要直接的網際網路連線，才能在防火牆、日誌收集器及 WildFire® 設備和設備叢集上排程支援的更新。如果沒有，您可以只執行依需求更新。（若要排程日誌收集器的防毒、WildFire 或 BrightCloud URL 更新，日誌收集器必須執行 Panorama 7.0.3 或更新版本。）每個接收更新的防火牆、日誌收集器或 WildFire 設備或設備叢集都會產生日誌，以指出安裝成功（設定日誌）或失敗（系統日誌）。若要在 Panorama 管理伺服器上排程更新，請參閱為有網際網路連線的 Panorama 安裝更新。

在部署更新之前，請參閱 Panorama、日誌收集器、防火牆和 WildFire 版本相容性，瞭解關於內容發行版本相容性的重要資訊。參考版本資訊，瞭解您必須為 *Panorama* 版本安裝的最低內容版本。

對於相同類型的更新，*Panorama* 一次只能下載一個更新，如果您排程在相同時段下載相同類型的多個更新，則只有第一個下載會成功。為了確保相同類型的多個更新成功，請交錯安排更新。

如果您的防火牆直接連線至 *Palo Alto Networks*® 更新伺服器，您還可以使用 *Panorama* 範本（*Device*（裝置）> *Dynamic Updates*（動態更新））將內容更新排程推送至防火牆。如果您想在更新發佈後延遲一段時間再安裝，您必須使用範本部署排程。在極少數的情況下，內容更新會包含錯誤；指定延遲可讓 *Palo Alto Networks* 更有機會發現這種更新，並從更新伺服器中移除，以免被防火牆安裝。

針對每個您想要排程的更新類型執行下列步驟。

STEP 1 | 選取 **Panorama** > **Device Deployment**（裝置部署）> **Dynamic Updates**（動態更新），按一下 **Schedules**（排程），然後 **Add**（新增）排程。

STEP 2 | 指定 **Name**（名稱）（用於識別排程）、更新 **Type**（類型），以及更新頻率（**Recurrence**（週期性））。頻率選項取決於更新 **Type**（類型）。

PAN-OS® 使用 *Panorama* 時區來排程更新。

如果您將 **Type**（類型）設定為 **App and Threat**（應用程式與威脅），日誌收集器都只需要並且只會安裝應用程式內容，而不會安裝威脅內容。防火牆則會同時使用應用程式和威脅內容。請參閱 Panorama、日誌收集器、防火牆和 WildFire 版本相容性。

STEP 3 | 從以下排程動作中選取一個，然後選取防火牆或日誌收集器：

- **Download And Install**（下載並安裝）（最佳作法）—選取 **Devices**（裝置）（防火牆）、**Log Collectors**（日誌收集器）或 **WildFire Appliances and Clusters**（**WildFire** 設備和叢集）。
- **Download Only**（僅下載）—Panorama 會下載更新，但不安裝。

STEP 4 | 按一下 **OK**（確定）。

STEP 5 | 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

© 2019 Palo Alto Networks, Inc.

當 Panorama 連線至網際網路時升級日誌收集器

如需可在日誌收集器上安裝的軟體和內容更新清單，請參閱 支援的更新 。

您必須同時在收集器群組內升級所有日誌收集器，以避免丟失日誌資料。如果收集器群組內的日誌收集器並非執行相同的 PAN-OS 版本，則無法進行日誌轉送或日誌收集。此外，除非所有日誌收集器執行相同的 PAN-OS 版本，否則收集器群組內的日誌收集器日誌資料在 **ACC** 或 **Monitor**（監控器）頁籤內不可見。例如，如果您在收集器群組內有三個日誌收集器，且您升級了其中兩個，則不會有日誌被轉送至收集器群組內的任何日誌收集器。

PAN-OS® 9.0 為本機和專用日誌收集器引入了新的日誌資料格式。在升級到 PAN-OS 10.0 的路徑上，當您升級至 PAN-OS 9.0 時，已有日誌資料自動移轉至新的格式。重新格式化過程中，日誌資料在 **ACC** 或 **Monitor**（監控器）頁籤中不可見。此外，重新格式化完成之前，新日誌資料不會被轉送至日誌收集器。在重新格式化時，新日誌被寫入防火牆系統磁碟，並在程序順利完成後，新日誌將被轉送至相應的日誌收集器。

Palo Alto Networks 建議您在維護時段升級日誌收集器。由於日期格式的轉移，整個升級程序需要額外花費數個小時，具體取決於本機和專用日誌收集器上的日誌資料量。

STEP 1 | 升級日誌收集器之前，請確定您在 Panorama 管理伺服器上是執行適當的 Panorama™ 軟體版本。

Palo Alto Networks® 高度建議 *Panorama* 和日誌收集器執行相同的 *Panorama* 軟體版本，而且 *Panorama*、日誌收集器和所有受管理的防火牆也都執行相同的內容發行版本。如需瞭解重要軟體和內容相容性的詳細資訊，請參閱 Panorama、日誌收集器、防火牆和 WildFire 版本相容性。

Panorama 執行的軟體版本必須與日誌收集器相同（或更新），但必須具有相同或更舊的內容發行版本：

- 軟體發行版本—如果 Panorama 管理伺服器執行的軟體版本，與您想更新的日誌收集器不是相同或更新的版本，則在更新任何日誌收集器之前，您必須先將相同或更新的 Panorama 版本安裝在 Panorama（請參閱安裝 Panorama 的內容與軟體更新）。
- 內容發行版本—在內容發行版本方面，您應該確定所有日誌收集器都執行最新的內容發行版本，或執行的版本至少比 Panorama 上正在執行的版本還要新；否則，請先更新受管理的防火牆（使用 Panorama），再更新日誌收集器，然後才在 Panorama 管理伺服器上更新內容發行版本。

檢查軟體和內容版本：

- **Panorama** 管理伺服器—若要查明 Panorama 管理伺服器上執行的軟體和內容版本，請登入 Panorama 網頁介面並移至 General Information（一般資訊）設定（**Dashboard**（儀表板））。
- 日誌收集器 —若要查明日誌收集器上執行的軟體和內容版本，請登入每個日誌收集器的 CLI 並執行 **`show system info`** 命令。

STEP 2 | 安裝最新內容更新。

請參閱版本資訊，瞭解 *Panorama* 軟體版本所需的最低內容發行版本。

1. **Check Now**（立即檢查）（**Panorama** > **Device Deployment**（裝置部署）> **Dynamic Updates**（動態更新））有無最新更新。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）適當的內容更新。成功下載後，Action（動作）欄中的連結會從 **Download**（下載）變更為 **Install**（安裝）。
3. **Install**（安裝）內容更新（「應用程式」或「應用程式和威脅」更新）先於其他任何更新：

   按一下 **Install**（安裝），選取日誌收集器，然後按一下 **OK**（確定）。

© 2019 Palo Alto Networks, Inc.

無論您的訂閱是否同時包含應用程式和威脅內容，*Panorama* 都只需要並且只會安裝應用程式內容。請參閱 Panorama、日誌收集器、防火牆和 WildFire 版本相容性。

4. 針對其他任何更新（防毒、WildFire 或 URL 篩選），依需要、一次一個、以任意順序重複上述子步驟 2 和 3。

STEP 3 | 決定升級到 PAN-OS 10.0 的路徑。

您無法略過路徑中任何功能發佈版本的安裝，從目前執行的 PAN-OS 版本到 PAN-OS 10.0 版本皆是如此。針對您在升級路徑中會經過的每個版本，檢閱版本資訊中的已知問題和預設行為變更，以及新功能指南中的升級/降級注意事項。

（ 如果您從 7.1 或更舊版本升級，則必須 ）PAN-OS 8.0 引用新的日誌儲存格式。升級至 PAN-OS 8.0 後，您必須在繼續升級路徑之前，將 Panorama 日誌移轉至新日誌格式。日誌移轉為一次性工作；如果您已在升級至 PAN-OS 8.0 時移轉了日誌收集器上的日誌，則不需要再移轉一次。

如果是升級多個日誌收集器，在您開始下載映之前，請決定您想升級的所有日誌收集器的升級路徑，讓過程順暢進行。

STEP 4 | 對於您想更新至 PAN-OS 10.0 的所有日誌收集器，請繼續使用步驟 3 中識別的升級路徑，將日誌收集器升級至目標 Panorama 版本。

1. 在 Panorama 上，**Check Now**（立即檢查）（**Panorama** > **Device Deployment**（裝置部署）> **Software**（軟體））有無最新更新。如果有可用的更新，Action（動作）欄會顯示 **Download**（下載）連結。
2. 針對升級路徑中的每個版本，**Download**（下載）適合您要升級到的發行版本的型號特定檔案。例如，若要將 M-Series 設備升級至 Panorama 10.-.0，請下載 `Panorama_m-10.0.0` 映像。

   成功下載之後，該映像的 Action（動作）欄會從 **Download**（下載）變更為 **Install**（安裝）。
3. 針對升級路徑中的第一個（或下一個）版本，按一下 **Install**（安裝），然後選取適當的日誌收集器。
4. 根據您在升級路徑內安裝的版本，選取下列其中一個（步驟3）：
   - **Upload only to device (do not install)**（僅上傳至裝置（不要安裝））。
   - **Reboot device after install**（安裝後重新啟動裝置）。
5. 按一下 **OK**（確定）以啟動上傳或安裝。
6. 重複上述子步驟 3 至 5，直到日誌收集器執行所需的版本。

STEP 5 | 成功升級至 PAN-OS 10.0 後，檢查日誌格式移轉的狀態。

1. 登入 Panorama CLI 日誌收集器。
2. 執行下列命令，檢查日誌格式轉移的狀態：

```
admin> debug logdb show-es-upgrade-time
```

當日誌格式轉移仍在進行中的回應示例：

```
Response from logger 23456212: 50.98% of indices upgraded complete.
 Approximately less than a minute remaining until migration is complete.
 Once the log migration is complete, please run the 'show log-collector-
es-cluster health' command to check the ElasticSearch cluster status to
 verify logging and reporting functionality is restored.
```

當日誌格式轉移完成時的回應：

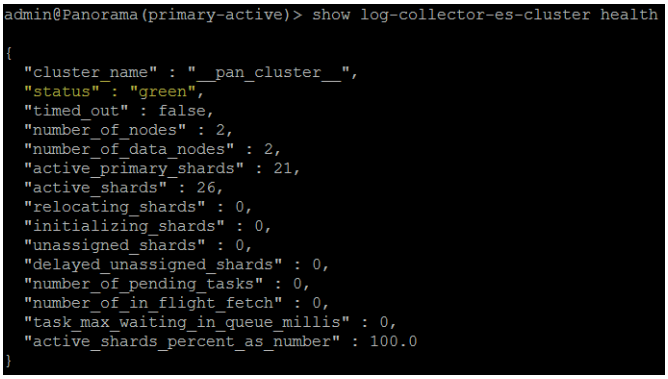
© 2019 Palo Alto Networks, Inc.

```
Response from logger 23456212: 100% of indices complete, please
 run the 'show log-collector-es-culster health' command to check
 the ElasticSearch cluster status to verify logging and reporting
 functionality is restored.
```

3. 日誌格式轉移完成後，在繼續下一步之前，請執行下列命令以檢查 ElasticSearch 叢集的狀態：

```
admin> show log-collector-es-cluster health
```

當 ElasticSearch 叢集健康 「狀態」 顯示 「綠色」 時，繼續下一步驟：



STEP 6 | 驗證日誌收集器上安裝的軟體和內容更新版本。

輸入 **show system info** 操作命令。輸出如下所示：

```
sw-version: 10.0.0
app-version: 8270-6076
app-release-date: 2020/05/08 18:21:51
```

當 Panorama 未連線至網際網路時升級日誌收集器

如需可在日誌收集器上安裝的軟體和內容更新清單，請參閱 支援的更新 。

PAN-OS® 9.0 為本機和專用日誌收集器引入了新的日誌資料格式。在升級到 PAN-OS 10.0 的路徑上，當您升級至 PAN-OS 9.0 時，已有日誌資料自動移轉至新的格式。重新格式化過程中，日誌資料在 **ACC** 或 **Monitor**（監控器）頁籤中不可見。此外，重新格式化完成之前，新日誌資料不會被轉送至日誌收集器。在重新格式化時，新日誌被寫入防火牆系統磁碟，並在程序順利完成後，新日誌將被轉送至相應的日誌收集器。

您必須同時在收集器群組內升級所有日誌收集器，以避免丟失日誌資料。如果收集器群組內的日誌收集器並非執行相同的 PAN-OS 版本，則無法進行日誌轉送或日誌收集。此外，除非所有日誌收集器執行相同的 PAN-OS 版本，否則收集器群組內的日誌收集器日誌資料在 **ACC** 或 **Monitor**（監控器）頁籤內不可見。例如，如果您在收集器群組內有三個日誌收集器，且您升級了其中兩個，則不會有日誌被轉送至收集器群組內的任何日誌收集器。

Palo Alto Networks 建議您在維護時段升級日誌收集器。由於日期格式的轉移，整個升級程序需要額外花費數個小時，具體取決於本機和專用日誌收集器上的日誌資料量。

STEP 1 | 升級日誌收集器之前，請確定您在 Panorama 管理伺服器上是執行適當的 Panorama™ 軟體版本。

© 2019 Palo Alto Networks, Inc.



Palo Alto Networks® 高度建議 *Panorama* 和日誌收集器執行相同的 *Panorama* 軟體版本，而且 *Panorama*、日誌收集器和所有受管理的防火牆也都執行相同的內容發行版本。如需瞭解重要軟體和內容相容性的詳細資訊，請參閱 Panorama、日誌收集器、防火牆和 WildFire 版本相容性。

Panorama 執行的軟體版本必須與日誌收集器相同（或更新），但必須具有相同或更舊的內容發行版本：

- 軟體發行版本—如果 Panorama 管理伺服器執行的軟體版本，與您想更新的日誌收集器不是相同或更新的版本，則在更新任何日誌收集器之前，您必須先將相同或更新的 Panorama 版本安裝在 Panorama（請參閱安裝 Panorama 的內容與軟體更新）。
- 內容發行版本—在內容發行版本方面，您應該確定所有日誌收集器都執行最新的內容發行版本，或執行的版本至少比您將安裝在 Panorama 上的版本或其正在執行的版本還要新；否則，請先更新受管理的防火牆（使用 Panorama），再更新日誌收集器，然後才在 Panorama 管理伺服器上更新內容發行版本（請參閱安裝 Panorama 的內容與軟體更新）。

檢查軟體和內容版本：

- **Panorama** 管理伺服器—若要查明 Panorama 管理伺服器上執行的軟體和內容版本，請登入 Panorama 網頁介面並移至 General Information（一般資訊）設定（**Dashboard**（儀表板））。
- 日誌收集器 —若要查明日誌收集器上執行的軟體和內容版本，請登入每個日誌收集器的 CLI 並執行 **`show system info`** 命令。

STEP 2 | 決定您需要安裝在日誌收集器上的內容更新。參考版本資訊，瞭解您必須為 Panorama 版本安裝的最低內容版本。



您必須先安裝內容更新，再安裝軟體更新。

1. 執行 **`show system info`** CLI 指令以檢視目前更新版本。
2. 針對每個內容更新，決定是否需要更新，並記下您在步驟 4 中需要下載哪些內容更新。



請確定 *Panorama* 執行的內容發行版本，與受管理的防火牆和日誌收集器相同，但並不是更新的版本。

3. （依需要）在日誌收集器上更新內容版本之前，請先 將受管理的防火牆升級至相同或更新的內容發行版本。

STEP 3 | 決定升級到 PAN-OS 9.2 的路徑。

您無法略過路徑中任何功能發佈版本的安裝，從目前執行的 PAN-OS 版本到 PAN-OS 10.0 版本皆是如此。針對您在升級路徑中會經過的每個版本，檢閱版本資訊中的已知問題和預設行為變更，以及新功能指南中的升級/降級注意事項。

（如果您從 7.1 或更舊版本升級，則必須）PAN-OS 8.0 引用新的日誌儲存格式。升級至 PAN-OS 8.0 後，您必須在繼續升級路徑之前，將 Panorama 日誌移轉至新日誌格式。日誌移轉為一次性工作；如果您已在升級至 PAN-OS 8.0 時移轉了日誌收集器上的日誌，則不需要再移轉一次。



如果是升級多個日誌收集器，在您開始下載映之前，請決定您想升級的所有日誌收集器的升級路徑，讓過程順暢進行。

STEP 4 | 將內容和軟體更新下載到可透過 SCP 或 HTTPS 連線至 Panorama 來上傳檔案的主機。

1. 使用可存取網際網路的主機登入 Palo Alto Networks 客戶支援網站。
2. 下載內容更新：
    1. 在 Resources（資源）部分中按一下 **Dynamic Updates**（動態更新）。

© 2019 Palo Alto Networks, Inc.

2. **Download**（下載）所需內容更新，然後將檔案儲存至主機。為您要更新的各內容類型執行此步驟。

3. 下載軟體更新：

   1. 返回 Palo Alto Networks 客戶支援網站的主頁面，然後在 Resources（資源）部分中按一下 **Software Updates**（軟體更新）。
   2. 檢閱下載欄以決定您要安裝的版本。M-Series 設備的更新套件檔名以 “Panorama_m” 開頭並緊接著版本號碼。例如，若要將 M-Series 設備升級至 Panorama 10.0.0，請下載 `Panorama_m-10.0.0` 映像。

      您可以從 *Filter By*（篩選依據）下拉式清單中選取 *Panorama M Images*（*Panorama M* 映像）（適用於 *M-Series* 設備），快速找到 *Panorama* 映像。

4. 按一下適當的檔名，並將檔案儲存至主機。

STEP 5 | 在日誌收集器上安裝內容更新。



如果您需要安裝內容更新，則必須在安裝軟體更新之前完成。此外，請先將內容更新安裝在防火牆，再安裝於日誌收集器，然後才在 *Panorama* 上更新內容發行版本。

先安裝「應用程式」或「應用程式和威脅」更新，再依需要、一次一個、以任意順序安裝其他任何更新（防毒、WildFire® 或 URL 篩選）。



無論您的訂閱是否同時包含應用程式和威脅內容，*Panorama* 都只需要並且只會安裝應用程式內容。請參閱 Panorama、日誌收集器、防火牆和 WildFire 版本相容性。

1. 在 Panorama 中，選取 **Panorama** > **Device Deployment**（設備部署）> **Dynamic Updates**（動態更新）。
2. 按一下 **Upload**（上傳），選取更新 **Type**（類型），**Browse**（瀏覽）至主機上適當的內容更新檔案，然後按一下 **OK**（確定）。
3. 按一下 **Install From File**（從檔案安裝），選取更新 **Type**（類型），並選取您剛上傳的更新的 **File Name**（檔案名稱）。
4. 選取日誌收集器。
5. 按一下 **OK**（確定）以啟動安裝。
6. 針對每個內容更新重複這些步驟。

STEP 6 | 安裝軟體更新。

1. 選取 **Panorama** > **Device Deployment**（設備部署）> **Software**（軟體）。
2. 按一下 **Upload**（上傳），**Browse**（瀏覽）至主機上適當的軟體更新檔案，然後按一下 **OK**（確定）。
3. 在您剛上傳的版本的 Action（動作）欄中，按一下 **Install**（安裝）。
4. 選取您要安裝更新的日誌收集器。
5. 根據您在升級路徑內安裝的軟體版本，選取下列其中一個（步驟 3）：
   - **Upload only to device (do not install)**（僅上傳至裝置（不要安裝））。
   - **Reboot device after install**（安裝後重新啟動裝置）。
6. 按一下 **OK**（確定）以啟動安裝。

STEP 7 | 成功升級至 PAN-OS 10.0 後，檢查日誌格式移轉的狀態。

1. 登入 Panorama CLI 日誌收集器。
2. 執行下列命令，檢查日誌格式轉移的狀態：

© 2019 Palo Alto Networks, Inc.

```
admin> debug logdb show-es-upgrade-time
```

當日誌格式轉移仍在進行中的回應示例：

```
Response from logger 23456212: 50.98% of indices upgraded complete.
 Approximately less than a minute remaining until migration is complete.
 Once the log migration is complete, please run the 'show log-collector-
es-cluster health' command to check the ElasticSearch cluster status to
 verify logging and reporting functionality is restored.
```

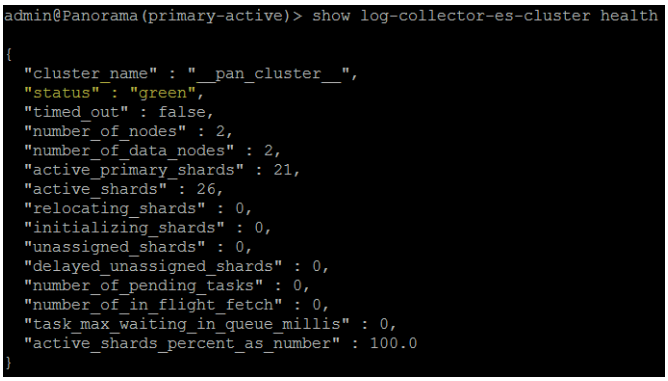
當日誌格式轉移完成時的回應：

```
Response from logger 23456212: 100% of indices complete, please
 run the 'show log-collector-es-culster health' command to check
 the ElasticSearch cluster status to verify logging and reporting
 functionality is restored.
```

3. 日誌格式轉移完成後，在繼續下一步之前，請執行下列命令以檢查 ElasticSearch 叢集的狀態：

```
admin> show log-collector-es-cluster health
```

當 ElasticSearch 叢集健康 「狀態」 顯示 「綠色」 時，繼續下一步驟：



STEP 8 | 驗證各日誌收集器上安裝的軟體和內容版本。

登入日誌收集器 CLI 並輸入 **show system info**（顯示系統資訊）操作命令。輸出如下所示：

```
sw-version: 10.0.0
app-version: 8270-6076
app-release-date: 2020/05/08 18:21:51
```

當 Panorama 連線至網際網路時升級防火牆

檢視 PAN-OS 10.0 版本資訊，然後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，則請遵循當 Panorama 未連線至網際網路時升級防火牆中的程序，以讓您可以手動下載映像至 *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：

© 2019 Palo Alto Networks, Inc.

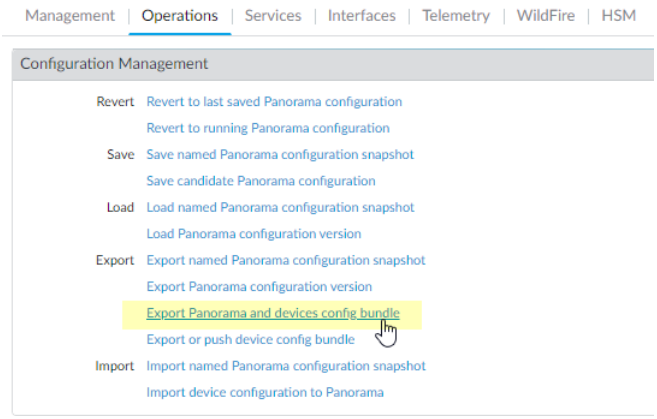
- 確定 Panorama 正執行您要升級版本相同或更新的 PAN-OS 版本。在升級受管理的防火牆到 PAN-OS 10.0 之前，您必須安裝 Panorama 的內容與軟體更新並使用 Panorama 將升級部署至防火牆、日誌收集器和 WildFire 設備，以升級 Panorama 和日誌收集器至 PAN-OS 10.0。
- 確保防火牆連接可靠的電源。升級過程中的電力損耗會使防火牆無法使用。

STEP 1 | 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。



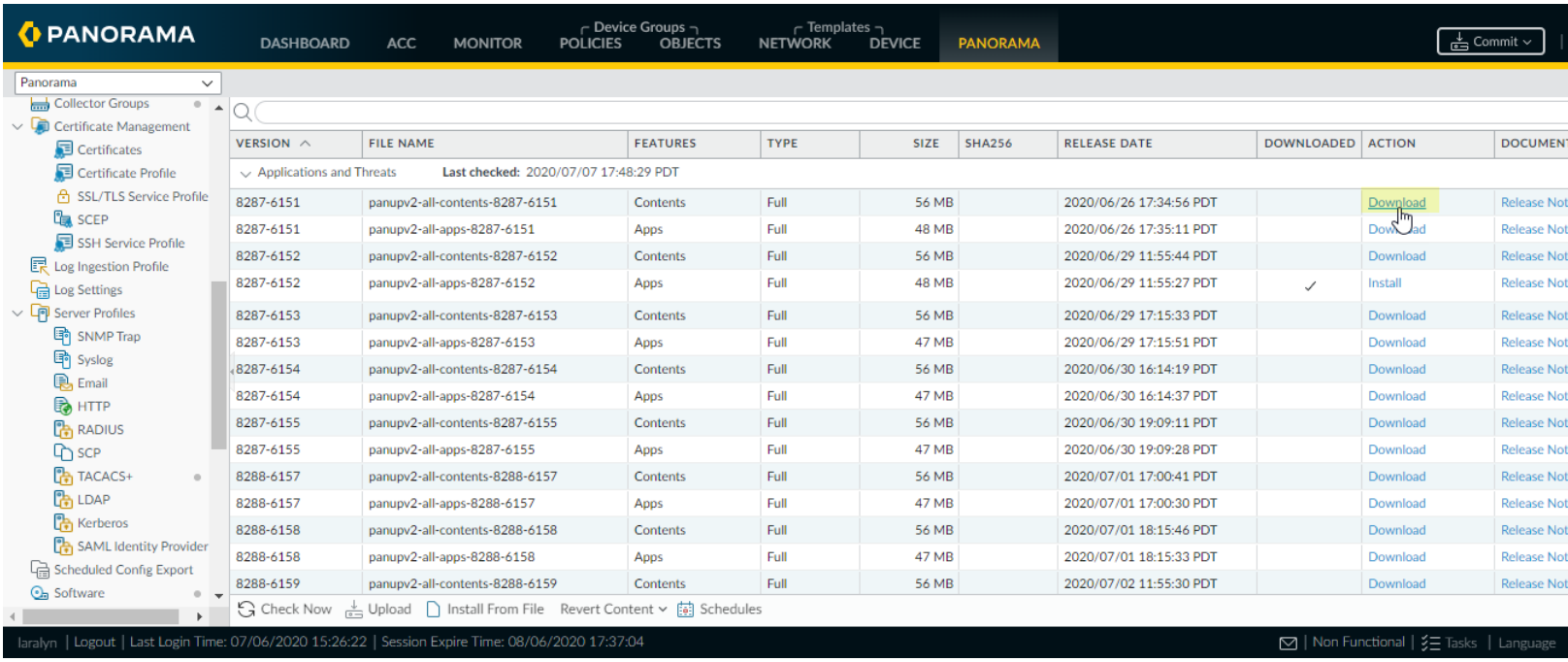
2. 將匯出的檔案儲存至防火牆外部的位置。如果您在升級時發生問題，便可使用此備份還原組態。

STEP 2 | 在您計劃要升級的防火牆上更新內容發行版本。

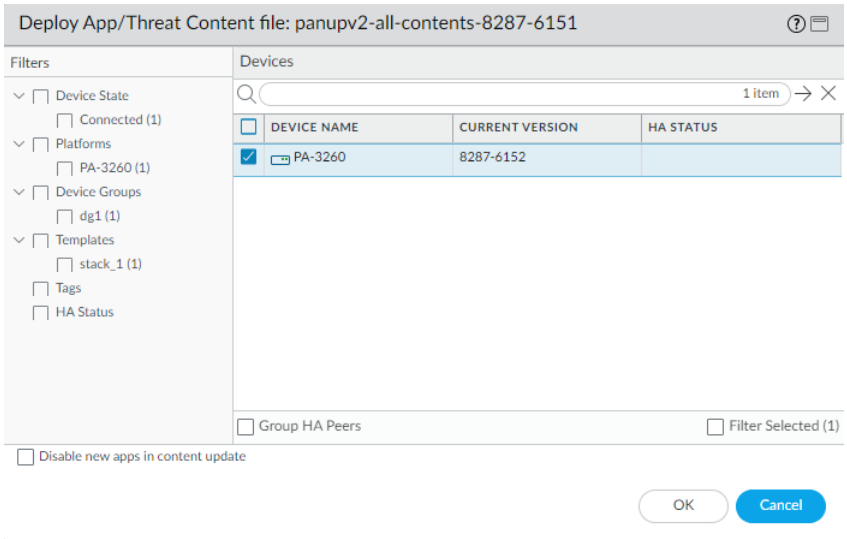
請參閱版本資訊，瞭解 PAN-OS 10.0 所需的最低內容發行版本。請確認在部署內容更新至 Panorama 和受管理的防火牆時，遵循 應用程式和威脅內容更新的最佳實踐方法。

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。

© 2019 Palo Alto Networks, Inc.



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。

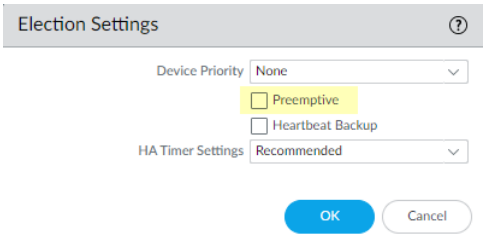


依預設，您可以將每種類型的最多兩個軟體或內容更新上傳至 *Panorama* 設備，如果您下載相同類型的第三個更新，*Panorama* 會刪除該類型最舊版本的更新。如果您需要上傳單一類型兩個以上的軟體更新或內容更新，請使用 ***setmax-num-images count <number>*** *CLI* 命令來增加數目上限。

STEP 3 | （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）。

© 2019 Palo Alto Networks, Inc.



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 4 | 決定升級到 PAN-OS 10.0 的路徑。

您無法略過路徑中任何功能發佈版本的安裝，從目前執行的 PAN-OS 版本到 PAN-OS 10.0.0 版本皆是如此。針對您在升級路徑中會經過的每個版本，檢閱版本資訊中的已知問題和預設行為變更，以及新功能指南中的升級/降級注意事項。

如果是升級多個防火牆，在您開始下載映之前，請決定您想升級的所有防火牆的升級路徑，讓過程順暢進行。

STEP 5 | 下載目標 PAN-OS 10.0 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。

   例如，若要將 PA-220 和 PA-5250 防火牆升級至 PAN-OS 10.0.0，請下載 `PanOS_220-10.0.0`、`PanOS_3000-10.0.0` 和 `PanOS_5200-10.0.0` 映像。在您成功下載映像後，該映像的動作欄位會變更為 **Install**（安裝）。

STEP 6 | 在防火牆上安裝 PAN-OS 10.0 軟體更新。

在升級分支防火牆之前，您必須將中樞防火牆從 *PAN-OS 10.0.0* 升級到 *PAN-OS 10.0.1* 或更新版本。在中樞防火牆之前升級分支防火牆可能會產生錯誤的監控資料（*Panorama* > *SD-WAN* > *Monitoring*（監控）），且 *SD -WAN* 連結會錯誤地顯示為 `down`（關閉）。

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）。舉例來說，如果您想要升級 PA-220 防火牆，請按一下 PanOS_220-10.0.0 對應行的 **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** 配對）。
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 10.0.0。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 7 | （僅限 HA 防火牆升級）升級每個 HA 配對中的次要 HA 配對。

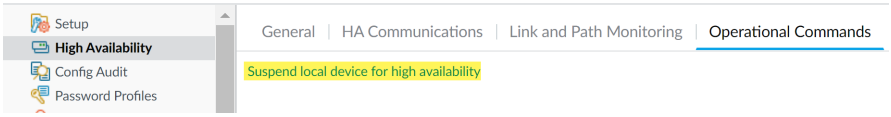
1. （僅限主動/被動升級）暫停在每個正在升級的主動/被動配對主動裝置。

© 2019 Palo Alto Networks, Inc.

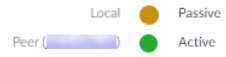
1. 切換內容至主動防火牆。
2. 在 **Dashboard**（儀表板）上的高可用性 Widget 中，驗證 **Local**（本機）防火牆狀態為 **Active**（主動）且 **Peer**（端點）為 **Passive**（被動）。



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）從您剛升級配對的 CLI 執行以下命令，以讓防火牆再次運作：

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

STEP 8 | 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。

	DEVICE NAME	MODEL	IP Address IPV4	TEMPLATE	Status DEVICE STATE	Status HA STATUS	Status CERTIFICATE	Status L... M... D...	SOFTWARE VERSION	APPS AND THREAT	ANTIVIRUS
	DG-VM (5/5 Devices Connected): Shared > DG-VM										
	PA-VM-6	PA-VM		Stack-VM	Connected		pre-defined		8.1.0	8320-6307	3881-4345
	PA-VM-73	PA-VM		Stack-Test73	Connected		pre-defined		9.1.3	8320-6307	3873-4337
	PA-VM-95	PA-VM		Stack-VM	Connected		pre-defined		10.0.0	8320-6307	3881-4345
	PA-VM-96	PA-VM		Stack-VM	Connected	Passive	pre-defined		10.0.0	8299-6216	3881-4345
	PA-VM			Stack-Test92	Connected	Active	pre-defined		10.0.0	8299-6216	3881-4345

© 2019 Palo Alto Networks, Inc.

STEP 9 | （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）。

當 Panorama 未連線至網際網路時升級防火牆

如需可在防火牆上安裝的軟體和內容更新清單，請參閱支援的更新。

STEP 1 | 升級受管理的防火牆之前，請確定您在 Panorama 管理伺服器和日誌收集器上是執行適當的 Panorama™ 軟體版本。

Palo Alto Networks® 高度建議 *Panorama* 和日誌收集器執行相同的 *Panorama* 軟體版本，而且 *Panorama*、日誌收集器和所有受管理的防火牆也都執行相同的內容發行版本。

如需瞭解重要軟體和內容相容性的詳細資訊，請參閱 Panorama、日誌收集器、防火牆和 WildFire 版本相容性。

Panorama 執行的軟體版本必須與防火牆相同（或更新），但必須具有相同或更舊的內容發行版本：

- 軟體發行版本—如果 Panorama 管理伺服器或日誌收集器執行的軟體版本，與您想更新的防火牆不是相同或更新的版本，則在更新任何防火牆之前，您必須先將相同或更新的 Panorama 版本安裝在 Panorama，再安裝於日誌收集器（請參閱安裝 Panorama 的內容與軟體更新）。
- 內容發行版本—在內容發行版本方面，您應該確定所有防火牆都執行最新的內容發行版本，或執行的版本至少比 Panorama 和日誌收集器上正在執行的版本還要新；否則，請先更新受管理的防火牆，接著當 Panorama 未連線至網際網路時升級日誌收集器，然後才在 Panorama 管理伺服器上更新內容發行版本（請參閱安裝 Panorama 的內容與軟體更新）。

檢查軟體和內容版本：

- **Panorama** 管理伺服器—登入 Panorama 網頁介面，然後移至 General Information（一般資訊）設定（**Dashboard**（儀表板））。
- 日誌收集器—登入每個日誌收集器的 CLI，並執行 **`show system info`** 命令。

STEP 2 | 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. **Export Panorama and devices config bundle**（匯出 **Panorama** 和裝置設定組合）（**Panorama** > **Setup**（設定）> **Operations**（操作）），產生並匯出 Panorama 和每個受管理裝置的最新設定備份。
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 3 | 決定您需要安裝的內容更新。請參閱版本資訊，瞭解您必須為 PAN-OS® 版本安裝的最低內容發行版本。

Palo Alto Networks 高度建議 *Panorama*、日誌收集器和所有受管理的防火牆執行相同的內容發行版本。

針對每個內容更新，決定是否需要更新，並記下您在步驟 5 中需要下載哪些內容更新。

請確定 *Panorama* 執行的內容發行版本，與受管理的防火牆和日誌收集器相同，但並不是更新的版本。

© 2019 Palo Alto Networks, Inc.

STEP 4 | 針對您想要更新至 Panorama 10.0 的防火牆，決定軟體升級路徑。請參閱新功能指南，以決定升級至 PAN-OS 10.0 的路徑。

登入 Panorama，選取 **Panorama** > **Managed Devices**（受管理的裝置），並注意您想升級的防火牆的目前軟體版本。

針對您在升級路徑中會經過的每個版本，高度建議您檢閱版本資訊中的已知問題和預設行為變更，以及新功能指南中的升級/降級注意事項。

STEP 5 | 將內容和軟體更新下載到可透過 SCP 或 HTTPS 連線至 Panorama 來上傳檔案的主機。

依預設，您可以將每種類型的最多兩個軟體或內容更新上傳至 Panorama 設備，如果您下載相同類型的第三個更新，Panorama 會刪除該類型最舊版本的更新。如果您需要上傳單一類型兩個以上的軟體更新或內容更新，請使用**`set max-num-images count <number>`** CLI 命令來增加 Panorama 可儲存的映像數目上限。

1. 使用可存取網際網路的主機登入 Palo Alto Networks 客戶支援網站。
2. 下載內容更新：
   1. 在 Resources（資源）部分中按一下 **Dynamic Updates**（動態更新）。
   2. **Download**（下載）最新的內容發行版本（或至少與您將安裝在 Panorama 管理伺服器上或其正在執行的版本相同或還要新），並將檔案儲存至主機；針對您需要更新的每種內容類型，重複此步驟。
3. 下載軟體更新：
   1. 返回 Palo Alto Networks 客戶支援網站的主頁面，然後在 Resources（資源）部分中按一下 **Software Updates**（軟體更新）。
   2. 檢閱下載欄以決定您需要安裝的版本。更新套件的檔案名稱會指出型號。例如，若要將 PA-220 和 PA-5260 防火牆升級至 PAN-OS 8.0.8，請下載 `PanOS_220-8.0.8`、`PanOS_3000-8.0.8` 和 `PanOS_5200-8.0.8` 映像。

      您可以從 *Filter By*（篩選依據）下拉式清單中選取 *PAN-OS for the PA-<series/model>*，快速找到特定的 *PAN-OS* 映像。
4. 按一下適當的檔名，並將檔案儲存至主機。

STEP 6 | 在受管理的防火牆上安裝內容更新。

您必須先安裝內容更新，再安裝軟體更新。

先安裝「應用程式」或「應用程式和威脅」更新，再依需要、一次一個、以任意順序安裝其他任何更新（防毒、WildFire® 或 URL 篩選）。

1. 選取 **Panorama** > **Device Deployment**（設備部署）> **Dynamic Updates**（動態更新）。
2. 按一下 **Upload**（上傳），選取更新 **Type**（類型），**Browse**（瀏覽）至適當的內容更新檔案，然後按一下 **OK**（確定）。
3. 按一下 **Install From File**（從檔案安裝），選取更新 **Type**（類型），並選取您剛上傳的內容更新的 **File Name**（檔案名稱）。
4. 選取您要安裝更新的防火牆。
5. 按一下 **OK**（確定）以啟動安裝。
6. 針對每個內容更新重複這些步驟。

STEP 7 | （僅限當作 GlobalProtect™ 入口網站的防火牆）將 GlobalProtect 代理程式/應用程式軟體更新上傳至防火牆並啟動。

© 2019 Palo Alto Networks, Inc.

您可在防火牆上啟動更新，供使用者下載至其端點（用戶端系統）。

1. 使用可存取網際網路的主機登入 Palo Alto Networks 客戶支援網站。
2. 下載適當的 GlobalProtect 代理程式/應用程式軟體更新。
3. 在 Panorama 上，選取 **Panorama** > **Device Deployment**（裝置部署）> **GlobalProtect Client**（**GlobalProtect** 用戶端）。
4. 按一下 **Upload**（上傳），在您已下載檔案的主機上 **Browse**（瀏覽）至適當的 GlobalProtect 代理程式/應用程式軟體更新，然後按一下 **OK**（確定）。
5. 按一下 **Activate From File**（從檔案啟動），選取您剛上傳的 GlobalProtect 代理程式/應用程式更新的 **File Name**（檔案名稱）。

   您一次只能啟動一個版本的代理程式/應用程式軟體。如果您啟動新版本，但某些代理程式需要上一個版本，則您必須再次重新啟動舊版本，讓這些代理程式下載上一個更新。
6. 選取要啟動更新的防火牆。
7. 按一下 **OK**（確定）以啟動。

STEP 8 | 上傳 PAN-OS 軟體更新。

1. 選取 **Panorama** > **Device Deployment**（設備部署）> **Software**（軟體）。
2. 按一下 **Upload**（上傳），**Browse**（瀏覽）至主機上適當的軟體更新檔案，然後按一下 **OK**（確定）。

STEP 9 | 安裝 PAN-OS 軟體更新。

若要避免在高可用性 *(HA)* 防火牆上更新軟體時的停機時間，每次更新一個 *HA* 端點。

對於主動/主動防火牆，更新端點的順序無關緊要。

對於主動/被動防火牆，您必須先更新被動端點，暫停主動端點（故障復原），更新主動端點，然後將主動端點返回至功能狀態（故障復原）。

在升級分支防火牆之前，您必須將中樞防火牆從 *PAN-OS 10.0.0* 升級到 *PAN-OS 10.0.1* 或更新版本。在中樞防火牆之前升級分支防火牆會產生錯誤的監控資料（*Panorama* > *SD-WAN* > *Monitoring*（監控）），且 *SD -WAN* 連結會錯誤地顯示為 `down`（關閉）。

1. 執行適用於您的防火牆組態的步驟，以安裝您剛上傳的 PAN-OS 軟體更新。
   - **Non-HA firewalls**（非 HA 防火牆）——按一下行動欄內的 **Install**（安裝），選取您正在升級的所有防火牆，選取 **Reboot device after install**（安裝後重新開機設備），然後按一下 **OK**（確定）。
   - 主動式/主動式 **HA** 防火牆：
     1. 在您想要升級的第一個對等上，確認先佔設定已停用（**Device**（裝置）> **High Availability**（高可用性）> Election Settings（選取設定））。如果已啟用，請編輯 **Election Settings**（選取設定），停用（清除）**Preemptive**（先佔）設定，然後 **Commit**（提交）您的變更。您只需要在每個 HA 配對中的一個防火牆上停用此設定，但要確定提交成功之後再繼續。
     2. 按一下 **Install**（安裝），停用（清除）**Group HA Peers**（群組 **HA** 對等），選取任一 HA 對等，選取 **Reboot device after install**（安裝後重新啟動裝置），然後按一下 **OK**（確定）。繼續之前，等候防火牆完成重新開機。
     3. 按一下 **Install**（安裝），停用（清除）**Group HA Peers**（群組 **HA** 對等），選取您在上一步未更新的 HA 對等、選取 **Reboot device after install**（安裝後重新啟動裝置），然後按一下 **OK**（確定）。
   - 主動式/被動式 **HA** 防火牆—在此示例中，主動防火牆名稱為 fw1 而被動防火牆名稱為 fw2：

© 2019 Palo Alto Networks, Inc.

1. 在您想要升級的第一個對等上，確認先佔設定已停用（**Device**（裝置）> **High Availability**（高可用性）> Election Settings（選取設定））。如果已啟用，請編輯 **Election Settings**（選取設定），停用（清除）**Preemptive**（先佔）設定，然後 **Commit**（提交）您的變更。您只需要在每個 HA 配對中的一個防火牆上停用此設定，但要確定提交成功之後再繼續。
2. 在適當更新的 Action（動作）欄中按一下 **Install**（安裝），停用（清除）**Group HA Peers**（群組 **HA** 對等），選取 fw2，選取 **Reboot device after install**（安裝後重新啟動裝置），然後按一下 **OK**（確定）。繼續之前，等候 fw2 完成重新開機。
3. 當 fw2 完成重新開機後，在 fw1 上確認（**Dashboard**（儀表板）> High Availability（高可用性））fw2 仍然是被動對等（Local（本機）防火牆狀態為 `active`（主動），Peer（對等）—fw2—為 `passive`（被動））。
4. 存取 fw1 和 **Suspend local device**（暫停本機裝置）（**Device**（裝置）> **High Availability**（高可用性）> **Operational Commands**（操作命令））。
5. 存取 fw2（**Dashboard**（儀表板）> High Availability（高可用性），確認本機防火牆狀態為 `active`（主動），對等為 `suspended`（暫停）。
6. 存取 Panorama，選取 **Panorama** > **Device Deployment**（裝置部署）> **Software**（軟體），在適當版本的 Action（動作）欄中按一下 **Install**（安裝），停用（清除）**Group HA Peers**（群組 **HA** 對等），選取 fw1，選取 **Reboot device after install**（安裝後重新啟動裝置），然後按一下 OK（確定）。繼續之前，等候 fw1 完成重新開機。
7. 存取 fw1（**Device**（裝置）> **High Availability**（高可用性）> **Operational Commands**（操作命令）），按一下 **Make local device functional**（讓本機裝置運作），然後在您繼續前稍等兩分鐘。
8. 在 fw1 上（**Dashboard**（儀表板）> High Availability（高可用性），確認 Local（本機）防火牆狀態為 `passive`（被動），對等（fw2）為 `active`（主動）。

2. 針對 PAN-OS 版本更新完成上述步驟之後，重複步驟 8 和步驟 9，依需要來上傳升級路徑中的下一個 PAN-OS 版本，直到所有防火牆都執行目標 PAN-OS 10.0 版本為止。

STEP 10 | 驗證各受管理的防火牆上安裝的軟體和內容版本。

1. 選取 **Panorama** > **Managed Devices**（受管理的裝置）。
2. 找到防火牆，並檢閱 Software Version（軟體版本）、Apps and Threat（應用程式與威脅）、Antivirus（防毒）、URL Filtering（URL 篩選）及 GlobalProtect Clien（GlobalProtect 用戶端）欄中的值。

STEP 11 | 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。

升級 ZTP 防火牆

成功新增 ZTP 防火牆至 Panorama™ 管理伺服器後，設定 ZTP 防火牆的目標 PAN-OS 版本。首次成功連線至 Panorama 後，Panorama 會檢查 ZTP 防火牆上安裝的 PAN-OS 版本是否比所設定目標 PAN-OS 版本更新或相同。如果 ZTP 防火牆上安裝的 PAN-OS 版本比目標 PAN-OS 版本更舊，則 ZTP 防火牆進行升級循環，直到安裝目標 PAN-OS 版本。

STEP 1 | 新增 ZTP 防火牆至 Panorama。

STEP 2 | 登入 Panorama 網頁介面 以管理員使用者身份。

STEP 3 | 選取 **Panorama** > **Device Deployment**（裝置部署）> **Updates**（更新）和 **Check Now**（立即檢查）以獲得最新 PAN-OS 版本。

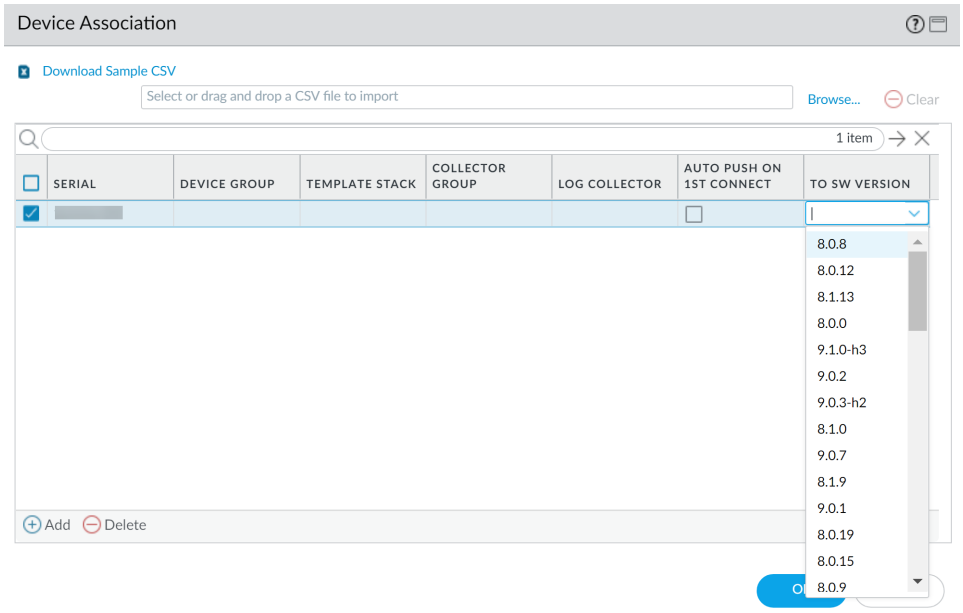
STEP 4 | 選取 **Panorama** > **Managed Devices**（受管理的裝置）> **Summary**（摘要）並選取一或多個 ZTP 防火牆。

© 2019 Palo Alto Networks, Inc.

STEP 5 | **Reassociate**（重新關聯）所選取 ZTP 防火牆。

STEP 6 | 在 **To SW Version**（至軟體版本）欄中，選取 ZTP 防火牆的目標 PAN-OS 版本。

STEP 7 | 按一下 **OK**（確定）儲存組態變更。



STEP 8 | 選取 **Commit**（認可）並 **Commit and Push**（認可和推送）設定變更。

STEP 9 | 確認 ZTP 防火牆軟體升級。

1. 選取 **Panorama** > **Managed Devices**（受管理的裝置）> **Summary**（摘要）並導覽至 ZTP 防火牆。
2. 確認 **Software Version**（軟體版本）欄中顯示正確的目標 PAN-OS 版本。

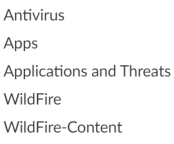
從 Panorama 復原內容更新

Panorama™ 讓您可以快速復原直接來自 Panorama 的一個或多個防火牆、日誌收集器或 WildFire 設備上的應用程式、應用程式與威脅、防毒、WildFire® 和 WildFire 內容版本。使用 Panorama 復原安裝中受管理的裝置上的內容版本，以利用集中化的工作流程，協助轉移任何與應用程式導入或修改，或內容更新中新威脅特徵碼相關的風險。當您復原內容時，Panorama 會為每個裝置生成一個系統日誌。請確認在部署內容更新至受管理的裝置時，使用 應用程式與威脅更新的最佳實踐方法 。

STEP 1 | 登入 Panorama 網頁介面。

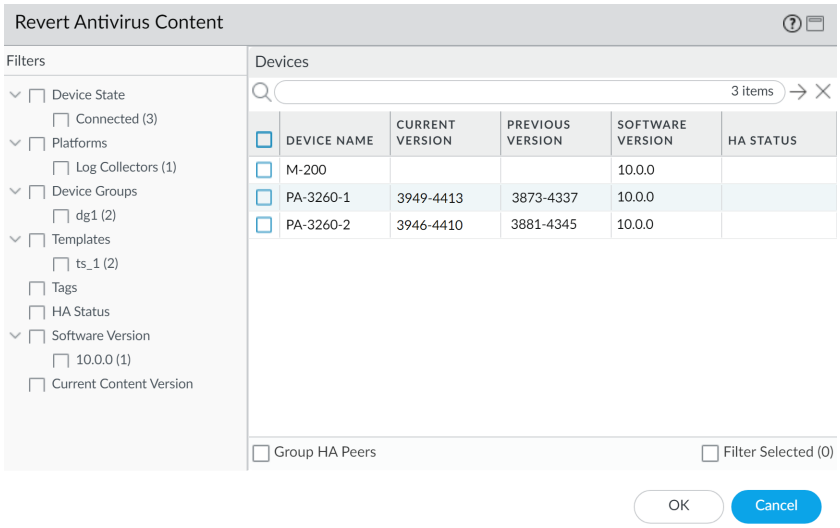
STEP 2 | 選取 **Panorama** > **Device Deployment**（設備部署）> **Dynamic Updates**（動態更新）和 **Revert Content**（復原內容）。

STEP 3 | 選取您需要復原的內容類型。



STEP 4 | 選取要復原其上內容的一個或多個防火牆，然後按一下 **OK**（確定）。您復原的內容版本必須早於目前安裝在裝置上的版本。

© 2019 Palo Alto Networks, Inc.


Revert Antivirus Content
Filters
Device State
Connected (3)
Platforms
Log Collectors (1)
Device Groups
dg1 (2)
Templates
ts_1 (2)
Tags
HA Status
Software Version
10.0.0 (1)
Current Content Version
Devices
3 items
DEVICE NAME
CURRENT VERSION
PREVIOUS VERSION
SOFTWARE VERSION
HA STATUS
M-200
10.0.0
PA-3260-1
3949-4413
3873-4337
10.0.0
PA-3260-2
3946-4410
3881-4345
10.0.0
Group HA Peers
Filter Selected (0)
OK
Cancel

監控網路活動

Panorama™ 管理伺服器提供網路流量的完整圖形化檢視。使用 Panorama 上的可視性工具 - Application Command Center（應用程式控管中心 - ACC）、日誌和報告產生功能 - 您可以集中分析、調查和報告所有網路活動、識別可能影響安全的區域，以及將它們轉換成安全的應用程式啟用原則。

本節包含以下主題：

> 使用 Panorama 增強可見度
> 在 Panorama 上擷取陷阱 ESM 日誌
> 使用案例：使用 Panorama 監控應用程式
> 使用案例：使用 Panorama 回應事件

使用 Panorama 增強可見度

除了中央部署和防火牆組態功能外，Panorama 也能讓您監控和報告周遊您網路的所有流量。雖然 Panorama 上的報告功能和防火牆極為類似，但 Panorama 的優點是提供單一的窗格檢視，該檢視彙總了所有受管理防火牆之間的資訊。此彙總檢視提供了您整個網路的使用者活動、流量模式和潛在威脅趨勢的可控管資訊。

您可以在 Panorama 上使用應用程式監測中心 (ACC)、應用程式層面、日誌檢視器，以及標準和可自訂的報告選項，快速地瞭解周遊網路的流量相關資訊。此資訊的檢視功能可讓您評估目前原則的適用處，及執行效果欠佳的區域。您接著可以使用此資料來增強網路安全性策略。例如，您可以增強安全性規則來增加跨網路的所有使用者的遵循性和責任感，或在管理網路容量和將資產風險降到最低的同時，滿足您網路使用者對大量應用程式的需求。

下列主題提供 Panorama 上報告功能的高階檢視，包含一些使用案例，告訴您如何在自身網路的基礎結構中使用這些功能。如需每一個可用的報表和圖表及其說明的完整清單，請參閱線上說明。

- 使用應用程式監測中心及應用程式層面以監控網路
- 分析日誌資料
- 產生、排程及以電子郵件傳送報告
- 為排程報告設定金鑰限制

使用應用程式監測中心及應用程式層面以監控網路

您可以使用應用程式監測中心和 AppScope 二者，監控與報告從周遊網路的流量中所記錄的資料。

Panorama 上的 ACC 會顯示網路流量的摘要。Panorama 可動態地查詢網路上所有受管理防火牆的資料，並在應用程式監測中心中顯示這些資料。您可以利用此畫面，按橫跨整個 Palo Alto Networks 新世代防火牆網路的應用程式、使用者和內容活動（URL 類別、威脅、有效封鎖資料或檔案的安全原則）來監控流量。

應用程式層面可協助您立即識別網路上非預期或異常的行為。它包含一個圖表和報告陣列（摘要報告、變更監控器、威脅監控器、威脅地圖、網路監測、流量地圖），可讓您按威脅或應用程式，或依流量的來源或目的地來分析流量。您也可以按工作階段或位元組計數加以排序。

裝置群組和範本管理員僅能在其存取網域內比較裝置群組的網路和 *ACC* 資料。

請使用應用程式監測中心和應用程式層面回答問題，例如：

ACC	監控 > AppScope
• 網路上使用的前幾大應用程式為何，其中有多少高風險的應用程式？網路上使用高風險應用程式的前幾大使用者為何？ • 前一個小時檢視的前幾大 URL 類別為何？	• 應用程式的使用趨勢為何，即最常使用及逐漸不被採用的前五大應用程式各為何？ • 相較於上週或上個月，本週的使用者活動有哪些變化？
• 最耗用頻寬的前幾大應用程式為何？耗用最高頻寬的使用者/主機有哪些？ • 正在封鎖哪些內容或檔案，且是否有特定的使用者觸發此類檔案封鎖/資料篩選規則？ • 兩個特定 IP 位址之間交換的流量數量為何，或特定使用者產生的流量數量有多少？目的地伺服器或用戶端位於何處？	• 哪些使用者和應用程式耗用最多網路頻寬？且此類耗用量在前 30 天有哪些變化？ • 網路上有哪些威脅，且這些傳入和傳出流量威脅在地理上的散佈方式為何？

© 2019 Palo Alto Networks, Inc.

您接著可以使用資訊，對網路上的流量模式進行維護或強制變更。請參閱 使用案例：使用 Panorama 監控應用程式，瞭解當您塑造網路的可接受使用原則的結構時，Panorama 上的可見度工具能發揮哪些作用。

以下是協助您導覽應用程式監測中心的一些提示：

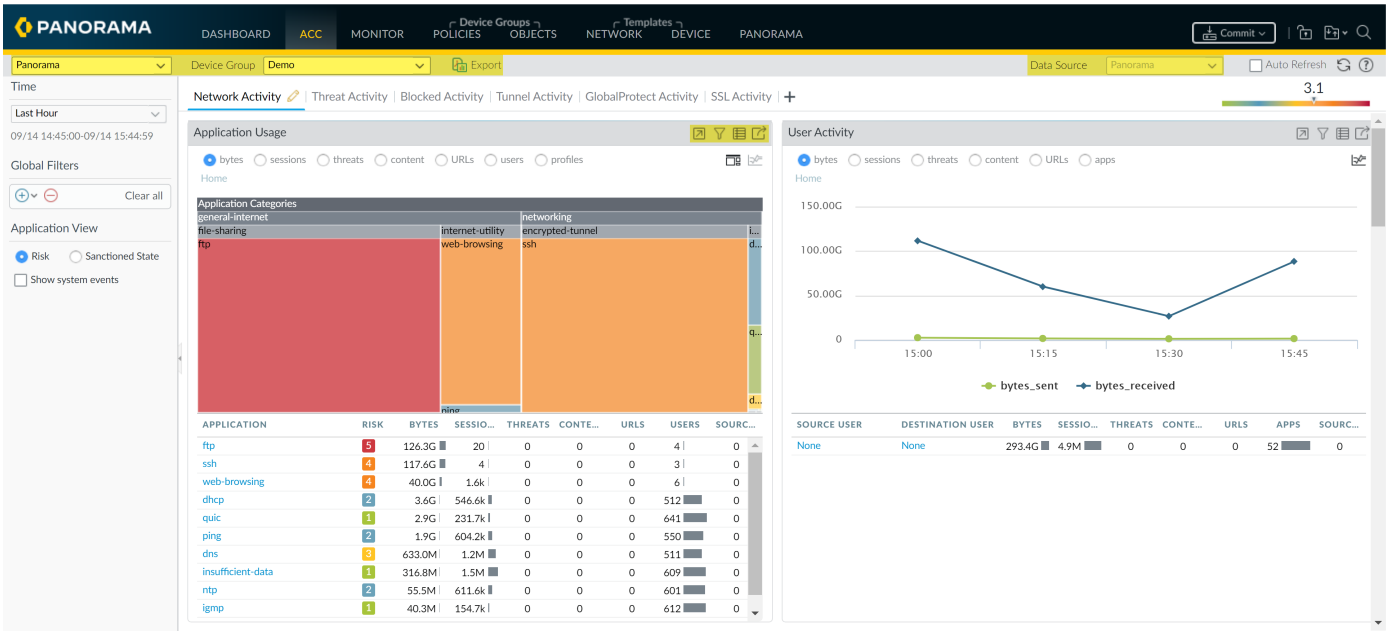


圖 24: ACC 導覽提示

- 從 **Panorama** 檢視切換至設備檢視——使用 **Context**（內容）下拉式清單存取任何受管理的防火牆 web 介面。如需詳細資料，請參閱內容切換—防火牆或 Panorama。
- 變更裝置群組和資料源——被用於顯示 ACC 內圖標上的統計資料預設 **Data Source**（資料源）是 **Panorama** 本機資料，且預設 **Device Group**（裝置群組）設定為 **All**（全部）。使用 Panorama 上的本機資料，為圖表提供快速的載入時間。但是，如果所有受管理的防火牆位於 PAN-OS 7.0 或更新版本上，您可以變更資料源至 **Remote Device Data**（遠端設備資料）。如果受管理的防火牆有 PAN-OS 7.0 和較低版本的混合，您僅可檢視 Panorama 資料。設定為使用遠端設備資料時，Panorama 將輪詢所有受管理防火牆並呈現資料的彙總檢視。螢幕上會指出正在輪詢的防火牆總數，以及已回應資訊查詢的防火牆數目。
- 選取頁籤和 **Widgets** 以檢視—ACC 包括三個頁籤和一個 Widgets 陣列，讓您可以尋找您關心的資訊。只有在防火牆上授權對應的功能，而且已啟用日誌記錄時，所有其他 widget 才會顯示資料（應用程式使用 widget 和主機資訊 widget 除外）。
- 調整時間範圍與資料—ACC 的報告時段範圍從前 15 分鐘，到前一小時、前一天、前一週、前一個月，或任何自行定義的時間。依預設，各 widget 顯示前 10 個項目，並將所有剩餘項目彙總為 **others**（其他）。您可以透過各種屬性在各 widget 中對資料排序—例如：工作階段、位元、威脅、內容和 URL。您也可以設定本機篩選器，篩選 widget 內表格和圖表的顯示內容，然後將 widget 篩選器作為全域篩選器在 ACC 內跨所有 widget 的檢視樞紐。

分析日誌資料

Panorama 上的 **Monitor**（監控）頁籤提供日誌資料的存取權；這些日誌是受管理防火牆已處理，並轉送至 Panorama 的工作階段封存清單。

日誌資料可廣泛地分組為兩種類型：您網路上流量的詳細資訊，例如應用程式、威脅、主機資訊設定檔、URL 類別、內容/檔案類型；以及記錄系統事件、設定變更和 User-ID™ 對應資訊。

根據受管理防火牆上的日誌轉送設定，**Monitor**（監控）> **Logs**（日誌）頁籤可能包含流量、威脅、URL 篩選、資料篩選、主機資訊設定檔 (HIP) 比對和 WildFire™ 提交的日誌。您可以藉著檢閱日誌，來確認特定工作階段或交易中的各種資訊。例如啟動工作階段的使用者、防火牆在工作階段上執行的動作（允許或拒

© 2019 Palo Alto Networks, Inc.

絕），以及來源與目的地連接埠、區域及位址等等。系統與設定日誌會指出設定異動，以及超過設定閾值時防火牆所觸發的警示。

如果 *Panorama* 要管理 *PAN-OS 7.0* 之前的防火牆執行軟體版，指定一個 *WildFire* 伺服器，從該伺服器中，*Panorama* 可以收集那些防火牆提交的 *WildFire* 樣本分析資訊。*Panorama* 使用該資訊完成 *WildFire* 提交日誌，該日誌是 *PAN-OS 7.0* 中引入的缺失欄位值。執行早期版本的防火牆不會填入這些欄位。若要指定伺服器，選取 *Panorama* > *Setup*（設定）> *WildFire*，編輯一般設定，然後輸入 *WildFire Server*（*WildFire* 伺服器）名稱。預設為 *wildfire-public-cloud*，這是位於美國的 *WildFire* 雲。

產生、排程及以電子郵件傳送報告

您可以將報告設定為立即執行，或排定在特定間隔時間執行。您可以儲存並匯出報告，或透過電子郵件傳送給特定收件者。如果您要將報告分享給無法存取 Panorama 的管理員，則寄送電子郵件特別有用。Panorama 與 Palo Alto Networks 防火牆支援相同的報告類型。

從 Panorama 10.0.2 和雲端服務外掛程式版本 1.8.0 開始，您可以產生有關 Cortex 資料湖資料的已排程報告。

在 *PAN-OS 10.0.3* 和更高版本中，此功能預設啟用。

為此，您必須先從 Panorama CLI 啟用此功能，方式為輸入

```
admin@Panorama> request plugins cloud_services logging-service sched-report-enable
```

常規提交不會啟用此變更。相反，您必須切換至設定模式：

```
admin@Panorama> configure
```

並輸入

```
admin@Panorama# commit force
```

然後，按照以下步驟產生已排程報告。

建議您為要產生報告的 *Panorama* 與防火牆安裝相同版本的軟體。例如，如果 *Panorama* 管理伺服器執行的是 *Panorama 10.0*，請先在其受管理的防火牆上安裝 *PAN-OS 10.0*，再產生報告。此作法可避免您建立的報告包含 *Panorama* 版本支援的欄位，但防火牆上舊版的 *PAN-OS* 不支援這些欄位時可能會發生的問題。

STEP 1 | 設定 Panorama 預先定義報告。

1. 選取 **Panorama** > **Setup**（設定）> **Management**（管理），然後編輯 **Logging and Reporting**（日誌記錄與報告）。
2. （選用）選取 **Log Export and Reporting**（日誌匯出和報告），然後啟用（核取）**Use Data for Pre-Defined Reports**（將資料用於預先定義報告），將每小時報告彙總卸載到日誌收集器。

   建議為 *VM-50*、*VM-50 Lite* 和 *PA-200* 防火牆啟用此設定。
3. 選取 **Pre-Defined Reports**（預先定義報告），然後啟用（核取）預先義報告以從 Panorama 進行推送。

© 2019 Palo Alto Networks, Inc.

4. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的設定變更。
5. （僅限 VM-50、VM-50 Lite 和 PA-200 防火牆）存取防火牆 CLI 以啟用預先定義報告..

   此命令必須在每個 VM-50、VM-50 Lite 和 PA-200 防火牆上執行。

```
admin> debug run-panorama-predefined-report yes
```

STEP 2 | 設定 Panorama 接收並儲存從防火牆收到的使用者和使用者群組資訊。

需要根據使用者名稱和群組（而非只根據 IP 位址）來產生報告。

1. 如果要讓 Panorama 在報告中包含使用者群組資訊，請將受管理的防火牆升級至 PAN-OS 8.1 或更新版本。Panorama 無法同步從執行更舊版本的防火牆送來的群組資訊。
2. 選取 **Panorama** > **Setup**（設定）> **Management**（管理），編輯 Panorama 設定，並 **Enable reporting and filtering on groups**（在群組中啟用報告和篩選）。
3. 新增裝置群組（如果尚未設定）。針對每個裝置群組：
   - 選取 **Master Device**（主要裝置），這是提供使用者和使用者群組資訊給 Panorama 的防火牆。
   - 讓 Panorama **Store users and groups from Master Device**（儲存來自主要裝置的使用者和群組）。

STEP 3 | 產生報告。

產生報告的步驟取決於類型。

- 自訂報告：
  1. 選取 **Monitor**（監控）> **Manage Custom Reports**（管理自訂報告），然後 **Add**（新增）報告。
  2. 輸入用來識別報告的 **Name**（名稱）。
  3. 選取用於產生報告的 **Database**（資料庫）。

     您可以使用 **Summary Databases**（摘要資料庫）或 **Detailed Logs**（詳細日誌）資料庫作為報告的基礎。

     若要以 Panorama 管理伺服器和日誌收集器上儲存的日誌為報告的基礎，請選取 **Panorama Data**（**Panorama** 資料）（建議使用以加快效能）。

     若要以受管理的防火牆上儲存的日誌為報告的基礎，請選取 **Remote Device Data**（遠端裝置資料）。此選項適用於防火牆可能有日誌尚未轉送至 Panorama 的情況。不過，因為 Panorama 必須直接查詢防火牆，此選項比較慢。
  4. 選取 **Scheduled**（排程）。
  5. 選取 **Time Frame**（時間範圍）、**Sort By**（排序依據）順序、**Group By**（分組依據）偏好設定，以及報告將顯示的欄（日誌屬性），以定義日誌篩選準則。

     必須選取 *Sort By*（排序依據）順序以產生準確報告。如果您沒有選取 *Sort By*（排序依據）順序，產生的自定義報告將使用與所選資料庫最近的日誌匹配進行填寫。
  6. （選用）使用 **Query Builder**（查詢產生器），以根據日誌屬性進一步調整日誌篩選準則。
  7. 若要測試報告設定，請選取 **Run Now**（立即執行）。如有必要，修改設定以變更報告顯示的資訊。
  8. 按一下 **OK**（確定）以儲存自訂報告。
- **PDF** 摘要報告：
  1. 選取 **Monitor**（監控）> **PDF Reports**（**PDF** 報告）> **Manage PDF Summary**（管理 **PDF** 摘要），然後新增報告。
  2. 輸入用來識別報告的 **Name**（名稱）。
  3. 使用每個報告群組的下拉式清單，並選取一或多個元素以設計 PDF 摘要報告。您可包含最多 18 個元件。

© 2019 Palo Alto Networks, Inc.

4. 按一下 **OK**（確定）以儲存設定。

STEP 4 | 設定 **Report Group**（報告群組）。

它可以包含預先定義的報告、PDF 摘要報告和自訂報告。Panorama 可將包含的所有包含的報告編譯至單一 PDF。

1. 選取 **Monitor**（監控）> **PDF Reports**（**PDF** 報告）> **Report Groups**（報告群組），然後 **Add**（新增）報告群組。
2. 輸入用來識別報告群組的 **Name**（名稱）。
3. （選用）選取 **Title Page**（標題頁面），並新增 PDF 輸出的 **Title**（標題）。
4. 在 Predefined Report（預先定義的報告）、Custom Report（自訂報告）和 PDF Summary Report（PDF 摘要報告）清單中選取報告。
5. 將選取的報告 **Add**（新增）至報告群組。
6. 按一下 **OK**（確定）以儲存設定。

STEP 5 | 設定電子郵件伺服器設定檔。

該設定檔定義防火牆如何連線至伺服器和傳送電子郵件。

1. 選取 **Panorama** > **Server Profiles**（伺服器設定檔）> **Email**（電子郵件），然後 **Add**（新增）伺服器設定檔。
2. 輸入用來識別設定檔的 **Name**（名稱）。
3. **Add**（新增）最多四個 SMTP 伺服器，並為每個伺服器 **Add**（新增）下列資訊：
   - **Name**（名稱）—用來識別 SMTP 伺服器的名稱（1 至 31 個字元）。此欄位只是標籤，不必成為現有伺服器的主機名稱。
   - **Email Display Name**（電子郵件顯示名稱）—顯示在電子郵件 From（寄件者）欄位的名稱。
   - **From**（從）—傳送通知電子郵件的電子郵件地址。
   - **To**（至）—傳送通知電子郵件的目標電子郵件地址。
   - **Additional Recipient**（其它收件人）—若要將通知傳送到第二個帳戶，請在此輸入其他地址。
   - **Email Gateway**（電子郵件閘道）——用來傳送電子郵件的 SMTP 閘道 IP 位址或主機名稱。
4. 按一下 **OK**（確定）來儲存設定檔。

STEP 6 | 排程以電子郵件傳遞報告。

1. 選取 **Monitor**（監控）> **PDF Reports**（**PDF** 報告）> **Email Scheduler**（電子郵件排程器），然後 **Add**（新增）電子郵件排程器設定檔。
2. 輸入用來識別設定檔的 **Name**（名稱）。
3. 針對報告，選取 **Report Group**（報告群組）、您剛建立的電子郵件伺服器設定檔（**Email Profile**（電子郵件設定檔）），以及 **Recurrence**（週期性）（預設值為 **Disable**（停用））。
4. **Send test email**（傳送測試電子郵件），以驗證電子郵件設定是否正確。
5. 按一下 **OK**（確定）儲存您的變更。
6. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

為排程報告設定金鑰限制

Panorama™ 管理伺服器和 PA-7000 系列防火牆報告利用來自一個或多個日誌收集器的金鑰（您可以對其進行彙總的唯一值）來構建和產生報告。為提高已排程報告的準確性，您現在可以配置最大和最小金鑰限制。透過增加支援的金鑰數，已排程報告現在可以包含更多能夠彙總、排序和分組的資料。

預設最小金鑰限制基於為已排程報告設定的 **Sort By**（排序依據）和 **Group By**（分組依據）值，計算方法如下：

<排序依據值> x 100 x <分組依據值>

© 2019 Palo Alto Networks, Inc.

例如，如果 **Sort By**（排序依據）設定為 **Top 25**（前 25 個），**Group By**（分組依據）設定為 **5 Groups**（5 個群組），則預設最小金鑰限制為 12,500 個金鑰。當 **Group By**（分組依據）值設定為 **None**（無）時，將不納入計算。預設最小金鑰限制受限於且不能超過最大金鑰限制。

您只能為 *M-Series* 設備和 *Panorama* 虛擬設備設定金鑰限制。*PA-7000* 系列金鑰限制不可設定。

以下 Panorama 型號增加了受支援的最大和最小金鑰限制：

Panorama 型號	最小金鑰限制	最大金鑰限制
PA-7000 系列	1,000 - 預設值，不可設定	25,000 - 預設值，不可設定
M-200	15,000	50,000
M-500	15,000	50,000
M-600	15,000	50,000
傳統模式的 Panorama 虛擬設備	5,000	25,000
Panorama 虛擬設備（所有受支援型號）	15,000	50,000

STEP 1 | 登入 Panorama CLI。

STEP 2 | 使用以下命令設定最大金鑰限制：

您可以將最大金鑰限制設定在 0 到 50 之間，其中 50 相當於 50,000 個金鑰。在此範例中，我們將 Panorama 虛擬設備的最大金鑰限制設定為 30,000 個金鑰。

```
admin@Panorama> request max-report-keys set limit <Key Limit>
```

```
admin@Panorama> request max-report-keys set limit 30

cfg.report.max-keys-limit: 30
```

STEP 3 | 使用以下命令設定最小金鑰限制：

您可以將最小金鑰限制設定在 0 到 15 之間，其中 15 相當於 15,000 個金鑰。在此範例中，我們將 Panorama 虛擬設備的最小金鑰限制設定為 15,000 個金鑰。

```
admin@Panorama> request min-report-keys set limit <Key Limit>
```

```
admin@Panorama> request min-report-keys set limit 15

cfg.report.min-keys-limit: 15
```

STEP 4 | （選用）將最小金鑰限制設定為預設設定。

```
admin@Panorama> request min-report-keys set limit 0
```

STEP 5 | 使用以下命令將新的最大和最小金鑰限制提交到 Panorama：

© 2019 Palo Alto Networks, Inc.

```
admin@Panorama> commit-all
```


© 2019 Palo Alto Networks, Inc.

在 Panorama 上擷取陷阱 ESM 日誌

可見性是防止和降低攻擊影響的關鍵第一步。為了協助您因應這項挑戰，Panorama 提供防火牆日誌（網路上的事件）和 Traps™ ESM Server 日誌（端點上的安全性事件）的綜合觀點，讓您追蹤任何可疑或惡意的活動。

對於網路和端點上觀察到的事件，為了察覺並追蹤其來龍去脈，請將 Traps 代理程式向 ESM Server 報告的安全性事件轉送至 Panorama。Panorama 可以充當 Syslog 接收端，利用 Syslog 並透過 TCP、UDP 或 SSL，從 Traps ESM 元件擷取這些日誌。然後，Panorama 就可以將端點和網路上不相關的安全性事件相互關聯起來，並產生比對證據。此證據讓您更充分瞭解事件的時序和流向，有利於調查問題並修正網路上的安全漏洞。

STEP 1 | 在 Panorama 上定義日誌擷取設定檔，並附加至收集器群組。



傳統模式的 *Panorama* 虛擬設備無法擷取 *Traps* 日誌。

1. 選取 **Panorama** > **Log Ingestion Profile**（日誌擷取設定檔），然後按一下 **Add**（新增）。
2. 輸入設定檔的 **Name**（名稱）。
3. 按一下 **Add**（新增），並輸入 ESM Server 的詳細資料。您最多可以對設定檔新增 4 個 ESM Server。
   1. 輸入 **Source Name**（來源名稱）。
   2. 指定 Panorama 將接聽 syslog 訊息的所在 **Port**（連接埠）。範圍是 23000 至 23999。
   3. 選取 **Transport**（傳輸）層通訊協定 - TCP、UDP 或 SSL。
   4. 選取 Traps_ESM 作為 **External Log type**（外部日誌類型）與您的陷阱 ESM **Version**（版本）。舉例來說，對陷阱 ESM 4.0 或 4.1，請選取 **3.4.1+**。

      隨著 Traps 日誌格式更新，更新的日誌定義將可透過 Panorama 上的內容更新取得。
4. 選取 **Panorama** > **Collector Groups**（收集器群組）> **Log Ingestion**（日誌擷取），並 **Add**（新增）日誌擷取設定檔，使得收集器群組可以從設定檔中列出的 ESM Server 接收日誌。

   如果您要啟用 SSL 以確保 Panorama 和 ESM Server 之間的安全 syslog 通訊，您必須將憑證附加至屬於收集器群組的受管理收集器（**Panorama** > **Managed Collectors**（受管理的收集器）> **General**（一般），並選取憑證作為 **Inbound Certificate for Secure Syslog**（安全 **Syslog** 的輸入憑證））。
5. **Commit**（認可）變更至 Panorama 和收集器群組。

STEP 2 | 在 ESM Server 上將 Panorama 設定為 Syslog 接收端。

陷阱 ESM 4.0 和更新版本支援日誌轉送至外部 syslog 接收端和 Panorama 兩者。因為較舊版本的陷阱 ESM 並不支援日誌轉送至多個 syslog 接收端，您必須在 **Syslog** 設定中將 Panorama 設定為 syslog 接收端（關於陷阱 ESM 3.4，請參閱允許日誌轉送至外部日誌記錄平台）。

對於陷阱 ESM 4.0 和更新版本：

1. 從 ESM 主控台選取 **Settings**（設定）> **ESM** > **Panorama**，然後 **Enable log forwarding to Panorama**（允許日誌轉送至 **Panorama**）。
2. 輸入 Panorama 主機名稱或 IP 位址作為 **Panorama Server**（**Panorama** 伺服器），以及 Panorama 接聽的 **Panorama Server Port**（**Panorama** 伺服器連接埠）。對選用的 **Panorama Failover Server**（**Panorama** 容錯伺服器）重覆此步驟。
3. 選取傳輸層**Communication Protocol**（通訊協定）：TCP、TCP with SSL（TCP 搭配 SSL）或 UDP。如果您選取 TCP with SSL（TCP 搭配 SSL），則 ESM Server 需要伺服器憑證才能啟用用戶端驗證。

   從 Panorama 中，您必須匯出 root CA 憑證作為「安全 Syslog 的輸入憑證」，再將憑證匯入主機（已安裝 ESM Server）的受信任根憑證庫。

© 2019 Palo Alto Networks, Inc.

STEP 3 | 檢視 ESM 日誌和關聯的事件。

1. 選取 **Monitor**（監控）> **External Logs**（外部記錄）> **Traps ESM** 以檢視擷取至 Panorama 的日誌。
2. 選取 **Monitor**（監控）> **Automated Correlation Engine**（自動化關聯引擎）> **Correlated Events**（關聯的事件），並篩選 **Wildfire and Traps ESM Correlated C2**（**Wildfire** 和 **Traps ESM** 關聯的 **C2**）關聯物件名稱，以尋找關聯的事件。當網路上的主機出現命令和控制活動，而且與 WildFire 虛擬環境中觀察到某個惡意檔案的行為相符時，Panorama 會產生關聯的事件。此關聯事件提醒您注意，Traps 代理程式和防火牆在網路上的一個或多個受感染的主機上已發現可疑活動。

© 2019 Palo Alto Networks, Inc.

使用案例：使用 Panorama 監控應用程式

此範例會引導您執行程序，評估您目前原則的效率，並判定是否需要調整原則來強化網路可接受的使用原則。

登入 Panorama 時，**Dashboard**（儀表板）上的 **Top Applications**（前幾名應用程式）Widget 會提供前一小時最常使用的應用程式。若要顯示該 Widget，可在工具列中選取 **Widgets** > **Application**（應用程式）> **Top Applications**（前幾名應用程式）。您可以瀏覽前幾大應用程式清單，並將滑鼠移到要檢閱其詳細資料的每一個應用程式區塊，或者選取 **ACC**（應用程式監測中心）頁籤，以檢視與排序清單相同的資訊。下列影像是 **Dashboard**（儀表板）上 **Top Applications**（前幾名應用程式）Widget 的檢視。

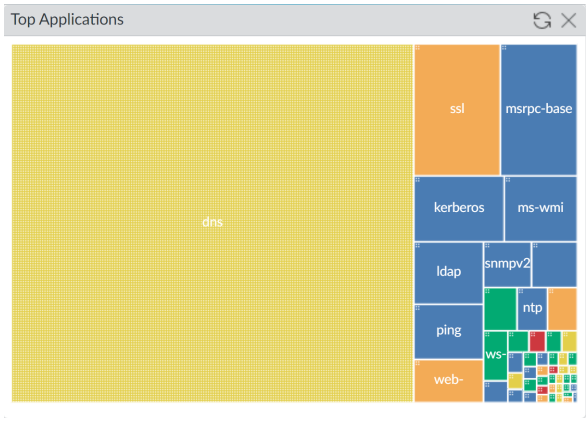


圖 26: 前幾名應用程式 Widget

此畫面的資料來源是應用程式統計資料資料庫；它並未使用流量日誌，且不論您是否啟用安全性規則的日誌記錄都會產生。此網路流量檢視描述該網路允許的所有內容，並且不會受已定義的任何原則規則封鎖而可自由流動。

在 **ACC**（應用程式監測中心）頁籤中，您可以選取 **Data Source**（資料來源）並將其切換成位於 **Panorama** 本機，或者查詢受管理防火牆（**Remote Device Data**（遠端設備資料））以找到資料；Panorama 將自動彙總與顯示資訊。若要加速流動，請考慮將 Panorama 做為資料來源（啟用至 Panorama 的日誌轉送），因為從受管理防火牆載入資料的時間，將隨著您選擇檢視資料的時段，以及網路上產生的流量數量而異。如果您受管理的防火牆綜合了 PAN-OS 7.0 和之前的版本，則 **Remote Device Data**（遠端設備資料）不可用。

圖 26: 前幾名應用程式 Widget中的 **Dashboard**（儀表板）範例顯示 DNS 為熱門應用程式。如果您按一下 DNS 應用程式區塊，Panorama 將開啟將 DNS 作為全域篩選器的 **ACC**（應用程式監測中心）> **Network Activity**（網路活動）頁籤，並顯示該應用程式的相關資訊、存取過該應用程式的使用者、風險等級的詳細資訊以及該應用程式的特性。

© 2019 Palo Alto Networks, Inc.

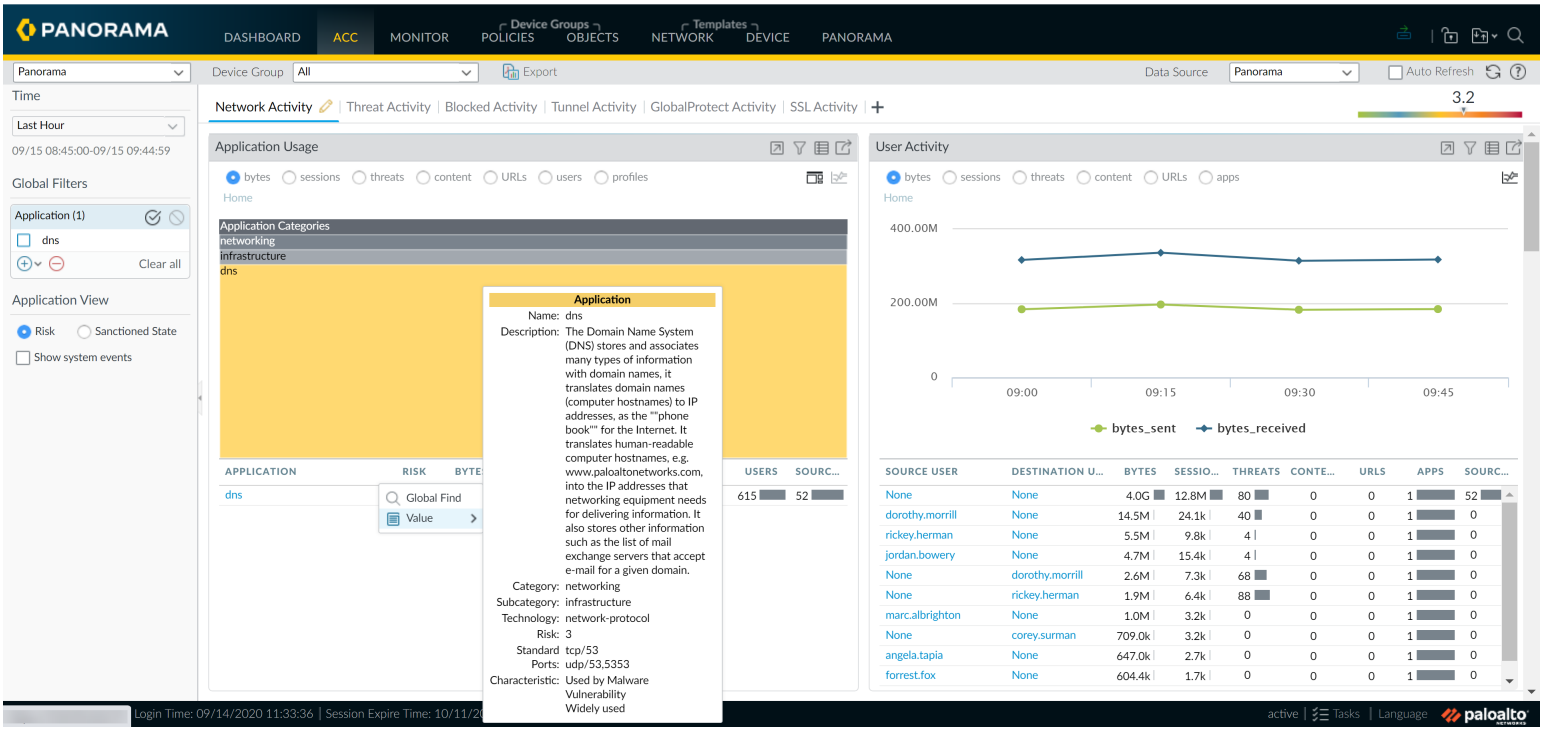


圖 27: 網路活動頁籤

在 **User Activity**（使用者活動）widget 中，您可以查看正在使用 DNS 的使用者數目，以及正在產生的流量數量。如果您已啟用使用者 ID，您將可以檢視產生此流量的使用者名稱，並深入檢閱與每位使用者相關聯的所有工作階段、內容或威脅。

在 **Threat Activity**（威脅活動）頁籤中，檢視 **Compromised Hosts**（受危害的主機）widget，以查閱相匹配的關聯物件，並檢視與使用者和應用程式相關聯的對比證據。您也可以檢視 **Threat Activity**（威脅活動）widget 中的威脅名稱、類別和 ID。

將 DNS 設為全域篩選器，使用 **Destination IP Activity**（目的地 **IP** 活動）和 **Destination Regions**（目的地區域）widget 以確認流量的目的地。您也可以檢視輸入和輸出區域以及允許此連線的安全規則。

如需更詳細的資訊，請進入流量日誌 的篩選檢視，並檢閱已使用的連接埠、傳送的封包，以及傳送和接收的位元組的每一個日誌項目。請根據您的需求，調整欄以檢視更多或更少資訊。

Monitor（監控）> **App-Scope** > **Traffic Map**（流量地圖）頁籤顯示流量的地圖，並且提供傳入與傳出流量的檢視。您也可以使用 **Monitor**（監控）> **App-Scope** > **Change Monitor**（變更監控器）頁籤來檢視流量模式的變化。例如，比較這個小時與上週或上個月所使用的前幾大應用程式，判斷是否能探索出模式或趨勢。

利用現在已發現的所有資訊，您可以評估應針對原則設定所做的變更。以下是需要考慮的某些建議：

- 嚴格地在 Panorama 上建立預先規則來封鎖或允許所有 DNS 流量。接著使用 Panorama 設備群組來建立此原則規則，並將該規則推送至一或多個防火牆。
- 強制執行頻寬使用限制及建立 QoS 設定檔和原則規則，解除非商業流量的優先順序排序。使用 Panorama 設備群組和範本以設定 QoS，然後推送規則至一道或多道防火牆。
- 排程自訂的報表群組，一起輪詢特定使用者的活動，及網路上使用的前幾大應用程式的活動，先觀察隔週或接下來兩週的走勢再採取行動。

除了檢查特定的應用程式外，您也可以在前幾大應用程式清單中檢查任何未知應用程式。這些是不符定義的 App-ID™ 簽章，並顯示為 unknown-udp 和 unknown-tcp 的應用程式。若要深入研究這些未知的應用程式，請按一下名稱來深入考察未分類流量的詳細資料。

© 2019 Palo Alto Networks, Inc.

使用相同的程序來調查啟動未知流量之主機的前幾大來源 IP 位址，以及建立工作階段之目的地主機的 IP 位址。若為未知流量，則在偵測到未知應用程式時，流量日誌預設會執行封包擷取 (pcap)。左欄中的綠色箭頭代表應用程式資料的封包擷取指令碼片段。在瀏覽器中按一下綠色箭頭以顯示 pcap。

擁有伺服器的 IP 位址（目的地 IP）、目的地連接埠及封包擷取，您便能更進一步地定位以識別應用程式，並且制定明智的決策，以便在網路上執行工作。例如，您可以建立自訂的應用程式來識別此流量，而非將它標示為未知 TCP 或 UDP 流量。請參閱識別未知應用程式一文以取得識別未知應用程式的詳細資訊，並參閱自訂應用程式簽章，取得開發自訂簽章以識別應用程式的詳細資訊。

© 2019 Palo Alto Networks, Inc.

使用案例：使用 Panorama 回應事件

網路威脅可能源自於不同的向量，包含因下載、網路釣魚攻擊、未修補的伺服器，以及隨機或目標式拒絕服務 (DoS) 攻擊所導致的惡意軟體和間諜軟體感染，從而執行一些攻擊行動。若要有效因應網路攻擊或感染，程序和系統需要向管理員發出攻擊警示，並提供必要的明確證據，追蹤用來發動攻擊的來源和方法。

Panorama 的優點是提供集中及整合的檢視，顯示跨網路的受管理防火牆所收集的模式和日誌。您可以單獨使用來自自動關聯引擎的資訊或與自安全性資訊事件管理員 (SIEM) 產生的報告和日誌搭配使用，來調查攻擊的觸發方式，以及瞭解如何防止進一步的攻擊及損害您的網路。

此使用案例探索下列問題：

- 系統如何向您通知事件？
- 如何確認事件不是誤報？
- 應立即採取哪些動作？
- 如何使用可用的資訊，重新建構觸發事件之前或之後所發生的事件順序？
- 在保護網路時，您需要考慮哪些變化？

此使用案例會追蹤特定的事件，並顯示 Panorama 上的可視性工具如何協助您回應報告。

- 事件通知
- 檢閱 ACC 內的 Widget
- 檢閱威脅日誌
- 檢閱 WildFire 日誌
- 檢閱資料篩選日誌
- 更新安全性規則

事件通知

依據您設定 Palo Alto Networks 防火牆的方式，以及使用於進一步分析的協力廠商工具，有數種方法可向您發出事件警示。您可能會收到電子郵件通知，它是由記錄到 Panorama 或系統日誌伺服器的日誌項目所觸發；或可能透過 SIEM 解決方案產生的特製化報告通知您；或者由協力廠商的付費服務或機構通知您。針對此範例，讓我們假設您收到來自 Panorama 的電子郵件通知。系統藉由比對間諜軟體簽章得出 Zero Access gent.Gen Command And Control Traffic（零存取 gent.Gen 命令與控制流量警示），利用電子郵件將該警示所觸發的事件通知您。電子郵件同時會列出工作階段的來源和目的地的 IP 位址、威脅 ID，以及記錄事件日誌時的時間戳記。

檢閱 ACC 內的 Widget

在 **ACC** > **Threat Activity**（威脅活動）頁籤中，檢查 **Compromised Hosts**（受危害的主機）widget 和 **Threat Activity**（威脅活動）widget 是否有任何關鍵性或高嚴重性威脅。在 **Compromised Hosts**（受危害的主機）widget 中，尋找相符的物件，然後按一下相符項目計數值，以檢視相關事件的相符證據。

檢閱威脅日誌

若要開始調查警示，請在 Panorama 上使用威脅 ID 來搜尋威脅日誌（**Monitor**（監控）> **Logs**（日誌）> **Threat**（威脅））。從威脅日誌中，您可以尋找受害者的 IP 位址，匯出封包擷取（PCAP，在日誌項目中按一下下載圖式 ），並使用網路分析器工具（例如 WireShark）來檢閱封包詳細資料。在 HTTP 案例中，在通訊協定、可疑的主機、URL 字串、使用者代理程式、IP 位址和連接埠中尋找格式錯誤或偽造的 HTTP REFERER，以便驗證事件。若要搜尋類似資料模式及建立自訂簽章或修改安全性原則，以便在未來更完善地解決威脅，則使用這些 pcaps 的資料也很有用。

執行此手動檢閱時，如果您對簽章有信心，請考慮將簽章從警示動作轉移至封鎖動作，以便採取更積極的方法。在某些情況下，您可能選擇將攻擊者 IP 新增至 IP 封鎖清單，防止該 IP 位址的後續流量進入內部網路。

© 2019 Palo Alto Networks, Inc.

如果您看到 *DNS* 式間諜軟體簽章，則您本機 *DNS* 伺服器的 *IP* 位址可能顯示為 *Victim Ip*（受害者 *IP*）位址。原因通常是防火牆位於本機 *DNS* 伺服器的北方，因此 *DNS* 查詢會將本機 *DNS* 伺服器顯示為來源 *IP*，而非顯示提出要求之用戶端的 *IP* 位址。

如果您看見這個問題，請在安全性規則的反間諜軟體設定檔中啟用 *DNS sinkholing* 動作，才能識別您網路上遭到感染的主機。*DNS sinkholing* 可讓您控制對惡意網域的輸出連線，並將 *DNS* 查詢重新導向至未使用的內部 *IP* 位址；*sinkhole* 不會發出回應。當受危害的主機啟動對惡意網域的連線時，而非連線至網際網路，防火牆會將要求導向至您定義的 *IP* 位址，這便遭到 *sinkhole* 攻擊。現在，檢查所有連線至 *sinkhole* 的主機其流量日誌，可讓找出所有受危害的主機，並採取補救措施防止擴散。

若要繼續調查事件，請使用攻擊者資訊及受害者 IP 位址來尋找更多資訊，例如：

- 攻擊者所在的地理位置為何？此 IP 位址是個別的 IP 位址或 NATed IP 位址？
- 此事件是因為使用者被誘騙至網站、下載，還是透過電子郵件附件傳送所導致？
- 此惡意軟體是否正在傳播？網路上是否有其他受危害的主機/端點？
- 它是否為零時差弱點？

每一個日誌項目的日誌詳細資料都會顯示事件的相關日誌。此資訊呈現您可以檢閱的流量、威脅、URL 篩選或其他日誌，並且相互關聯導致此事件的事件。例如，篩選流量日誌（**Monitor**（監控）> **Logs**（日誌）> **Traffic**（流量）），方法是將 IP 位址做為來源和目的地 IP，以全盤瞭解此受害者 IP 位址已建立連線的所有外部和內部主機/用戶端。

檢閱 WildFire 日誌

除了威脅日誌外，使用受害者 IP 位址來篩選 WildFire 提交日誌。WildFire 提交日誌包含上傳至 WildFire 服務進行分析的檔案資訊。由於間諜軟體一般會隱含自我內嵌，因此檢閱 WildFire 提交日誌能顯示受害者最近是否下載可疑的檔案。WildFire 明確報告可顯示取得的檔案或 .exe 所在的 URL 資訊，以及內容的行為。它會通知您檔案是否有惡意、它是否修改登錄機碼、讀取/寫入至檔案、已建立新檔案、已開啟網路通訊通道、已導致應用程式損毀、已產生大量程序、已下載檔案，或已出現其他惡意行為。使用此資訊來決定是否封鎖導致感染的應用程式（網頁瀏覽、SMTP、FTP）、制訂更嚴格的 URL 篩選規則，或限制部分應用程式/動作（例如，將檔案下載至特定的使用者群組）。

從 *Panorama* 存取 *WildFire* 日誌需要具備下列條件：*WildFire* 使用授權、附加至安全性規則的檔案封鎖設定檔，及轉送至 *Panorama* 的威脅日誌。

如果 *Panorama* 要管理 *PAN-OS 7.0* 之前的防火牆執行軟體版，指定一個 *WildFire* 伺服器，從該伺服器中，*Panorama* 可以收集那些防火牆提交的 *WildFire* 樣本分析資訊。*Panorama* 使用該資訊完成 *WildFire* 提交日誌，該日誌是 *PAN-OS 7.0* 中引入的缺失欄位值。執行早期版本的防火牆不會填入這些欄位。若要指定伺服器，選取 *Panorama* > *Setup*（設定）> *WildFire*，編輯一般設定，然後輸入 *WildFire Server Cloud*（*WildFire* 伺服器雲端）名稱。預設為 *wildfire-public-cloud*，這是位於美國的 *WildFire* 雲。

如果 WildFire 判斷檔案是惡意的，則會在 24 - 48 小時內建立新的防毒簽章，並提供給您使用。如果您擁有 WildFire 使用授權，則會在下一次更新 WildFire 簽章時的 30 - 60 分鐘內提供可用的簽章。當 Palo Alto Networks 新世代防火牆接收到它的簽章，如果您的設定是設為封鎖惡意軟體，則將立即封鎖檔案，威脅日誌也會立即顯示封鎖檔案的資訊。此程序經過嚴密的整合，可保護您免受此威脅攻擊，並阻止在您的網路上散佈惡意軟體。

檢閱資料篩選日誌

資料篩選日誌（**Monitor**（監控）> **Logs**（日誌）> **Data Filtering**（資料篩選））是調查惡意網路活動的另一個珍貴的來源。雖然您可以定期檢閱出現警示之所有檔案的日誌，但您也可以使用日誌，追蹤傳輸至受害者 IP 位址或使用者的檔案和資料，或從中傳輸的檔案和資料，並驗證流量的方向和流動：伺服器至用戶

© 2019 Palo Alto Networks, Inc.

端，或用戶端至伺服器。若要重新建立某個事件之前和之後所發生的事件，請篩選做為目的地的受害者 IP 位址的日誌，並檢閱網路活動的日誌。

由於 Panorama 會彙總所有受管理防火牆的資訊，因此它會呈現網路中所有活動的清晰概觀。您可以用來調查網路流量的部分其他視覺工具有 **Threat Map**（威脅地圖）、**Traffic Map**（流量地圖）和 **Threat Monitor**（威脅監控器）。威脅地圖和流量地圖（**Monitor**（監控）> **AppScope** > **Threat Map**（威脅地圖）或 **Traffic Map**（流量地圖））可讓您以視覺方式呈現傳入和傳出流量的區域。若要檢視可能來自於外部攻擊的異常活動，例如 DDoS 攻擊，則上述地圖特別有用。例如，如果您與東歐沒有許多業務交易，且地圖洩露該區域的異常流量等級，請按一下地圖的對應區域來啟動與檢視前幾大應用程式的應用程式監測中心資訊、工作階段計數上的流量詳細資料、已傳送和接收的位元組數、前幾大來源和目的地、使用者或 IP 位址，以及偵測到的威脅嚴重性（若有）。威脅監控器（**Monitor**（監控）> **AppScope** > **Threat Monitor**（威脅監控器））顯示網路上的前十大威脅，或網路上的前幾大攻擊者或前幾大受害者清單。

更新安全性規則

利用您現在已發現的所有資訊，您可以全盤瞭解威脅如何影響您的網路（攻擊的範圍、來源、受危害的主機、風險係數），並評估要追蹤的變更（若有）。以下是需要考慮的某些建議：

- 增強 DoS 保護設定檔以設定隨機早期丟棄，或丟棄 TCP Flood 的 SYN Cookie，以預先阻止 DDoS 攻擊。考量設定 ICMP 和 UDP 流量限制。根據您在記錄中注意到的趨勢與模式來評估您的可用選項，並使用 Panorama 範本實作變更。

  建立動態封鎖清單（**Objects**（物件）> **Dynamic Block Lists**（動態封鎖清單）），封鎖您已從數個智慧型來源發現的特定 IP 位址：您自己的威脅日誌分析、特定 IP 位址的 DDOS 攻擊，或協力廠商 IP 封鎖清單。

  清單必須是位於網頁伺服器上的文字檔。使用 Panorama 上的裝置群組，將物件推送到受管理防火牆，讓防火牆可以存取網頁伺服器，並以定義的頻率匯入清單。建立動態封鎖清單物件後，在來源和目的地欄位中，定義使用位址物件的安全性規則，以封鎖與定義的 IP 位址、範圍或子網路之間往來的流量。此方法可讓您在解決問題前封鎖入侵者，並進行更大規模的原則變更來保護網路的安全。
- 決定是否建立共用原則規則或裝置群組規則，封鎖導致感染的應用程式（網頁瀏覽、SMTP、FTP）、制訂更嚴格的 URL 篩選規則，或限制部分應用程式/動作，例如將檔案下載至特定的使用者群組。
- 在 Panorama 上，您也可以切換至防火牆內容並設定殭屍網路報告的防火牆，這些報告可識別網路上可能受殭屍網路感染的主機。

Panorama 高可用性

為了提供備援以防系統或網路失效，您可以在高可用性 (HA) 設定中部署兩個 Panorama™ 管理伺服器。Panorama 支援 HA 設定，其中，一個對等是主動-主要，另一個是被動-次要。如果主要對等失效，則會自動容錯移轉，而次要對等會變成主動。

> Panorama HA 先決條件
> HA 中 Panorama 上的優先順序與容錯移轉
> 故障復原觸發程序
> Panorama HA 中的日誌記錄注意事項
> Panorama HA 端點之間同步化
> 管理 Panorama HA 配對

Panorama HA 先決條件

若要設定 HA 中的 Panorama，您需要一對相同的 Panorama 伺服器，且每台伺服器必須符合下列需求：

- 相同的表格要素—對等體必須為相同型號和模式：兩者皆為 M-600 設備；M-500 設備；M-200 設備；在 AWS、Azure、GCP 及 ESXi 上處於 Panorama 模式、僅管理模式或傳統模式（僅限 ESXi 和 vCloud Air）的 Panorama 虛擬設備。日誌收集器模式的 Panorama 設備不支援 HA。
- 相同的 **Panorama** 作業系統版本——必須執行相同的 Panorama 版本，才能同步設定資訊及維持無縫故障復原的同位檢查。
- 相同的授權集—必須有相同的防火牆管理容量授權。
- （僅限 Panorama 虛擬設備）唯一序號—必須有唯一的序號；如果兩個 Panorama 實例的序號相同，則會處於暫停模式，直到您解決問題為止。

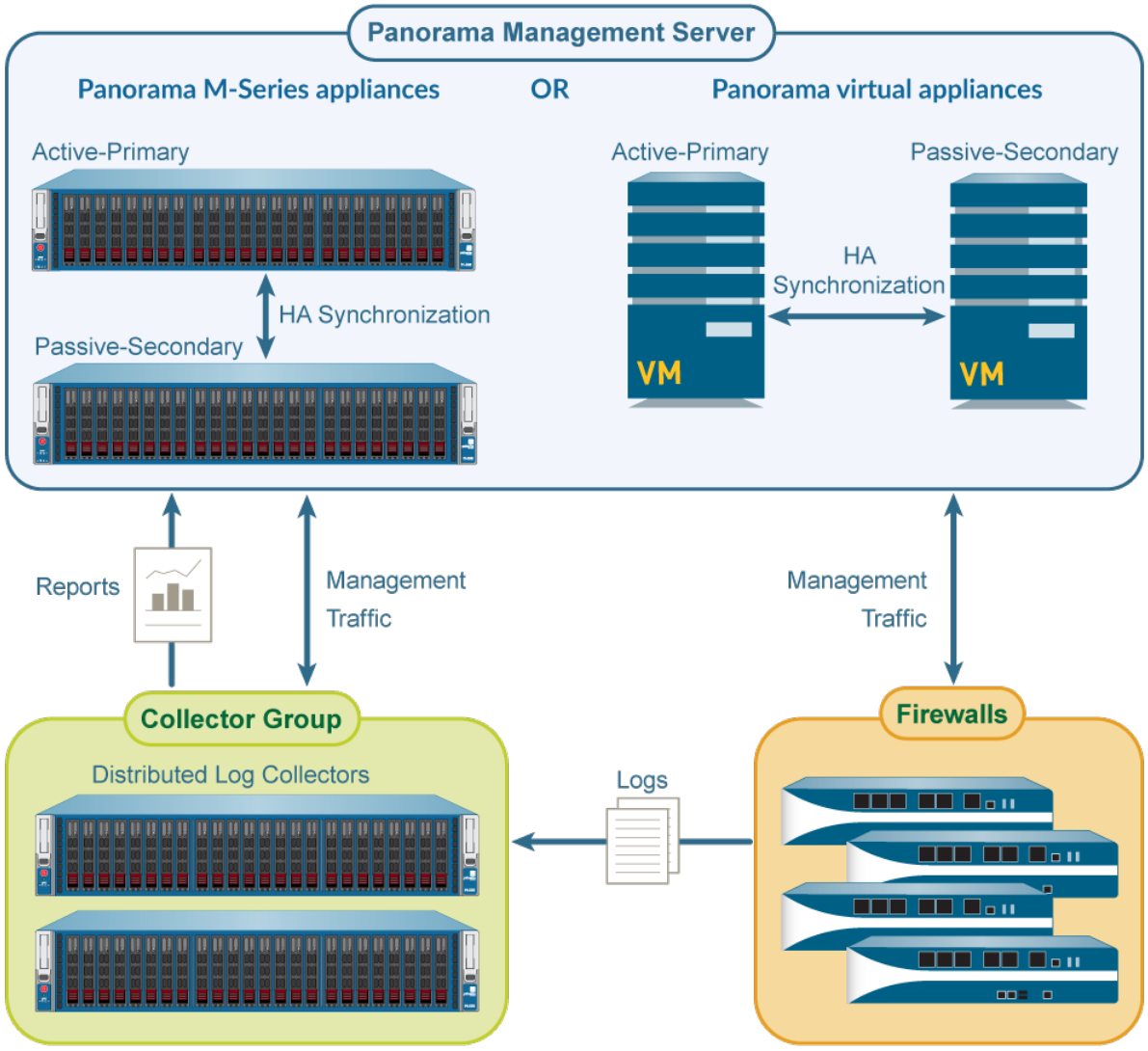


圖 28: Panorama HA 組織

HA 設定中的 Panorama 伺服器是對等，您可以使用任一個（主動或被動）來集中管理防火牆、日誌收集器，以及 WildFire 設備和設備叢集，只有少數例外（請參閱 Panorama HA 端點之間同步化）。HA 對等使用管理 (MGT) 連接埠來同步設定元素，這些元素推送至受管理的防火牆、日誌收集器，以及 WildFire 設備和設備叢集，以維護狀態資訊。Panorama HA 對等在地理上通常位於不同網站，因此，您需要確定指派給每

© 2019 Palo Alto Networks, Inc.

個對等的 MGT 介面 IP 位址，可透過您的網路而路由到達。HA 連線使用已啟用加密的 TCP 連接埠 28。如果加密未啟用，則會使用連接埠 28769 與 28260 進行 HA 連線，並同步處理 HA 端點間的設定。我們建議端點之間的延遲要少於 500ms。若要決定延遲，請在一般流量期間使用 Ping。

© 2019 Palo Alto Networks, Inc.

HA 中 Panorama 上的優先順序與容錯移轉

系統會將一個優先順序值指定給 HA 配對中的每一個 Panorama 端點。主要或次要端點的優先順序值可決定哪個端點有資格成為管理和日誌管理的主端點。設定為主要的端點將預設為主動狀態，次要則成為被動。主動端點可處理所有設定變更，並將變更推送至受管理防火牆；被動端點無法進行任何設定變更，也無法將設定推送至受管理防火牆。然而，任一端點皆可用來執行報告或執行日誌查詢。

被動端點已同步並準備好移轉至主動狀態，以因應主動 Panorama 發生路徑、連結、系統或網路失敗的狀況。

發生故障復原時，只會變更 Panorama 端點的狀態（主動或被動）；不會變更優先順序（主要和次要）。例如，當主要端點失敗時，其狀態將從主動主要變為被動主要。

除了兩個例外狀況外，主動次要狀態中的端點可執行所有功能：

- 該端點不能管理防火牆或日誌收集器部署功能，例如授權更新或軟體升級。
- 直到您將其優先順序手動變更為主要後，該端點才能將日誌記錄至 NFS。只有傳統模式的 Panorama 虛擬設備支援 NFS。

下表根據其狀態和優先順序設定列出 Panorama 的功能：

Capability	active-primary	passive-primary passive-secondary	active-secondary
Switch device context	■	■	■
Perform distributed reporting	■	■	■
Manage shared policy	■	■	■
Log to local disk	■	■ (Optional on the Panorama virtual appliance only)	■ (Optional on the Panorama virtual appliance only)
Log to an NFS partition (Panorama virtual appliance only)	■	■	■
Deploy software and licenses	■	■	■
Export Panorama configuration	■	■	■

圖 29: Panorama HA 功能

如需詳細資訊，請參閱 Panorama HA 先決條件 或 在 Panorama 上設定 HA。

© 2019 Palo Alto Networks, Inc.

故障復原觸發程序

主動 Panorama 發生故障時，被動 Panorama 隨即接管管理防火牆的工作，此事件稱之為故障復原。主動 Panorama 上的監控公制失敗時，就會觸發故障復原。此失敗會將主要 Panorama 上的狀態從主動主要移轉至被動主要，且次要 Panorama 將成為主動次要。

觸發容錯移轉的條件如下：

- Panorama 端點無法彼此通訊，且主動端點未回應健康和狀態輪詢；使用的公制是 HA 活動訊號輪詢與您好訊息。

  當 Panorama 端點無法彼此通訊時，主動端點可先監控端點是否仍與其連線，然後再觸發故障復原。這項檢查有助於避免故障復原，及造成兩個 Panorama 端點皆處於主動狀態的難題。
- 無法連線主動端點上指定的一或多個目的地（IP 位址）；使用的公制為 HA 路徑監控。

除了以上容錯移轉觸發程序外，管理員在放置暫停狀態的 Panorama 端點時或有先佔狀態時，也會發生容錯移轉。當主要 Panorama 從失敗（或使用者啟動的暫停）復原後，在恢復主動角色時習慣會使用先佔。依預設，系統會啟用先佔，且當主要 Panorama 從失敗復原並變為可用時，次要 Panorama 會交出控制權並返回被動狀態。發生先佔時，會在系統日誌中記錄事件。

若是將日誌記錄至 NFS 資料存放，請勿停用先佔，因為它允許主要端點（安裝至 NFS）恢復主動角色並寫入至 NFS 資料存放。若為其他所有部署，則只有當您想要確定特定的 Panorama 是慣用的主動端點時，才需要先佔。

HA 活動訊號輪詢與您好訊息

HA 端點使用您好訊息和活動訊號來驗證端點可回應及可操作。您好訊息會以設定的您好間隔在端點間傳送，以確認另一個端點的狀態。活動訊號是對 HA 端點的 ICMP ping，而該端點會回應 ping 以建立端點間的連線與回應。依預設，活動訊號的間隔為 1,000 毫秒，而問候訊息為 8,000 毫秒。

HA 路徑監控

路徑監控檢查網路連線和 IP 位址或 IP 位址群組的連結狀態（路徑群組）。主動端點使用 ICMP ping 來驗證可連線一或多個目的地 IP 位址。例如，您可以監控互連網路裝置（如路由器或交換器）的可用性、伺服器的連線，或流量中的其他部分重要裝置。請確定您為監控設定的節點/裝置不至於無法回應，特別是在承受負載時，因為這可能會造成路徑監控失敗並觸發故障復原。

預設 ping 間隔為 5,000 毫秒。連續三個 ping（預設）皆失敗時，則會將該 IP 位址視為無法連線，而當任何或所有監控的 IP 位址無法連線時，就會觸發端點故障。依預設，若其中任一 IP 位址變成無法連線，HA 狀態會移轉至非作用。

© 2019 Palo Alto Networks, Inc.

Panorama HA 中的日誌記錄注意事項

設定 HA 中的 Panorama 可提供日誌收集備援。由於受管理防火牆會透過 SSL 連線至兩個 Panorama 端點，因此當發生狀態變更時，每一個 Panorama 會將訊息傳送給受管理防火牆。系統會將 Panorama HA 狀態通知防火牆，防火牆可視情況轉送日誌。



依預設，受管理的防火牆在無法連線至 *Panorama* 時會緩衝日誌；恢復連線後，就會從前次離開的位置繼續傳送日誌。

硬體式 Panorama 及 Panorama 虛擬設備上的日誌記錄選項不同：

- 傳統模式 Panorama 虛擬設備上的日誌記錄容錯移轉
- M-Series 設備或 Panorama 模式 Panorama 虛擬設備上的日誌記錄容錯移轉

傳統模式 Panorama 虛擬設備上的日誌記錄容錯移轉

傳統模式的 Panorama 虛擬設備提供下列日誌容錯移轉選項：

日誌儲存類型	說明
虛擬磁碟	依預設，受管理防火牆會將日誌做為獨立的串流傳送給每一個 Panorama HA 端點。依預設，如果端點變成無法使用，受管理防火牆將緩衝日誌，並且在端點重新連線時，從離開的位置繼續傳送日誌（受限於磁碟儲存容量和中斷連線的持續時間）。 日誌儲存容量上限取決於虛擬平台（VMware ESXi 或 vCloud Air）；如需詳細資訊，請參閱 Panorama 型號。  您可以選擇是否只將日誌轉送至主動對等（請參閱 修改日誌轉送及緩衝預設值）。然而，*Panorama* 不支援跨 *HA* 配對的日誌彙總。因此，如果您將日誌記錄至虛擬磁碟，若要監控和報告，您必須查詢從受管理防火牆收集日誌的 *Panorama* 對等。
網路檔案系統 (NFS)	您只能將 NFS 儲存空間掛載至 VMware ESXi 伺服器上執行的 Panorama 虛擬設備。只有主動-主要 Panorama 會掛載至 NFS 式日誌分割區，並且可接收日誌。在故障復原時，主要裝置會進入被動主要狀態。在此案例中，主動次要 Panorama 會在發生先佔前管理防火牆，但不會接收日誌，也不會寫入 NFS 中。若要允許主動次要端點將日誌記錄至 NFS，您必須將它手動切換至主要，以便將其安裝至 NFS 分割區。如需指示，請參閱 Panorama 故障復原後切換優先順序以恢復 NFS 日誌記錄。

M-Series 設備或 Panorama 模式 Panorama 虛擬設備上的日誌記錄容錯移轉

如果您將防火牆日誌轉送至 Panorama 模式 M-600 設備、M-500 設備、M-200 設備或 Panorama 虛擬設備的 HA 配對上的本機日誌收集器，當您設定收集器群組時，您可以指定哪些防火牆將日誌傳送至哪些日誌收集器。您可以為每個 Panorama 對等的日誌收集器，設定個別的收集器群組，或設定單一收集器群組，以包含兩個對等的日誌收集器。在包含兩個本機日誌收集器的收集器群組中，日誌轉送偏好設定清單決定哪個日誌收集器從防火牆接收日誌。若為 PA-7000 Series 和 PA-5200 Series 防火牆，您可以選擇將日誌傳送至收集器群組中的所有日誌收集器，在此情況下，Panorama 會採用循環負載平衡，隨時選擇由哪個日誌收集器接收日誌。

© 2019 Palo Alto Networks, Inc.

在包含兩個日誌收集器的收集器群組中，您還可以啟用備援，讓每個日誌都有兩個複本，而每個複本位於不同的日誌收集器。如果任何日誌收集器變成無法使用，此備援可確保不會遺失任何日誌：您可以看到所有轉送至收集器群組的日誌，並針對所有日誌資訊執行報告。只有當收集器群組內的每一個日誌收集器都具有相同數量的磁碟時，日誌備援才可用。



任何特定收集器群組的所有日誌收集器都必須是相同型號：全部是 *M-200* 設備、全部是 *M-500* 設備、全部是 *M-600* 設備，或全部是 *Panorama* 虛擬設備（*Panorama* 模式）。

由於啟用備援會建立更多日誌，因此此設定需要更多儲存容量。由於每個日誌收集器都必須散佈每個接收的日誌複本，因此啟用備援會讓收集器群組中的日誌處理流量加倍，並讓最大日誌記錄速率減半。（收集器群組空間用盡時，其會刪除較舊的日誌。）

© 2019 Palo Alto Networks, Inc.

Panorama HA 端點之間同步化

每當您在主動 Panorama 端點上提交變更時，Panorama HA 端點就會同步執行中的設定。每當您在主動端點上儲存設定，或只是在發生故障復原前儲存設定，就會在端點之間同步候選設定。

會在 Panorama HA 端點之間同步跨對等的共同設定，例如共用物件和原則規則、裝置群組物件和規則、範本組態、憑證和 SSL/TLS 服務設定檔及管理存取設定。

當您 啟用自動提交復原 時，HA 同步僅發生在從 Panorama 推送之後成功測試本身與 Panorama 之間的連線之後。

只有每個端點的唯一設定才不會同步，例如下列設定：

- Panorama HA 組態—優先順序設定、端點 IP 位址、路徑監控群組和 IP 位址
- Panorama 組態—管理介面 IP 位址、FQDN 設定、登入橫幅、NTP 伺服器、時區、地理位置、DNS 伺服器、可存取 Panorama 的許可 IP 位址、SNMP 系統設定，以及動態內容更新排程
- 排程設定匯出
- 用於記錄日誌的 NFS 分割區設定及所有磁碟配額配置。這僅適用於 VMware ESXi 伺服器上執行的傳統模式 Panorama 虛擬設備。
- Panorama 本機儲存空間 (SSD) 上不同類型的日誌和資料庫的磁碟配額配置



如果您使用主要金鑰來加密 *Panorama* 上的私人金鑰與憑證，則必須在兩個 *HA* 端點上使用相同的主要金鑰。如果主要金鑰不同，*Panorama* 無法同步 *HA* 端點。

如需詳細資訊，請參閱 Panorama HA 先決條件 或 在 Panorama 上設定 HA。

© 2019 Palo Alto Networks, Inc.

管理 Panorama HA 配對

- 在 Panorama 上設定 HA
- 設定在 HA 對等之間使用自訂憑證進行驗證
- 測試 Panorama HA 故障復原
- Panorama 故障復原後切換優先順序以恢復 NFS 日誌記錄
- 將主要 Panorama 還原至主動狀態

若要安裝軟體或內容更新，請參閱 在 HA 組態中為 Panorama 安裝更新。

在 Panorama 上設定 HA

請先檢閱 Panorama HA 先決條件，再執行下列步驟：

STEP 1 | 在 HA 端點上設定 MGT 連接埠之間的連線。

Panorama 端點可使用 MGT 連接埠彼此通訊。確定您指定給 HA 配對中 Panorama 伺服器的 MGT 連接埠是可路由的 IP 位址，且端點可跨網路彼此通訊。若要設定 MGT 連接埠，請參閱 執行 Panorama 虛擬設備的初始設定 或 執行 M-Series 設備的初始設定。

在配對中挑選 **Panorama** 端點並完成剩下的工作。

STEP 2 | 啟用 HA 及（選用）啟用 HA 連線的加密。

1. 選取 **Panorama** > **High Availability**（高可用性），然後編輯 **Setup**（設定）部分。
2. 選取 **Enable HA**（啟用 **HA**）。
3. 在 **Peer HA IP Address**（端點 **HA IP** 位址）欄位中，輸入指派給端點設備的 IP 位址。
4. 在 **Peer HA Serial**（**HA** 對等序號）欄位，輸入對等 Panorama 的序號。

   輸入 Panorama HA 對等序號，以減少對 Panorama IP 進行暴力密碼破解的攻擊面。
5. 在 **Monitor Hold Time**（監控保留時間）欄位中，以毫秒為單位輸入系統在由於控制連結失敗而採取動作之前將會等待的時間（範圍為 1000-60000，預設值為 3000）。
6. 如果您不要加密，請清除 **Encryption Enabled**（加密已啟用）核取方塊，然後按一下 **OK**（確定）：不需要其他的步驟。如果您要加密，請選取 **Encryption Enabled**（加密已啟用）核取方塊，然後按一下 **OK**（確定），並執行下列工作：
   1. 選取 **Panorama** > **Certificate Management**（憑證管理） > **Certificates**（憑證）。
   2. 選取匯出 **Export HA key**（匯出 **HA** 金鑰）。將 HA 金鑰儲存至端點 Panorama 可存取的網路位置。
   3. 在端點 Panorama 上，導覽至 **Panorama** > **Certificate Management**（憑證管理） > **Certificates**（憑證），選取 **Import HA key**（匯入 **HA** 金鑰），瀏覽到金鑰儲存的位置，然後匯入金鑰。

STEP 3 | 設定 HA 優先順序。

1. 在 **Panorama** > **High Availability**（高可用性）中，編輯 **Election Settings**（選取設定）部分。
2. 將 **Device Priority**（設備優先順序）定義為 **Primary**（主要）或 **Secondary**（次要）。確定將一個端點設為主要，並將另一個端點設為次要。

   如果兩個端點具有相同的優先順序設定，則會將序號較高的端點置於暫停狀態。
3. 定義 **Preemptive**（先佔）行為。預設會啟用先佔。兩個端點上的先佔選項（已啟用或已停用）必須相同。

© 2019 Palo Alto Networks, Inc.

如果使用 *NFS* 執行日誌記錄，並且已停用先佔，則若要繼續將日誌記錄至 *NFS*，請參閱 Panorama 故障復原後切換優先順序以恢復 NFS 日誌記錄。

STEP 4 | 若要設定路徑監控，請定義一或多個路徑群組。

路徑群組會列出目的地 IP 位址（節點），Panorama 必須 ping 該 IP 位址才能驗證網路連線。

為每個包含所要監控節點的路徑群組執行下列步驟。

1. 選取 **Panorama** > **High Availability**（高可用性），然後在 Path Group（路徑群組）部分中按一下 **Add**（新增）。
2. 輸入路徑群組的 **Name**（名稱）。
3. 選取此群組的 **Failure Condition**（失敗條件）：
   - **any**（任一），此條件會在有任何一個 IP 位址無法連線時觸發路徑監控失敗。
   - **all**（所有），此條件只會在全部的 IP 位址皆無法連線時才觸發路徑監控失敗。
4. **Add**（新增）您想要監控的各目的地 IP 位址。
5. 按一下 **OK**（確定）。Path Group（路徑群組）部分會顯示新群組。

STEP 5 | （選用）在 Panorama 上選取路徑監控的失敗條件。

1. 選取 **Panorama** > **High Availability**（高可用性），然後編輯 Path Monitoring（路徑監控）部分。
2. 選取 **Failure Condition**（失敗條件）：
   - **all**（所有），此條件只會在所有監控的路徑群組皆失敗時才會觸發故障復原。
   - **any**（任一），此條件會在監控的任一路徑群組失敗時觸發故障復原。
3. 按一下 **OK**（確定）。

STEP 6 | 提交組態變更。

選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

STEP 7 | 設定其他 Panorama 端點。

在 HA 配對的另一個對等上，重複步驟 2 至步驟 6。

STEP 8 | 同步 Panorama 對等。

1. 存取主動 Panorama 上的 **Dashboard**（儀表板），並選取 **Widgets** > **System**（系統）> **High Availability**（高可用性）來顯示 HA Widget。
2. **Sync to peer**（同步至對等），按一下 **Yes**（是），等待 **Running Config**（執行中設定）顯示 **Synchronized**（已同步）。
3. 存取被動 Panorama 上的 **Dashboard**（儀表板），並選取 **Widgets** > **System**（系統）> **High Availability**（高可用性）來顯示 HA Widget。
4. 確認 **Running Config**（執行中設定）顯示 **Synchronized**（已同步）。

設定在 HA 對等之間使用自訂憑證進行驗證

您可以使用自訂憑證進行驗證以保證 Panorama 端點間的 HA 連線。

STEP 1 | 在 Panorama 上產生憑證授權單位 CA 憑證。

1. 選取 **Panorama** > **Certificate Management**（憑證管理）> **Certificates**（憑證）。
2. 建立自我簽署根 CA 憑證或從企業 CA 匯入憑證。

STEP 2 | 設定包含 root CA 和中繼 CA 的憑證設定檔。

1. 選取 **Panorama** > **Certificates Management**（憑證管理）> **Certificate Profile**（憑證設定檔）。

© 2019 Palo Alto Networks, Inc.

2. 設定憑證設定檔。

STEP 3 | 設定 SSL/TLS 服務設定檔。

1. 選取 **Panorama** > **Certificate Management**（憑證管理）> **SSL/TLS Service Profile**（**SSL/TLS** 服務設定檔）。
2. 設定 SSL/TLS 設定檔，以定義憑證和通訊協定供 Panorama 及其受管理的裝置用於 SSL/TLS 服務。

STEP 4 | 在 Panorama 上設定安全伺服器通訊。

1. 選取 **Panorama** > **Setup**（設定）> **Management**（管理），再 **Edit**（編輯）[Panorama 設定]。
2. 確認未選取 **Custom Certificate Only**（僅限自訂憑證）核取方塊。這樣可讓您在移轉至自訂憑證期間繼續管理所有裝置。

   選取 *Custom Certificate Only*（僅限自訂憑證）核取方塊時，*Panorama* 不會使用預先定義的憑證來驗證裝置，也無法使用這種憑證來管理裝置。
3. 從 **SSL/TLS Service Profile**（**SSL/TLS** 服務設定檔）下拉式清單中，選取 SSL/TLS 服務設定檔。此 SSL/TLS 服務設定檔會套用至 Panorama、防火牆、日誌收集器和 Panorama HA 對等之間的所有 SSL 連線。
4. 從 **Certificate Profile**（憑證設定檔）下拉式清單中，選取憑證設定檔。
5. （選用）設定授權清單。
   1. 按一下 Authorization List（授權清單）下的 **Add**（新增）。
   2. 選取 **Subject**（主體）或 **Subject Alt Name**（主體別名）作為識別項類型。
   3. 輸入通用名稱
6. 在 **Disconnect Wait Time (min)**（中斷連線等候時間（分鐘））中，輸入 Panorama 在中斷並重新建立與受管理裝置間的連線之前應該等候的時間量。依預設，此欄位是空白，範圍是 0 至 44,640 分鐘。

   直到您提交新設定，中斷連線等候時間才會開始倒數計時。

1. 按一下 **OK**（確定）。
2. **Commit**（提交）您的變更。

STEP 5 | 將用戶端 Panorama 升級至 8.1。

升級 Panorama。

STEP 6 | 設定安全用戶端通訊。

1. 選取 **Panorama** > **High Availability**（高可用性），然後 **Edit**（編輯）HA 設定。
2. 選取 **Certificate**（憑證）和 **Certificate Profile**（憑證設定檔）。
3. 按一下 **OK**（確定）。
4. **Commit**（提交）您的變更。

測試 Panorama HA 故障復原

若要測試 HA 設定是否正常運作，可觸發手動故障復原，並確認端點已成功移轉狀態。

STEP 1 | 登入主動 Panorama 端點。

您可以在網頁介面的右下角驗證 Panorama 伺服器的狀態。

STEP 2 | 暫停主動 Panorama 端點。

選取 **Panorama** > **High Availability**（高可用性），然後在 Operational Commands（操作命令）部分中按一下 **Suspend local Panorama**（暫停本機 **Panorama**）連結。

© 2019 Palo Alto Networks, Inc.

STEP 3 | 確認被動 Panorama 端點已經以主動身分接管。

在 Panorama **Dashboard**（儀表板）上，**High Availability**（高可用性） Widget 中，確認 **Local**（本機）被動伺服器的狀態為 **active**（主動），**Peer**（端點）的狀態為 **suspended**（暫停）。

STEP 4 | 將暫停的端點還原為作用狀態。如果已啟用先佔，請等候幾分鐘後，再確認先佔結果。

在先前暫停的 Panorama 上：

1. 選取 **Panorama** > **High Availability**（高可用性），然後在 Operational Commands（操作命令）部分中，按一下 **Make local Panorama functional**（讓本機 **Panorama** 運作）。
2. 在 **Dashboard**（儀表板）的 **High Availability**（高可用性）Widget 中，確認（本機）Panorama 已經作為主動端點接管，且另一個端點目前為被動狀態。

Panorama 故障復原後切換優先順序以恢復 NFS 日誌記錄

ESXi 伺服器上執行的傳統模式 Panorama 虛擬設備可以使用 NFS 資料存放來記錄日誌。在 HA 設定下，只有主要 Panorama 端點會被掛載到基於 NFS 的日誌分割區並可寫入 NFS。發生故障復原，且被動 Panorama 成為主動時，其狀態變為主動-次要。雖然次要 Panorama 端點可主動管理防火牆，但它無法接收日誌或寫入 NFS，因為該端點沒有 NFS 分割區。當防火牆無法向主要 Panorama 端點轉送日誌時，每個防火牆都會將日誌寫入本機磁碟。防火牆會針對轉送至 Panorama 的最後一組日誌項目維護一個指標，如此當被動主要 Panorama 再次變為可用時，它們即可將日誌繼續轉送至其中。

請使用本節的指示，在主動次要 Panorama 端點上手動切換優先順序，使其開始將日誌記錄至 NFS 分割區。以下是可能需要觸發此變更的一般案例：

- 先佔已停用。依預設，會在 Panorama 上啟用先佔，且當主要端點再次變為可用時將恢復成主動。停用先佔時，您需要將次要對等上的優先順序切換成主要，它才能安裝 NFS 分割區、從受管理的防火牆接收日誌，以及寫入 NFS 分割區。
- 主動 Panorama 失敗，且無法在短期內從失敗中復原。如果未切換優先順序，則在達到防火牆上的日誌儲存容量上限時將覆寫最舊的日誌，讓它繼續將日誌記錄至其本機磁碟。這種情況可能導致日誌遺失。

STEP 1 | 登入至目前的被動主動 Panorama，選取 **Panorama** > **Setup**（設定） > **Operations**（操作），然後在 [設備操作] 部分中，按一下 **Shutdown Panorama**（關閉 **Panorama**）。

STEP 2 | 登入主動次要 Panorama，選取 **Panorama** > **High Availability**（高可用性），編輯 Election Settings（選取設定），然後將 **Priority**（優先順序） 設為 **Primary**（主要）。

STEP 3 | 按一下 **OK**（確定）儲存您的變更。

STEP 4 | 選取 **Commit**（提交） > **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

出現提示時不要重新啟動。

STEP 5 | 登入 Panorama CLI，然後輸入下列命令，將 NFS 分割區的擁有權變更為此端點：**`request high-availability convert-to-primary`**

STEP 6 | 選取 **Panorama** > **Setup**（設定） > **Operations**（操作），然後在 Device Operations（裝置操作）部分中，按一下 **Reboot Panorama**（重新啟動 **Panorama**）。

STEP 7 | 將您在步驟 1 關閉的 Panorama 對等開啟電源。此端點現在將處於被動次要狀態。

© 2019 Palo Alto Networks, Inc.

將主要 Panorama 還原至主動狀態

依預設，Panorama 上的先佔功能可在主要 Panorama 變為可用時，立即讓它以主動端點身分繼續運作。然而，如果已停用先佔，則在從失敗、非作用或暫停狀態復原後，若要強制主要 Panorama 變為主動，唯一的方法是暫停次要 Panorama 端點。

在主動次要 Panorama 進入暫停狀態前，它會將候選設定移轉至被動 Panorama，以便儲存所有未提交的設定變更，並允許在另一個端點上存取。

STEP 1 | 暫停 Panorama。

1. 登入您要在暫停狀態中放置的 Panorama 端點。
2. 選取 **Panorama** > **High Availability**（高可用性），然後在 [操作命令] 部分中按一下 **Suspend local Panorama**（暫停本機 Panorama）連結。

STEP 2 | 確認狀態顯示了已按照使用者的要求暫停 Panorama。

在 **Dashboard**（儀表板）的 **High Availability**（高可用性） Widget 上，確認 **Local**（本機）狀態顯示為 **suspended**（暫停）。

當您暫停端點，且另一個 Panorama 以主動端點身分接管時，將觸發故障復原。

STEP 3 | 將暫停的 Panorama 還原為作用狀態。

1. 在 **Panorama** > **High Availability**（高可用性） 頁籤中，在 Operational Commands（操作命令）部分中按一下 **Make local Panorama functional**（讓本機 **Panorama** 運作） 連結。
2. 在 **Dashboard**（儀表板）的 **High Availability**（高可用性）Widget 中，確認 Panorama 已移轉至主動或被動狀態。

© 2019 Palo Alto Networks, Inc.

管理 *Panorama*

本節說明如何管理與維護 Panorama™ 管理伺服器。本節包含以下主題：

- 預覽、驗證或提交組態變更
- 啟用自動提交復原
- 管理 Panorama 和防火牆組態備份
- 比較 Panorama 組態中的變更
- 管理限制組態變更的鎖定
- 將自訂標誌新增至 Panorama
- 使用 Panorama 工作管理員
- 管理日誌和報告儲存配額和到期日期
- 監控 Panorama
- 重新啟動或關閉 Panorama
- 設定 Panorama 密碼設定檔及複雜性

如需完成初始設定的指示，包含定義網路存取設定、授權、升級 Panorama 軟體版本，及設定管理存取 Panorama，請參閱 設定 Panorama。

預覽、驗證或提交組態變更

對於 Panorama 組態的擱置中變更，您可以執行 Panorama 認可、驗證和預覽操作，然後將這些變更推送至 Panorama 所管理的裝置，包括防火牆、日誌收集器，以及 WildFire 設備和設備叢集。您可依管理員或位置篩選擱置中變更，然後只提交、推送、驗證或預覽這些變更。位置可能是特定裝置群組、範本、收集器群組、日誌收集器、共用設定或 Panorama 管理伺服器。

因為 Panorama 會推送其執行中的設定，您必須先將變更提交至 Panorama，才能將變更推送至裝置。如果變更尚未準備好在裝置上生效，您可以選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），將變更提交至 Panorama，而不要推送至裝置。稍後，當變更已準備好在裝置上生效時，您可以選取 **Commit**（提交）> **Push to Devices**（推送至裝置）。如果變更已準備好在 Panorama 和裝置上生效，請選取 **Commit**（提交）> **Commit and Push**（提交並推送），如下列程序所述。

STEP 1 | 設定您要提交、驗證或預覽的組態變更范圍。

1. 按一下 Web 介面上方的 **Commit**（交付）。
2. 選取下列其中一個選項：
   - **Commit All Changes**（交付所有變更）（預設）—對您擁有管理員權限的所有變更套用提交。選取此選項後，您無法手動篩選提交范圍。而指派給您用於登入之帳戶的管理員角色將決定提交範圍。
   - **Commit Changes Made By**（交付以下所做的變更）—允許您按管理員或位置篩選提交范圍。指派給您用來登入之帳戶的管理員角色，將決定您可以篩選的變更。

   若要提交其他管理員的變更，您用于登入的帳戶必須被指派超級使用者角色或管理員角色設定檔（其中*Commit For Other Admins*（為其他管理員提交）權限已啟用）。
3. （選用）若要按管理員篩選提交范圍，則選取 **Commit Changes Made By**（提交以下所做的變更），按一下旁邊的連結，選取管理員，然後按一下 **OK**（確定）。
4. （選用）若要按位置篩選，**Commit Changes Made By**（提交以下所做的變更），清除任何您要從提交范圍中排除的變更。

   如果包含與排除的組態變更之間的相依性導致驗證錯誤，請對所有包含的變更執行提交。例如，當您將變更提交至裝置群組時，必須包含對該裝置群組中的相同規則庫新增、刪除或重新定位規則的所有管理員所做的變更。

STEP 2 | 預覽提交將啟用的變更。

當您刪除並重新新增相同裝置至原則規則後預覽變更時，*Panorama* 將該裝置顯示為執行設定中的被刪除項和候選設定中的新增項。此外，執行設定中的裝置目標清單內裝置順序可能與候選設定的不同，並在您預覽變更時顯示為變更狀態（即使沒有任何組態變更）。

例如，如果您不記得所有變更，以及不確定要啟動所有變更，則此選項十分有用。

Panorama 將比較您在 Commit Scope（提交範圍）中選取的設定與執行中的設定。預覽視窗將並列顯示組態，並以不同的顏色指出哪些變更是新增（綠色）、修改（黃色）或刪除（紅色）。

Preview Changes（預覽變更）並選取 **Lines of Context**（內容行數），這是比較的組態檔案要在反白顯示的差異前後出現的行數。這些行可幫助您將預覽輸出關聯至 Web 介面中的設定。完成變更檢閱後，關閉預覽視窗。

由於預覽結果顯示在新視窗中，您的瀏覽器必須允許快顯視窗。如果預覽視窗未開啟，請參閱瀏覽器文件，瞭解如何解除封鎖快顯視窗的步驟。

STEP 3 | 預覽要提交變更的個別設定。

如果您想要知曉變更的詳細資訊，例如設定類型以及變更者，這將很有用。

© 2019 Palo Alto Networks, Inc.

1. 按一下 **Change Summary**（變更摘要）。
2. （選用）按欄名稱（例如設定 **Type**（類型））**Group By**（分組）。
3. 完成變更檢閱後，**Close**（關閉）Change Summary（變更摘要）對話方塊。

STEP 4 | 驗證變更後再提交以確保提交成功。

1. **Validate Changes**（驗證變更）。

   結果顯示實際提交將顯示的所有錯誤和警告。
2. 解析驗證結果識別的任何錯誤。

STEP 5 | （選用）修改 Push Scope（推送範圍）。

依預設，推送範圍包含需要 Panorama 提交變更的所有位置。



如果您選取 *Commit*（提交）> *Push to Devices*（推送至裝置），則推送範圍包含與 *Panorama* 執行中設定不同步的裝置的所有相關聯位置。

1. **Remove Selections**（移除選擇）以移除推送範圍內列出的防火牆。
2. **Edit Selections**（編輯選擇）並選取：
   - **Device Groups**（裝置群組）—選取裝置群組或個別防火牆或虛擬系統。
   - **Templates**（範本）—選取範本、範本堆疊或個別防火牆。
   - **Collector Groups**（收集器群組）—選取收集器群組。
3. 按一下 **Ok**（確定），以儲存您對 Push Scope（推送範圍）所做的變更。

STEP 6 | 驗證您將推送至裝置群組或範本的變更。

1. **Validate Device Group Push**（驗證裝置群組推送）或 **Validate Template Push**（驗證範本推送）。

   結果會顯示實際推送操作將顯示的所有錯誤和警告。
2. 解析驗證結果識別的任何錯誤。

STEP 7 | 將變更提交至 Panorama，並將變更推送至裝置。

Commit and Push（提交並推送）設定變更。



使用 Panorama 工作管理員 以查看擱置中（您可以選擇取消這些提交）、進行中、已完成或失敗提交的詳細資訊。

© 2019 Palo Alto Networks, Inc.

啟用自動提交復原

若要確保由組態變更導致的組態故障從 Panorama™ 管理伺服器推送至受管理的防火牆，或在防火牆上本機認可，請啟用 **Automated Commit Recovery**（自動認可復原），使受管理的防火牆能夠在每次認可時測試組態變更，並確認變更不會使 Panorama 與受管理防火牆之間的連線中斷。您可以設定在受管理的防火牆自動將其組態還原至先前執行的組態之前，每台受管理防火牆執行的測試次數，及每次測試發生的時間間隔。啟用自動認可復原時，受管理的防火牆組態會還原，但 Panorama 組態不會還原。此外，受管理的防火牆每 60 分鐘測試一次其與 Panorama 的連線，以在不相關的網路組態變更中斷防火牆與 Panorama 之間的連線時，或過去認可的組態影響連線時，確保繼續通訊。對於高可用性 (HA) 組態，只有在經過連線測試後，HA 對等才會在 Panorama 推送後進行同步。

依預設會啟用自動認可復原。然而，如果您停用自動認可復原，然後想要在現有生產環境中重新啟用此功能，請先確認沒有任何原則規則會中斷 Panorama 與受管理防火牆之間的連線。例如，在管理流量周遊資料平面的情況中，可能有原則規則限制從防火牆傳送至 Panorama 的流量。

防火牆組態成功還原至上次執行的組態後，防火牆會產生組態日誌。此外，當管理員停用此功能時、當組態推送後連線測試失敗而導致組態還原事件開始時，及當每 60 分鐘執行一次的 Panorama 連線測試失敗且造成防火牆組態還原時，防火牆會產生系統日誌。

啟用 *Automated Commit Recovery*（自動認可復原），獨立於任何其他組態變更。如果與導致 *Panorama* 與受管理防火牆之間連線中斷的任何其他組態變更一併啟用，防火牆組態將無法自動還原。

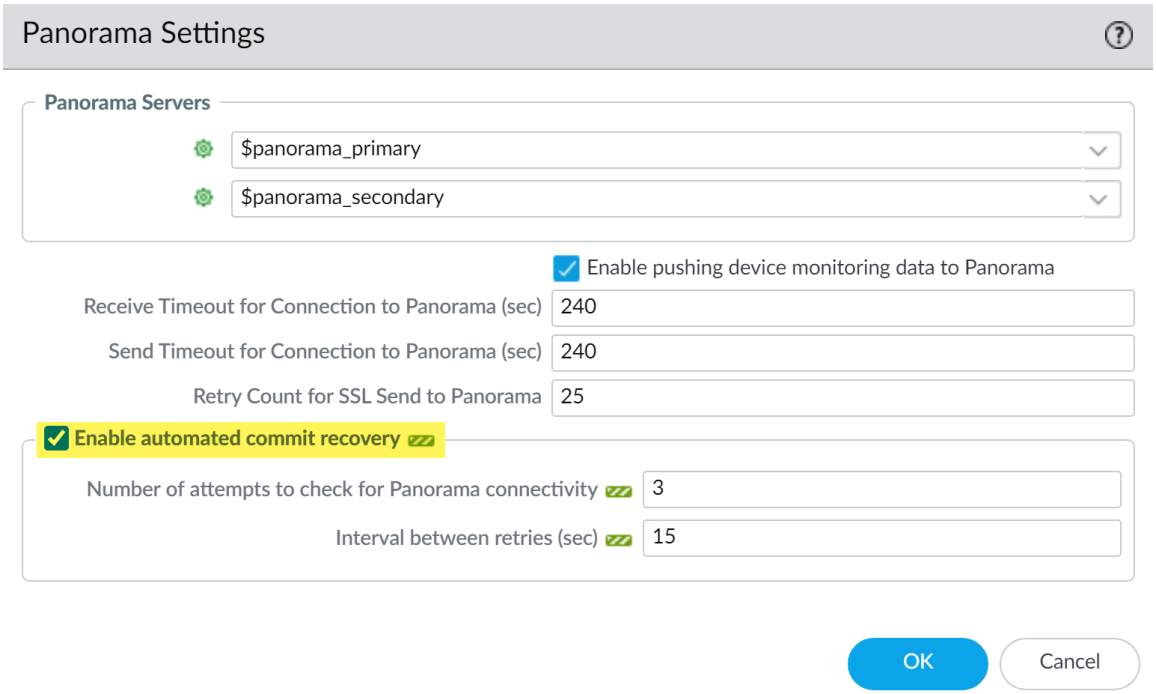
STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 選取 **Device**（裝置）> **Setup**（設定）> **Management**（管理），然後從 **Template**（範本）內容下拉式清單選取所需範本或範本堆疊。

STEP 3 | 啟用自動認可復原。

1. **Edit**（編輯）() Panorama 設定。
2. 啟用自動認可復原。
3. 設定 **Number of attempts to check for Panorama connectivity**（檢查 **Panorama** 連線的嘗試次數）（預設值為 1 次嘗試）。
4. 設定 **Interval between retries**（重試時間間隔）（預設值為 10 秒）。
5. 按一下 **OK**（確定）儲存您的變更。

© 2019 Palo Alto Networks, Inc.



STEP 4 | **Commit**（認可）> **Commit and Push**（認可並推送），然後 **Commit and Push**（認可並推送）您的變更。

STEP 5 | 確認您的受管理防火牆上已啟用自動認可復原功能。

1. 啟動防火牆 Web 介面。
2. 選取 **Device**（裝置）> **Setup**（設定）> **Management**（管理），並且在 Panorama Settings（Panorama 設定）中，確認已啟用（已勾選）**Enable automated commit recovery**（啟用自動認可復原）。

© 2019 Palo Alto Networks, Inc.

管理 Panorama 和防火牆組態備份

Panorama 上正在執行的組態包含您已認可並且正在使用的所有設定。候選組態是執行中組態的副本，以及上次提交後做出的任何未啟用變更。儲存執行中或候選組態的備份版本可讓您稍後還原這些版本。例如，如果提交驗證顯示目前的候選組態具有多個錯誤，使得您不想修復，您可以還原之前的候選組態。您也可以將還原至目前執行中的組態，而先不儲存備份。



如需將設定變更提交至 *Panorama* 和將變更推送至受管理裝置的詳細資訊，請參閱 Panorama 認可、驗證和預覽操作。

在執行 PAN-OS 5.0 或更新版本的本機防火牆上提交之後，執行中設定的備份會傳送至 Panorama。在本機防火牆上執行的任何提交會觸發備份，包括管理員在防火牆本機執行的提交，或 PAN-OS 啟動的自動提交（例如 FQDN 重新整理）。依預設，Panorama 會為每一個防火牆最多儲存 100 個備份，此數量可以設定。若要在外部主機上儲存 Panorama 和防火牆組態備份，您可以排程從 Panorama 匯出或視需要匯出。您還可以從防火牆將設定匯入 Panorama 裝置群組和範本，以 移轉防火牆至 Panorama 進行管理。

（僅限 VMware ESXi 和 vCloud Air）部署在 VMware ESXi 和 vCloud Air 上的 Panorama 虛擬設備不支援 VMware 快照功能。擷取 Panorama 虛擬設備的快照會影響效能，導致間歇性和不一致的封包遺失，且 Panorama 可能會變得無回應。此外，您可能失去對 Panorama CLI 和 Web 介面的存取權限，且不支援切換至 Panorama 模式。請將您命名的設定快照 save and export（儲存並匯出）到任何網路位置。

- 排程組態檔案匯出
- 儲存及匯出 Panorama 和防火牆組態
- 還原 Panorama 組態變更
- 設定 Panorama 上的最大組態份數
- 載入受管理防火牆上的組態備份

排程組態檔案匯出

Panorama 可儲存其執行的組態備份和所有受管理的防火牆執行組態。備份格式為 XML，且檔案名稱以（Panorama 或防火牆）序號為基礎。使用這些說明將備份每日匯出排程至遠端主機。Panorama 將備份作為單一 gzip 檔案匯出。您需要超級使用者權限才能排程匯出。



如果 *Panorama* 具備高可用性 *(HA)* 組態，就必須為每個端點執行這些指示，才能確保已排程的匯出在容錯移轉後會繼續進行。*Panorama* 不會在 *HA* 端點之間同步排程的組態匯出。

若要依需要匯出備份，請參閱儲存及匯出 Panorama 和防火牆組態。

STEP 1 | 選取 **Panorama** > **Scheduled Config Export**（已排程的組態匯出），然後按一下 **Add**（新增）。

STEP 2 | 輸入已排程檔案匯出的 **Name**（名稱）和 **Description**（描述），然後 **Enable**（啟用）它。

STEP 3 | 透過 24 小時時鐘格式，輸入每日 **Scheduled Export Start Time**（已排程的匯出開始時間）或從下拉式清單中選取一個。



如果您正在設定至兩個或更多個伺服器的排程匯出，請錯開排程匯出的開始時間。將多個匯出排程在相同開始時間會導致匯出的組態之間有差異。

STEP 4 | 設定匯出 **Protocol**（協定）為安全複製 (**SCP**) 或檔案傳輸協定 (**FTP**)。

© 2019 Palo Alto Networks, Inc.

STEP 5 | 輸入存取伺服器的詳細資料，包括：**Hostname**（主機）或 IP 位址、**Port**（入口網站）、上傳檔案的 **Path**（路徑）、**Username**（使用者名稱）以及 **Password**（密碼）。

Path（路徑）支援下列字元：**.**（句號）、**+**、**{** 和 **}**、**/**、**-**、**_**、**0-9**、**a-z** 及 **A-Z**。檔案 **Path**（路徑）中不支援空格。

如果您正在匯出至使用 *IPv6* 位址作為主機名稱的 *FTP* 伺服器，您輸入的位址必須用方括號 (*[ ]*)括住。例如，***[2001:0db8:0000:0000:0000:8a2e:0370:7334]***。

如果要匯出至 *BSD* 伺服器，您需要將 *SSHD* 密碼提示修改為 ***<username>@<hostname> <password>:***。

STEP 6 | （僅限 SCP）按一下 **Test SCP server connection**（測試 **SCP** 伺服器連線）。若要啟用資料的安全傳輸，您必須確認並接受 SCP 伺服器的主機金鑰。在接受主機金鑰之前，Panorama 不會建立連線。如果 Panorama 具備 HA 組態，為每個 HA 端點執行此步驟，讓每個 HA 端點接受 SCP 伺服器的主機金鑰。如果 Panorama 可成功連線至 SCP 伺服器，則會建立及上傳名為 ssh-export-test.txt. 的測試檔。

STEP 7 | 按一下 **OK**（確定）儲存您的變更。

STEP 8 | 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

儲存及匯出 Panorama 和防火牆組態

將候選組態的備份儲存至防火牆上的永續性儲存空間，可讓您以後還原該備份（請參閱 還原 Panorama 組態變更）。此外，Panorama 允許您儲存並匯出您指定的裝置群組、範本、範本堆疊組態。這對於保留變更非常有用，否則會因為系統事件或管理員動作導致防火牆重新啟動，而遺失這些變更。重新啟動後，Panorama 會自動還原至 Panorama 儲存在 `running-config.xml` 檔案中的目前執行中組態版本。如果您要還原至比目前執行中組態更早的 Panorama 組態，儲存備份也非常有用。Panorama 不會自動將候選組態儲存在永續性儲存空間。您必須手動儲存候選組態為預設快照檔案 (`.snapshot.xml`) 或自訂名稱的快照檔案。Panorama 會在本機儲存快照檔案，但您可以將其匯出至外部主機。

您不必儲存組態變更，即可還原自上次提交或重新啟動以來所做的變更；只需選取 *Config*（設定）> *Revert Changes*（還原變更）即可（請參閱 還原 Panorama 組態變更）。

Palo Alto Networks 建議您將任何重要的組態備份至外部主機。

STEP 1 | 將變更儲存至候選組態。

- 若要覆寫儲存有所有管理員所做變更的預設快照檔案 (`.snapshot.xml`)，可執行下列任何步驟：
  - 選取 **Device**（裝置）> **Setup**（設定）> **Operations**（操作），然後 **Save candidate Panorama configuration**（儲存候選 **Panorama** 組態）。
  - 使用被指派超級使用者角色的管理帳戶，或已啟用 **Save For Other Admins**（為其他管理員儲存）權限的管理員角色設定檔，登入 Panorama。然後選取 Web 介面頂端的 **Config**（組態）> **Save Changes**（儲存變更），再選取 **Save All Changes**（儲存所有變更）和 **Save**（儲存）。
- 要使用管理員所做的變更覆寫預設快照 (`.snapshot.xml`) 以指定裝置群組、範本或範本堆疊組態：
  1. 選取 **Panorama** > **Setup**（設定）> **Operations**（操作）、**Save candidate Panorama configuration**（儲存候選 **Panorama** 組態），然後 **Select Device Group & Templates**（選取裝置群組與範本）。
  2. 選取指定裝置群組、範本或範本堆疊以還原。
  3. 按一下 **OK**（確定）以確認操作。
  4. （選用）請選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更，以使用快照覆寫執行中組態。

© 2019 Palo Alto Networks, Inc.

- 若要建立包含所有管理員所做變更的快照，但不覆寫預設快照檔案：
  1. 選取 **Panorama** > **Setup**（設定）> **Operations**（操作），然後 **Save named Panorama configuration snapshot**（儲存具名 **Panorama** 組態快照）。
  2. 指定新組態檔案或現有組態檔案的 **Name**（名稱）。
  3. 按一下 **OK**（確定）與 **Close**（關閉）。
- 若要僅儲存候選組態的特定變更，而不覆寫預設快照檔案的任何部分：
  1. 使用具有必要角色權限可儲存所需變更的管理帳戶，登入 Panorama。
  2. 按一下 Web 介面頂端的 **Config**（組態）> **Save Changes**（儲存變更）。
  3. 選取 **Save Changes Made By**（儲存下列管理員所做的變更）。
  4. 若要按管理員篩選儲存範圍，按一下 **<***administrator-name***>**，選取管理員，然後按一下 **OK**（確定）。
  5. 若要按位置篩選儲存範圍，可清除要排除的位置。位置可能是特定裝置群組、範本、收集器群組、日誌收集器、共用設定或 Panorama 管理伺服器。
  6. 按一下 **Save**（儲存），指定新組態檔案或現有組態檔案的 **Name**（名稱），然後按一下 **OK**（確定）。
- 要儲存指定裝置群組、範本或範本堆疊組態：
  1. 選取 **Panorama** > **Setup**（設定）> **Operations**（操作）、**Save named Panorama configuration**（儲存具名 **Panorama** 組態），然後 **Select Device Group & Templates**（選取裝置群組與範本）。
  2. 選取指定裝置群組、範本或範本堆疊以儲存。
  3. 按一下 **OK**（確定）以確認操作。

STEP 2 | 將候選或執行中組態匯出至 Panorama 或防火牆外部主機。

您可以排程每日匯出至 SCP 或 FTP 伺服器（請參閱 排程組態檔案匯出），或依需要匯出組態。若要依需要匯出，請選取 **Panorama** > **Setup**（設定）> **Operations**（操作），並選取下列其中一個選項：

- **Export named Panorama configuration snapshot**（匯出具名 **Panorama** 組態快照）—匯出目前的執行中組態，即具名候選組態快照，或之前匯入的組態（候選組態或執行中組態）。Panorama 將組態匯出為您指定 **Name**（名稱）的 XML 檔案。**Select Device Groups & Templates**（選取裝置群組及範本）指定要匯出的裝置群組、範本或範本堆疊組態。
- **Export Panorama configuration version**（匯出 **Panorama** 組態版本）—選取執行中組態 **Version**（版本）以匯出 XML 檔案格式。**Select Device Groups & Templates**（選取裝置群組及範本）指定要以 XML 檔案匯出的裝置群組、範本或範本堆疊組態。
- **Export Panorama and devices config bundle**（匯出 **Panorama** 和設備的組態組合）—此選項用於手動產生並匯出 Panorama 和每個受管理防火牆的最新版組態備份。若要將每天建立設定套件，並將該套件匯出至安全複製 (SCP) 或 FTP 伺服器的程序自動化，請參閱 排程組態檔案匯出。
- **Export or push device config bundle**（匯出或推送裝置組態組合）—在匯入防火牆組態至 Panorama 中後，Panorama 建立名稱為 <firewall_name>_import.tgz 的防火牆組態組合，並移除其中所有本機政策和物件。您可以 **Export or push device config bundle**（匯出或推送設備組態組合）以執行以下動作之一：
  - **Push & Commit**（推送和提交）組態組合到防火牆，以移除其中的任何本機設定並讓您可以從 Panorama 管理防火牆。
  - 將組態 **Export**（匯出）至防火牆，但不進行載入。準備好載入設定時，登入防火牆 CLI 並執行設定模式命令 **`load device-state`**。此命令會清理防火牆，方式如同 **Push & Commit**（推送和提交）選項。



移轉防火牆至 Panorama 進行管理 的完整程序還需要其他步驟。

© 2019 Palo Alto Networks, Inc.

還原 Panorama 組態變更

當還原變更時，還原操作將用其他組態中的設定取代目前候選組態中的設定。若您希望復原多項設定的變更，還原操作將非常有用，因為只需要執行一次操作，無需手動重新設定每項設定。

您可以還原自上次提交以來對 Panorama 組態所做的擱置中變更。您可以還原 Panorama 上所有擱置變更或選擇指定裝置群組、範本或範本堆疊。Panorama 可讓您選擇依管理員或位置來篩選擱置中變更。位置可能是特定裝置群組、範本、收集器群組、日誌收集器、共用設定或 Panorama 管理伺服器。如果您已經為比目前執行中組態更早的候選組態儲存快照檔案（請參閱 儲存及匯出 Panorama 和防火牆組態），則您也可以還原至該快照。還原至快照可讓您還原上次提交之前就已存在的候選組態。每當您提交變更時，Panorama 會自動儲存新版本的執行中組態，並且您可以還原任何這些版本。

還原 Panorama 管理伺服器組態需要完整認可，並且必須由超級使用者執行。執行某些 Panorama 操作時需要完整認可，諸如還原及載入 Panorama 組態，並且不支援自訂管理員角色設定檔。

- 還原至 Panorama 目前執行中的組態（檔案名稱為 **`running-config.xml`**）。

  此操作將復原自上次提交以來對候選組態做出的變更。

  - 若要還原所有管理員做出的變更，可執行下列任何步驟：
    - 選取 **Panorama** > **Setup**（設定）> **Operations**（操作），**Revert to running Panorama configuration**（還原至執行中 **Panorama** 組態），然後按一下 **Yes**（是）以確認操作。
    - 使用被指派超級使用者角色的管理帳戶，或已啟用 **Commit For Other Admins**（為其他管理員提交）權限的管理員角色設定檔，登入 Panorama。然後選取 **Config**（組態）> **Revert Changes**（還原變更），再選取 **Revert All Changes**（還原所有變更）和 **Revert**（還原）。
  - 若要還原對候選組態做出的特定變更：
    1. 使用具有必要角色權限可還原所需變更的管理帳戶，登入 Panorama。

       控制提交操作的權限也用於控制還原操作。
    2. 選取 **Config**（組態）> **Revert Changes**（還原變更）。
    3. 選取 **Revert Changes Made By**（還原下列管理員所做的變更）。
    4. 若要按管理員篩選還原範圍，按一下 *<administrator-name>*，選取管理員，然後按一下 **OK**（確定）。
    5. 若要按位置篩選還原範圍，可清除要排除的位置。
    6. **Revert**（還原）變更。
  - 要還原指定裝置群組、範本或範本堆疊變更至執行中組態：
    1. 選取 **Panorama** > **Setup**（設定）> **Operations**（操作）、**Save candidate Panorama configuration**（儲存候選 **Panorama** 組態），然後 **Select Device Group & Templates**（選取裝置群組與範本）。
    2. 選取指定裝置群組、範本或範本堆疊以還原。
    3. 按一下 **OK**（確定）以確認操作。
    4. （選用）選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後將您的變更 **Commit**（提交）以覆寫執行中組態。

- 還原至 Panorama 候選組態的預設快照（**`.snapshots.xml`**）。
  - 要還原所有管理員所做的變更：
    1. 選取 **Panorama** > **Setup**（設定）> **Operations**（操作），然後 **Revert to last saved Panorama configuration**（還原至上次儲存的 **Panorama** 組態）。
    2. 按一下 **Yes**（是）以確認操作。
    3. （選用）請選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更，以使用快照覆寫執行中組態。

© 2019 Palo Alto Networks, Inc.

- 要還原指定裝置群組、範本或範本堆疊變更至執行中組態：
  1. 選取 **Panorama** > **Setup**（設定）> **Operations**（操作）、**Revert to last saved Panorama configuration**（還原至上次儲存的 **Panorama** 組態），然後 **Select Device Group & Templates**（選取裝置群組與範本）。
  2. 選取指定裝置群組、範本或範本堆疊以還原。
  3. 按一下 **OK**（確定）以確認操作。
  4. （選用）若要覆寫執行中組態，請選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

- 還原至 Panorama 上儲存的前一版執行中組態。
  - 要還原所有管理員所做的變更：
    1. 選取 **Panorama** > **Setup**（設定）> **Operations**（操作）、**Load Panorama configuration version**（載入 **Panorama** 組態版本），然後 **Select Device Group & Templates**（選取裝置群組與範本）。
    2. 選取組態 **Version**（版本），然後按一下 **OK**（確定）。
    3. （選用）若要使用您剛還原的版本覆寫執行中組態，請選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。
  - 要還原指定裝置群組、範本或範本變更至執行中組態：
    1. 選取 **Panorama** > **Setup**（設定）> **Operations**（操作）、**Load Panorama configuration version**（載入 **Panorama** 組態版本），然後選取組態版本 **Name**（名稱）。
    2. **Select Device Group & Templates**（選取裝置群組以及範本）並選取要還原的特定裝置群組、範本或範本堆疊。
    3. 按一下 **OK**（確定）以確認操作。
    4. （選用）若要使用快照覆寫執行中組態，請選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

- 還原至下列其中一項：
  - 您之前匯入的自訂名稱 Panorama 執行中組態。
  - 自訂名稱的 Panorama 候選組態快照（而非預設快照）。

  1. 選取 **Panorama** > **Setup**（設定）> **Operations**（操作），**Load named Panorama configuration snapshot**（載入具名 **Panorama** 組態快照），並選取您匯入的組態檔案 **Name**（名稱）。
  2. （選用）**Load Shared Objects**（載入共用物件）或 **Load Shared Policies**（載入共用原則）以載入所有共用的物件或原則。您可以載入所有共用物件和原則，同時載入您在下一步中指定的裝置群組和範本中設定的物件和原則。
  3. （選用）**Select Device Groups & Templates**（選取裝置群組以及範本），並選取要載入的特定裝置群組、範本或範本堆疊組態。如果您想要還原整個 Panorama 組態，請跳過此步驟。
  4. 按一下 **OK**（確定）以確認操作。
  5. （選用）若要使用快照覆寫執行中組態，請選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

- 還原您之前匯出至外部主機的 Panorama 執行中組態或候選組態。
  1. 選取 **Panorama** > **Setup**（設定）> **Operations**（操作），**Import named Panorama configuration snapshot**（匯入具名 **Panorama** 組態快照），**Browse**（瀏覽）至外部主機上的組態檔案，然後按一下 **OK**（確定）。
  2. **Load named configuration snapshot**（載入具名組態快照），選取您剛才匯入的組態 **Name**（名稱）。

© 2019 Palo Alto Networks, Inc.

3. （選用）**Load Shared Objects**（載入共用物件）或 **Load Shared Policies**（載入共用原則）以載入所有共用的物件或原則。您可以載入所有共用物件和原則，同時載入您在下一步中指定的裝置群組和範本中設定的物件和/或原則。
4. （選用）**Select Device Groups & Templates**（選取裝置群組以及範本），並選取要載入的特定裝置群組、範本或範本堆疊組態。如果您想要還原整個 Panorama 組態，請跳過此步驟。
5. 按一下 **OK**（確定）以確認操作。
6. （選用）若要使用您剛匯入的快照覆寫執行中組態，請選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

設定 Panorama 上的最大組態份數

STEP 1 | 選取 **Panorama** > **Setup**（設定）> **Management**（管理），然後編輯 [日誌與報告設定]。

STEP 2 | 選取 **Log Export and Reporting**（日誌匯出與報告），然後輸入 **Number of Versions for Config Backups**（設定備份的版本數目）（預設值為 100；範圍為 1 至 1,048,576）。

STEP 3 | 按一下 **OK**（確定）儲存您的變更。

STEP 4 | 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

載入受管理防火牆上的組態備份

使用 Panorama 來載入受管理防火牆上的設定備份。您可以選擇還原到防火牆上先前儲存或提交的設定。Panorama 會將選取的版本推送至受管理防火牆，然後覆寫防火牆上目前的候選組態。

STEP 1 | 選取 **Panorama** > **Managed Devices**（受管理的裝置）> **Summary**（摘要）。

STEP 2 | 選取 Backups（備份）欄中的 **Manage**（管理）。

STEP 3 | 選取 Saved Configurations（儲存的組態）或 Committed Configurations（認可的組態）。

- 按一下版本號碼以檢視該版本的內容。
- **Load**（載入）組態版本。

STEP 4 | 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

© 2019 Palo Alto Networks, Inc.

比較 Panorama 組態中的變更

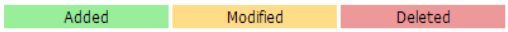
若要在 Panorama 上比較設定變更，您可以選取任兩組設定檔：候選設定、執行中設定，或之前已在 Panorama 上儲存或提交的任何其他設定版本。逐步比較可讓您：

- 先預覽設定變更，再將變更提交至 Panorama。例如，您可以預覽候選設定與執行中設定之間的變更。最佳的作法是選取左窗格的較舊版本，並選取右窗格的較新版本，以輕鬆地比較及識別修改的內容。
- 執行設定稽核來檢閱與比較兩組組態檔案之間的變更。

裝置群組和範本管理員僅能在其存取網域內比較裝置群組和範本的設定。

- 比較 Panorama 組態中的變更。
  1. 選取 **Panorama** > **Config Audit**（設定稽核）。
  2. 在每一個下拉式清單中，選取要比較的設定。
  3. 選取您要包含在**Context**（內容）中的行數，然後按一下**Go**（執行）。

     Panorama 利用色彩強調顯示您新增（綠色）、修改（黃色）或刪除（紅色）的項目。

- 設定 Panorama 儲存用於組態稽核的版本數目。
  1. 選取 **Panorama** > **Setup**（設定） > **Management**（管理），然後編輯 [日誌與報告設定]。
  2. 輸入**Number of Versions for Config Audit**（設定稽核的版本數量）（範圍為 1–1,048,576；預設為 100）。
  3. 按一下 **OK**（確定）儲存您的變更。
  4. 選取 **Commit**（提交） > **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

- 提交前先檢視和比較 Panorama 組態檔案。
  1. 選取 **Commit**（提交） > **Commit to Panorama**（提交至 **Panorama**），然後 **Preview Changes**（預覽變更）。
  2. 選取您要查看的 **Lines of Context**（內容行數），然後按一下 **OK**（確定）。

© 2019 Palo Alto Networks, Inc.

管理限制組態變更的鎖定

鎖定候選組態或執行中組態，以防止其他管理員變更組態，直至您手動移除鎖定，或 Panorama 自動移除鎖定（認可後）。鎖定可確保在並行登入工作階段期間，管理員不會對相同的設定或相互依存的設定做出產生衝突的變更。



如果您變更的設定與其他管理員在並行工作階段中變更的設定無關，則您將無需設定鎖來防止認可衝突。*Panorama* 將認可操作排入佇列並按照管理員啟動認可的順序執行。如需詳細資料，請參閱Panorama 認可、驗證和預覽操作。

在指派給範本或裝置群組的防火牆上，如果有管理員在該防火牆本機設定的提交或設定鎖定，則範本或裝置群組設定推送會失敗。

- 檢視目前鎖定的詳細資訊。

  例如，您可以查看其他管理員是否設定鎖定，並閱讀其輸入的鎖定說明註解。

  按一下網頁介面上方的鎖定掛鎖 ( )。旁邊的數字指示目前的鎖定數。

- 鎖定組態。

  無法修改防火牆或 Panorama 組態的唯讀管理員不能設定鎖定。

  1. 按一下 Web 介面右上角的掛鎖圖示。

     圖示根據現有鎖定是已設定 ( ) 還是未設定 ( ) 而不同。
  2. **Take a Lock**（鎖定）並選取鎖 **Type**（類型）：
     - **Config**（組態）—封鎖其他管理員對候選組態進行變更。

       無法認可變更的自訂角色管理員可以設定 *Config*（設定）鎖定，並將變更儲存至候選組態。但是，由於該管理員無法認可變更，*Panorama* 將不會在認可後自動解除鎖定；管理員在進行所需的變更後，必須手動解除 *Config*（設定）鎖定。

     - **Commit**（提交）—阻止其他管理員對執行中設定進行變更。
  3. 選取 **Location**（位置）以確定鎖定範圍：
     - **Shared**（共用）—限制對 Panorama 的整體設定進行變更，包括所有設定群組和範本。
     - **Template**（範本）—限制對所選範本內包含的防火牆進行變更。（您無法鎖定範本堆疊，僅可鎖定堆疊內的單個範本。）
     - **Device group**（裝置群組）—限制對所選裝置群組進行變更，但不限制其子系裝置群組。
  4. （選用）最佳作法是輸入 **Comment**（註解）來說明設定鎖定的原因。
  5. 按一下 **OK**（確定）與 **Close**（關閉）。

- 解鎖組態。

  只有鎖定組態的超級使用者或管理員可手動解鎖組態。但是，在完成設定鎖定的管理員啟動的認可操作後，Panorama 將會自動解除鎖定。

  1. 按一下網頁介面上方的鎖定掛鎖 ( )。
  2. 選取清單中的鎖定項目。
  3. 按一下 **Remove Lock**（移除鎖定）、**OK**（確定）與 **Close**（關閉）。

- 設定 Panorama 在變更候選組態後，自動鎖定執行中組態。此設定適用於所有 Panorama 管理員。

© 2019 Palo Alto Networks, Inc.

1. 選取 **Panorama** > **Setup**（設定） > **Management**（管理），再編輯 [一般設定]。
2. 選取 **Automatically Acquire Commit Lock**（自動擷取提交鎖定），然後按一下 **OK**（確定）。
3. 選取 **Commit**（提交） > **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交） 您的變更。

© 2019 Palo Alto Networks, Inc.

將自訂標誌新增至 Panorama

您可以在 Panorama 上傳映像檔案以自訂下列區域：

- 登入畫面上的背景映像
- Web 介面左上角的標頭；您也可以隱藏 Panorama 預設背景
- PDF 報告中的標題頁面和頁尾映像

支援的映像類型包括 .jpg、.gif 和 .png。PDF 報告中使用的映像檔案不可包含 Alpha 色板。映像的大小必須小於 128 KB（131,072 位元組）；畫面上會顯示建議的尺寸。如果尺寸大於建議的大小，將自動裁剪映像。

STEP 1 | 選取 **Panorama** > **Setup**（設定） > **Operations**（操作）。

STEP 2 | 在 Miscellaneous（雜項）區段中，按一下 **Custom Logos**（自訂標誌）。

STEP 3 | 按一下上傳標誌圖示，再選取下列任何選項的映像：登入畫面、主要使用者介面的左側角落、PDF 報告的標題頁面及 PDF 報告的頁尾。

STEP 4 | 按一下 **Open**（開啟）以新增映像。若要預覽映像，按一下預覽標誌圖示。

STEP 5 | （選用）若要清除 Panorama 網頁介面上的綠色背景標頭，請選取 **Remove Panorama background header**（移除 **Panorama** 背景標頭）的核取方塊。

STEP 6 | 按一下 **Close**（關閉）儲存您的變更。

STEP 7 | 選取 **Commit**（提交） > **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

© 2019 Palo Alto Networks, Inc.

使用 Panorama 工作管理員

按一下 Web 介面底部的 **Tasks**（工作）（Tasks）以開啟工作管理員，其中將顯示子 Panorama 或防火牆上次重新啟動以來，管理員（例如手動提交）或 Panorama 或受管理防火牆（例如已排程的報告產生）啟動的所有操作的詳細資訊。您可以使用工作管理員來排解失敗操作，調查與已完成的提交相關的警告，或取消擱置中的提交。



裝置群組和範本管理員僅能在其存取網域內檢視工作的工作。

STEP 1 | 按一下 **Tasks**（工作）。

STEP 2 | **Show**（顯示）**Running**（進行中）的工作或 **All**（所有）工作（預設），可以按照類型（**Reports**（報告）；**Log Requests**（日誌請求）；或提交、下載和安裝 **Jobs**（工作）進行篩選，並選取您要查看哪個 **Panorama**（預設）或防火牆的工作。

STEP 3 | 執行下列任何動作：

- 顯示或隱藏工作詳細資訊—依預設，工作管理員顯示類型、狀態、開始時間及每項工作的訊息。若要查看工作的結束時間及工作 ID，您必須手動顯示這些欄。若要顯示或隱藏欄，在任何欄標頭中開啟下拉式清單，選取 **Columns**（欄），然後視需要選取或清除欄名稱。
- 調查警告或失敗—閱讀 Messages（訊息）欄中的項目，瞭解工作詳細資訊。如果欄顯示 `Too many messages`（太多訊息），則按一下 Type（類型）欄中的相應項目，以檢視更多資訊。
- 顯示提交說明—如果管理員在提交時輸入了說明，可以按一下 Messages（訊息）欄中的 **Commit Description**（提交說明）以顯示說明。
- 在佇列中檢查提交的位置—Messages（訊息）欄表示正在進行之提交的佇列位置。
- 取消擱置的提交—**Clear Commit Queue**（清除提交佇列）以取消所有擱置的提交（僅適用於預先定義的管理角色）。若要取消個別提交，按一下 Action（動作）欄中的 **x**（提交將保留在佇列中，直至 Panorama 將其移除佇列）。您無法取消正在進行的提交。

© 2019 Palo Alto Networks, Inc.

管理日誌和報告儲存配額和到期日期

- 日誌和報告儲存
- 日誌和報告到期日期
- 設定日誌和報告儲存配額和到期日期
- 設定 Panorama 報告的執行階段

日誌和報告儲存

您可以編輯各日誌類型的預設儲存配額。當日誌配額達到大小上限時，Panorama 會開始以新日誌項目覆寫最舊的日誌項目。報告的儲存容量不可設定。日誌儲存位置和報告儲存容量依 Panorama 型號而異：

- **Panorama** 模式的 **Panorama** 虛擬設備—報告的儲存空間為 200MB。設備會使用其虛擬系統磁碟，儲存 Panorama 和日誌收集器所產生的系統和設定日誌。虛擬系統磁碟還儲存 Panorama 每 15 分鐘自動從所有管理的防火牆接收的應用程式統計資料 (App Stats) 日誌。Panorama 會將其他所有日誌類型儲存至虛擬日誌記錄磁碟（1 至 12）。
- 僅管理模式的 **Panorama** 虛擬設備—報告的儲存空間為 500MB。設備會使用其虛擬系統磁碟，儲存 Panorama 和日誌收集器所產生的系統和設定日誌。虛擬系統磁碟還儲存 Panorama 每 15 分鐘自動從所有管理的防火牆接收的應用程式統計資料 (App Stats) 日誌。您必須設定一個受管理的收集器以從受管理的防火牆轉送日誌，因為僅管理模式下的 Panorama 無法儲存任何其他日誌類型。
- 傳統模式的 **Panorama** 虛擬設備—若為 Panorama 8.0 或更舊版本，報告的儲存空間為 200MB，若為 Panorama 8.0.1 和更新版本，則為 500MB。Panorama 將所有日誌寫入其指派的儲存空間，可以是下列任何一個：
  - 虛擬系統磁碟—依預設，在您安裝 Panorama 時所建立的虛擬系統磁碟上，大約會配置 11GB 作為日誌儲存空間。如果您新增虛擬日誌記錄磁碟或 NFS 分割區，Panorama 仍會使用系統磁碟，儲存 Panorama 和日誌收集器所產生的系統和設定日誌，以及儲存從防火牆收集的 App Stats 日誌。
  - 專用虛擬日誌記錄磁碟—儲存所有日誌類型，但位於系統磁碟上的日誌除外。
  - **NFS** 分割區—此選項僅適用於 VMware ESXi 伺服器上執行的 Panorama。NFS 分割區儲存所有日誌類型，但位於系統磁碟上的日誌除外。
- **M-600**、**M-500** 或 **M-200** 設備 - 若為 Panorama 6.1 或更新版本，報告的儲存空間為 500MB，若為更舊版本，則為 200MB。M-Series 設備會使用其內部 SSD，儲存 Panorama 和日誌收集器所產生的設定日誌和系統日誌，以及儲存從防火牆收集的 App Stats 日誌。Panorama 將所有其他日誌類型儲存至啟用 RAID 的磁碟。RAID 磁碟為 Panorama 模式下的 M-Series 設備本機磁碟，或位於專門的日誌收集器中（日誌收集器模式下的 M-Series 設備）。當您設定收集器群組時，您會編輯 RAID 磁碟上的日誌儲存配額。



如需日誌儲存選項和容量的詳細資訊，請參閱Panorama 型號。您可以透過新增 *NFS* 儲存空間上的虛擬日誌記錄磁碟，來擴充 Panorama 虛擬設備上的日誌儲存容量。您可以透過新增 *RAID* 磁碟機，或透過從 *1TB* 磁碟機升級至 *2TB* 磁碟機，以增加 M-Series 設備上的儲存空間。

日誌和報告到期日期

您可以根據日誌時間設定自動刪除 Panorama 管理伺服器和日誌收集器從防火牆收集的日誌，以及 Panorama 和日誌收集器本機產生的日誌和報告。這對部署內需要定期刪除監控資訊的情況非常適用。例如，由於法務原因，您的公司要求在一定時間後務必刪除使用者資訊。您可以為下列項目設定獨立的到期日期：

- 報告—Panorama 在產生新報告的同時會刪除過期報告（請參閱設定 Panorama 報告的執行階段）。
- 各日誌類型—Panorama 在接收日誌時對其進行評估，然後刪除超出設定到期日期的日誌。

© 2019 Palo Alto Networks, Inc.

- *Panorama* 在高可用性 *(HA)* 配對之間同步到期日期。由於僅主動 *HA* 端點產生日誌，被動端點無日誌或報告可刪除，除非其發生故障並開始產生日誌。

  即使未設定到期日期，當日誌配額達到最大大小時，*Panorama* 會開始以新日誌項目取代最舊的日誌項目。

設定日誌和報告儲存配額和到期日期

STEP 1 | 設定下列內容的儲存配額和到期日期：

- 傳統模式的 Panorama 虛擬設備從防火牆接收的所有日誌類型。
- Panorama 從防火牆接收的 App Stats 日誌。
- Panorama 和日誌收集器在本機產生的系統日誌和設定日誌。

Panorama 管理伺服器會將這些日誌儲存在本機。

如果您減少儲存配額，導致目前日誌超出該配額，在提交變更後，*Panorama* 會移除最早的日誌以適應該配額。

1. 選取 **Panorama** > **Setup**（設定）> **Management**（管理），然後編輯 [日誌與報告設定]。
2. 在 **Log Storage**（日誌儲存）設定中，輸入各日誌類型的 **Quota (%)**（配額 %）。

   當您變更百分比值時，頁面會重新整理畫面以根據配置給 Panorama 的總空間來顯示對應的絕對值（配額 GB/MB 欄）。
3. 輸入各日誌類型的 **Max Days**（最大天數）（到期時間）（範圍為 1 至 2,000）。

   依預設，欄位為空，意味著日誌從不過期。

   如果您要將配額和到期時間重設為原廠預設值，請選取 *Restore Defaults*（還原預設值）。

STEP 2 | 設定 Panorama 產生之報告的到期時間。

1. 選取 **Log Export and Reporting**（日誌匯出與報告），然後輸入 **Report Expiration Period**（報告到期時間），以天為單位（範圍為 1 至 2,000）。

   依預設，欄位為空，意味著日誌從不過期。
2. 按一下 **OK**（確定）儲存您的變更。

STEP 3 | 針對 M-600、M-500、M-200 設備，或 Panorama 模式的 Panorama 虛擬設備從防火牆接收的所有日誌類型（App Stats 日誌除外），設定儲存配額和到期時間。

本機或專用日誌收集器會儲存這些日誌。

您可以在收集器群組層級設定這些儲存配額，而非單個日誌收集器。

1. 選取 **Panorama** > **Collector Groups**（收集器群組），然後編輯收集器群組。
2. 在 **General**（一般）設定中，按一下 **Log Storage**（日誌儲存）值。

   直到您將日誌收集器指派給收集器群組，才會出現值。如果欄位在您指派日誌收集器後顯示 *0MB*，請確認您在 設定日誌收集器時 已啟用磁碟配對，也已提交變更（*Panorama* > *Managed Collectors*（受管理的收集器）> *Disks*（磁碟））。
3. 輸入每個日誌類型的儲存 **Quota**（配額）(%)。

© 2019 Palo Alto Networks, Inc.

當您變更百分比值時，頁面會重新整理畫面以根據配置給收集器群組的總儲存空間來顯示對應的絕對值（配額 GB/MB 欄）。

4. 輸入各日誌類型的 **Max Days**（最大天數）（到期時間）（範圍為 1 至 2,000）。

   依預設，欄位為空，意味著日誌從不過期。

   如果您要將配額和到期時間重設為原廠預設值，請選取 *Restore Defaults*（還原預設值）。

5. 按一下 **OK**（確定）儲存您的變更。

STEP 4 | 將變更提交至 Panorama，並將變更推送至收集器群組。

1. 選取 **Commit**（提交）> **Commit and Push**（提交並推送），然後在 Push Scope（推送範圍）中 **Edit Selections**（編輯選擇）。
2. 選取 **Collector Groups**（收集器群組），並選取您修改的收集器群組，然後按一下 **OK**（確定）。
3. **Commit and Push**（提交並推送）您的變更。

STEP 5 | 確認 Panorama 套用儲存配額變更。

1. 選取 **Panorama** > **Setup**（設定）> **Management**（管理），然後在日誌與報告設定中，確認 **Log Storage**（日誌儲存）值正確適配 Panorama 管理伺服器儲存的日誌。
2. 選取 **Panorama** > **Collector Groups**（收集器群組），選取您修改的收集器群組，然後確認 **General**（一般）頁籤內的 **Log Storage**（日誌儲存）值正確適配日誌收集器儲存的日誌。

   您也可以透過登入日誌收集器 *CLI* 和輸入操作命令 ***show log-diskquota-pct*** 確認收集器群組儲存配額。

設定 Panorama 報告的執行階段

Panorama 每天會在您指定的時間產生報告。Panorama 產生新報告之後會刪除任何過期的報告。

STEP 1 | 選取 **Panorama** > **Setup**（設定）> **Management**（管理），然後編輯 [日誌與報告設定]。

STEP 2 | 選取 **Log Export and Reporting**（日誌匯出與報告），將 **Report Runtime**（報告執行時間）設定為 24 小時制的整點（預設為 02:00；範圍為 00:00 [午夜] 到 23:00）。

STEP 3 | 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

© 2019 Palo Alto Networks, Inc.

監控 Panorama

若要監控 Panorama 及其管理的收集器，您可以定期檢視其系統和設定日誌（依類型篩選日誌），設定 SNMP 管理員以定期收集 (GET) Panorama 統計資料，或設定 SNMP 設陷或電子郵件警示，在監控的度量變更狀態或達到 Panorama 上的閾值時通知您。發生需要立即處理的嚴重系統事件時，使用電子郵件警示及 SNMP 設陷可有效地立即發出通知。若要設定電子郵件警示或 SNMP 設陷，請參閱 設定日誌從 Panorama 轉送至外部目的地。

- Panorama 系統與組態日誌
- 透過 SNMP 監控 Panorama 和日誌收集器統計資料

Panorama 系統與組態日誌

您可以設定 Panorama，在發生系統事件或變更設定時傳送通知。依預設，Panorama 會將每個設定變更記錄在設定日誌中。在系統日誌上，每一個事件皆有表示其急迫性和影響的嚴重性等級。當您 設定日誌從 Panorama 轉送至外部目的地 時，您可以轉送所有系統和設定日誌，或根據屬性來篩選日誌，例如接收時間或嚴重性等級（僅限系統日誌）。下表概括系統日誌的嚴重性等級：

severity	說明
嚴重	表示失敗且必須立即處理，例如硬體故障，包含高可用性 (HA) 故障復原和連結失敗。
高	將危害系統操作的嚴重問題，包含日誌收集器中斷連線或提交失敗。
中	中等級通知，例如防毒套件升級，或收集器群組設定提交。
低	低等級嚴重性通知，例如使用者密碼變更。
僅供參考	通知事件，例如登入或登出、任何設定變更、驗證成功和失敗通知、提交成功，以及其他嚴重性等級未涵蓋的所有其他事件。

Panorama 將系統和設定日誌儲存在本機；確切位置和儲存容量隨 Panorama 型號而異（請參閱 日誌和報告儲存）。達到容量限時，Panorama 會刪除最舊的日誌，以騰出空間給新的日誌。如果日誌需要保存的比本機儲存更久，您可以 設定日誌從 Panorama 轉送至外部目的地。



關於透過 *Panorama* 監控防火牆日誌的資訊，請參閱 監控網路活動。

透過 SNMP 監控 Panorama 和日誌收集器統計資料

您可以設定 SNMP 管理程式以要求來自 Panorama 管理伺服器的資訊和設定 Panorama 以進行回應。例如，SNMP 管理程式可以要求高可用性 (HA) 模式、Panorama 狀態和 Panorama 版本。如果 Panorama 管理伺服器有本機日誌收集器，則 Panorama 還可提供日誌記錄統計資料：每秒平均日誌數、儲存持續時間、保留期限、日誌磁碟使用量、從個別防火牆至 Panorama 和外部伺服器的日誌轉送狀態，以及防火牆至日誌收集器的連線狀態。Panorama 不會同步 HA 端點之間的 SNMP 設定；您必須啟用 SNMP 要求並回應每個端點。

針對與 Panorama 管理伺服器相同的日誌記錄統計資料，您也可以設定專用日誌收集器來回應請求。此資訊在評估您是否需要擴充儲存容量時非常有用。

© 2019 Palo Alto Networks, Inc.

您無法（透過 *SET* 訊息）設定 *SNMP* 管理程式控制 *Panorama* 或日誌收集器；*SNMP* 管理程式僅可（透過 *GET* 訊息）收集統計資料。

關於 *Panorama* 如何實作 *SNMP* 的詳細資訊，請參閱 SNMP 支援。

STEP 1 | 設定 SNMP 管理程式以從 Panorama 和日誌收集器獲得統計資料。

下列步驟是您在 SNMP 管理程式上所執行工作的概要。如需特定步驟，請參閱 SNMP 管理員文件。

1. 若要啟用 SNMP 管理員以判讀統計資料，可載入支援的 MIB，並在必要時將其編譯。
2. 對於 SNMP 管理員將監控的各 Panorama 設備，請定義其連線設定（IP 位址和連接埠）和驗證設定（SNMPv2c 社群字串或 SNMPv3 使用者名稱和密碼）。所有 Panorama 設備都使用連接埠 161。

   SNMP 管理員可以針對多個 Panorama 管理伺服器和日誌收集器，使用相同或不同的連線和驗證設定。這些設定必須符合您在 Panorama 上設定 SNMP 時所定義的設定（請參閱設定 Panorama 管理伺服器以回應來自 SNMP 管理員的統計資料要求和設定專用日誌收集器（如有）以回應 SNMP 要求）。例如，如果您使用 SNMPv2c，您在設定 Panorama 時定義的社群字串，必須與您針對 Panorama 在 SNMP 管理員中定義的社群字串相符。
3. 決定您將監控的統計資料物件識別碼 (OIDs)。例如，若要監控日誌記錄速率，MIB 瀏覽器顯示對應 OID 1.3.6.1.4.1.25461.2.3.30.1.1 的統計資料位於 PAN-PRODUCT-MIB.my 中。詳細資訊，請參閱使用 SNMP 管理程式探索 MIB 和物件。
4. 設定 SNMP 管理員以監控所需 OID。

STEP 2 | 啟用 Panorama 管理伺服器管理 (MGT) 介面上的 SNMP 流量。

1. 選取 **Panorama** > **Setup**（設定）> **Management**（管理），然後編輯管理介面設定。
2. 在服務部分中，選取 **SNMP** 核取方塊，然後按一下 **OK**（確定）。

STEP 3 | 啟用日誌收集器模式下任何 M 系列設備管理 (MGT) 介面上的 SNMP 流量：

1. 選取 **Panorama** > **Managed Collectors**（受管理的收集器），再選取日誌收集器。
2. 選取 **Management**（管理）頁籤，選取 **SNMP** 核取方塊，然後按一下 **OK**（確定）。

STEP 4 | 設定 Panorama 管理伺服器以回應來自 SNMP 管理程式的統計資料要求。

1. 選取 **Panorama** > **Setup**（設定）> **Operations**（操作），然後在 [雜項] 部分中，按一下 **SNMP Setup**（**SNMP** 設定）。
2. 選取 SNMP **Version**（版本），然後設定驗證值，如下所示。關於版本的詳細資訊，請參閱 SNMP 支援。

   - **V2c**—輸入 **SNMP Community String**（**SNMP** 社群字串）以便識別 SNMP 管理員社群和受監控設備（此處為 Panorama），同時也作為密碼以進行社群成員彼此驗證。

     請勿使用預設社群字串 ***public***；其廣為人知，因此不具有安全性。

   - **V3**—建立至少一個 SNMP 檢視群組和一個使用者。當 SNMP 管理員取得統計資料時，使用者帳戶和檢視提供驗證、隱私和存取控制。

     檢視—每個檢視有一組配對的 OID 和 Bitwise 遮罩：OID 會指定一個 MIB，而遮罩（使用十六進位格式）會指定在 MIB 之中（包含相符）或之外（排除相符）的相關聯物件。在第一個清單中按一下 **Add**（新增）並輸入檢視群組的 **Name**（名稱）。對於群組內的各個檢視，按一下 **Add**（新增）並和設定檢視 **Name**（名稱）、**OID**，相符 **Option**（選項）（**include**（包括）或 **exclude**（排除）），和 **Mask**（遮罩）。

     Users（使用者）——按一下第二個清單中的 **Add**（新增），在使用者欄中輸入使用者名稱，從下拉式清單中選取 **View**（檢視）群組，輸入驗證密碼 (**Auth Password**) 用於驗證至 SNMP 管理員，然後輸入隱私密碼 (**Priv Password**) 用於加密 SNMP 訊息至 SNMP 管理員。
3. 按一下 **OK**（確定）以儲存設定。

© 2019 Palo Alto Networks, Inc.

STEP 5 | 設定專用的日誌收集器（如有），以回應 SNMP 要求。

對於各個收集器群組：

1. 選取 **Panorama** > **Collector Groups**（收集器群組），再選取收集器群組。
2. 選取 **Monitoring**（監控）頁籤，設定如步驟設定 Panorama 管理伺服器以回應來自 SNMP 管理員的統計資料要求，然後按一下 **OK**（確定）。

STEP 6 | 將變更提交至 Panorama，並將變更推送至收集器群組。

1. 選取 **Commit**（提交）> **Commit and Push**（提交並推送），然後在 Push Scope（推送範圍）中 **Edit Selections**（編輯選擇）。
2. 選取 **Collector Groups**（收集器群組），並選取您編輯的收集器群組，然後按一下 **OK**（確定）。
3. **Commit and Push**（提交並推送）您的變更。

STEP 7 | 監控 SNMP 管理程式內的 Panorama 和日誌收集器統計資料。

請參閱 SNMP 管理員文件。

© 2019 Palo Alto Networks, Inc.

重新啟動或關閉 Panorama

重新啟動選項可在不失誤的情況下重新啟動 Panorama。關閉將中斷系統並關閉系統電源。若要重新啟動 Panorama，請在關閉後，以手動方式拔掉系統電源線，然後重新接上。

STEP 1 | 選取 **Panorama** > **Setup**（設定） > **Operations**（操作）。

STEP 2 | 在 Device Operations（裝置操作）部分中，選取 **Reboot Panorama**（重新啟動 **Panorama**）或**Shutdown Panorama**（關閉 **Panorama**）。

© 2019 Palo Alto Networks, Inc.

設定 Panorama 密碼設定檔及複雜性

若要保護本機管理員帳戶，您可以定義當管理員變更或建立新密碼時，必須強制符合的密碼複雜性需求。不像密碼設定檔只能套用至個別帳戶，密碼複雜性規則不但可供防火牆全域使用，還能套用至所有密碼。

若要定期強制執行密碼更新，請建立密碼設定檔來定義密碼的有效期間。

STEP 1 | 進行最小密碼複雜性設定。

1. 選取 **Panorama** > **Setup**（設定）> **Management**（管理），再編輯 [最小密碼複雜性] 部分。
2. 選取 **Enabled**（已啟用）。
3. 定義 **Password Format Requirements**（密碼格式需求）。您可以強制規定密碼必須包含大寫、小寫、數字和特殊字元。
4. 若要防止在密碼中使用帳戶使用者名稱（或與名稱順序相反的字元），請選取 **Block Username Inclusion (including reversed)**（封鎖加入使用者名稱 (包含順序相反的字元)）。
5. 定義密碼 **Functionality Requirements**（功能需求）。

   如果已設定管理員的密碼設定檔，則密碼設定檔中定義的值將取代您已在此部分定義的值。

STEP 2 | 建立密碼設定檔。

您可視需要建立多個密碼設定檔，並將其套用至管理員帳戶以強制規範安全性。

1. 選取**Panorama** > **Password Profiles**（密碼設定檔），然後按一下 **Add**（新增）。
2. 輸入密碼設定檔的 **Name**（名稱）並定義下列選項：
   1. **Required Password Change Period**（需要變更密碼週期）—密碼必須變更的頻率，以天為單位。
   2. **Expiration Warning Period**（到期警告期間）—在到期之前，管理員收到密碼提醒的天數。
   3. **Post Expiration Grace Period**（到期後寬限期）—密碼到期後，管理員仍可登入系統的天數。
   4. **Post Expiration Admin Login Count**（到期後管理員登入次數）—密碼到期後，管理員可登入系統的次數。

Panorama 外掛程式

Panorama 可擴展外掛程式架構允許支援第三方整合外掛程式，如 VMware、NSX 和其他 Palo Alto Networks 產品，如 GlobalProtect 雲端服務。使用此模組化架構，您可以不需等待新的 PAN-OS 版本，即可利用新的功能。

您也可以從 Panorama 設定 VM-Series 外掛程式。VM-Series 外掛程式是可以與公共雲端環境（如 Google Cloud Platform (GCP)、Azure、AWS）以及私人雲端 Hypervisor（KVM、ESXi 等）整合的單外掛程式。VM-Series 外掛程式允許您從部署在公共雲端的 VM-Series 防火牆發佈度量。您可以使用 Panorama 為公共雲端設定 VM-Series 外掛程式設置，並將您的設定推送至您的受管理防火牆。

> 關於 Panorama 外掛程式
> VM-Series 外掛程式和 Panorama 外掛程式

關於 Panorama 外掛程式

Panorama 支援一個啟用以下外掛程式的整合和設定的可擴充外掛程式架構：

- **AWS**—AWS 外掛程式可讓您監控 AWS 上的 EC2 工作負載。透過外掛程式，您可以啟用 Panorama（執行 PAN-OS 8.1.3 和更新版本）與 AWS VPC 間的通訊，使 Panorama 能夠收集預先定義的屬性集（或中繼資料元件），作為您的 EC2 實例的標籤，以及在您的 Palo Alto Networks 防火牆上註冊資訊。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 VPC 內的所有資產一致地執行原則。
- **Azure**—Azure 外掛程式可讓您監控 Azure 公共雲端上的虛擬機器。透過外掛程式，您可以啟用 Panorama（執行 PAN-OS 8.1.6 和更新版本）與 Azure 訂閱間的通訊，使 Panorama 能夠收集預先定義的屬性集（或中繼資料元件），作為您的 Azure 虛擬設定的標籤，以及在您的 Palo Alto Networks 防火牆上註冊資訊。當您參考 動態位址群組 中的這些標籤，並將其與安全性原則規則進行比對時，您可以在訂閱時對在 VNet 內部署的所有資產一直強制執行該原則。
- **Cisco ACI**—Cisco ACI 外掛程式讓您可以在 Cisco ACI 網狀架構中監控您的端點。透過外掛程式，您可以啟用 Panorama（8.1.6 和更新版本）與 Cisco APIC 間的通訊，使 Panorama 能夠收集端點資訊，作為您的端點群組的標籤，以及在您的 Palo Alto Networks 防火牆上註冊資訊。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 Cisco ACI 網狀架構內的所有資產一致地執行原則。
- **Cisco TrustSec**— Cisco TrustSec 外掛程式讓您能夠監控 Cisco TrustSec 環境中的端點。透過外掛程式，您可以啟用 Panorama 與 Cisco pxGrid 伺服器之間的通訊，使 Panorama 能夠收集端點資訊，作為您的端點的標籤，以及在您的 Palo Alto Networks 防火牆上註冊資訊。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 Cisco TrustSec 環境內的所有資產一致地執行原則。
- 雲端服務—Cloud Services 外掛程式讓您能夠使用 Cortex Data Lake（Cortex 資料湖）及 Prisma Access。Cortex Data Lake（Cortex 資料湖）可解決操作上日誌記錄方面的挑戰，Prisma Access 雲端服務則會將安全性基礎設施擴展到遠端網路位置與行動工作者。
- 企業資料遺失防護 **(DLP)**— 企業資料遺失防護 (DLP) 是一組工具和程序，可幫助您保護敏感資料，以防被未經授權存取、誤用、擷取或共用。企業 DLP 透過雲端服務啟用，用於幫助您檢查內容和分析正確上下文中的資料，以便您能夠準確地識別敏感資料，並提供保護以防止發生意外。企業 DLP 在執行 PAN-OS 10.0.2 和更高版本的 Panorama 和受管理防火牆上受支援。
- **GCP**—讓您可以在 Google Kubernetes 引擎 (GKE) 叢集中 保證 Kubernetes 服務的安全 。為 Google 雲端平台 (GCP) 設定 Panorama 外掛程式，以連線至您的 GKE 叢集，並了解公開至網際網路的服務。
- **Interconnect**—Interconnect 外掛程式讓您可以 管理大規模防火牆部署。使用 Interconnect 外掛程式來設定兩層 Panorama 部署（在執行 PAN-OS 8.1.3 和更新版本的 Panorama 上），從而實現水平向外延展架構。透過 Interconnect 外掛程式，您可以為一個 Panorama 控制器部署多達 64 個 Panorama 節點，或 32 個 Panorama HA 配對，集中管理大量防火牆。
- **Nutanix**—用於 Nutanix 的 Panorama 外掛程式讓您可在 Nutanix 環境中監控 VM。以便您追蹤 Nutanix Prism Central 內的虛擬機器詳細目錄，從而一致地強制執行安全性原則，自動適應 Nutanix 環境中的變化。隨著虛擬機器的佈建、解除佈建及移動，此解決方案允許您收集 IP 位址及相關聯的屬性集（或中繼資料元素）作為標籤。然後，您可以使用這些標籤來定義 Dynamic Address Groups（動態位址群組）並在安全性原則中使用。用於 Nutanix 的 Panorama 外掛程式需要 Panorama 9.0.4 或更新版本。
- **SD-WAN**—軟體定義廣域網路 (SD-WAN) 外掛程式可讓您使用多個網際網路和專用服務建立一個動態的智慧型廣域網路，這有助於降低成本，並最大程度提升應用程式的品質和可用性。無需在路由器、防火牆、WAN 路徑控制器和WAN 最佳化程式等元件上使用昂貴且耗時的 MPLS 來將廣域網連線到網際網路，Palo Alto Networks 防火牆上的 SD-WAN 可為您提供價格優惠的網際網路服務，且所需設備更少。
- **VMware NSX**—VMware NSX 外掛程式支援 VMware NSX 上 VM-Series 防火牆與 VMware NSX 管理員間的整合。此整合允許您將 VM-Series 防火牆作為服務部署在 ESXi 伺服器的叢集上。
- **VMware vCenter**—用於 VMware vCenter 的 Panorama 外掛程式可讓您監控 vCenter 環境中的虛擬機器。此外掛程式可以擷取 vCenter 環境中虛擬機器 的 IP 位址並且將其轉換為標籤，您可以使用這些標籤透過動態位址群組來建立原則。

© 2019 Palo Alto Networks, Inc.

- 零接觸佈建—零接觸佈建 (ZTP) 旨在簡化及自動化 Panorama 上新防火牆的安裝。ZTP 允許網路管理員將受管理的防火牆直接運送至分公司且自動將防火牆新增至 Panorama，從而簡化防火牆的初始部署流程，這樣，企業在部署新防火牆時可以節省時間及資源。PAN-OS 9.1.3 和更新版本支援 ZTP。
- **IPS** 特徵碼轉換器—用於 Panorama 的 IPS 特徵碼轉換器外掛程式提供了一種自動化解決方案，用於將規則從第三方入侵預防系統（Snort 和 Suricata）轉換為自訂的 Palo Alto Networks 威脅特徵碼。然後，您可以在屬於所指定裝置群組的防火牆上註冊這些特徵碼，並使用它們在漏洞保護和反間諜軟體設定檔中強制執行原則。

您可以安裝多個外掛程式，並在單個 Panorama 執行個體上從多個來源擷取 IP 位址更新。這讓您能夠建立並強制執行一致的安全性原則，以跨多個雲端環境保護應用程式和工作負載。擷取的 IP 位址透過動態位址群組在安全性原則中使用；當您在環境中新增或移除工作負載時，Panorama 會註冊變更並將更新推送到防火牆。在 Panorama 上部署多個外掛程式時，必須仔細計劃裝置群組階層，以確保將更新正確地傳遞到防火牆。

請參閱 Palo Alto Networks 相容性矩陣 ，瞭解有關不同 外掛程式版本 和相容性資訊的詳情。

安裝 Panorama 外掛程式

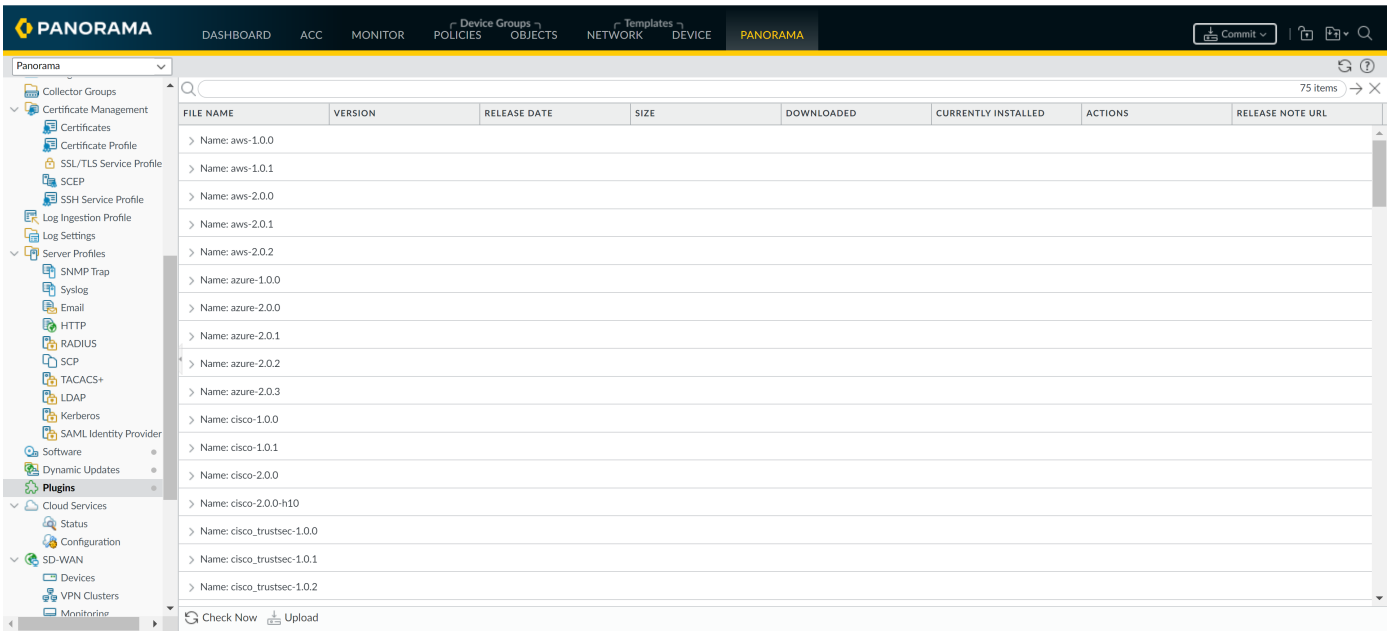
您可以在 Panorama 上安裝一個或多個可用的外掛程式，實現 GlobalProtect 雲端服務和 Cortex Data Lake（Cortex 資料湖）以及VMware NSX 的整合，或者監控 AWS 或 Azure 公共雲端上的虛擬機器。

對於雲端服務外掛程式，您必須在自訂支援入口網站啟動有效驗證碼並選取您想要傳送日誌的區域（美洲或歐洲）。

若您目前已有安裝的外掛程式版本，但想要 *Install*（安裝）外掛程式的新版本，則 *Panorama* 會取代目前安裝的版本。

STEP 1 | 下載外掛程式。

1. 選取**Panorama** > 外掛程式 。



2. 選取 **Check Now**（立即檢查）以擷取可用更新清單。
3. 選取 Action（動作）欄中的 **Download**（下載）以下載外掛程式。

   請參閱相容性矩陣，瞭解每個 Panorama 外掛程式支援的最低 PAN-OS 版本。

STEP 2 | 安裝外掛程式。

© 2019 Palo Alto Networks, Inc.

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。詳情請參閱安裝 VMware NSX 外掛程式或 雲端服務外掛程式。



第一次在 *Panoramas HA* 配對上安裝外掛程式時，請先將外掛程式安裝於被動端點，再安裝於主動端點。在被動端點上安裝外掛程式之後會轉換為非運作狀態。接著，在成功在主動端點安裝外掛程式後，被動端點會再轉為運作狀態。

© 2019 Palo Alto Networks, Inc.

VM-Series 外掛程式和 Panorama 外掛程式

VM-Series 外掛程式與各種 Panorama 外掛程式之間有何差異？

VM-Series 外掛程式適用於 VM-Series 防火牆，是可以與公共雲端環境（如 Google Cloud Platform (GCP)、Azure 和 AWS）以及私人雲端 Hypervisor（KVM、ESXi 等）整合的單一外掛程式。當您部署防火牆時，內建外掛程式會自動偵測已部署防火牆的虛擬環境，並載入必要的外掛程式元件讓您管理與該雲端環境的互動。例如，當您在 GCP 上部署 VM-Series 防火牆時，VM-Series 防火牆會載入可啟用 GCP 整合的外掛程式元件。其後，您可以使用 VM-Series 外掛程式在 GCP 上設定 VM-Series 防火牆，以將度量發佈至 Google Stackdriver Monitoring。同樣地，「Azure 上的 VM-Series 防火牆」的 VM-Series 外掛程式，可讓您設定防火牆以將度量發佈至 Azure Application Insights，或設定防火牆要作為 HA 配對所需的詳細資料。VM-Series 外掛程式會預先安裝在 VM-Series 防火牆上，您可加以升級或降級，但無法將其刪除。在 Panorama 上可以使用 VM-Series 外掛程式，但並不會預先安裝。如果您選擇使用 Panorama 來管理防火牆上的整合，請在 Panorama 上安裝 Azure 外掛程式，以對防火牆上的 VM-Series 外掛程式建立通訊。

Panorama 外掛程式對於硬體型防火牆與 VM-Series 防火牆均適用。Panorama 外掛程式是選用的，因此您可以在 Panorama 上予以新增、移除、重新安裝或升級。Panorama 外掛程式不會內建，且您必須安裝此外掛程式，才能與您所需的管理環境通訊。例如，您可以使用 Panorama 上的雲端服務外掛程式，啟用 Panorama/防火牆與 Cortex Data Lake 之間的設定。Panorama 上的 GCP 外掛程式可讓 Panorama 與您的 GCP 部署進行通訊，讓您在流量進入或離開部署於 Google Kubernetes Engine (GKE) 叢集中的服務時，都能保護流量。

在 Panorama 上安裝 VM-Series 外挂程式

要檢視和設定 VM-Series防火牆上部署的雲端整合，VM-Series外掛程式必須安裝在 Panorama 和 VM-Series防火牆上。外掛程式自動安裝在防火牆上，但您必須手動將外掛程式安裝至 Panorama，之後才可以推送組態至您的 裝置群組 。

*VM-Series*外掛程式支援所有雲端，因此升級可能不適用於您的 *VM-Series*防火牆。升級外掛程式之前，請查閱版本資訊。僅在有與您的雲端相關的變更時更新外掛程式。

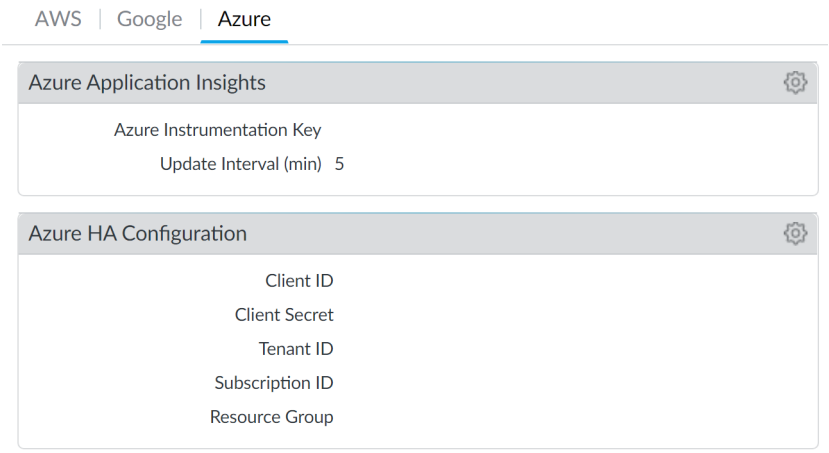
STEP 1 | 下載 VM-Series外掛程式。

1. 選擇 **Panorama** > **Plugins**（外掛程式） 並使用 **Check Now**（立即檢查）尋找新的外掛程式包。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）。

STEP 2 | 安裝 VM-Series外掛程式。

1. 按一下 Action（動作）欄中的 **Install**（安裝）。安裝完成時，Panorama 會通知您。
2. 要檢視外掛程式，選取 **Device**（裝置） > **VM-Series**（**VM-Series**）。
   - 如果您的防火牆安裝在私人雲端上，且 Hypervisor 或服務沒有整合，您將看到名為 VM-Series的頁籤和預設消息，`VM Series plugin infrastructure support is installed to allow the firewall's functionality to be enhanced in response to new features launched by hypervisor, or to meet new security needs`（已安裝 `VM-Series`外掛程式基礎結構支援，以允許根據 `Hypervisor` 啟動的新功能增強防火牆功能，或滿足新安全需要）。
   - 如果您的防火牆部署在公共雲端上，Panorama 顯示所有支援雲端的頁籤。

© 2019 Palo Alto Networks, Inc.



STEP 3 | （ 選用 ）儲存您的設定，並推送至您的受管理防火牆。

STEP 4 | （ 選用 ）在 VM-Series防火牆上，選取 **Device**（裝置） > **VM-Series**（**VM-Series**）。如果您為您的平台設定了整合，您將看到防火牆部署雲端的單頁籤。如果您沒有設定整合，您將看到關於 VM-Series外掛程式基礎結構的預設消息。

疑難排解

下列主題解決 Panorama™ 管理伺服器和專用日誌收集器的問題：

> 疑難排解 Panorama 系統問題
> 疑難排解儲存與連線問題
> 更換 RMA 防火牆
> 疑難排解提交失敗
> 疑難排解註冊或序號錯誤
> 疑難排解報告錯誤
> 疑難排解裝置管理授權錯誤
> 疑難排解自動復原防火牆組態
> 當 Panorama HA 對等關閉時，完成內容更新
> 檢視工作成功或失敗狀態
> 為受管理裝置測試原則比對和連線
> 從 Panorama 10.0 降級

疑難排解 Panorama 系統問題

- 產生 Panorama 診斷檔案
- 診斷 Panorama 暫停狀態
- 監控檔案系統完整性檢查
- 管理 Panorama 儲存軟體與內容更新
- 從 Panorama HA 部署中的腦分裂復原

產生 Panorama 診斷檔案

診斷檔案可協助監控系統的活動，及找出 Panorama 問題的可能原因。為了協助 Palo Alto Networks 技術支援疑難排解問題，支援代表可能會要求技術支援檔案。下列程序說明如何下載技術支援檔案，並將檔案上傳到您的支援案例。

STEP 1 | 選取 **Panorama** > **Support**（支援）並按一下 **Generate Tech Support File**（產生技術支援檔案）。

STEP 2 | 下載檔案並將檔案儲存至電腦。

STEP 3 | 在 Palo Alto Networks 客戶支援網站上，將檔案上傳到您的案例。

診斷 Panorama 暫停狀態

如果 Panorama 處於暫停狀態，請檢查下列狀況：

- 序號—確認每個 Panorama 虛擬設備上的序號是唯一的。如果使用相同的序號來建立 Panorama 的兩個或多個實例，則將暫停使用相同序號的所有實例。
- 模式—如果您在高可用性 (HA) 設定中部署 Panorama 虛擬設備，請確認兩個 HA 對等都是相同模式：Panorama 模式或傳統模式。
- **HA** 優先順序 - 確認已將一個對等上的 HA 優先順序設為主要，並將另一個對等上的 HA 優先順序設為次要。如果兩個端點具有一致的優先順序設定，則序號數值較高的 Panorama 端點將置於暫停狀態。
- **Panorama** 軟體版本 - 確認兩個 Panorama HA 對等都執行相同的 Panorama 軟體版本（主要和次要版本號碼）。

監控檔案系統完整性檢查

Panorama 會定期執行檔案系統完整性檢查 (FSCK)，以防止 Panorama 系統檔案損毀。此檢查會在重新啟動八次之後，或在上次執行 FSCK 90 天之後重新啟動時發生。如果 Panorama 正在執行 FSCK，網頁介面和 Secure Shell (SSH) 登入畫面將顯示警告，指出 FSCK 正在進行中。在此程序完成後您才能登入。完成此程序的時間因儲存系統的大小而有所不同；視大小而定，可能會花費幾小時的時間才能讓您重新登入 Panorama。

在 Panorama 或受管理防火牆上成功下載並安裝 PAN-OS 軟體更新後，作為軟體安裝程序的一部分，Panorama 或受管理防火牆會重新啟動，在此之後，會對軟體更新進行驗證，以確保 PAN-OS 軟體的完整性。這樣可確保現在執行的軟體更新已知良好，且 Panorama 或受管理防火牆不會因遠端或實體漏洞而受到危害。

若要檢視 FSCK 上的進度，請設定主控台來存取 Panorama 及檢視狀態。

© 2019 Palo Alto Networks, Inc.

管理 Panorama 儲存軟體與內容更新

您可以安裝 Panorama 的內容與軟體更新和使用 Panorama 將更新部署至防火牆、日誌收集器和 WildFire 設備。您無法在 Panorama 上設定儲存更新的可用空間量。當所配置儲存空間的使用容量達到 90% 時，Panorama 會提醒您釋出空間（刪除儲存的更新）來容納新的下載或上傳項目。更新數目上限為全域設定，會套用到 Panorama 儲存的所有更新。您必須存取 CLI 以進行此設定。預設值是各類型的兩個更新。

- 修改各類型更新的數目上限。

  存取 Panorama CLI 並輸入下列內容，其中 *<number>* 可以是 2 至 64 的值：

  ```
  > set max-num-images count <number>
  ```

- 檢視 Panorama 目前儲存的更新數。

  輸入：

  ```
  > show max-num-images
  ```

- 使用網頁介面刪除更新，為在 Panorama 上留出空間。
  1. 選取要刪除的更新類型：
     - 防火牆或日誌收集器更新：

       PAN-OS/Panorama 軟體映像 —選取 **Panorama** > **Device Deployment**（裝置部署）> **Software**（軟體）。

       GlobalProtect™ 代理程式/應用程式軟體更新 —選取 **Panorama** > **Device Deployment**（裝置部署）> **GlobalProtect Client**（**GlobalProtect** 用戶端）。

       內容更新 —選取 **Panorama** > **Device Deployment**（裝置部署）> **Dynamic Updates**（動態更新）。
     - Panorama 軟體映像 — 選取 **Panorama** > **Software**（軟體）。
     - Panorama 內容更新 — 選取 **Panorama** > **Dynamic Updates**（動態更新）。
  2. 按一下映像或更新最右欄內的 **X** 圖示。

- 使用 CLI 刪除更新，為在 Panorama 上留出空間。

  若要依版本刪除軟體映像：

  ```
  > delete software version <version_number>
  ```

  刪除內容更新：

  ```
  > delete content update <filename>
  ```

從 Panorama HA 部署中的腦分裂復原

當 Panorama 已設定為高可用性 (HA) 設定時，受管理的防火牆會同時連線至主動與被動的 Panorama HA 端點。一旦主動與被動 Panorama 端點之間的連線失敗，則在被動 Panorama 接管成為主動端點之前，會先檢查是否有任何防火牆同時連線至主動與被動端點。只要有一個防火牆同時連線至這兩個端點，故障復原就不會觸發。

© 2019 Palo Alto Networks, Inc.

在極罕見的狀況下，如有一組防火牆連線至主動端點，而另一組防火牆連線至被動端點，且沒有任何一個防火牆同時連線至這兩個端點時，會觸發故障復原，這稱做「腦分裂」。下列狀況會隨著「腦分裂」一同發生：

- Panorama 端點無法感知另一個端點的狀態或 HA 角色。
- Panorama 端點成為主動端點，並管理唯一一組的防火牆。

若要解決 「腦分裂」問題，請為您的網路問題偵錯，並還原 Panorama HA 端點之間的連線。

然而，如果您需要變更防火牆的設定，但不需還原端點之間的連線，以下有一些方法可供選擇：

- 在兩 Panorama 端點上手動新增相同的設定變更。這個方法能夠在重新建立連結時，確保兩者的設定保持同步。
- 如果您只需要在一個 Panorama 位置新增/變更設定，請在 Panorama 端點之間的連結重新建立時進行變更，並讓同步處理設定（務必從要進行變更的端點啟動同步處理）。若要同步端點，選取 **Dashboard**（儀錶盤）頁籤，然後按一下高可用性 widget 中的 **Sync to peer**（同步至端點）連結。
- 如果您只需要為每個位置的已連線防火牆新增/變更設定，則可以在 Panorama 各端點獨立地變更設定。由於端點的連線中斷，因此不會有複寫，且每個端點現在會有完全不同的設定檔（這些設定檔未維持同步）。因此，為確保不會在連線還原時遺失各個端點上的設定，請勿允許設定自動重新同步處理。若要解決此問題，請匯出 Panorama 各端點的設定，並使用外部的區分與合併工具手動合併變更。在變更整合後，您可以在 Panorama 上匯入主要的統一設定檔，再將其與該端點同步處理。

© 2019 Palo Alto Networks, Inc.

疑難排解儲存與連線問題

僅 *M-Series* 設備支援移轉日誌。請參閱 將 Panorama 虛擬設備移轉至不同的 Hypervisor 以移轉 *Panorama* 虛擬設備。

- 驗證 Panorama 連接埠的使用
- 解決收集器群組的零日誌儲存容量問題
- 更換 M-Series 設備的故障磁碟
- 更換 ESXi 伺服器上的虛擬磁碟
- 更換 vCloud Air 上的虛擬磁碟
- 移轉日誌至日誌收集器模式內的新 M-Series 設備
- 移轉日誌至 Panorama 模式內的新 M-Series 設備
- 移轉日誌至高可用性 Panorama 模式內的新 M-Series 設備型號
- 移轉日誌至高可用性 Panorama 模式內的新 M-Series 設備型號
- 非 HA Panorama 故障/ RMA 後轉移日誌收集器
- 重新產生 M-Series 設備 RAID 配對的中繼資料
- 檢視日誌查詢作業

驗證 Panorama 連接埠的使用

為確保 Panorama 能與受管理的防火牆、日誌收集器、WildFire 設備和設備叢集，以及其高可用性 (HA) 對等通訊，請使用下表驗證您必須在網路上開啟的連接埠。Panorama 使用 TCP 通訊協定進行連接埠通訊。

依預設，Panorama 會使用管理 (MGT) 介面來管理裝置（防火牆、日誌收集器，以及 WildFire 設備和設備叢集）、收集日誌、與收集器群組通訊，以及將軟體和內容更新部署至裝置。不過，在執行 Panorama 6.1 至 7.1 的 M-600、M-500 或 M-200 設備上，您可以選擇將日誌收集和收集器群組通訊功能指派給 Eth1 或 Eth2 介面。如果設備執行 Panorama 8.0 或更高版本，則可以將任何功能指派給 M-600、M-500 或 M-200 設備上的 Eth1、Eth2、Eth3、Eth4 或 Eth5 介面。無論您將何種功能指派給何種介面，皆會套用下表中所列的連接埠。例如，如果您將日誌收集器指派給 MGT，並將收集器群組通訊指派給 Eth2，則 MGT 將使用連接埠 3978，且 Eth2 將使用連接埠 28270。（Panorama 虛擬設備對上述所有的功能只會使用 MGT 介面。）

與系統通訊並建立連線方向	用於 Panorama 5.x 的連接埠	用於 Panorama 6.x 至 7.x 的連接埠	用於 Panorama 8.x 和更新版本的連接埠	說明
Panorama 與 Panorama (HA) 方向：端點會各自啟動對其他端點的連線	28	28	28	啟用加密時，用於 HA 連線與同步。 用於收集器群組中日誌收集器之間為了散佈日誌進行的通訊。
Panorama 與 Panorama (HA) 方向：端點會各自啟動對其他端點的連線	28769 與 28260 (5.1) 28769 與 49160 (5.0)	28260 與 28769	28260 與 28769	未啟用加密時，用於 HA 連線與同步。

© 2019 Palo Alto Networks, Inc.

與系統通訊並建立連線方向	用於 Panorama 5.x 的連接埠	用於 Panorama 6.x 至 7.x 的連接埠	用於 Panorama 8.x 和更新版本的連接埠	說明
Panorama 與受管理的防火牆 方向：由防火牆啟動	3978	3978	3978	將日誌從防火牆轉送至 Panorama，以及將設定變更從 Panorama 推送至受管理防火牆的雙向連線。會透過相同的連線傳送內容切換命令。
Panorama 與日誌收集器 方向：由日誌收集器啟動	3978	3978	3978	用於管理及日誌收集/報告。 用於 Panorama 模式的 Panorama 上本機日誌收集器之間的通訊，以及用於分散式日誌收集部署中與日誌收集器通訊。
Panorama 和受管理的裝置（防火牆、日誌收集器，以及 WildFire 設備和設備叢集） 方向： • 由執行 PAN-OS 8.x 或更新版本的受管理裝置啟動。 • 由 Panorama 針對執行 PAN-OS 7.x 或更舊版本的裝置啟動。	3978	3978	28443	執行 PAN-OS 8.x 或更新版本的裝置使用連接埠 28443，從 Panorama 擷取軟體和內容更新檔案。 執行 7.x 或更舊版本的裝置不會從 Panorama 擷取更新檔案；Panorama 會透過連接埠 3978 將更新檔案推送至裝置。 受管理的 WildFire 設備上需要安裝 PAN-OS 8.0.1 或更新版本，才能支援由 Panorama 管理 WildFire 設備和設備叢集。建議 Panorama 執行 8.0.1 或更新版本來管理 WildFire 設備和設備叢集。
日誌收集器對日誌收集器 方向：每個日誌收集器會各自對收集器群組中的其他日誌收集器啟動連線	49190	28270	28270	用於日誌收集器之間的分散區域與所有二進位資料。
Panorama to Cortex Data Lake（Panorama 至 Cortex 資料湖）	NA	NA	444 *8.0.5* 版及更新版本。	對 Cortex Data Lake（Cortex 資料湖）設定安全通訊通道。 受管理的防火牆使用連接埠 3978，以便 與 Cortex Data Lake（Cortex 資料湖）通訊。

© 2019 Palo Alto Networks, Inc.

解決收集器群組的零日誌儲存容量問題

若未針對在日誌收集器中記錄日誌啟用磁碟配對，則收集器群組的日誌儲存容量可能顯示為 0 MB。若要啟用磁碟配對，請針對收集器群組中的每個日誌收集器，執行下列步驟。

STEP 1 | 新增 RAID 磁碟配對。

1. 選取 **Panorama** > **Managed Collectors**（受管理的收集器），然後按一下收集器名稱。
2. 選取 **Disks**（磁碟），**Add**（新增）每一個 RAID 磁碟配對，然後按一下 **OK**（確定）。

STEP 2 | 將變更提交至 Panorama，並將變更推送至收集器群組。

1. 選取 **Commit**（提交）> **Commit and Push**（提交並推送），然後在 Push Scope（推送範圍）中 **Edit Selections**（編輯選擇）。
2. 選取 **Collector Groups**（收集器群組），並選取您修改的收集器群組，然後按一下 **OK**（確定）。
3. **Commit and Push**（提交並推送）您的變更。

STEP 3 | 驗證日誌收集器和磁碟配對的狀態。

1. 選取 **Panorama** > **Managed Collectors**（受管理的收集器），確認每一個日誌收集器的設定是否已與 Panorama 同步。

   Configuration Status（組態狀態）欄應該顯示 **In Sync**（同步），Run Time Status（執行階段狀態）欄應該顯示 **connected**（已連線）。
2. 針對每一個日誌收集器，按一下最後一欄中的 **Statistics**（統計資料），確認磁碟配對 **Enabled**（已啟用）並且 **Available**（可用）。

更換 M-Series 設備的故障磁碟

如果 M-Series 設備上的磁碟故障，您必須更換該磁碟並在 RAID 1 陣列中重新設定磁碟。詳情請參閱 M-Series 設備硬體參考指南。

更換 ESXi 伺服器上的虛擬磁碟

將虛擬磁碟新增至 VMware ESXi 伺服器上執行的 Panorama 虛擬設備後，即無法調整該磁碟的大小。由於傳統模式的 Panorama 虛擬設備僅允許一個日誌儲存位置，您必須如下更換虛擬磁碟，才能修改日誌儲存容量。在 Panorama 模式中，您可以直接新增另一個磁碟（最多 12 個）以 擴展 Panorama 虛擬設備的日誌儲存容量。

在傳統模式的 *Panorama* 虛擬設備上，更換現有磁碟時，磁碟上的日誌會遺失。關於保留現有日誌的選項，請參閱 在傳統模式的 Panorama 虛擬設備上新增儲存空間時保留現有日誌。

STEP 1 | 移除舊的虛擬磁碟。

1. 存取 VMware vSphere 用戶端並選取 **Virtual Machines**（虛擬電腦）頁籤。
2. 右鍵按一下 Panorama 虛擬設備並選取 **Power**（電源）> **Power Off**（關閉電源）。
3. 右鍵按一下 Panorama 虛擬設備並選取 **Edit Settings**（編輯設定）。
4. 在 **Hardware**（硬體）頁籤中選取虛擬磁碟，然後按一下 **Remove**（移除）。
5. 選取一個移除選項，然後按一下 **OK**（確定）。

STEP 2 | 新增新的虛擬磁碟。

1. 新增虛擬磁碟至 ESXi 伺服器上的 Panorama。

   在 ESXi 5.5 或更新版本上運行的 Panorama 支援多達 8TB 的虛擬磁碟。在較早 ESXi 版本上運行的 Panorama 支援最多 2TB 的虛擬磁碟。

© 2019 Palo Alto Networks, Inc.

2. 在 vSphere 用戶端中，右鍵按一下 Panorama 虛擬設備並選取 **Power**（電源）> **Power On**（開啟電源）。

   重新啟動程序可能會耗費數分鐘，`cache data unavailable`（無法使用快取資料）訊息將顯示。

STEP 3 | 確認修改的日誌儲存容量正確。

1. 登入 Panorama 虛擬設備。
2. 選取 **Panorama** > **Setup**（設定）> **Management**（管理），然後確認 [日誌與報告設定] 部分的 [日誌儲存] 欄位中是否正確顯示修改後的日誌儲存容量。

更換 vCloud Air 上的虛擬磁碟

將虛擬磁碟新增至 VMware vCloud Air 上執行的 Panorama 虛擬設備後，即無法調整該磁碟的大小。由於傳統模式的 Panorama 虛擬設備僅允許一個日誌儲存位置，您必須如下更換虛擬磁碟，才能修改日誌儲存容量。在 Panorama 模式中，您可以直接新增虛擬磁碟至 vCloud Air 上的 Panorama（最多 12 個）。

在傳統模式的 *Panorama* 虛擬設備上，更換現有磁碟時，磁碟上的日誌會遺失。關於保留現有日誌的選項，請參閱 在傳統模式的 Panorama 虛擬設備上新增儲存空間時保留現有日誌。

STEP 1 | 移除舊的虛擬磁碟。

1. 存取 vCloud Air web 主控台並選取您的 **Virtual Private Cloud OnDemand**（虛擬私人雲 **OnDemand**）地區。
2. 在 **Virtual Machines**（虛擬機器）頁籤內，選取 Panorama 虛擬設備。
3. 選取 **Actions**（動作）> **Edit Resources**（編輯資源）。
4. 針對您正在移除的虛擬磁碟，按一下 **x**。

STEP 2 | 新增新的虛擬磁碟。

1. **Add another disk**（新增其他虛擬磁碟）。
2. 將 **Storage**（儲存空間）設為 8TB 並指定儲存層（**Standard**（標準）或 **SSD-Accelerated**（**SSD** 加速）。
3. **Save**（儲存）變更。

STEP 3 | 重新啟動 Panorama。

1. 登入 Panorama 虛擬設備。
2. 選取 **Panorama** > **Setup**（設定）> **Operations**（操作），再按一下 **Reboot Panorama**（重新啟動 **Panorama**）。

STEP 4 | 確認修改的日誌儲存容量正確。

1. 重新開機後，登入 Panorama 虛擬設備。
2. 選取 **Panorama** > **Setup**（設定）> **Management**（管理），然後確認 [日誌與報告設定] 部分的 [日誌儲存] 欄位中是否正確顯示修改後的日誌儲存容量。

移轉日誌至日誌收集器模式內的新 M-Series 設備

如果您需要更換日誌收集器模式的 M-600、M-500、M-200 或 M-100 設備（專用日誌收集器），您可以將其 RAID 磁碟移至新的 M-Series 設備，以移轉它從防火牆收集的日誌。此程序讓您可以在 M-Series 設備上發生系統故障後復原日誌，或在硬體升級過程中移轉日誌（從 M-100 設備至 M-500 設備）。

不支援藉由將日誌記錄磁碟從任何 M-Series 設備移除並載入至 *M-600 Panorama* 管理伺服器來移轉日誌。若要移轉至 *M-600* 設備，請設定 M-600 設備、設定日誌轉送至新 M-600 設備及將 M-Series 設備設定為受管理的日誌收集器，直至您不再需要取 *M-Series* 設備上所儲存的日誌。

© 2019 Palo Alto Networks, Inc.

STEP 1 | 對將作為專用日誌收集器的 M-Series 設備執行初始設定。

1. 在機架中安裝 M-Series 設備。請參閱 M-Series 設備硬體參考指南的指示。
2. 執行 M-Series 設備的初始設定。

   在設定介面時，僅設定管理 *(MGT)* 介面。切換至日誌收集器模式（稍後在此程序中）會移除其他任何介面的設定。如果日誌收集器*ishiyong MGT* 以外的其他介面，在設定日誌收集器時新增（請參閱第 2 步）。
3. 註冊 Panorama。
4. 購買並啟動 Panorama 支援授權，或只有在新的 M-Series 設備與舊的 M-Series 設備為相同硬體型號時，才如下轉移授權。如果新的 M-Series 設備與舊的 M-Series 設備是不同型號，您必須購買新的授權。
   1. 登入 Palo Alto Networks 客戶支援網站。
   2. 選取 **Assets**（資產）頁籤並按一下 **Spares**（備用）連結。
   3. 按一下新 M-Series 設備的序號。
   4. 按一下 **Transfer Licenses**（傳輸授權）。
   5. **Select**（選取）舊 M-Series 設備並按一下 **Submit**（提交）。
5. 啟動防火牆管理授權。如果您從 M-100 設備轉移至 M-500 設備，輸入與轉移授權相關聯的授權碼。
6. 安裝 Panorama 的內容與軟體更新。如需瞭解軟體版本的重要詳細資訊，請參閱 Panorama、日誌收集器、防火牆和 WildFire 版本相容性。
7. 從 Panorama 模式切換至日誌收集器模式：
   1. 存取日誌收集器 CLI 並切換至日誌收集器模式：

      ```
      > request system system-mode logger
      ```
   2. 輸入 **Y** 以確認模式變更。M-Series 設備重新啟動。重新啟動會終止終端機模擬軟體的工作階段並重新連線至 M-Series 設備以顯示 Panorama 登入提示。

      如果您看到 ***CMS Login***（*CMS* 登入）提示，請按下 *Enter*，無須鍵入使用者名稱或密碼。
8. 使用日誌收集器 CLI 啟用日誌收集器和 Panorama 管理伺服器之間的連線。<Ipaddress1> 用於主要 Panorama 的 MGT 介面，<IPaddress2> 用於次要 Panorama 的 MGT 介面。

```
> configure
# set deviceconfig system panorama-server <IPaddress1> panorama-server-2
 <IPaddress2>
# commit
# exit
```

STEP 2 | 在 Panorama 管理伺服器上，新增新日誌收集器作為受管理的收集器。

對於需要序號的命令步驟，您必須輸入整個序號；按下 *Tab* 鍵不會完成部分序列號填寫。

1. 使用 Panorama 網頁介面或使用下列 CLI 命令，將日誌收集器設定為受管理的收集器：

```
> configure
# set log-collector <LC_serial_number> deviceconfig system hostname
 <LC_hostname>
# exit
```


© 2019 Palo Alto Networks, Inc.

如果舊日誌收集器將 *MGT* 介面以外的介面用於日誌收集和收集器群組通訊，當您將其設定為受管理的收集器 時，必須在新日誌收集器上定義這些介面（*Panorama* > *Managed Collectors*（受管理的收集器）> *Interfaces*（介面））。

2. 確認日誌收集器連線至 Panorama，且其磁碟配對狀態為有/可用。

```
> show log-collector serial-number <log-collector_SN>
```

磁碟配對在還原程序的這個階段將顯示為 Disabled（停用）。

3. 將您的變更提交至 Panorama。此時還不要將變更提交至收集器群組。

```
> configure
# commit
# exit
```

STEP 3 | 將 RAID 磁碟從舊的日誌收集器中移除。

1. 按下電源按鈕，直至系統關機，關閉舊日誌收集器。
2. 移除磁碟配對。詳情請參閱 M-Series 設備硬體參考指南中的磁碟更換程序。

STEP 4 | 準備進行磁碟移轉。

各磁碟配對產生中繼資料時均會重新建立索引。因此，此程序視資料大小而定，可能需要較長的時間完成。若要加速程序，您可以啟動多個 *CLI* 工作階段並在各工作階段中執行中繼資料重新產生的命令，為每個配對同時完成程序。詳細資訊，請參閱重新產生 M-Series 設備 RAID 配對的中繼資料。

1. 將磁碟插入新的日誌收集器。詳情請參閱 M-Series 設備硬體參考指南中的磁碟更換程序。

M-100 設備的磁碟載體與 *M-500* 設備的不相容。由此，當在這類硬體型號之間轉移時，您必須從舊載體上擰鬆各磁碟，並在將磁碟插入新設備之前，將磁碟插入新載體。

您必須保留磁碟配對關聯。儘管您可以將舊設備 A1/A2 槽的磁碟配對裝入新設備的 B1/B2 槽，您必須將磁碟放在相同的槽內；否則，Panorama 可能無法順利恢復資料。

2. 透過執行下列各配對的 CLI 命令，啟用磁碟配對：

```
> request system raid add <slot> force no-format
```

例如：

```
> request system raid add A1 force no-format
> request system raid add A2 force no-format
```

force 和**no-format** 引數是必要的。**force** 引數將磁碟配對與新日誌收集器關聯。**no-format** 引數可防止磁碟機的重新格式化，並保留磁碟上儲存的日誌。

3. 為每個磁碟配對產生中繼資料。

```
> request metadata-regenerate slot <slot_number>
```

例如：

© 2019 Palo Alto Networks, Inc.

```
> request metadata-regenerate slot 1
```

STEP 5 | 將沒有磁碟的日誌收集器新增至收集器群組。

從這裡開始，只需要提交以便在 *Panorama* 和日誌收集器上完成移轉程序。暫停其他任何變更。

1. 存取 Panorama CLI。
2. 覆寫 Panorama 限制，以允許將沒有磁碟的日誌收集器新增至收集器群組：**request log-migration-set-start**

STEP 6 | 移轉日誌。

您必須為此步驟使用 *Panorama CLI*，而非 *Web* 介面。

您必須指派新日誌收集器至包含舊日誌收集器的收集器群組。

1. 指派新日誌收集器至收集器群組並將您的變更提交至 Panorama。

```
> configure
# set log-collector-group <collector_group_name> logfwd-setting collectors
 <new_LC_serial_number>
# commit
# exit
```

2. 對於各磁碟配對，從舊日誌收集器轉移日誌至新日誌收集器，並連結磁碟配對至新日誌收集器。

```
> request log-migration from <old_LC_serial_number> old-disk-pair
 <log_disk_pair> to <new_LC_serial_number> new-disk-pair <log_disk_pair>
```

例如：

```
> request log-migration from 003001000010 old-disk-pair A to 00300100038
 new-disk-pair A
```

STEP 7 | 重新設定收集器群組。

1. 使用 Web 介面指派新日誌收集器至防火牆，由新防火牆轉送日誌（**Panorama** > **Collector Groups**（收集器群組）> **Device Log Forwarding**（設備日誌轉送））。為新日誌收集器提供與舊日誌收集器在防火牆偏好設定清單中相同的優先級。

您無法使用 *CLI* 來變更防火牆偏好設定清單的優先順序指派。

2. 將舊的日誌收集器從收集器群組中刪除。

```
> configure
# delete log-collector-group <group_name> logfwd-setting collectors
 <old_LC_serial_number>
```

例如：

© 2019 Palo Alto Networks, Inc.

```
# delete log-collector-group DC-Collector-Group logfwd-setting collectors
 003001000010
```

3. 刪除 Panorama 組態中舊的日誌收集器，並將您的變更提交至 Panorama。

```
# delete log-collector <old_LC_serial_number>
# commit
# exit
```

4. 提交收集器群組變更，讓受管理的防火牆能夠將日誌傳送到新的日誌收集器。

```
> commit-all log-collector-config log-collector-
group <collector_group_name>
```

例如：

```
> commit-all log-collector-config log-collector-group DC-Collector-Group
```

STEP 8 | 在新的專用日誌收集器上產生新的金鑰。

需要此命令才能將新的日誌收集器新增至收集器群組，而且只能對要更換的日誌收集器的收集器群組執行此命令。此步驟會刪除現有 *RSA* 金鑰，還可讓 *Panorama* 建立新的 *RSA* 金鑰。

1. 存取 Panorama CLI。
2. 在新的日誌收集器上刪除所有 RSA 金鑰：

   request logdb update-collector-group-after-replace collector-group *<collector-group-name>*

   程序可能需要 10 分鐘才會完成。

STEP 9 | 確認收集器群組中所有日誌收集器的 SearchEngine Status 為 Active。

在收集器群組中所有日誌收集器的 *SearchEngine Status* 成為 *Active* 之前，請勿繼續。這會導致從要更換的日誌收集器中清除日誌。

1. 存取 Panorama CLI。
2. 在以下任一位置執行下列命令，以顯示日誌收集器詳細資料：
   - 所有日誌收集器的 Panorama 上：

     show log-collector all

     或者，您可以在每個專用日誌收集器上執行下列命令：

     ```
     show log-collector detail
     ```

3. 確認 SearchEngine Status 為 Active。

```
Redistribution status:       none
```

```
Last commit-all: commit succeeded, current ring version 1
```


© 2019 Palo Alto Networks, Inc.

```
SearchEngine status:     Active
```

```
md5sum 4e5055a359f7662fab8f8c4f57e24525 updated at 2017/06/14 09:58:19
```

STEP 10 | 在新的日誌收集器上，以新的日誌收集器序號取代前一個日誌收集器序號。

您必須以新的日誌收集器序號取代舊的日誌收集器序號，新的日誌收集器才不會遇到清除問題，而導致日誌收集器在需要時無法從移轉的日誌中清除舊資料。

1. 存取日誌收集器 CLI。
2. 以新的日誌收集器序號取代舊的日誌收集器序號：

   request log-migration-update-logger from *<old-log-collector-serial-number>* to *<new-log-collector-serial-number>*

移轉日誌至 Panorama 模式內的新 M-Series 設備

如果您需要更換 Panorama 模式（Panorama 管理伺服器）的 M-600、M-500、M-200 或 M-100 設備，您可以將其 RAID 磁碟移至新的 M-Series 設備，以移轉它從防火牆收集的日誌。移動磁碟可以讓您可以在 M-Series 設備上的系統發生故障後，恢復日誌或將日誌作為硬體升級的一部分進行移轉（從 M-100 設備移轉至 M-500 設備）。

不支援藉由將日誌記錄磁碟從任何 M-Series 設備移除並載入至 *M-600 Panorama* 管理伺服器來移轉日誌。若要移轉至 *M-600* 設備，請設定 M-600 設備、設定日誌轉送至新 M-600 設備及將 M-Series 設備設定為受管理的日誌收集器，直至您不再需要取 *M-Series* 設備上所儲存的日誌。

此移轉程序涵蓋了下列案例：用收集器群組中的受管理收集器（日誌收集器）取代非 HA 設定的單一 M-Series 設備。

STEP 1 | 轉送舊 M-Series 設備 SSD 上的任何日誌至您想要保留它們的外部目的地。

SSD 儲存 Panorama 和日誌收集器產生的系統和設定日誌。您無法在 M-Series 設備之間移動 SSD。

設定日誌從 Panorama 轉送至外部目的地。

STEP 2 | 從停止運作的 Panorama 模式的 M-Series 設備匯出 Panorama 組態。

1. 登入 Panorama 設備，然後選取 **Panorama** > **Setup**（設定）> **Operations**（操作）。
2. 按一下 **Save named Panorama configuration snapshot**（儲存具名 **Panorama** 組態快照），輸入 **Name**（名稱）以識別設定，然後按一下 **OK**（確定）。
3. 按一下 **Export named Panorama configuration snapshot**（匯出具名 **Panorama** 組態快照），選取您剛儲存的設定 **Name**（名稱），然後按一下 **OK**（確定）。Panorama 以 XML 檔案格式匯出設定至您的用戶端系統。

STEP 3 | 將 RAID 磁碟從舊 M-Series 設備中移除。

1. 按下電源按鈕，直至系統關機，關閉舊 M-Series 設備。
2. 移除磁碟配對。詳情請參閱 M-Series 設備硬體參考指南中的磁碟更換程序。

STEP 4 | 執行新 M-Series 設備的初始設定。

1. 在機架中安裝 M-Series 設備。請參閱 M-Series 設備硬體參考指南的指示。
2. 執行 M-Series 設備的初始設定。
3. 註冊 Panorama。

© 2019 Palo Alto Networks, Inc.

4. 購買並啟動 Panorama 支援授權，或只有在新的 M-Series 設備與舊的 M-Series 設備為相同硬體型號時，才如下轉移授權。如果新的 M-Series 設備與舊的 M-Series 設備是不同型號，您必須購買新的授權。
   1. 登入 Palo Alto Networks 客戶支援網站。
   2. 選取 **Assets**（資產）頁籤並按一下 **Spares**（備用）連結。
   3. 按一下新 M-Series 設備的序號。
   4. 按一下 **Transfer Licenses**（傳輸授權）。
   5. **Select**（選取）舊 M-Series 設備並按一下 **Submit**（提交）。
5. 啟動防火牆管理授權。如果您從 M-100 設備轉移至 M-500 設備，輸入與轉移授權相關聯的授權碼。
6. 安裝 Panorama 的內容與軟體更新。如需瞭解軟體版本的重要詳細資訊，請參閱 Panorama、日誌收集器、防火牆和 WildFire 版本相容性。

STEP 5 | 將從停止運作的 M-Series 設備匯出的 Panorama 組態快照載入 Panorama 模式的新 M-Series 設備。

1. 登入 Panorama 網頁介面 在新的 M-Series 設備上，選取 **Panorama** > **Setup**（設定）> **Operations**（操作）。
2. 按一下 **Import named Panorama configuration snapshot**（匯入具名 **Panorama** 組態快照），**Browse**（瀏覽）至您從停止運作的 M-Series 設備匯出的組態檔案，然後按一下 **OK**（確定）。
3. 按一下 **Load named Panorama configuration snapshot**（載入具名 **Panorama** 組態快照），選取您剛匯入的設定 **Name**（名稱），選取 **Decryption Key**（解密金鑰）（Panorama 主要金鑰），然後按一下 **OK**（確定）。Panorama 透過載入的設定覆寫其當前應徵者設定。Panorama 顯示載入設定檔時所發生的任何錯誤。如果發生錯誤，請將錯誤儲存至本機檔案。解決各錯誤，確保轉移設定有效。

   若要取代 *RMA Panorama*，請確保在載入具名 *Panorama* 組態快照時 *Retain Rule UUIDs*（保留規則 *UUID*）。如果沒有選取此選項，*Panorama* 將從組態快照中移除所有先前的規則 *UUID*，並在 *Panorama* 上為規則指定新的 *UUID*，這表示其不會保留與先前 *UUID* 相關的資訊，例如原則規則命中數。
4. 根據需要執行任何額外組態變更。

   如果舊的 *M-Series* 設備將 *MGT* 介面以外的介面用於 *Panorama* 服務（例如日誌收集），則對於新的 *M-Series* 設備，您必須 在初始設定期間定義這些介面（*Panorama* > *Setup*（設定）> *Interfaces*（介面））。
5. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Validate Commit**（驗證提交）。繼續前解決任何錯誤。
6. **Commit**（提交）您對 Panorama 組態所做的變更。

STEP 6 | 將磁碟插入新的 M-Series 設備。詳情請參閱 M-Series 設備硬體參考指南中的磁碟更換程序。

M-100 設備的磁碟載體與 *M-500* 設備的不相容。由此，當在這類硬體型號之間轉移時，您必須從舊載體上擰鬆各磁碟，並在將磁碟插入新設備之前，將磁碟插入新載體。

您必須保留磁碟配對關聯。儘管您可以將舊設備 A1/A2 槽的磁碟配對裝入新設備的 B1/B2 槽，您必須將磁碟放在相同的槽內；否則，Panorama 可能無法順利恢復資料。

STEP 7 | 聯絡 Palo Alto Networks 客戶支援，將日誌收集器群組中繼資料從停止運作的 M-Series 設備複製到新的 M-Series 設備，然後重新啟動 mgmtsrvr 程序。

STEP 8 | 如果 M-Series 設備屬於收集器群組，請確認解除的 M-Series 設備序號仍屬於正確的收集器群組：

```
debug log-collector-group show name <Log Collector Group name>
```


© 2019 Palo Alto Networks, Inc.

若停止運作的 M-Series 設備序號不再屬於正確的收集器群組，則表示之前步驟未正確複製技術支援資料夾。請再次聯絡 Palo Alto Networks 客戶支援，將技術支援資料夾複製到正確位置。

STEP 9 | 準備進行磁碟移轉。



各磁碟配對產生中繼資料時均會重新建立索引。因此，此程序視資料大小而定，可能需要較長的時間完成。若要加速程序，您可以啟動多個 *CLI* 工作階段並在各工作階段中執行中繼資料重新產生的命令，為每個配對同時完成程序。詳細資訊，請參閱重新產生 M-Series 設備 RAID 配對的中繼資料。

1. 將磁碟插入新的 M-Series 設備。詳情請參閱 M-Series 設備硬體參考指南中的磁碟更換程序。

   M-100 設備的磁碟載體與 *M-500* 設備的不相容。由此，當在這類硬體型號之間轉移時，您必須從舊載體上擰鬆各磁碟，並在將磁碟插入新設備之前，將磁碟插入新載體。

   您必須保留磁碟配對關聯。儘管您可以將舊設備 A1/A2 槽的磁碟配對裝入新設備的 B1/B2 槽，您必須將磁碟放在相同的槽內；否則，Panorama 可能無法順利恢復資料。
2. 透過執行下列各配對的 CLI 命令，啟用磁碟配對：

   ```
   admin> request system raid add <slot> force no-format
   ```

   例如：

   ```
   admin> request system raid add A1 force no-format
   admin> request system raid add A2 force no-format
   ```

   force 和**no-format** 引數是必要的。**force** 引數將磁碟配對與新設備關聯。**no-format** 引數可防止磁碟機的重新格式化，並保留磁碟上儲存的日誌。
3. 為每個磁碟配對產生中繼資料。

   視磁碟上的日誌資料量而定，此步驟可能需最多 *6* 小時。

   ```
   admin> request metadata-regenerate slot <slot_number>
   ```

   例如：

   ```
   admin> request metadata-regenerate slot 1
   ```

STEP 10 | 設定新 M-Series 設備上的本機日誌收集器。

對於需要序號的命令步驟，您必須輸入整個序號；按下 *Tab* 鍵不會完成部分序列號填寫。

此時不要啟用新 M-Series 設備上的磁碟。當您成功轉移日誌時，Panorama 會自動啟用磁碟。

1. 使用 Panorama Web 介面或使用下列 CLI 命令，設定本機日誌收集器作為受管理的收集器：

   ```
   admin> configure
   admin# set log-collector <log-collector_SN> deviceconfig system hostname
    <log-collector-hostname>
   ```


© 2019 Palo Alto Networks, Inc.

```
admin# exit
```

2. 確認本機日誌收集器連線至 Panorama，且其磁碟配對狀態為有/可用。

```
admin> show log-collector serial-number <log-collector_SN>
```

磁碟配對在還原程序的這個階段將顯示為 Disabled（停用）。

3. 將您的變更提交至 Panorama。此時還不要將變更提交至收集器群組。

```
admin> configure
admin# commit
```

STEP 11 | 將沒有磁碟的日誌收集器新增至收集器群組。

從這裡開始，只需要提交以便在 *Panorama* 和日誌收集器上完成移轉程序。暫停其他任何變更。

1. 存取 Panorama CLI（新 M-Series 設備）。
2. 覆寫 Panorama 限制，以允許將沒有磁碟的日誌收集器新增至收集器群組：**request log-migration-set-start**
3. 提交覆寫的限制：

```
admin> configure
admin# commit force
```

STEP 12 | 移轉日誌。

1. 存取 Panorama CLI（新 M-Series 設備）。
2. 新增新本機日誌收集器作為收集器群組的成員，並將您的變更提交至 Panorama。

```
admin# set log-collector-group <collector_group_name> logfwd-setting
 collectors <SN_managed_collector>
admin# commit
admin# exit
```

舊的本機日誌收集器仍會在成員清單中顯示，因為您尚未將它從設定中刪除。

3. 對於各磁碟配對，轉移日誌至新設備。

```
admin> request log-migration from <old_LC_serial_number> old-disk-pair
 <log_disk_pair> to <new_LC_serial_number> new-disk-pair <log_disk_pair>
```

例如：

```
admin> request log-migration from 003001000010 old-disk-pair A to
 00300100038 new-disk-pair A
```

4. 將變更提交至 Panorama。

```
admin> configure
admin# commit
```


© 2019 Palo Alto Networks, Inc.

STEP 13 | 重新設定收集器群組。

1. 登入 Panorama 網頁介面 使用新 M-Series 設備 指派新日誌收集器至防火牆 ，由新防火牆轉送日誌（**Panorama** > **Collector Groups**（收集器群組） > **Device Log Forwarding**（設備日誌轉送））。為新日誌收集器提供與舊日誌收集器在防火牆偏好設定清單中相同的優先級。

   您無法使用 *CLI* 來變更防火牆偏好設定清單的優先順序指派。

2. 存取 Panorama CLI（新 M-Series 設備）。
3. 將舊的日誌收集器從收集器群組中刪除。

```
admin# delete log-collector-group <group_name> logfwd-setting collectors
 <old_LC_serial_number>
```

例如：

```
admin# delete log-collector-group DC-Collector-Group logfwd-setting
 collectors 003001000010
```

4. 刪除 Panorama 組態中舊的日誌收集器，並將您的變更提交至 Panorama。

```
admin# delete log-collector <old_LC_serial_number>
admin# commit
admin# exit
```

5. 提交收集器群組變更，讓受管理的防火牆能夠將日誌傳送到新的日誌收集器。

```
admin> commit-all log-collector-config log-collector-
group <collector_group_name>
```

例如：

```
admin> commit-all log-collector-config log-collector-group DC-Collector-
Group
```

STEP 14 | 在新的日誌收集器上產生新的金鑰。

需要此命令才能將新的日誌收集器新增至收集器群組，而且只能對要更換的日誌收集器的收集器群組執行此命令。此步驟會刪除現有 *RSA* 金鑰，還可讓 *Panorama* 建立新的 *RSA* 金鑰。

1. 存取 Panorama CLI（新 M-Series 設備）。
2. 在新的日誌收集器上刪除所有 RSA 金鑰：

   ```
   request logdb update-collector-group-after-replace collector-group
   <collector-group-name>
   ```

   程序可能需要 10 分鐘才會完成。

STEP 15 | 確認收集器群組中所有日誌收集器的 SearchEngine Status 為 Active。

在收集器群組中所有日誌收集器的 *SearchEngine Status* 成為 *Active* 之前，請勿繼續。這會導致從要更換的日誌收集器中清除日誌。

© 2019 Palo Alto Networks, Inc.

1. 存取 Panorama CLI（新 M-Series 設備）。
2. 在以下任一位置執行下列命令，以顯示日誌收集器詳細資料：
   - 所有日誌收集器的 Panorama 上：

     show log-collector all

     或者，您可以在每個專用日誌收集器上執行下列命令：

     ```
     show log-collector detail
     ```
3. 確認 SearchEngine Status 為 Active。

```
Redistribution status:       none
```

```
Last commit-all: commit succeeded, current ring version 1
```

```
SearchEngine status:     Active
```

```
md5sum 4e5055a359f7662fab8f8c4f57e24525 updated at 2017/06/14 09:58:19
```

STEP 16 | 在新的日誌收集器上，以新的日誌收集器序號取代前一個日誌收集器序號。

您必須以新的日誌收集器序號取代舊的日誌收集器序號，新的日誌收集器才不會遇到清除問題，而導致日誌收集器在需要時無法從移轉的日誌中清除舊資料。

1. 存取日誌收集器 CLI。
2. 以新的日誌收集器序號取代舊的日誌收集器序號：

   request log-migration-update-logger from *<old-log-collector-serial-number>* to *<new-log-collector-serial-number>*

移轉日誌至高可用性 Panorama 模式內的新 M-Series 設備型號

如果您需要用與被更換的 M-Series 設備不同的 M-Series 設備，來更換 Panorama 模式（Panorama 管理伺服器）的 M-600、M-500、M-200 或 M-100 設備，您可以將其 RAID 磁碟移至新的 M-Series 設備，以移轉它從防火牆收集的日誌。移動磁碟可以讓您將日誌作為硬體升級的一部分進行轉移（從 M-100 設備轉移至 M-500 設備）。您可以將 M-100 設備移轉至 M-500 設備，及將 M-500 設備移轉 M-100 設備。無法從 M-100 移轉至 M-200 設備，或從 M-500 設備移轉至 M-600 設備，反之亦然。



不支援藉由將日誌記錄磁碟從任何 M-Series 設備移除並載入至 *M-600 Panorama* 管理伺服器來移轉日誌。若要移轉至 *M-600* 設備，請設定 M-600 設備、設定日誌轉送至新 M-600 設備及將 M-Series 設備設定為受管理的日誌收集器，直至您不再需要取 *M-Series* 設備上所儲存的日誌。

此轉移程序涵蓋了下列案例：

- 一個 Panorama HA 端點有收集器群組內的受管理的收集器（日誌收集器）。

© 2019 Palo Alto Networks, Inc.

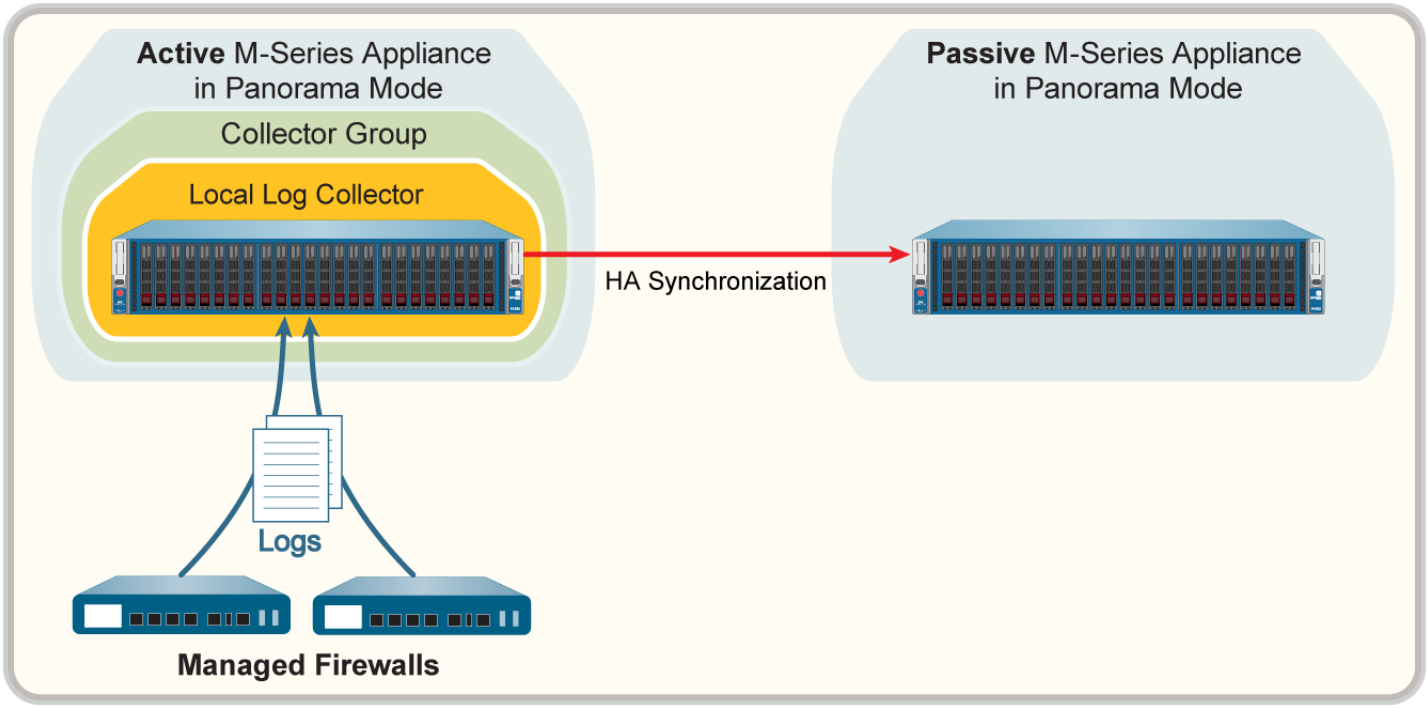


圖 **30:** 具備收集器群組的 **Panorama HA** 對等

- 兩個 Panorama HA 端點均有受管理的收集器，且同屬於單一收集器群組。如需詳細資訊，請參閱每個收集器群組多個本機日誌收集器。
- 兩個 Panorama HA 端點均有受管理的收集器，且每個都被指派了一個獨立的收集器群組。如需詳細資訊，請參閱每個收集器群組一個本機日誌收集器。

STEP 1 | 轉送舊 M-Series 設備 SSD 上的任何日誌至您想要保留它們的外部目的地。

SSD 儲存 Panorama 和日誌收集器產生的系統和設定日誌。您無法在 M-Series 設備之間移動 SSD。

設定日誌從 Panorama 轉送至外部目的地。

STEP 2 | 從停止運作的主要 Panorama 模式的 M-Series 設備匯出 Panorama 組態。

1. 登入 Panorama 網頁介面在更換的 M-Series 設備上，選取 **Panorama** > **Setup**（設定）> **Operations**（操作）。
2. 按一下 **Save named Panorama configuration snapshot**（儲存具名 **Panorama** 組態快照），輸入 **Name**（名稱）以識別設定，然後按一下 **OK**（確定）。
3. 按一下 **Export named Panorama configuration snapshot**（匯出具名 **Panorama** 組態快照），選取您剛儲存的設定 **Name**（名稱），然後按一下 **OK**（確定）。Panorama 以 XML 檔案格式匯出設定至您的用戶端系統。

STEP 3 | 將 RAID 磁碟從舊 M-Series 設備中移除。

1. 按下電源按鈕，直至系統關機，關閉舊 M-Series 設備。
2. 移除磁碟配對。詳情請參閱 M-Series 設備硬體參考指南中的磁碟更換程序。

STEP 4 | 執行新 M-Series 設備的初始設定。

針對 HA 設定中的每個新 M-Series 設備重複此步驟。

1. 在機架中安裝 M-Series 設備。請參閱 M-Series 設備硬體參考指南的指示。
2. 執行 M-Series 設備的初始設定。
3. 註冊 Panorama。

© 2019 Palo Alto Networks, Inc.

4. 購買並啟動 Panorama 支援授權，或只有在新的 M-Series 設備與舊的 M-Series 設備為相同硬體型號時，才如下轉移授權。如果新的 M-Series 設備與舊的 M-Series 設備是不同型號，您必須購買新的授權。
   1. 登入 Palo Alto Networks 客戶支援網站。
   2. 選取 **Assets**（資產）頁籤並按一下 **Spares**（備用）連結。
   3. 按一下新 M-Series 設備的序號。
   4. 按一下 **Transfer Licenses**（傳輸授權）。
   5. **Select**（選取）舊 M-Series 設備並按一下 **Submit**（提交）。
5. 啟動防火牆管理授權。如果您從 M-100 設備轉移至 M-500 設備，輸入與轉移授權相關聯的授權碼。
6. 安裝 Panorama 的內容與軟體更新。如需瞭解軟體版本的重要詳細資訊，請參閱 Panorama、日誌收集器、防火牆和 WildFire 版本相容性。
7. 在 Panorama 上設定 HA。新 M-Series 設備必須與更換的 HA 端點優先級一致。

STEP 5 | 將從停止運作的主要 M-Series 設備匯出的 Panorama 組態快照載入 Panorama 模式的新的主要 M-Series 設備。

1. 登入 Panorama 網頁介面 在新的 M-Series 設備上，選取 **Panorama** > **Setup**（設定）> **Operations**（操作）。
2. 按一下 **Import named Panorama configuration snapshot**（匯入具名 **Panorama** 組態快照），**Browse**（瀏覽）至您從停止運作的 M-Series 設備匯出的組態檔案，然後按一下 **OK**（確定）。
3. 按一下 **Load named Panorama configuration snapshot**（載入具名 **Panorama** 組態快照），選取您剛匯入的設定 **Name**（名稱），選取 **Decryption Key**（解密金鑰）（Panorama 主要金鑰），然後按一下 **OK**（確定）。Panorama 透過載入的設定覆寫其當前應徵者設定。Panorama 顯示載入設定檔時所發生的任何錯誤。如果發生錯誤，請將錯誤儲存至本機檔案。解決各錯誤，確保轉移設定有效。

   若要取代 *RMA Panorama*，請確保在載入具名 *Panorama* 組態快照時 *Retain Rule UUIDs*（保留規則 *UUID*）。如果沒有選取此選項，*Panorama* 將從組態快照中移除所有先前的規則 *UUID*，並在 *Panorama* 上為規則指定新的 *UUID*，這表示其不會保留與先前 *UUID* 相關的資訊，例如原則規則命中數。
4. 根據需要執行任何額外組態變更。

   如果舊的 *M-Series* 設備將 *MGT* 介面以外的介面用於 *Panorama* 服務（例如日誌收集），則對於新的 *M-Series* 設備，您必須 在初始設定期間定義這些介面（*Panorama* > *Setup*（設定）> *Interfaces*（介面））。
5. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Validate Commit**（驗證提交）。繼續前解決任何錯誤。
6. **Commit**（提交）您對 Panorama 組態所做的變更。提交之後，Panorama 組態即會在 HA 對等中同步。

STEP 6 | 將磁碟插入新的 M-Series 設備。詳情請參閱 M-Series 設備硬體參考指南中的磁碟更換程序。

針對 HA 設定中的每個新 M-Series 設備重複此步驟。

M-100 設備的磁碟載體與 *M-500* 設備的不相容。由此，當在這類硬體型號之間轉移時，您必須從舊載體上擰鬆各磁碟，並在將磁碟插入新設備之前，將磁碟插入新載體。

您必須保留磁碟配對關聯。儘管您可以將舊設備 A1/A2 槽的磁碟配對裝入新設備的 B1/B2 槽，您必須將磁碟放在相同的槽內；否則，Panorama 可能無法順利恢復資料。

STEP 7 | 聯絡 Palo Alto Networks 客戶支援，將日誌收集器群組中繼資料從停止運作的 M-Series 設備複製到新的 M-Series 設備，然後重新啟動 mgmtsrvr 程序。

© 2019 Palo Alto Networks, Inc.

STEP 8 | 如果 M-Series 設備屬於收集器群組，請確認解除的 M-Series 設備序號仍屬於正確的收集器群組：

```
debug log-collector-group show name <Log CollectorGroup name>
```

若停止運作的 M-Series 設備序號不再屬於正確的收集器群組，則表示之前步驟未正確複製技術支援資料夾。請再次聯絡 Palo Alto Networks 客戶支援，將技術支援資料夾複製到正確位置。

STEP 9 | 準備進行磁碟移轉。



各磁碟配對產生中繼資料時均會重新建立索引。因此，此程序視資料大小而定，可能需要較長的時間完成。若要加速程序，您可以啟動多個 *CLI* 工作階段並在各工作階段中執行中繼資料重新產生的命令，為每個配對同時完成程序。詳細資訊，請參閱重新產生 M-Series 設備 RAID 配對的中繼資料。

1. 透過執行下列各配對的 CLI 命令，啟用磁碟配對：

```
admin> request system raid add <slot> force no-format
```

例如：

```
admin> request system raid add A1 force no-format
admin> request system raid add A2 force no-format
```

force 和**no-format** 引數是必要的。**force** 引數將磁碟配對與新設備關聯。**no-format** 引數可防止磁碟機的重新格式化，並保留磁碟上儲存的日誌。

2. 為每個磁碟配對產生中繼資料。



視磁碟上的日誌資料量而定，此步驟可能需最多 *6* 小時。

```
admin> request metadata-regenerate slot <slot_number>
```

例如：

```
admin> request metadata-regenerate slot 1
```

STEP 10 | 設定新 M-Series 設備上的本機日誌收集器。



對於需要序號的命令步驟，您必須輸入整個序號；按下 *Tab* 鍵不會完成部分序列號填寫。

此時不要啟用新 M-Series 設備上的磁碟。當您成功轉移日誌時，Panorama 會自動啟用磁碟。

1. 使用 Panorama Web 介面或使用下列 CLI 命令，設定本機日誌收集器作為受管理的收集器：

```
admin> configure
admin# set log-collector <log-collector_SN> deviceconfig system hostname
 <log-collector-hostname>
admin# exit
```

2. 將您的變更提交至 Panorama。此時還不要將變更提交至收集器群組。

© 2019 Palo Alto Networks, Inc.

```
admin> configure
admin# commit
```

3. 確認本機日誌收集器連線至 Panorama，且其磁碟配對狀態為有/可用。

```
admin> show log-collector serial-number <log-collector_SN>
```

磁碟配對在還原程序的這個階段將顯示為 Disabled（停用）。

STEP 11 | 將沒有磁碟的日誌收集器新增至收集器群組。

從這裡開始，只需要提交以便在 *Panorama* 和日誌收集器上完成移轉程序。暫停其他任何變更。

1. 存取 Panorama CLI（新 M-Series 設備）。
2. 覆寫 Panorama 限制，以允許將沒有磁碟的日誌收集器新增至收集器群組：**request log-migration-set-start**
3. 將變更提交至 Panorama。

```
admin> configure
admin# commit force
```

STEP 12 | 移轉日誌。

1. 存取 Panorama CLI（新 M-Series 設備）。
2. 新增新本機日誌收集器作為收集器群組的成員，並將您的變更提交至 Panorama。

```
admin# set log-collector-group <collector_group_name> logfwd-setting
 collectors <SN_managed_collector>
admin# commit
admin# exit
```

舊的本機日誌收集器仍會在成員清單中顯示，因為您尚未將它從設定中刪除。

3. 對於各磁碟配對，轉移日誌至新設備。

```
admin> request log-migration from <old_LC_serial_number> old-disk-pair
 <log_disk_pair> to <new_LC_serial_number> new-disk-pair <log_disk_pair>
```

例如：

```
admin> request log-migration from 003001000010 old-disk-pair A to
 00300100038 new-disk-pair A
```

4. 將變更提交至 Panorama。

```
admin> configure
admin# commit
```

STEP 13 | 重新設定收集器群組。

© 2019 Palo Alto Networks, Inc.

1. 登入 Panorama 網頁介面 使用新 M-Series 設備 指派新日誌收集器至防火牆 ，由新防火牆轉送日誌（**Panorama** > **Collector Groups**（收集器群組） > **Device Log Forwarding**（設備日誌轉送））。為新日誌收集器提供與舊日誌收集器在防火牆偏好設定清單中相同的優先級。

   您無法使用 *CLI* 來變更防火牆偏好設定清單的優先順序指派。

2. 存取 Panorama CLI（新 M-Series 設備）。
3. 將舊的日誌收集器從收集器群組中刪除。

```
admin# delete log-collector-group <group_name> logfwd-setting collectors
 <old_LC_serial_number>
```

   例如：

```
admin# delete log-collector-group DC-Collector-Group logfwd-setting
 collectors 003001000010
```

4. 刪除 Panorama 組態中舊的日誌收集器，並將您的變更提交至 Panorama。

```
admin# delete log-collector <old_LC_serial_number>
admin# commit
admin# exit
```

5. 提交收集器群組變更，讓受管理的防火牆能夠將日誌傳送到新的日誌收集器。

```
admin> commit-all log-collector-config log-collector-
group <collector_group_name>
```

   例如：

```
admin> commit-all log-collector-config log-collector-group DC-Collector-
Group
```

STEP 14 | 在新的日誌收集器上產生新的金鑰。

需要此命令才能將新的日誌收集器新增至收集器群組，而且只能對要更換的日誌收集器的收集器群組執行此命令。此步驟會刪除現有 *RSA* 金鑰，還可讓 *Panorama* 建立新的 *RSA* 金鑰。

1. 存取 Panorama CLI（新 M-Series 設備）。
2. 在新的日誌收集器上刪除所有 RSA 金鑰：

   ```
   request logdb update-collector-group-after-replacecollector-group
   <collector-group-name>
   ```

   程序可能需要 10 分鐘才會完成。

STEP 15 | 確認收集器群組中所有日誌收集器的 SearchEngine Status 為 Active。

在收集器群組中所有日誌收集器的 *SearchEngine Status* 成為 *Active* 之前，請勿繼續。這會導致從要更換的日誌收集器中清除日誌。

1. 存取 Panorama CLI（新 M-Series 設備）。

© 2019 Palo Alto Networks, Inc.

2. 在以下任一位置執行下列命令，以顯示日誌收集器詳細資料：
   - 所有日誌收集器的 Panorama 上：

     show log-collector all

     或者，您可以在每個專用日誌收集器上執行下列命令：

     show log-collector detail
3. 確認 SearchEngine Status 為 Active。

```
Redistribution status:       none
```

```
Last commit-all: commit succeeded, current ring version 1
```

```
SearchEngine status:     Active
```

```
md5sum 4e5055a359f7662fab8f8c4f57e24525 updated at 2017/06/14 09:58:19
```

STEP 16 | 在新的日誌收集器上，以新的日誌收集器序號取代前一個日誌收集器序號。

您必須以新的日誌收集器序號取代舊的日誌收集器序號，新的日誌收集器才不會遇到清除問題，而導致日誌收集器在需要時無法從移轉的日誌中清除舊資料。

1. 存取日誌收集器 CLI。
2. 以新的日誌收集器序號取代舊的日誌收集器序號：

   request log-migration-update-logger from *<old-log-collector-serial-number>* to *<new-log-collector-serial-number>*

STEP 17 | 設定新的次要 Panorama 高可用性對等。

1. 轉送舊 M-Series 設備 SSD 上的任何日誌至您想要保留它們的外部目的地。
2. 將 RAID 磁碟從舊 M-Series 設備中移除。
3. 執行新 M-Series 設備的初始設定。
4. 將磁碟插入新的 M-Series 設備。
5. 重複步驟 7 至 16，從舊的 M-Series 設備移轉至新的 M-Series 設備。
6. 在 Panorama 上設定 HA。新 M-Series 設備必須與更換的 HA 端點優先級一致。
7. 登入 Panorama 網頁介面 在主要 HA 對等上，按一下 **Dashboard**（儀表板）> **High Availability**（高可用性）> **Sync to peer**（同步至對等），以同步 M-Series 設備 HA 對等的設定。

移轉日誌至高可用性 Panorama 模式內的新 M-Series 設備型號

如果您需要用與被更換的 M-Series 設備相同的 M-Series 設備，來更換以 Panorama 模式（Panorama 管理伺服器）高可用性 (HA) 設定部署的 M-600、M-500、M-200 或 M-100 設備，您可以將其 RAID 磁碟移至新的 M-Series 設備，以移轉它從防火牆收集的日誌。移動磁碟可讓您在 M-Series 設備出現系統故障後復原日誌。

此轉移程序涵蓋了下列案例：

- 一個 Panorama HA 端點有收集器群組內的受管理的收集器（日誌收集器）。

© 2019 Palo Alto Networks, Inc.

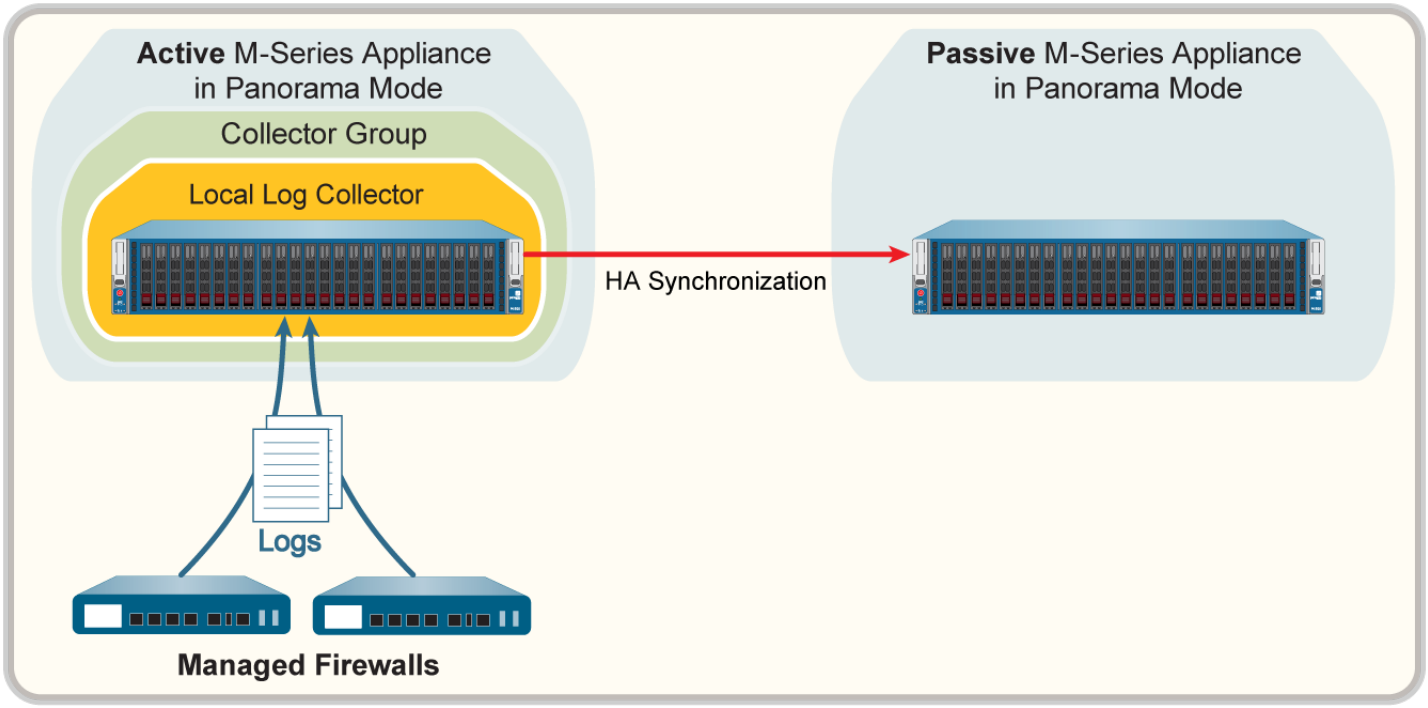


圖 **31:** 具備收集器群組的 **Panorama HA** 對等

- 兩個 Panorama HA 端點均有受管理的收集器，且同屬於單一收集器群組。如需詳細資訊，請參閱每個收集器群組多個本機日誌收集器。
- 兩個 Panorama HA 端點均有受管理的收集器，且每個都被指派了一個獨立的收集器群組。如需詳細資訊，請參閱每個收集器群組一個本機日誌收集器。

STEP 1 | 轉送舊 M-Series 設備 SSD 上的任何日誌至您想要保留它們的外部目的地。

SSD 儲存 Panorama 和日誌收集器產生的系統和設定日誌。您無法在 M-Series 設備之間移動 SSD。

設定日誌從 Panorama 轉送至外部目的地。

STEP 2 | 將 RAID 磁碟從舊 M-Series 設備中移除。

1. 按下電源按鈕，直至系統關機，關閉舊 M-Series 設備。
2. 移除磁碟配對。詳情請參閱 M-Series 設備硬體參考指南中的磁碟更換程序。

STEP 3 | 執行新 M-Series 設備的初始設定。

1. 在機架中安裝 M-Series 設備。請參閱 M-Series 設備硬體參考指南的指示。
2. 執行 M-Series 設備的初始設定。

   如果舊的 *M-Series* 設備將 *MGT* 介面以外的介面用於 *Panorama* 服務（例如日誌收集），則對於新的 *M-Series* 設備，您必須在初始設定期間定義這些介面（*Panorama* > *Setup*（設定）> *Interfaces*（介面））。
3. 註冊 Panorama。
4. 購買並啟動 Panorama 支援授權，或只有在新的 M-Series 設備與舊的 M-Series 設備為相同硬體型號時，才如下轉移授權。如果新的 M-Series 設備與舊的 M-Series 設備是不同型號，您必須購買新的授權。
   1. 登入 Palo Alto Networks 客戶支援網站。
   2. 選取 **Assets**（資產）頁籤並按一下 **Spares**（備用）連結。
   3. 按一下新 M-Series 設備的序號。

© 2019 Palo Alto Networks, Inc.

4. 按一下 **Transfer Licenses**（傳輸授權）。
5. **Select**（選取）舊 M-Series 設備並按一下 **Submit**（提交）。

5. 啟動防火牆管理授權。如果您從 M-100 設備轉移至 M-500 設備，輸入與轉移授權相關聯的授權碼。
6. 安裝 Panorama 的內容與軟體更新。如需瞭解軟體版本的重要詳細資訊，請參閱 Panorama、日誌收集器、防火牆和 WildFire 版本相容性。
7. 根據需要執行任何額外組態變更。



如果舊的 *M-Series* 設備將 *MGT* 介面以外的介面用於 *Panorama* 服務（例如日誌收集），則對於新的 *M-Series* 設備，您必須 在初始設定期間定義這些介面（*Panorama* > *Setup*（設定）> *Interfaces*（介面））。

8. 在 Panorama 上設定 HA。新 M-Series 設備必須與更換的 HA 端點優先級一致。

STEP 4 | 將磁碟插入新的 M-Series 設備。詳情請參閱 M-Series 設備硬體參考指南中的磁碟更換程序。



M-100 設備的磁碟載體與 *M-500* 設備的不相容。由此，當在這類硬體型號之間轉移時，您必須從舊載體上擰鬆各磁碟，並在將磁碟插入新設備之前，將磁碟插入新載體。

您必須保留磁碟配對關聯。儘管您可以將舊設備 A1/A2 槽的磁碟配對裝入新設備的 B1/B2 槽，您必須將磁碟放在相同的槽內；否則，Panorama 可能無法順利恢復資料。

STEP 5 | 如果 M-Series 設備屬於收集器群組，請確認解除的 M-Series 設備序號仍屬於正確的收集器群組：

```
debug log-collector-group show name <Log CollectorGroup name>
```

STEP 6 | 準備進行磁碟移轉。



各磁碟配對產生中繼資料時均會重新建立索引。因此，此程序視資料大小而定，可能需要較長的時間完成。若要加速程序，您可以啟動多個 *CLI* 工作階段並在各工作階段中執行中繼資料重新產生的命令，為每個配對同時完成程序。詳細資訊，請參閱重新產生 M-Series 設備 RAID 配對的中繼資料。

1. 透過執行下列各配對的 CLI 命令，啟用磁碟配對：

```
admin> request system raid add <slot> force no-format
```

例如：

```
admin> request system raid add A1 force no-format
admin> request system raid add A2 force no-format
```

force 和**no-format** 引數是必要的。**force** 引數將磁碟配對與新設備關聯。**no-format** 引數可防止磁碟機的重新格式化，並保留磁碟上儲存的日誌。

2. 為每個磁碟配對產生中繼資料。

```
admin> request metadata-regenerate slot <slot_number>
```

例如：

```
admin> request metadata-regenerate slot 1
```

STEP 7 | 設定新 M-Series 設備上的本機日誌收集器。

© 2019 Palo Alto Networks, Inc.

對於需要序號的命令步驟，您必須輸入整個序號；按下 *Tab* 鍵不會完成部分序列號填寫。

此時不要啟用新 M-Series 設備上的磁碟。當您成功轉移日誌時，Panorama 會自動啟用磁碟。

1. 使用 Panorama Web 介面或使用下列 CLI 命令，設定本機日誌收集器作為受管理的收集器：

```
admin> configure
admin# set log-collector <log-collector_SN> deviceconfig system hostname
 <log-collector-hostname>
admin# exit
```

2. 將您的變更提交至 Panorama。此時還不要將變更提交至收集器群組。

```
admin> configure
admin# commit
```

3. 確認本機日誌收集器連線至 Panorama，且其磁碟配對狀態為有/可用。

```
admin> show log-collector serial-number <log-collector_SN>
```

磁碟配對在還原程序的這個階段將顯示為 Disabled（停用）。

STEP 8 | 將沒有磁碟的日誌收集器新增至收集器群組。

從這裡開始，只需要提交以便在 *Panorama* 和日誌收集器上完成移轉程序。暫停其他任何變更。

1. 存取 Panorama CLI。
2. 覆寫 Panorama 限制，以允許將沒有磁碟的日誌收集器新增至收集器群組：**request log-migration-set-start**
3. 提交覆寫的限制：

```
admin> configure
admin# commit force
```

STEP 9 | 移轉日誌。

1. 存取 Panorama CLI。
2. 新增新本機日誌收集器作為收集器群組的成員，並將您的變更提交至 Panorama。

```
admin# set log-collector-group <collector_group_name> logfwd-setting
 collectors <SN_managed_collector>
admin# commit
admin# exit
```

舊的本機日誌收集器仍會在成員清單中顯示，因為您尚未將它從設定中刪除。

3. 對於各磁碟配對，轉移日誌至新設備。

```
admin> request log-migration from <old_LC_serial_number> old-disk-pair
 <log_disk_pair> to <new_LC_serial_number> new-disk-pair <log_disk_pair>
```

例如：

© 2019 Palo Alto Networks, Inc.

```
admin> request log-migration from 003001000010 old-disk-pair A to
 00300100038 new-disk-pair A
```

4. 將變更提交至 Panorama。

```
admin> configure
admin# commit
```

STEP 10 | 重新設定收集器群組。

1. 使用 Web 介面 指派新日誌收集器至防火牆 ，由新防火牆轉送日誌（**Panorama** > **Collector Groups**（收集器群組）> **Device Log Forwarding**（設備日誌轉送））。為新日誌收集器提供與舊日誌收集器在防火牆偏好設定清單中相同的優先級。



您無法使用 *CLI* 來變更防火牆偏好設定清單的優先順序指派。

2. 將舊的日誌收集器從收集器群組中刪除。

```
admin# delete log-collector-group <group_name> logfwd-setting collectors
 <old_LC_serial_number>
```

例如：

```
admin# delete log-collector-group DC-Collector-Group logfwd-setting
 collectors 003001000010
```

3. 刪除 Panorama 組態中舊的日誌收集器，並將您的變更提交至 Panorama。

```
admin# delete log-collector <old_LC_serial_number>
admin# commit
admin# exit
```

4. 同步處理 M-Series 設備 HA 端點的設定。

```
admin> request high-availability sync-to-remote running-config
```

5. 提交收集器群組變更，讓受管理的防火牆能夠將日誌傳送到新的日誌收集器。

```
admin> commit-all log-collector-config log-collector-
group <collector_group_name>
```

例如：

```
admin> commit-all log-collector-config log-collector-group DC-Collector-
Group
```

STEP 11 | 在新的日誌收集器上產生新的金鑰。



需要此命令才能將新的日誌收集器新增至收集器群組，而且只能對要更換的日誌收集器的收集器群組執行此命令。此步驟會刪除現有 *RSA* 金鑰，還可讓 *Panorama* 建立新的 *RSA* 金鑰。

© 2019 Palo Alto Networks, Inc.

1. 存取 Panorama CLI。
2. 在新的日誌收集器上刪除所有 RSA 金鑰：

   request logdb update-collector-group-after-replacecollector-group *<collector-group-name>*

   程序可能需要 10 分鐘才會完成。

STEP 12 | 確認收集器群組中所有日誌收集器的 SearchEngine Status 為 Active。

在收集器群組中所有日誌收集器的 *SearchEngine Status* 成為 *Active* 之前，請勿繼續。這會導致從要更換的日誌收集器中清除日誌。

1. 存取 Panorama CLI。
2. 在以下任一位置執行下列命令，以顯示日誌收集器詳細資料：
   - 所有日誌收集器的 Panorama 上：

     show log-collector all

   或者，您可以在每個專用日誌收集器上執行下列命令：

   ```
   show log-collector detail
   ```

3. 確認 SearchEngine Status 為 Active。

```
Redistribution status:       none
```

```
Last commit-all: commit succeeded, current ring version 1
```

```
SearchEngine status:     Active
```

```
md5sum 4e5055a359f7662fab8f8c4f57e24525 updated at 2017/06/14 09:58:19
```

STEP 13 | 在新的日誌收集器上，以新的日誌收集器序號取代前一個日誌收集器序號。

您必須以新的日誌收集器序號取代舊的日誌收集器序號，新的日誌收集器才不會遇到清除問題，而導致日誌收集器在需要時無法從移轉的日誌中清除舊資料。

1. 存取日誌收集器 CLI。
2. 以新的日誌收集器序號取代舊的日誌收集器序號：

   request log-migration-update-logger from *<old-log-collector-serial-number>* to *<new-log-collector-serial-number>*

非 HA Panorama 故障/ RMA 後轉移日誌收集器

如果 Panorama 伺服器上發生系統故障，且 Panorama 伺服器未在高可用性 (HA) 設定中部署，請使用此程序在更換 Panorama 上還原設定，並重新取得 Panorama 管理專用日誌收集器上日誌的存取權。允許的移轉案例隨 Panorama 管理伺服器型號而異：

© 2019 Palo Alto Networks, Inc.

舊/失效 Panorama	新/更換 Panorama
Panorama 虛擬設備	• Panorama 虛擬設備 • M-200 設備 • M-500 設備 • M-600 設備
M-100 設備	• Panorama 虛擬設備 • M-200 設備 • M-500 設備 • M-600 設備
M-500 設備	• Panorama 虛擬設備 • M-200 設備 • M-500 設備 • M-600 設備

Panorama 保留對應區段和分割區（專用日誌收集器使用它們儲存日誌）的環檔。Panorama 模式下的 M-Series 設備在其內部 SSD 上儲存環檔；Panorama 虛擬設備在其內部磁碟上儲存環檔。當系統故障時，非 HA Panorama 無法自動恢復環檔。由此，當您更換 Panorama 時，您必須恢復環檔以存取專用日誌收集器上的日誌。

此程序要求您在發生系統故障之前已備份並匯出您的 Panorama 組態。

Palo Alto Networks 建議在 *HA* 設定中部署 *Panorama*。主動 *Panorama* 端點自動同步環檔至 *HA* 設定內的被動端點，保留對專用日誌收集器上日誌的存取，即使您必須更換其中一個端點。

STEP 1 | 執行新 Panorama 設備的初始設定。

1. 依據您的需求設定 M-Series 設備或設定 Panorama 虛擬設備。若您要設定新的 M-Series 設備，請參閱 M-Series 設備硬體參考指南以獲得如何在機架中安裝 M-Series 設備。
2. 執行 M-Series 設備的初始設定或執行 Panorama 虛擬設備的初始設定。

   如果舊的 *M-Series* 設備將 *MGT* 介面以外的介面用於 *Panorama* 服務（例如日誌收集），則對於新的 *M-Series* 設備，您必須在初始設定期間定義這些介面（*Panorama* > *Setup*（設定）> *Interfaces*（介面））。*Panorama* 虛擬設備不支援 *MGT* 以外的介面。
3. 註冊 Panorama。
4. 僅當新的 Panorama 設備與舊設備為相同型號時，才能如下轉移授權。否則，必須購買新授權。
   1. 登入 Palo Alto Networks 客戶支援網站。
   2. 選取 **Assets**（資產）頁籤並按一下 **Spares**（備用）連結。
   3. 按一下新 M-Series 設備的序號。
   4. 按一下 **Transfer Licenses**（傳輸授權）。
   5. **Select**（選取）舊設備並按一下 **Submit**（提交）。
5. 啟動 Panorama 支援授權。
6. 啟動防火牆管理授權。
7. 安裝 Panorama 的內容與軟體更新。

© 2019 Palo Alto Networks, Inc.

M-500 設備需要 *Panorama 7.0* 或更新版本。*M-200* 和 *M-600* 設備需要 *Panorama 8.1*。如需瞭解軟體版本的重要詳細資訊，請參閱 Panorama、日誌收集器、防火牆和 WildFire 版本相容性。

STEP 2 | 將 Panorama 的舊設定還原至欲更換的 Panorama。

1. 登入新 Panorama 設備，然後選取 **Panorama** > **Setup**（設定）> **Operations**（操作）。
2. 按一下 **Import named Panorama configuration snapshot**（匯入具名 **Panorama** 組態快照）、**Browse**（瀏覽）至備份設定檔，並按一下 **OK**（確定）。
3. 按一下 **Load named configuration snapshot**（載入具名組態快照），選取您剛才匯入的檔案 **Name**（名稱），然後按一下 **OK**（確定）。

   若要取代 *RMA Panorama*，請確保在載入具名 *Panorama* 組態快照時 *Retain Rule UUIDs*（保留規則 *UUID*）。如果沒有選取此選項，*Panorama* 將從組態快照中移除所有先前的規則 *UUID*，並在 *Panorama* 上為規則指定新的 *UUID*，這表示其不會保留與先前 *UUID* 相關的資訊，例如原則規則命中數。
4. 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。
5. 選取 **Panorama** > **Managed Collectors**（受管理的收集器）並確認連線的欄顯示專用日誌收集器的核取標記。

   如果未出現專用日誌收集器，您必須重新設定收集器及收集器群組，如下一步驟中所述。否則，請跳過以下步驟，到擷取環檔以恢復存取專用日誌收集器上儲存的日誌。

STEP 3 | 如果其在 Panorama 上缺失，重新設定專用日誌收集器和收集器群組。

1. 存取專用日誌收集器的 CLI，並輸入下列命令以顯示收集器群組的名稱。
   1. 輸入命令：

      ```
      > request fetch ring from log-collector <serial_number>
      ```

      將顯示下列錯誤：

      ```
      Server error: Failed to fetch ring info from <serial_number>
      ```
   2. 輸入命令：

      ```
      > less mp-log ms.log
      ```

      將顯示下列錯誤：

      ```
      Dec04 11:07:08 Error:
       pan_cms_convert_resp_ring_to_file(pan_ops_cms.c:3719): Current
       configuration does not contain group CA-Collector-Group
      ```

      此示例中，錯誤訊息表示缺少的收集器群組擁有具名 CA-Collector-Group。
2. 設定收集器群組並指派專用日誌收集器。

   ```
   > configure
   # set log-collector-group <collector-group-name>
   # set log-collector-group <collector-group-name> logfwd-setting
   collector <serial-number>
   ```


© 2019 Palo Alto Networks, Inc.

3. 將變更提交至 Panorama 而非收集器群組。

```
# commit
# exit
```

STEP 4 | 擷取環檔以還原在專用日誌收集器上所儲存日誌檔的存取權。

1. 存取新 Panorama 的 CLI。
2. 擷取環檔：

```
> request fetch ring from log-collector <serial-number>
```

例如：

```
> request fetch ring from log-collector 009201000343
```



如果您不知道專用日誌收集器的序號，登入其 *CLI* 並輸入 ***show system info*** 操作命令。

3. 將您的變更提交至收集器群組。

```
> commit-all log-collector-config log-collector-group <collector-group-name>
```

重新產生 M-Series 設備 RAID 配對的中繼資料

當 M-600、M-500 或 M-200 設備發生系統故障，且您需要將一個裝置的磁碟實際移至另一個裝置時，就需要重新產生中繼資料。必須有中繼資料，才能在磁碟上找到日誌；當使用者發出日誌查詢時，查詢會查閱此中繼資料以存取要求的日誌資料。

對於 M-Series 設備中的各設定 RAID 磁碟配對，您必須存取裝置 CLI 並執行下列命令以重新產生中繼資料：

```
> request metadata-regenerate slot <slot_number>
```

例如：

```
> request metadata-regenerate slot 1
```

RAID 磁碟大小決定重新產生中繼資料所需的時長。平均每 100GB 需要一小時。當您執行命令時，會鎖定 CLI 工作階段，直到命令完全執行為止。您可以使用多個 CLI 工作階段以節省時間。例如，若要更換四個 RAID 配對的 1TB 磁碟機（日誌資料總計為 4TB），請啟動四個 CLI 工作階段，並在各工作階段中執行命令，為所有配對/槽內同時重新產生中繼資料，大約需要 10 小時。

正在重新產生中繼資料時，這些磁碟所屬的收集器群組尚無法使用，且磁碟配對無法供任何記錄或報告操作（寫入/查詢）使用。然而，您可以執行其他工作，如處理新防火牆連線，或在受管理防火牆上管理設定變更。Panorama 所管理不屬於 RMA 程序的其他所有收集器群組，可正常執行指派的日誌記錄與報告功能。

檢視日誌查詢作業

您可以檢視日誌查詢作業以進行調查並更好地瞭解為什麼查詢日誌資料花費的時間超出預期。首先，您必須先顯示 Panorama 上執行的所有日誌查詢作業。識別需要調查的日誌查詢作業後，使用作業 ID 檢視有關查

© 2019 Palo Alto Networks, Inc.

詢的詳細資訊，以更好地瞭解日誌查詢為什麼會出現問題。在 Panorama 上查詢日誌資料時，隨著新日誌查詢作業的執行，詳細的作業 ID 資訊將被覆寫。

STEP 1 | 登入 Panorama CLI。

STEP 2 | 檢視 Panorama 上執行的日誌查詢作業。

CLI 輸出包括有關每個已執行日誌查詢的常規資訊，例如作業 ID、執行查詢的時間、查詢狀態、查詢的日誌資料庫、查詢的日誌數、查詢返回結果所花費的時間（以毫秒為單位）、執行查詢的管理員以及套用至查詢的所有篩選器。

```
admin@Panorama> show query jobs
```

```
admin@bingdot34> show query jobs

ID        Enqueue Time         State       Database  nlogs     Runtime(ms)    Us
er            Filter
------------------------------------------------------------------------------
------------------------------------------------------------------------------
42        2020/01/02 14:35:46  COMPLETE    threat    110       166.27         ad
min           ((((receive_time leq 'now')) and (((subtype eq 'file')) or ((subty
pe eq 'data')))) and ((receive_time in 'last-hour')))


41        2020/01/02 14:35:46  COMPLETE    system    110       163.84         ad
min           (((receive_time leq now)) and (receive_time in last-hour))

40        2020/01/02 14:35:46  COMPLETE    config    110       158.23         ad
min           (((receive_time leq now)) and (receive_time in last-hour))

39        2020/01/02 14:35:36  COMPLETE    config    110       162.58         ad
min           (((receive_time leq now)) and (receive_time in last-hour))

38        2020/01/02 14:35:36  COMPLETE    system    110       172.68         ad
min           (((receive_time leq now)) and (receive_time in last-hour))

37        2020/01/02 14:35:36  COMPLETE    threat    110       188.80         ad
min           ((((receive_time leq 'now')) and (((subtype eq 'file')) or ((subty
pe eq 'data')))) and ((receive_time in 'last-hour')))
```

STEP 3 | 使用作業 ID 檢視有關特定作業的詳細日誌查詢資訊。

```
admin@Panorama> show query jobid <Job ID>
```

```
admin@bingdot34> show query jobid 42

Serial          ID        State     Num Req   Num Proc  RTT(Max)      Avg Recs/R
TTSoftware Ver    CG                                Last Update Time
------------------------------------------------------------------------------
------------------------------------------------------------------------------
LOGDB           42        DONE      110       0         0.00      0.00
9.2.0           LOCAL                             2020/01/02 14:35:46

PODABCD12       42        FAILED    110       0         0.00      0.00
9.2.0           PODABCD12                         2020/01/02 14:35:46
```


© 2019 Palo Alto Networks, Inc.

更換 RMA 防火牆

若要以最少的心力還原需退貨商品授權 (RMA) 有關的受管理防火牆組態，您可以在 Panorama 上以全新防火牆的序號取代舊防火牆的序號。接著若要還原更換防火牆的設定，您可以匯入先前從防火牆產生和匯出的防火牆狀態，或者使用 Panorama 針對執行 PAN-OS 5.0 及更新版本的受管理防火牆產生部分裝置狀態。藉由取代序號及匯入防火牆狀態，您可以繼續使用 Panorama 管理防火牆。

- 為防火牆產生部分裝置狀態
- 開始 RMA 防火牆更換前
- 更換後還原防火牆組態

為防火牆產生部分裝置狀態

當您使用 Panorama 產生部分裝置狀態時，它會複製受管理防火牆的設定，對於大規模 VPN (LSVPN) 設定則有一些例外。您可以藉由結合防火牆組態的兩個面向來建立部分裝置狀態：

- 由 Panorama 管理的集中設定—Panorama 會維護其推送至防火牆的共用原則規則與範本快照。
- 防火牆上的本機設定—在防火牆上提交設定變更時，每個防火牆會將其本機組態檔案的副本傳送給 Panorama。Panorama 會儲存此檔案，並用於編譯部分的裝置狀態包。



在 *LSVPN* 設定中，您在 *Panorama* 上產生的部分設備狀態包，與您從防火牆匯出的版本（選取 *Device*（設備）> *Setup*（設定）> *Operations*（操作），然後按一下 *Export device state*（匯出設備狀態））不同。如果您已手動執行裝置狀態匯出，或排程 *XML API* 指令碼，將檔案匯出至遠端伺服器，則可在以下的防火牆更換工作流程中使用匯出的裝置狀態。

如果您未匯出裝置狀態，則在更換工作流程中產生的裝置狀態不會包含動態設定資訊（例如憑證詳細資料和註冊的防火牆），它是還原以 *LSVPN* 入口網站形式運作的防火牆其完整設定時必須使用的資訊。如需詳細資訊，請參閱 開始 RMA 防火牆更換前。

Panorama 未儲存裝置狀態，而是在提出要求使用 更換後還原防火牆組態 中所列的 CLI 命令來產生該狀態。

開始 RMA 防火牆更換前

- 您要更換的防火牆必須已使用 PAN-OS 5.0.4 或更新版本。Panorama 無法為執行舊版 PAN-OS 的防火牆產生設備狀態。
- 記錄以下關於您要更換的防火牆的詳細資訊：
  - 序號—您必須在 Palo Alto Networks 客戶支援網站上輸入序號，才能將授權從舊防火牆傳輸到更換的防火牆。您也必須在 Panorama 上輸入此資訊，才能使用更換設備的新序號，取代舊序號的所有參考。
  - （建議）**PAN-OS** 版本與內容資料庫版本—安裝相同的軟體和內容資料庫版本（包括 URL 資料庫廠商）可讓您在更換防火牆上建立相同的狀態。如果決定安裝最新版的內容資料庫，您可能會注意到更新及新增至資料庫所出現的差異。若要確定防火牆上安裝的版本，請存取 Panorama 上儲存的防火牆系統日誌。
- 準備更換防火牆進行部署。匯入裝置狀態包和還原設定之前，您必須：
  - 確認更換防火牆具有和舊防火牆相同的型號，並且針對類似的操作功能啟用。請考量下列操作功能：更換的防火牆是否必須要有多個虛擬系統啟用它？是否支援 Jumbo 框架，或可在 CC 或 FIPS 模式中操作？
  - 設定網路存取權、傳輸授權，以及安裝適當的 PAN-OS 版本和內容資料庫版本。
- 您必須使用 Panorama CLI 完成防火牆更換程序，因此您的管理員帳戶必須具有超級使用者或 Panorama 管理員使用者角色。

© 2019 Palo Alto Networks, Inc.

- 如果您有 LSVPN 設定，並且正在取代部署為衛星設備或 LSVPN 入口網站的 Palo Alto Networks 防火牆，則在還原 Panorama 上產生的部分裝置狀態時，將無法使用還原 LSVPN 連線時所需要的動態設定資訊。如果已依照下列建議，針對 LSVPN 設定中的防火牆頻繁地產生和匯出裝置狀態，請使用您先前從防火牆本身匯出的裝置狀態，而非在 Panorama 上產生裝置狀態。

  如果您尚未從防火牆手動匯出裝置狀態，並且需要在 Panorama 上產生部分裝置狀態，則遺失的動態設定將影響防火牆更換程序，如下所示：

  - 如果正在更換的防火牆是 **GlobalProtect** 入口網站設備 ，並且是使用衛星設備的序號所明確設定（**Network**（網路）> **GlobalProtect** > **Portals**（入口網站）> **Satellite Configuration**（衛星設備組態），則在還原防火牆組態時，即使動態設定已遺失，入口網站防火牆仍可成功地驗證衛星設備。成功驗證時將產生動態設定資訊，並將重新啟動 LSVPN 連線。
  - 如果是更換衛星防火牆，則其將無法連線及驗證入口網站。連線失敗是因為未在防火牆上明確設定序號（**Network**（網路）> **GlobalProtect** > **Portals**（入口網站）> **Satellite Configuration**（衛星組態）），或雖然已明確設定序號，但更換防火牆的序號與舊防火牆的序號不符。若要還原連線，則在匯入裝置狀態包後，衛星管理員必須登入防火牆，並輸入認證（使用者名稱和密碼）以驗證入口網站。驗證後，會在入口網站上產生 LSVPN 連線的動態設定。

  然而，若是在高可用性設定中設定防火牆，則在還原設定後，防火牆將會將正在執行的設定及其端點自動同步，並執行最新的必要動態設定以順暢地運作。

更換後還原防火牆組態

若要在新防火牆上還原防火牆組態，您首先要在新防火牆上執行初始設定，包括設定操作模式、升級 PAN-OS 軟體和內容版本以使其與舊防火牆上安裝的版本相符。然後將舊防火牆的裝置狀態從 Panorama 匯出，再匯入新防火牆。最後，返回到 Panorama，驗證新防火牆是否已連續，然後將其與 Panorama 同步。

STEP 1 | 在新防火牆上執行初始設定並確認網路連線。

使用序列連接埠連線或 Secure Shell (SSH) 連線來新增 IP 位址、DNS 伺服器 IP 位址，及確認新防火牆可存取 Palo Alto Networks 更新伺服器。

STEP 2 | （選用）將新防火牆上的操作模式設為符合舊防火牆上的操作模式。

需要序列連接埠才能執行此工作。

1. 在防火牆上輸入下列 CLI 命令以存取維護模式：

```
> debug system maintenance-mode
```

2. 對於操作模式，從主功能表中，選取 **Set FIPS Mode**（設定 FIPS 模式）或 **Set CCEAL 4 Mode**（設定 CCEAL 4 模式）。

STEP 3 | 在新防火牆上擷取授權。

輸入下列命令以擷取授權：

```
> request license fetch
```

STEP 4 | （選用）讓新防火牆的操作狀態與舊防火牆的操作狀態相符。例如，對於為了多虛擬系統（多 VSYS）功能而啟用的防火牆啟用多 VSYS 功能。

輸入與您的防火牆組態相關的命令：

```
> set system setting multi-vsys on
> set system setting jumbo-frame on
```


© 2019 Palo Alto Networks, Inc.

STEP 5 | 升級新防火牆上的 PAN-OS 版本。

必須升級成與舊防火牆上所安裝 PAN-OS 相同的版本。必須升級成與舊防火牆上所安裝內容發佈版本相同或更新的版本。

輸入下列命令：

1. 若要升級內容版本：

```
> request content upgrade download latest
> request content upgrade install version latest
```

2. 若要升級防毒版本：

```
> request anti-virus upgrade download latest
> request anti-virus upgrade install version latest
```

3. 若要升級 PAN-OS 軟體版本：

```
> request system software download version <version>
> request system software install version <version>
```

STEP 6 | 前往 Panorama CLI，使用 Secure Copy（安全複本 - SCP）或 TFTP，將裝置狀態包從舊防火牆匯出至電腦（無法從網頁介面執行此操作）。



如果您從防火牆手動匯出裝置狀態，可跳過此步驟。

export 命令會以 tar 壓縮檔形式產生裝置狀態包，並將該檔案匯出至指定的位置。此裝置狀態不包含 LSVPN 動態設定（衛星資訊和憑證詳細資料）。

輸入下列其中一個命令：

```
> scp export device-state device <old serial#> to <login> @ <serverIP>:
 <path>
```

或

```
> tftp export device-state device <old serial#> to <login> @ <serverIP>:
 <path>
```

STEP 7 | 在 Panorama 上以新更換設備的序號取代舊防火牆的序號。

透過更換 Panorama 上的序號，即表示在還原防火牆上的設定後，您允許新防火牆連線至 Panorama。

1. 在操作模式中輸入下列命令：

```
> replace device old <old SN#> new <new SN#>
```

2. 進入設定模式並提交您的變更。

```
> configure
# commit
```

3. 退出設定模式。

© 2019 Palo Alto Networks, Inc.

```
# exit
```

STEP 8 | 在新防火牆上，匯入裝置狀態並提交變更。

1. 存取新防火牆的 Web 介面。
2. 選取 **Device**（設備）> **Setup**（設定）> **Operations**（操作），再按一下 [設定管理] 部分中的 **Import Device State**（匯入設備狀態）連結。
3. 瀏覽以找出檔案，再按一下 **OK**（確定）。
4. 將您的變更 **Commit**（提交）至防火牆上執行中的設定。

STEP 9 | 在 Panorama 上確認是否已成功還原防火牆組態。

1. 存取 Panorama Web 介面中，選取 **Panorama** > **Managed Devices**（受管理裝置）。
2. 確認新防火牆其 Connected（已連線）欄有核取標記。

STEP 10 | 將防火牆與 Panorama 同步。

1. 存取 Panorama 網頁介面，選取 **Commit**（提交）> **Commit and Push**（提交並推送），然後在 Push Scope（推送範圍）中 **Edit Selections**（編輯選擇）。
2. 選取 **Device Groups**（裝置群組），選取包含防火牆的裝置群組，以及 **Include Device and Network Templates**（包括裝置和網路範本）。
3. 選取 **Collector Groups**（收集器群組），並選取包含防火牆的收集器群組。
4. 按一下 **Ok**（確定），以儲存您對 Push Scope（推送範圍）所做的變更。
5. **Commit and Push**（提交並推送）您的變更。



如果您需要產生報告，且報告的期間橫跨舊防火牆的運作期間，到安裝新防火牆後之間所歷經的時間，則您必須針對每道防火牆的序號分別產生查詢，因為在 *Panorama* 上更換序號並不會覆寫日誌中的資訊。

© 2019 Palo Alto Networks, Inc.

疑難排解提交失敗

如果 Panorama 上的提交或推送操作失敗，請檢查下列狀況：

徵兆	條件	解析度
範本或裝置群組推送失敗	防火牆上已停用從 Panorama 接收範本和裝置群組設定變更時，會發生這種情況。	請存取防火牆的 Web 介面，選取 **Device**（裝置）> **Setup**（設定），編輯 Panorama Settings（Panorama 設定），然後按一下 **Enable Device and Network Template**（啟用設備與網路範本）及 **Enable Panorama Policy and Objects**（啟用 **Panorama** 原則與物件）。
Panorama 提交失敗，或是範本、裝置群組或收集器群組推送失敗	Panorama 管理伺服器軟體版本比其管理的專用日誌收集器或防火牆版本要早。	將 Panorama 管理伺服器的軟體版本升級至與受管理的防火牆、日誌收集器及 WildFire 設備和設備叢集相同或更新的版本。如需詳細資料，請參閱Panorama、日誌收集器、防火牆和 WildFire 版本相容性。

© 2019 Palo Alto Networks, Inc.

疑難排解註冊或序號錯誤

在 M-600、M-500 或 M-200 設備上，如果 **Panorama** > **Support**（支援）頁面不顯示支援授權詳細資訊或 **Panorama** > **Setup**（設定）> **Management**（管理）頁面顯示 **Serial Number**（序號）未知，即使在您註冊 Panorama 之後也是如此，執行下列步驟：

STEP 1 | 記錄下您在向 Panorama 下單時 Palo Alto 網路寄給您的訂購完成電子郵件中的 Panorama 序號。

STEP 2 | 選取 **Panorama** > **Setup**（設定）> **Management**（管理），再編輯 [一般設定]。

STEP 3 | 輸入 **Serial Number**（序號），然後按一下 **OK**（確定）。

STEP 4 | 選取 **Commit**（提交）> **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

© 2019 Palo Alto Networks, Inc.

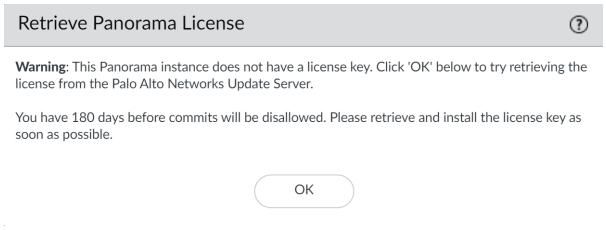
疑難排解報告錯誤

如果 Panorama 無法產生報告，或報告缺少預期的資料，則表示其內容版本（例如，應用程式資料庫）可能與受管理收集器和防火牆上的版本不同。Panorama 上的內容版本必須與受管理收集器和防火牆上的內容版本相同或更舊。如需詳細資料，請參閱Panorama、日誌收集器、防火牆和 WildFire 版本相容性。

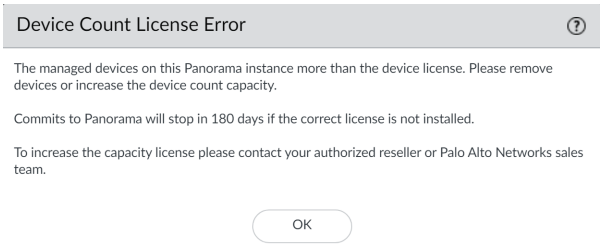
© 2019 Palo Alto Networks, Inc.

疑難排解裝置管理授權錯誤

在升級至 PAN-OS 8.1 後，Panorama 虛擬設備將檢查裝置管理授權是否已成功安裝。若裝置管理授權並未成功安裝，或 Panorama 虛擬設備管理的防火牆數量過裝置管理授權數量，則您有180 天的時間安裝有效的裝置管理授權。如果沒有安裝有效的裝置管理授權，則下列警告會在每次您登入 Panorama 網頁介面時出現：



如果受 Panorama 虛擬設備管理的防火牆數量超過裝置管理授權上限，則下列警告會在每次您登入 Panorama 網頁介面時出現：



若要解決此問題，請安裝有效的裝置管理授權：

STEP 1 | 聯絡您的 Palo Alto 網路銷售代表，或您授權的經銷商以購買合適的裝置管理授權。

STEP 2 | 登入 Panorama 網頁介面。

STEP 3 | 依據 Panorama 虛擬設備是否為在線或離線，來啟動/擷取裝置的管理授權。

- 在 Panorama 虛擬設備與網際網路連線時，啟動/擷取防火牆管理授權。
- 在 Panorama 虛擬設備並未與網際網路連線時，啟動/擷取防火牆管理授權。

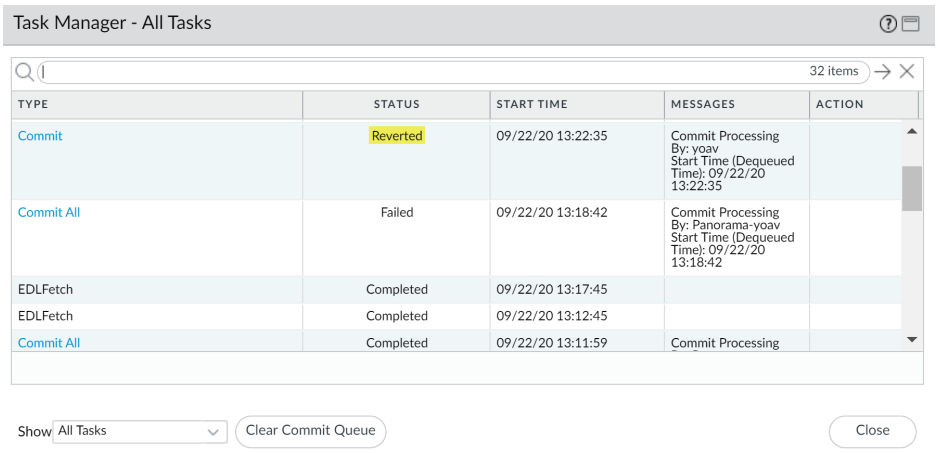
© 2019 Palo Alto Networks, Inc.

疑難排解自動復原防火牆組態

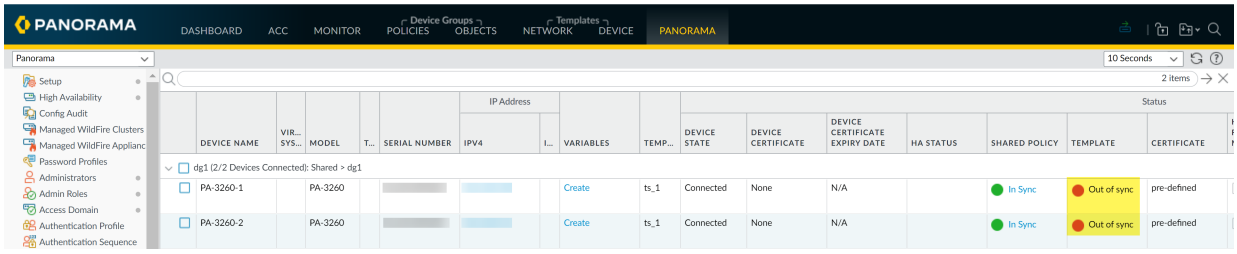
如果組態變致使受管理防火牆自動還原其組態，進而導致 Panorama™ 管理伺服器與受管理防火牆之間連線中斷，則您可以對不同步的防火牆進行疑難排解，以判定所做的變更，並判定上次組態推送的哪些方面造成了防火牆還原其組態。

STEP 1 | 確認受管理防火牆已自動還原至上次執行的組態。

- 在防火牆上
  1. 啟動防火牆 Web 介面。
  2. 按一下 **Tasks**（工作）（在網頁介面右下角）。
  3. 確認上次的認可操作（從 Panorama 推送或在本機認可）顯示 `Reverted`（已還原）狀態。

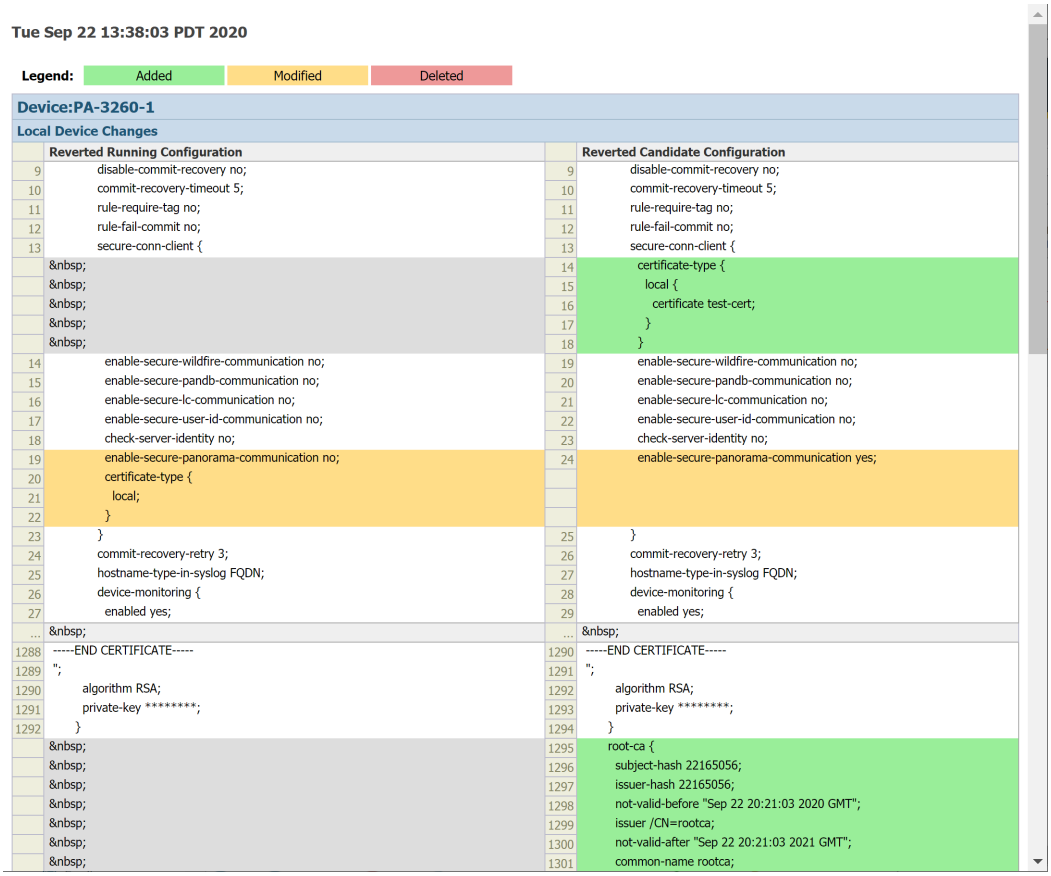


- 在 Panorama 上
  1. 登入 Panorama 網頁介面。
  2. 選取 **Panorama** > **Managed Devices**（受管理的裝置） > **Summary**（摘要）。
  3. 檢視 Shared Policy（共用原則）與 Template（範本）同步狀態。如果您最近從 Panorama 推送組態至您的受管理防火牆並且組態已還原，Shared Policy（共用原則）與 Template（範本）會顯示為 `Out of Sync`（不同步）（取決於所做的組態變更）



STEP 2 | 在受管理防火牆的 Last Merged Diff（上次合併差異）欄中，**Show Last Merged Config Diff**（顯示上次合併組態差異）（ ），以比較目前執行的組態及還原的組態。在此範例中，從 Panorama 推送的原則規則拒絕了受管理防火牆與 Panorama 之間的所有流量，致使防火牆組態自動還原。

© 2019 Palo Alto Networks, Inc.



Tue Sep 22 13:38:03 PDT 2020

Legend: Added Modified Deleted

Device:PA-3260-1

Local Device Changes

	Reverted Running Configuration		Reverted Candidate Configuration
9	disable-commit-recovery no;	9	disable-commit-recovery no;
10	commit-recovery-timeout 5;	10	commit-recovery-timeout 5;
11	rule-require-tag no;	11	rule-require-tag no;
12	rule-fail-commit no;	12	rule-fail-commit no;
13	secure-conn-client {	13	secure-conn-client {
		14	certificate-type {
		15	local {
		16	certificate test-cert;
		17	}
		18	}
14	enable-secure-wildfire-communication no;	19	enable-secure-wildfire-communication no;
15	enable-secure-pandb-communication no;	20	enable-secure-pandb-communication no;
16	enable-secure-lc-communication no;	21	enable-secure-lc-communication no;
17	enable-secure-user-id-communication no;	22	enable-secure-user-id-communication no;
18	check-server-identity no;	23	check-server-identity no;
19	enable-secure-panorama-communication no;	24	enable-secure-panorama-communication yes;
20	certificate-type {		
21	local;		
22	}		
23	}	25	}
24	commit-recovery-retry 3;	26	commit-recovery-retry 3;
25	hostname-type-in-syslog FQDN;	27	hostname-type-in-syslog FQDN;
26	device-monitoring {	28	device-monitoring {
27	enabled yes;	29	enabled yes;
...		...	
1288	-----END CERTIFICATE-----	1290	-----END CERTIFICATE-----
1289	";	1291	";
1290	algorithm RSA;	1292	algorithm RSA;
1291	private-key ********;	1293	private-key ********;
1292	}	1294	}
		1295	root-ca {
		1296	subject-hash 22165056;
		1297	issuer-hash 22165056;
		1298	not-valid-before "Sep 22 20:21:03 2020 GMT";
		1299	issuer /CN=rootca;
		1300	not-valid-after "Sep 22 20:21:03 2021 GMT";
		1301	common-name rootca;

STEP 3 | 在重新推送組態之前，視需要修改組態物件，使受管理防火牆與 Panorama 之間的連線不會中斷。

© 2019 Palo Alto Networks, Inc.

當 Panorama HA 對等關閉時，完成內容更新

當 Panorama™ 為高可用性組態，且部署內容更新至受管理的裝置時，Panorama 將對 HA 對等之間的內容更新工作進行平衡，以減輕各 Panorama 上的負載。當內容更新時某個 HA 對等變得無法存取，對於停止運作的 HA 對等通常推送內容更新的受管理裝置，其內容更新工作失敗。這種情況同時出現在已排程和手動內容更新上。要完成內容更新，您必須手動推動內容更新至那些受管理裝置。

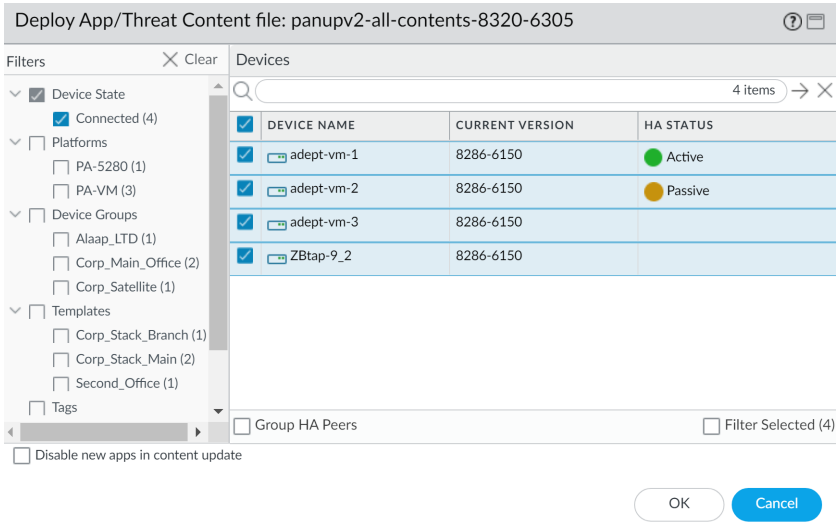
STEP 1 | 登入 Panorama CLI 並為內容更新禁用負載平衡：

```
admin> set dlsrvr distribute no
```

STEP 2 | 登入 Panorama 網頁介面。

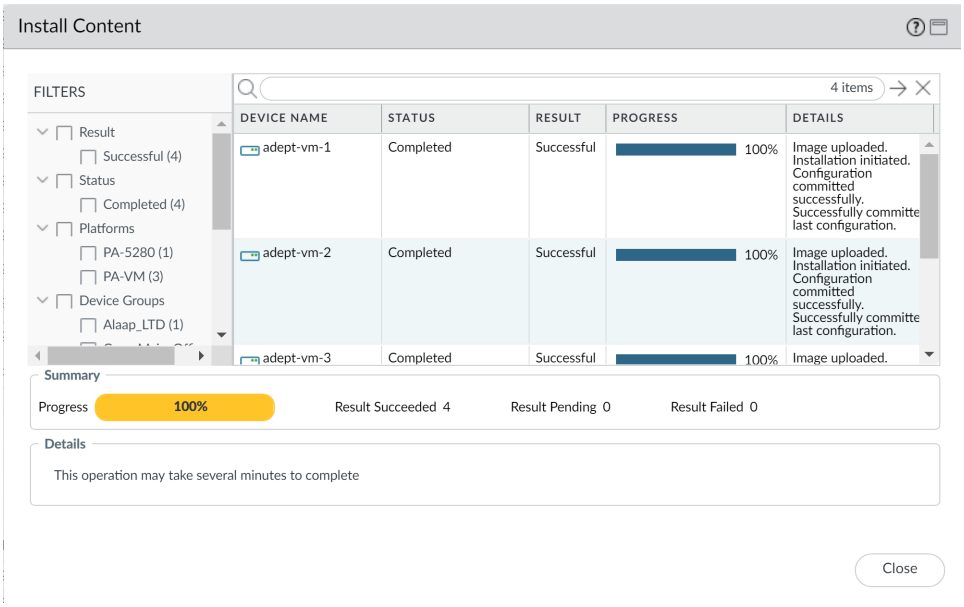
STEP 3 | 選取 **Panorama** > **Device Deployment**（設備部署）> **Dynamic Updates**（動態更新）和 **Install**（安裝）動態更新。

STEP 4 | 選擇內容更新失敗的受管理壯漢子，並按一下 **OK**（確定）。



STEP 5 | 確認內容更新被正確推送至所選受管理裝置。

© 2019 Palo Alto Networks, Inc.



STEP 6 | 登入 Panorama CLI 並為內容更新啟用負載平衡：

```
admin> set dlsrvr distribute yes
```


© 2019 Palo Alto Networks, Inc.

檢視工作成功或失敗狀態

按一下 Panorama 網頁介面右下角的工作管理員圖示 

，以檢視工作的成功或失敗。工作管理員也會顯示專用的訊息來幫助偵錯問題。如需詳細資料，請參閱使用 Panorama 工作管理員。

© 2019 Palo Alto Networks, Inc.

為受管理裝置測試原則比對和連線

在成功推送裝置群組和範本堆疊組態至您的防火牆、日誌收集器和 WF- 500 設備後，測試流量是否與推送至受管理裝置的原則規則匹配，且您的防火牆可以成功連線至所有相關網路資源。

- 疑難排解原則規則流量匹配
- 疑難排解網路資源連線

疑難排解原則規則流量匹配

要為受管理的防火牆執行原則匹配測試，測試您的受管理裝置原則規則設定，確保執行中組態透過允許和拒絕正確流量，保證您的網路安全。與設定規則匹配的流量結果產生後，您可以 **Export to PDF**（匯出至 **PDF**）進行稽核。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 選取 **Panorama** > **Managed Devices**（受管理裝置）> **Troubleshooting**（疑難排解）以執行原則匹配。

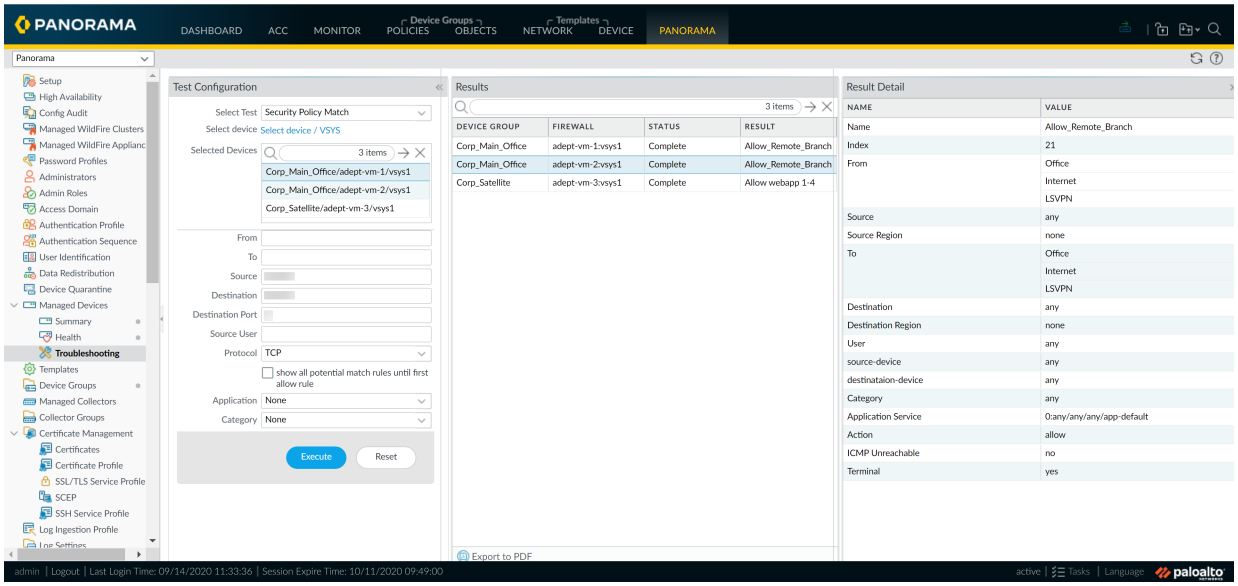
您也可以從 *Policies*（原則）頁籤執行原則匹配測試。

STEP 3 | 輸入必要資訊以執行原則比對測試。此示例中，執行安全原則匹配測試。

1. 從 **Select Test**（選取測試）下拉式清單中選取 **Security Policy Match**（安全原則匹配）。
2. **Select device/VSYS**（選取裝置/VSYS）並選取受管理的防火牆進行測試。
3. 輸入流量的來源 IP 位址。
4. 輸入流量的目標裝置之 IP 位址。
5. 輸入流量所用的協定 IP 位址。
6. 如有必要，請輸入任何與安全原則規則測試相關的其他資訊。

STEP 4 | **Execute**（執行）安全性原則比對測試。

STEP 5 | 選取安全原則匹配結果，以查看符合測試準則的原則規則。



© 2019 Palo Alto Networks, Inc.

疑難排解網路資源連線

為受管理防火牆執行連線測試，確保您的受管理裝置可以連線至所有相關網路資源。為您的受管理裝置測試裝置組態，確保執行中組態可保證網路安全，方法是透過允許您確認推送至受管理裝置的組態仍允許裝置連線至各資源，如您的日誌收集器、設定的外部動態清單和 Palo Alto Networks 更新伺服器。此外，您可以執行路由、WildFire®、威脅資料庫、ping 和追蹤路由連線測試，確認 Panorama™ 和受管理裝置可存取任何與您的網路操作和安全密切相關的外部網路資源。產生結果後，您可以 **Export to PDF**（匯出至 **PDF**）用於稽核。

Ping 連線測試僅在執行 *PAN-OS 9.0* 或更高版本的防火牆上受支援。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 選取 **Panorama** > **Managed Devices**（受管理裝置）> **Troubleshooting**（疑難排解）以執行連線測試。

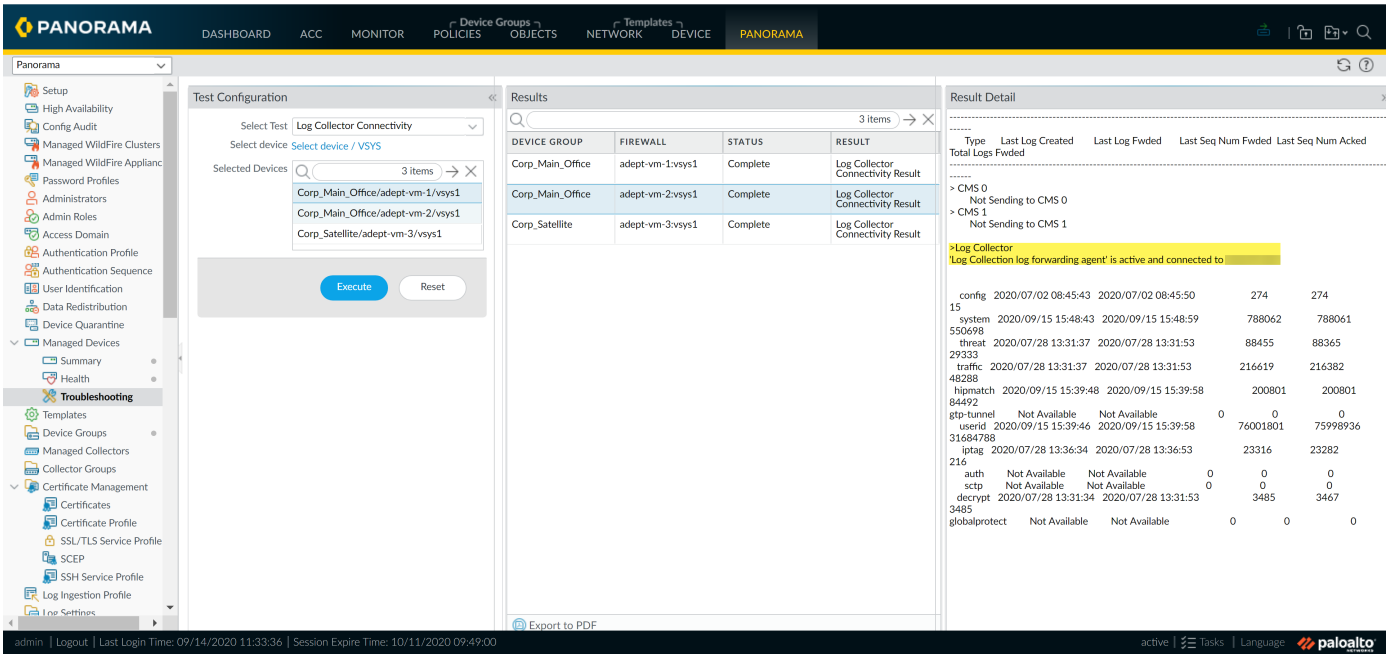
您也可以從 *Policies*（原則）頁籤執行原則匹配測試。

STEP 3 | 輸入必要資訊以執行連線測試。此示例中，執行日誌收集器連線測試。

1. 從 **Select Test**（選取測試）下拉式清單中選取 **Log Collector Connectivity**（日誌收集器連線）。
2. **Select device/VSYS**（選取裝置/VSYS）並選取受管理的防火牆進行測試。
3. 如有必要，請輸入任何與連線測試相關的其他資訊。

STEP 4 | **Execute**（執行）日誌收集器連線測試。

STEP 5 | 選取日誌收集器連線結果，以檢閱所選裝置的日誌收集器連線狀態。



© 2019 Palo Alto Networks, Inc.

從 Panorama 10.0 降級

PAN-OS®10.0 引入了為專用日誌收集器和 WildFire 設備設定本機和 Panorama 管理員的功能，透過乙太網路介面轉送日誌的功能，氣隙 Panorama™ 管理伺服器的自動動態更新，對原則最佳化工具中的篩選後規則執行動作的功能，以及用於監控、ACC、按需報告的額外 60 天和 90 天篩選器。但是，這些功能與執行 PAN-OS 9.1 或更舊版本的 Panorama 不相容。使用以下工作流程在降級日誌收集器和執行 Panorama 10.0 版的 Panorama 至更舊的功能版本前，先降級防火牆。對於管理本機日誌收集器的 Panorama 與管理一個或多個專用日誌收集器的 Panorama，此程序都適用。

檢閱 Palo Alto Networks 相容性矩陣，確認您想要降級的防火牆和設備相容於您想要降級的 *PAN-OS* 發佈版本。對於您可以降級的防火牆和設備，您也應該檢閱升級/降級注意事項，確保您了解降級之後會不同或無法使用的所有功能和組態設定。

STEP 1 | 為 Panorama 和受管理裝置儲存設定檔案備份。

1. **Export Panorama and device configuration snapshot**（匯出 **Panorama** 和裝置組態快照）（**Panorama** > **Setup**（設定）> **Operations**（操作））。
2. 將匯出的 .tgz 檔案儲存至 Panorama、日誌收集器和防火牆外部的位置。如果發生問題而必須重來，您可以使用此備份來還原設定。

STEP 2 | 如果您為專用日誌收集器設定了驗證，且移除了 **admin** 管理員，請設定新的 **admin** 使用者並推送到您的專用日誌收集器。

專用日誌收集器必須設定 `admin` 使用者才可降級至 PAN-OS 9.1 和更早版本。

STEP 3 | 降級每個執行 PAN-OS 10.0 版的防火牆。

如果降級一個以上的防火牆，請先將防火牆特定的每個 *PAN-OS 9.1* 映像下載至 *Panorama* 再開始降級，讓過程順暢進行。例如，若要將 *PA-220* 防火牆降級至 *PAN-OS 9.1.0*，請下載 *`PanOS_220-9.1.0`* 或 *`PanOS_3000-9.1.0`* 映像。

Panorama 要求所有防火牆必須執行相同或更舊的 PAN-OS 版本。因此，請根據您的環境，使用並重複下列適當的工作，將所有受管理的防火牆降級之後，您才能降級 Panorama：

1. **Check Now**（立即檢查）有無可用的映像（**Panorama** > **Device Deployment**（裝置）> **Software**（軟體））。
2. 針對您想要降級的每個防火牆型號或系列，尋找 PAN-OS 9.1 映像。如果尚未下載映像，請 **Download**（下載）。

非 **HA** 防火牆

Install（安裝）（動作欄）適當的 PAN-OS 9.1 版本，選取您想要降級的所有防火牆，選取 **Reboot device after install**（安裝後重新啟動裝置），然後按一下 **OK**（確定）。

主動/主動 **HA** 防火牆

1. 按一下 **Install**（安裝），停用（清除）**Group HA Peers**（群組 **HA** 對等），選取任一 HA 對等，選取 **Reboot device after install**（安裝後重新啟動裝置），然後按一下 **OK**（確定）。繼續之前，等候防火牆完成重新開機。
2. 按一下 **Install**（安裝），停用（清除）**Group HA Peers**（群組 **HA** 對等），選取您在上一步未更新的 HA 對等、選取 **Reboot device after install**（安裝後重新啟動裝置），然後按一下 **OK**（確定）。

主動/被動 **HA** 防火牆

在此範例中，主動防火牆名為 fw1，被動防火牆名為 fw2：

© 2019 Palo Alto Networks, Inc.

1. **Install**（安裝）（動作欄）適當的更新，停用（清除）**Group HA Peers**（群組 **HA** 對等），選取 fw2，選取 **Reboot device after install**（安裝後重新啟動裝置），然後按一下 **OK**（確定）。
2. 當 fw2 完成重新開機後，向 fw1 確認（**Dashboard**（儀表板）> **High Availability**（高可用性）Widget）仍然是主動對等，且 fw2 仍然是被動對等（Local（本機）防火牆狀態為 `active`（主動），Peer（對等）-fw2 為 `passive`（被動））。
3. 存取 fw1 和 **Suspend local device**（暫停本機裝置）（**Device**（裝置）> **High Availability**（高可用性）> **Operational Commands**（操作命令））。
4. 存取 fw2（**Dashboard**（儀表板）> **High Availability**（高可用性）），確認 Local（本機）防火牆狀態 `active`（主動），Peer（對等）防火牆—fw1—為 `suspended`（暫停）。
5. 存取 Panorama，選取 **Panorama** > **Device Deployment**（裝置部署）> **Software**（軟體）**Install**（安裝）（操作欄）適當更新，停用（清除）**Group HA Peers**（群組 **HA** 對等），選取 fw1，選取 **Reboot device after install**（安裝後重新啟動裝置），然後按一下 **OK**（確定）。繼續之前，等候 fw1 完成重新開機。
6. 存取 fw1（**Dashboard**（儀表板）> **High Availability**（高可用性）Widget），確認 Local（本機）防火牆狀態為 `passive`（被動），Peer（對等）(fw2) 為 `active`（主動）。

如果在 *Election*（選取）設定中啟用先佔（*Device*（裝置）> *High Availability*（高可用性）> *General*（一般））*fw1* 在重新開機之後會恢復為主動對等。

STEP 4 | 降級每個執行 Panorama 10.0 的日誌收集器。

1. **Check Now**（立即檢查）有無可用的映像（**Panorama** > **Device Deployment**（裝置）> **Software**（軟體））。
2. 尋找 Panorama 9.1 映像。如果尚未下載映像，請 **Download**（下載）（Action（動作）欄）。
3. 下載完成之後，將映像 **Install**（安裝）在每個執行 Panorama 10.0 的日誌收集器上。選取 **Reboot device after install**（安裝後重新啟動裝置），可在升級完成之後自動重新啟動裝置。

STEP 5 | 降級 Panorama。

1. **Check Now**（立即檢查）有無可用的映像（**Panorama** > **Device Deployment**（裝置）> **Software**（軟體））。
2. 尋找 Panorama 9.1 映像。如果尚未下載映像，請 **Download**（下載）。
3. 下載完成之後，將映像 **Install**（安裝）在 Panorama 上。
4. 按照下列方式重新啟動 Panorama：
   - 如果提示您重新啟動，請按一下**Yes**（是）。如果您看到 **CMS Login**（**CMS** 登入）提示，請按下 Enter，無須鍵入使用者名稱或密碼。當 Panorama 登入提示出現時，請輸入您在初始設定期間設定的使用者名稱與密碼。
   - 如果未提示重新啟動，請選取**Panorama** > **Setup**（設定）> **Operations**（操作），然後按一下 **Reboot Panorama**（重新啟動 **Panorama**）（裝置操作）。

STEP 6 | 將 Panorama 日誌移轉為 PAN-OS 8.1 日誌格式。

轉移過程中，日誌資料在 *ACC* 或 *Monitor*（監控器）頁籤中不可見。此外，轉移完成之前，新日誌資料不會被轉送至日誌收集器。

1. 檢視進入日誌記錄速率。

   最佳作法是在傳入日誌速率較低時開始日誌移轉。若要檢查速率，請從日誌收集器 CLI 執行下列命令：

```
admin@FC-M500-1> debug log-collector log-collection-stats show incoming-logs
```


© 2019 Palo Alto Networks, Inc.

在日誌移轉期間，*CPU* 使用率通常很高（接近 *100%*），操作會繼續正常運作。在資源競用的情況下，日誌移轉會調節以利於傳入日誌和其他程序。

2. 開始將每個日誌收集器上的日誌移轉為之前的格式。

   若要開始移轉，請從每個日誌收集器的 CLI 輸入下列命令：

```
admin@FC-M500-1> request logdb migrate lc serial-number <ser_num> 開始
```

3. 檢視日誌移轉狀態，以估計將所有現有日誌移轉為之前格式所需的時間。

```
admin@FC-M500-1> request logdb migrate lc serial-number <ser_num> 狀態
 Slot: all
Migration State: In Progress
Percent Complete: 0.04
Estimated Time Remaining: 451 hour(s) 47 min(s)
```


© 2019 Palo Alto Networks, Inc.