paloalto TECHDOCS

WildFire 設備管理

docs.paloaltonetworks.com

Contact Information

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

About the Documentation

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

Copyright

Last Revised

April 8, 2025

Table of Contents

WildFire 設備概要

WildFire™ 透過同時使用動態和靜態分析來偵測威脅並封鎖惡意程式，可偵測並防範零時差惡意軟體的攻擊。WildFire 擴展 Palo Alto Networks 新一代防火牆的功能，可識別並封鎖已鎖定及未知的惡意軟體。

關於 WildFire 設備

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

WildFire 設備提供內部部署的 WildFire 私人雲端，能夠讓您在沙箱環境中分析可疑的檔案，完全不需要讓防火牆將檔案傳送到網路之外。若要使用 WildFire 設備託管 WildFire 私人雲端，請設定提交樣本至 WildFire 設備進行分析的防火牆。WildFire 設備會在本機進行所有檔案的沙箱作業，並使用 WildFire 公共雲端所用的同一個引擎分析檔案是否有惡意行為。幾分鐘內，私人雲端將返回分析結果至防火牆 **WildFire Submissions**（**WildFire** 提交）日誌。

WildFire 設備管理涵蓋 *WildFire* 設備的設定和配置，但與 *WildFire* 公共雲端共用許多操作設計和功能。如需 *WildFire* 分析功能的詳細資訊，請參閱進階 *WildFire* 管理。

您可以繼續啟用 WildFire 設備以：

- ❑ 為發現的惡意軟體產生本機防毒和 DNS 特徵碼，並指派 URL 類別至惡意連結。之後，您可以啟用連接的防火牆來每五分鐘擷取最新特徵碼和 URL 類別。
- ❑ 提交惡意軟體至 WildFire 公共雲端。WildFire 公共雲端重新分析該樣本，並產生檢測惡意軟體的特徵碼——該特徵碼可在數分鐘內實現可用，以保護全球的使用者
- ❑ 提交本機產生的惡意軟體報告（不傳送原樣本內容）至 WildFire 公共雲端，這有助於收集 WildFire 統計資料及威脅情報。

您可以使用有效的 WildFire 使用授權設定多達 100 個 Palo Alto Networks 防火牆來轉送至單一 WildFire 設備。除 WildFire 防火牆使用授權以外，啟用 WildFire 私人雲端部署無需額外的 WildFire 使用授權。

您可以使用本機設備 CLI 管理 WildFire 設備，或者您可以使用 Panorama 集中管理 WildFire 設備。從 PAN-OS 8.0.1 開始，您可以將 WildFire 設備分組至 WildFire 設備叢集並在本機或從 Panorama 管理叢集。

WildFire 私人雲端

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

在 Palo Alto Networks 私人雲端部署中，Palo Alto Networks 防火牆將檔案轉送至用於託管私人雲端分析位置的公司網路上的 WildFire 設備。一個 WildFire 私人雲端可以接收多達 100 個 Palo Alto Networks 防火牆的檔案進行分析。

由於 WildFire 私人雲端是本機沙箱，其分析的良性、灰色和釣魚網路樣本並未離開您的網路。預設情況下，私人雲端也不傳送您的網路之外已發現的惡意軟體；然而，您可選擇自動轉送惡意軟體至 WildFire 公共雲端進行特徵碼產生和散佈。此情況下，WildFire 公共雲端重新分析樣本，產生特徵碼識別該樣本，並將特徵碼散佈至具有威脅防範或 WildFire 使用授權的全球 Palo Alto Networks 防火牆。

如果您不希望 WildFire 私人雲端轉送惡意樣本至您的網路以外，您可以：

- 啟用 WildFire 設備以轉送惡意軟體報告（而非樣本本身）至 WildFire 公共雲端。WildFire 報告提供統計資訊，有助於 Palo Alto Networks 評估惡意軟體的廣泛性及傳播性。如需詳細資訊，請參閱 透過 WildFire 設備提交惡意軟體或報告。
- 手動上傳檔案至 WildFire 入口網站取代自動轉送所有惡意軟體，或使用 WildFire API 提交檔案至 WildFire 公共雲端。

您也可以在 WildFire 設備上進行 啟用本機特徵碼及 URL 類別產生。WildFire 設備產生的特徵碼將散佈至連接的防火牆，以便防火牆下次偵測到惡意軟體時進行有效封鎖。

Android 應用程式套件 (APK) 和 MAC OSX 檔案不支援 WildFire 私人雲端分析。

WildFire 混合型雲端

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

在 WildFire 混合型雲端部署中，防火牆可將某些樣本轉送至 Palo Alto Networks 託管的一個 WildFire 公共雲端，以及將其他樣本轉送至由 WildFire 設備託管的 WildFire 私人雲端。WildFire 混合型雲端部署可在本機及網路內靈活分析私人文件，而 WildFire 公共雲端則分析源自網際網路的檔案。例如只轉送支付卡行業 (PCI) 及受保護的健康醫療資訊 (PHI) 資料至 WildFire 私人雲端進行分析，同時轉送可攜式執行檔 (PE) 至 WildFire 公共雲端進行分析。在 WildFire 混合型雲端部署中，將檔案卸載至公共雲端進行分析可讓您從之前在 WildFire 公共雲端中所處理檔案的提示裁定中受益，還可釋放 WildFire 設備容量來處理敏感性內容。此外，您可將某些檔案類型轉送至目前不支援 WildFire 設備分析的 WildFire 公共雲端，例如 Android 應用程式套件 (APK) 檔案。

在 WildFire 混合型雲端部署中，一個檔案可能同時符合進行公共雲端分析和私人雲端分析的標準；在這種情況下，該檔案將作為預警措施僅提交至私人雲端。

若要設定混合雲端轉送，請參閱 轉送檔案以進行 WildFire 設備分析。

WildFire 設備介面

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

WF-500 設備配備有四個 RJ-45 Ethernet 連接埠，位於設備背面。這些連接埠標示為 **MGT**、**1**、**2** 和 **3**，並對應特定介面。

WildFire 設備有三個介面：

- **MGT**——接收所有從防火牆轉送的檔案，並且將載明結果的日誌傳回防火牆。請參閱 設定 WildFire 設備。
- **Virtual Machine Interface (VM interface)**（虛擬電腦介面（**VM** 介面））—可供網路存取 WildFire 沙箱系統，使樣本檔案能夠與網際網路通訊，這讓 WildFire 能夠更進一步分析樣本的行為。設定 VM 介面之後，WildFire 即可觀察惡意軟體通常不會在無法存取網路時執行的惡意行為，例如回撥活動。不過，為了避免惡意軟體從沙箱進入網路，請在有網際網路連線的隔離網路上設定 VM 介面。您也可以啟用 Tor 選項來向樣本所存取的惡意網站隱藏由司使用的公共 IP 位址。如需 VM 介面的詳細資訊，請參閱 設定 WildFire 設備 VM 介面。
- 叢集管理介面—在屬於 WildFire 設備叢集的 WildFire 設備節點之間提供叢集範圍內的通訊。它和用於防火牆操作的 MGT 介面不同。您可以將 Ethernet2 介面或 Ethernet3 介面（分別標示為 **2** 和 **3**）設定為叢集管理介面。

取得由網路管理員對 MGT 連接埠、VM 介面及叢集管理介面（僅限 WildFire 設備叢集）設定網路連線所需的資訊（IP 位址、子網路遮罩、閘道、主機名稱、DNS 伺服器）。防火牆與設備之間所有的通訊都透過 MGT 連接埠進行，包括檔案提交、WildFire 日誌傳遞和設備管理。因此，請確定防火牆可連線到設備的 MGT 連接埠。此外，設備必須能夠連線到 updates.paloaltonetworks.com，擷取本身的作業系統軟體更新。

WildFire 設備檔案類型支援

下表列出支援在 WildFire 設備私人雲端中以及透過 WildFire 入口網站直接上傳進行分析的檔案類型。

支援進行分析的檔案類型	**WildFire** 私人雲端（**WildFire** 設備）	**WildFire Portal | API**（直接上傳；所有區域）
電子郵件包含的連結	✓	✓
Android 應用程式套件 (APK) 檔案	✗	✓
Adobe Flash 檔案	✓	✓
Java 歸檔 (JAR) 檔案	✓	✓
Microsoft Office 檔案（包括 SLK 和 IQY 檔案**）	✓	✓
可攜可執行檔（包括 MSI 檔案**）	✓	✓
可攜式文件格式 (PDF) 檔案	✓	✓
Mac OS X 檔案	✗	✓
Linux（ELF 檔案和 Shell 指令碼）檔案	✗	✓
封存檔（RAR、7-Zip 和 ZIP）檔案*	✓	✓
指令碼（BAT、JS、VBS、PS1 和 HTA）檔案	✓	✓
指令碼（Perl 和 Python）指令碼	✗	✓

支援進行分析的檔案類型	**WildFire** 私人雲端（**WildFire** 設備）	**WildFire Portal | API**（直接上傳；所有區域）
封存檔（ZIP [直接上傳] 和 ISO）檔案*	✗	✓

* ZIP 檔案不會直接轉送到 Wildfire 雲端進行分析。而是首先由防火牆解碼，與 WildFire 分析設定檔條件相符的檔案將單獨轉送以進行分析。

** WildFire 設備不支援 MSI、IQY 和 SLK 檔案分析。

設定和管理 WildFire 設備

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

WildFire™ 設備可被設定為本機託管的 WildFire 私人雲端。下列主題說明備妥 WildFire 設備來接收檔案進行分析，如何管理設備，以及如何啟用設備在本機產生威脅特徵碼及 URL 類別。

- 關於 WildFire 設備
- 設定 WildFire 設備
- 設定在獨立 WildFire 設備上使用自訂憑證進行驗證
- 設定 WildFire 設備 VM 介面
- 啟用 WildFire 設備分析功能
- 利用網際網路連線安裝 WildFire 設備裝置憑證

設定 WildFire 設備

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

本節說明在網路整合 WildFire 設備和執行基本設定所需的步驟。

STEP 1 | 將 WildFire 設備安裝在機架並進行佈線。

請參閱 WildFire 設備硬體參考指南的指示。

STEP 2 | 使用 MGT 或主控台連接埠將電腦連接到設備，然後開啟設備的電源。

1. 連接到主控台連接埠或 MGT 連接埠。這兩者均位於設備的背面。
   - **Console Port**（主控台連接埠）—這是 9 針腳公序列接頭。對於主控台應用程式，使用下列設定：9600-8-N-1。將提供的纜線連接到管理電腦的序列連接埠或 USB 轉序列轉換頭。
   - **MGT Port**（**MGT** 連接埠）—這是 Ethernet RJ-45 連接埠。依預設，MGT 連接埠 IP 位址是 192.168.1.1。管理電腦的介面必須位於 MGT 連接埠所在的同一個子網路。例如，將管理電腦的 IP 位址設定為 192.168.1.5。
2. 開啟設備的電源。

   設備將在您連接電源至首個電源供應器時啟動，並發出警告嗶聲，直到您連接第二個電源供應器為止。如果設備的插頭已經插上，而且設備處於關閉狀態，請使用設備正面的電源按鈕開啟電源。

STEP 3 | 註冊 WildFire 應用程式。

1. 從設備的 S/N 標籤取得序號，或執行下列命令並參閱 `serial`（序號）欄位：

```
admin@WF-500> show system info
```

2. 從瀏覽器登入 Palo Alto Networks 支援入口網站。
3. 註冊設備，如下所示：
   - 如果這是第一台註冊的 Palo Alto Networks 設備且您尚未登入，請在頁面底部按一下 **Register**（註冊）。

     若要註冊，請提供電子郵件地址和設備的序號。出現提示時，請設定用來存取 Palo Alto Networks 支援社群的使用者名稱與密碼。
   - 對於現有帳戶，請登入，然後按一下 **My Devices**（我的設備）。向下捲動至畫面下方的 **Register Device**（註冊設備）部分，然後輸入設備的序號、您的城市及郵遞區號，然後按一下 **Register Device**（註冊設備）。
4. 若要確認 WildFire 在 WildFire 設備上註冊，使用 SSH 用戶端或主控台連接埠登入設備。輸入管理員的使用者名稱/密碼，然後在設備上輸入下列命令：

```
admin@WF-500> test wildfire registration
```

下列輸入指示已經向其中一個 Palo Alto Networks WildFire Cloud 伺服器註冊設備。

```
Test wildfire wildfire registration: successful download
 server list:  successful select the best server: cs-
s1.wildfire.paloaltonetworks.com
```

STEP 4 | 重設管理密碼。

1. 執行命令以設定新密碼：

```
admin@WF-500> set password
```

2. 輸入舊密碼，按下輸入，然後輸入並確認新密碼。交付設定以確保重新啟動時儲存新密碼。

   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，以及一個數字與特殊字元。

   務必採用密碼強度最佳做法 以確保嚴格的密碼。
3. 輸入 **`exit`** 登出，然後再次登入，確認已設定新密碼。

STEP 5 | 進行管理介面設定。

本範例使用了以下 IPv4 值，但該設備也支援 IPv6 位址：

- IPv4 位址 - 10.10.0.5/22
- 子網路遮罩 - 255.255.252.0
- 預設閘道 - 10.10.0.1
- 主機名稱 - wildfire-corp1
- DNS 伺服器 - 10.0.0.246

1. 使用 SSH 用戶端或主控台連接埠登入設備，並進入設定模式：

```
admin@WF-500> configure
```

2. 設定 IP 資訊：

```
admin@WF-500# set deviceconfig system ip-address 10.10.0.5
 netmask 255.255.252.0 default-gateway 10.10.0.1 dns-setting
 servers primary 10.0.0.246
```

將以上命令的 *primary* 改為 *secondary*，並排除其他 *IP* 參數，設定次要 *DNS* 伺服器。例如：

```
admin@WF-500# set deviceconfig system dns-setting servers
 secondary 10.0.0.247
```

3. 設定主機名稱（此範例為 wildfire-corp1）：

```
admin@WF-500# set deviceconfig system hostname wildfire-corp1
```

4. 交付設定以啟動新的管理 (MGT) 連接埠設定：

```
admin@WF-500# commit
```

5. 將 MGT 介面連接埠連接到網路交換器。
6. 在公司網路上，或者在存取管理網路上的設備時，所需要的任何網路上，重新放置管理 PC。
7. 從管理電腦使用 SSH 用戶端連線至新 IP 位址，或指派給設備 MGT 連接埠的主機名稱。在此範例中，IP 位址是 10.10.0.5。

STEP 6 | 使用 Palo Alto Networks 發給的 WildFire 授權碼啟動設備。

雖然 *WildFire* 設備在缺少授權碼的情況下可運作，但如果欠缺有效的授權碼，則無法擷取軟體更新。

1. 變更為操作模式：

```
admin@WF-500# exit
```

2. 擷取並安裝 WildFire 授權：

```
admin@WF-500> request license fetch auth-code <auth-code>
```

3. 確認授權：

```
admin@WF-500> request support check
```

顯示支援網站及支援合約日期的相關資訊。確認所顯示的日期有效。

STEP 7 | 設定 WildFire 設備時鐘。

設定時鐘有兩種方式。您可以手動設定日期、時間及時區，或者可以設定 WildFire 設備以將其本機時鐘與網路時間協定 (NTP) 伺服器同步。

- 要手動設定時鐘，請輸入下列命令：

```
admin@WF-500> set clock date <YYYY/MM/DD> time <hh:mm:ss>
 admin@WF-500> configure admin@WF-500# set deviceconfig system
 timezone <timezone>
```

WildFire 詳細報告中顯示的時間戳记將使用設備上設定的時區。如果多個地區的管理員會檢視報告，請考慮將時區設為 *UTC*。

- 要將 WildFire 設備設定為與 NTP 伺服器同步，請輸入下列命令：

```
admin@WF-500> configure admin@WF-500# set deviceconfig system
 ntp-servers primary-ntp-server ntp-server-address <NTP primary
 server IP address> admin@WF-500# set deviceconfig system ntp-
servers secondary-ntp-server ntp-server-address <NTP secondary
 server IP address>
```

WildFire 設備不會優先考慮主要或次要 *NTP* 伺服器；它會與任一伺服器同步。

STEP 8 | （NTP 設定選用）設定 NTP 驗證。

- 停用 NTP 驗證：

```
admin@WF-500#set deviceconfig system ntp-servers primary-ntp-server authentication-type none
```

- 啟用對稱金鑰交換（共用密碼）以驗證 NTP 伺服器時間更新：

```
admin@WF-500#set deviceconfig system ntp-servers primary-ntp-server authentication-type symmetric-key
```

  繼續輸入 **key-ID**(1 - 65534)，選擇要在 NTP 驗證中使用的 **algorithm**（**MD5** 或 **SHA1**），然後輸入並確認驗證演算法 **authentication-key**。

- 使用 Autokey（公開金鑰密碼）來驗證 NTP 伺服器時間更新：

```
admin@WF-500# set deviceconfig system ntp-servers primary-ntp-server authentication-type autokey
```

STEP 9 | 選擇設備將用於分析檔案的虛擬電腦影像檔。

影像檔應以最準確代表使用者電腦所安裝軟體的屬性為基礎。每個虛擬影像皆包含不同版本的作業系統與軟體，例如 Windows XP、Windows 7 32 位元或 64 位元、特定版本的 Adobe Reader 及 Flash。雖然您將設備設定為使用一個虛擬電腦影像檔設定，但設備會使用影像檔的多個執行個體以提升效能。

- 若要檢視可用虛擬電腦清單，以判定最能代表您環境的虛擬電腦：

```
admin@WF-500> show wildfire vm-images
```

- 請執行下列命令檢視目前的虛擬電腦影像檔，並參閱 `Selected VM` 欄位：

```
admin@WF-500> show wildfire status
```

- 選取設備將用於分析的影像檔：

```
admin@WF-500# set deviceconfig setting wildfire active-vm <vm-image-number>
```

  例如，若要使用 vm-5：

```
admin@WF-500# set deviceconfig setting wildfire active-vm vm-5
```

STEP 10 | 啟用 WildFire 設備，在分析的檔案尋找網路存取時，觀察惡意軟體行為。

設定 WildFire 設備 VM 介面。

STEP 11 | #unique_16

STEP 12 | （選用）啟用 WildFire 設備，以執行快速裁定查找並將裁定與 WildFire 公共雲端同步。

下列 CLI 命令可以啟用 WildFire 設備，以執行快速裁定查找並將裁定與 WildFire 公共雲端同步。此功能預設為停用；設定命令為 **yes** 以啟用此功能。

```
admin@WF-500# set deviceconfig setting wildfire cloud-intelligence
 cloud-query yes | no
```

STEP 13 | （選用）啟用 WildFire 設備，以獲得每日 Palo Alto Networks 內容更新，以輔助和提高惡意軟體分析。

啟用 WildFire 設備分析功能

STEP 14 | （選用）啟用 WildFire 設備，以產生 DNS、防毒特徵碼和 URL 類別，以及散佈新特徵碼和 URL 類別至連接的防火牆。

啟用本機特徵碼及 URL 類別產生

STEP 15 | （選用）自動提交 WildFire 私人雲端發現的惡意軟體至 WildFire 公共雲端，以支援針對惡意軟體的全球保護。

提交惡意軟體至 WildFire 公共雲端。

STEP 16 | （選用）如果您不想轉送 WildFire 私人雲端之外的惡意軟體樣本，可轉而提交報告至 WildFire 公共雲端。

如果不希望提交本機發現的惡意軟體至 *WildFire* 公共雲端，則最佳做法是啟用惡意軟體分析報告提交，以促進及改善 *WildFire* 威脅情報。

提交分析報告至 WildFire 公共雲端。

STEP 17 | （選用）允許其他使用者管理 WildFire 設備。

您可指派兩個角色類型：超級使用者和超級讀取者。超級使用者相當於管理員帳戶，超級讀取者僅擁有讀取權。

在此範例中，您將建立使用者 bsimpson 的超級讀取者帳戶：

1. 進入組態模式：

```
admin@WF-500> configure
```

2. 建立使用者帳戶：

```
admin@WF-500# set mgt-config users bsimpson <password>
```

3. 輸入並確認新密碼。
4. 指派超級讀取者角色：

```
admin@WF-500# set mgt-config users bsimpson permissions role-
based superreader yes
```

STEP 18 | 設定 RADIUS 驗證供管理者存取。

1. 使用下列選項建立 RADIUS 設定檔：

```
admin@WF-500# set shared server-profile radius <profile-name>
```

（設定 RADIUS 伺服器與其他屬性。）

2. 建立驗證設定檔：

```
admin@WF-500# set shared authentication-profile <profile-name>
 method radius server-profile <server-profile-name>
```

3. 為本機管理員帳戶指派設定檔：

```
admin@WF-500# set mgt-config users username authentication-
profile <authentication-profile-name>
```

轉送檔案以進行 WildFire 設備分析

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

設定 Palo Alto Networks 防火牆，轉送未知檔案或電子郵件連結及與現有防毒特徵碼相符的封鎖檔案，以進行分析。使用 **WildFire Analysis**（**WildFire** 分析）設定檔來定義轉送至 WildFire 私人雲端的檔案（或除此之外，用於混合雲端部署的公共雲端），然後附加設定檔至安全性規則，以觸發零時差惡意軟體檢查。

根據使用中的應用程式、偵測到的檔案類型、電子郵件訊息中包含的連結或樣本的傳輸方向（上載、下載或兩者）指定轉送進行分析的流量。例如，您可以將防火牆設定為轉送可攜式可執行檔 (PE) 或使用者瀏覽網頁時嘗試下載的任何檔案。除未知樣本外，防火牆還會轉送與現有防毒特徵碼相符的封鎖檔案。這樣，可以根據特徵碼已成功阻止，但 WildFire 和防火牆之前都沒有遇到過的惡意軟體變體，為 Palo Alto Networks 提供有價值的威脅情報來源。

您可以將 WildFire 分析資源擴展到 WildFire 混合型雲端，透過設定防火牆繼續將敏感檔案轉送到您的 WildFire 私人雲端進行本機分析，並將不太敏感或不受支援的檔案類型轉送到 WildFire 公共雲端。

此外，您可使用 WildFire 設備資源分析特定檔案類型，包括文件（Microsoft Office 檔案和 PDF）或 PE。例如，如果您部署 WildFire 混合型雲端 以在一個 WildFire 公共雲端中分析本機文件和 PE，可以使用所有分析環境來分析文件。這讓您可以將 PE 的分析轉移到公共雲端，並配置額外 WildFire 設備資源處理敏感文件。

開始之前：

- ❑ 如果設定為轉送檔案的防火牆與 WildFire 雲端或 WildFire 設備之間有其他防火牆，請確定介於中間的防火牆允許下列連接埠：

連接埠	使用方式
443	• 報名 • PCAP 下載 • 樣本下載 • 報告擷取 • 檔案提交 • PDF 報告下載
10443	動態更新

STEP 1 | （僅限 PA-7000 系列防火牆）若要啟用 PA-7000 系列防火牆來轉送樣本進行 WildFire 分析，您首先必須在 NPC 上將一個資料連接埠設定為記錄卡介面。如果您的 PA-7000 系列設備配備了 LFC（記錄轉送卡），則必須設定 LFC 使用的連接埠。設定後，當轉送 WildFire 樣本時，記錄卡連接埠或 LFC 介面將優先於管理連接埠。

STEP 2 | 指定要將範例轉送到的 WildFire 私人雲端或混合雲端。

選取 **Device**（裝置） > **Setup**（設定） > **WildFire** 並根據您的 WildFire 雲端部署（私人或混合）編輯一般設定。

WildFire 私人雲端：

1. 在 **WildFire Private Cloud**（**WildFire** 私人雲端）欄位中輸入 WildFire 設備的 IP 位址或 FQDN。

WildFire 混合型雲端：

1. 輸入 **WildFire Public Cloud**（**WildFire** 公共雲端） URL：
   - 美國：**wildfire.paloaltonetworks.com**
   - 歐洲：**eu.wildfire.paloaltonetworks.com**
   - 日本：**jp.wildfire.paloaltonetworks.com**
   - 新加坡：**sg.wildfire.paloaltonetworks.com**
   - 英國：**uk.wildfire.paloaltonetworks.com**
   - 加拿大：**ca.wildfire.paloaltonetworks.com**
   - 澳洲：**au.wildfire.paloaltonetworks.com**
   - 德國：**de.wildfire.paloaltonetworks.com**
   - 印度：**in.wildfire.paloaltonetworks.com**
   - 瑞士：**ch.wildfire.paloaltonetworks.com**
   - 波蘭：**pl.wildfire.paloaltonetworks.com**
   - 印尼：**id.wildfire.paloaltonetworks.com**
   - 台灣：**tw.wildfire.paloaltonetworks.com**
   - 法國：**fr.wildfire.paloaltonetworks.com**
   - 卡達：**qatar.wildfire.paloaltonetworks.com**
   - 韓國：**kr.wildfire.paloaltonetworks.com**
   - 以色列：**il.wildfire.paloaltonetworks.com**
   - 沙烏地阿拉伯：**sa.wildfire.paloaltonetworks.com**
   - 西班牙：**es.wildfire.paloaltonetworks.com**
2. 在 **WildFire Private Cloud**（**WildFire** 私人雲端）欄位中輸入 WildFire 設備的 IP 位址或 FQDN。

STEP 3 | 定義防火牆轉送的檔案大小限制並設定 WildFire 記錄和報告設定。

繼續編輯 WildFire 一般設定（**Device**（裝置） > **Setup**（設定） > **WildFire**）。

- 檢閱從防火牆轉送的檔案的 **File Size Limits**（檔案大小上限）。

  建議的 WildFire 最佳做法是將 *PE* 的 ***File Size***（檔案大小）設定為大小上限 *10 Mb*，並將其他檔案類型的 ***File Size***（檔案大小）設定為預設值。

- 選取 **Report Benign Files**（報告良性檔案），允許記錄收到 WildFire 良性裁定的檔案。
- 選取 **Report Grayware Files**（報告灰色檔案），允許記錄收到 WildFire 灰色裁定的檔案。
- 透過編輯工作階段資訊設定，定義 WildFire 分析報告中記錄的工作階段資訊。依預設，WildFire 分析報告中顯示所有工作階段資訊。取消選取核取方塊，從 WildFire 分析報告中移除相應欄位，然後按一下 **OK**（確定）儲存設定。

STEP 4 | （僅限 Panorama）設定 Panorama，以收集從執行 PAN-OS 7.0 之前版本 PAN-OS 的防火牆所收集樣本的其他資訊。

對於運行早期軟體版本的防火牆所提交的樣本，PAN-OS 7.0 中推出的部分 WildFire Submissions 日誌欄位未被填入。如果您正使用 Panorama 管理運行 PAN-OS 7.0 之前軟體版本的防火牆，Panorama 可與 WildFire 進行通訊，並為這些防火牆提交的樣本收集完整的分析資訊，包括定義的 **WildFire Server**（**WildFire** 伺服器）（預設情況下為 WildFire 全域雲端）及日誌詳細資訊。

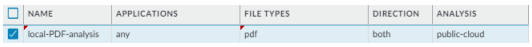
如果您希望修改預設設定以允許 Panorama 收集來自指定 WildFire 雲端或 WildFire 設備的詳細資訊，請選取 **Panorama** > **Setup**（設定） > **WildFire** 並輸入 **WildFire Server**（**WildFire** 伺服器）。

STEP 5 | 定義要轉送進行 WildFire 分析的流量。

如果您設定了 *WildFire* 設備，可在混合型雲端部署中使用私人雲端及公共雲端。在網路上分析本機機敏檔案，同時將所有其他未知檔案傳送至 *WildFire* 公共雲端進行綜合分析及返回提示裁定。

1. 選取 **Objects**（物件） > **Security Profiles**（安全性設定檔） > **WildFire Analysis**（**WildFire** 分析），**Add**（新增） 新的 WildFire 分析檔案，以及為設定檔提供描述性 **Name**（名稱）。
2. **Add**（新增）設定檔規則以定義要轉送進行分析的流量，並為規則提供描述性**Name**（名稱），例如 local-PDF-analysis。
3. 定義設定檔規則以符合未知瀏覽及根據下列各項轉送樣本進行分析：
   - **Applications**（應用程式）—根據使用中的應用程式轉送檔案進行分析。
   - **File Types**（檔案類型）—根據檔案類型，包括電子郵件訊息中包含的連結，轉送檔案進行分析。例如，選取 **PDF** 轉送防火牆偵測到的未知 PDF 進行分析。
   - **Direction**（方向）—根據檔案的傳輸方向（上載、下載或兩者）轉送檔案進行分析。例如選取**both**（兩者）以轉送所有未知 PDF 進行分析，無論傳輸方向為何。
4. 設定 **Analysis**（分析）位置，讓防火牆轉送符合規則的檔案。
   - 選取**public-cloud**（公共雲端），讓符合的樣本轉送至 WildFire 公共雲端以進行分析。
   - 選取**private-cloud**（私人雲端），讓符合的樣本轉送至 WildFire 私人雲端以進行分析。

     例如，若要分析可能包含某些機敏或專有資訊的 PDF，而不從您的網路傳送這些文件，將規則 local-PDF-analysis 的 **Analysis**（分析）位置設定為 **private-cloud**（私人雲端）。



不同規則可轉送相符的樣本至不同的分析位置，具體視您的需要而定。上述範例所示為在 *WildFire* 私人雲端中轉送本機分析的機敏檔案類型。您可以建立了一條規則來轉送較不機敏的檔案類型（如 *PE*）至 *WildFire* 公共雲端。此靈活性透過 WildFire 混合型雲端部署獲得支援。

在混合型雲端部署中，符合 ***private-cloud***（私人雲端）及 ***public-cloud***（公共雲端）規則的檔案僅作為預警措施轉送至私人雲端。

5. （選用）視需繼續新增規則至 WildFire 分析設定檔。例如，您可以新增第二項規則以轉送 Android 應用程式套件 (APK)、可攜式執行檔 (PE) 及 Flash 檔案至 WildFire 公共雲端進行分析。
6. 按一下 **OK**（確定）來儲存 WildFire 分析設定檔。
7. （選用）視需繼續新增規則至 WildFire 分析設定檔。例如，您可以新增第二項規則以轉送 Android 應用程式套件 (APK)、可攜式執行檔 (PE) 及 Flash 檔案至 WildFire 公共雲端進行分析。

8. 按一下 **OK**（確定）來儲存 WildFire 分析設定檔。

STEP 6 | （選用）配置 WildFire 設備資源以分析文件或可執行檔。

如果您部署混合型雲端以在本機和 *WildFire* 公共雲端分析特定檔案類型，可以使用分析環境來處理檔案類型。這讓您能夠根據分析環境設定更好地配置資源。如果您沒有為分析環境配置資源，資源會使用預設設定配置。

使用下列 CLI 命令：

```
admin@WF-500# set deviceconfig setting wildfire preferred-analysis-environment documents | executables | default
```

以及選擇以下一項：

- 文件—使用分析資源同時分析 25 個文件、1 個 PE 及 2 個電子郵件連結。
- 可執行檔—使用分析資源同時分析 25 個 PE、1 個文件及 2 個電子郵件連結。
- 預設—設備同時分析 16 個文件、10 個可攜式執行檔 (PE) 及 2 個電子郵件連結。

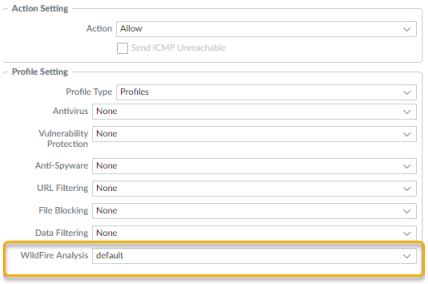
確認所有 WildFire 設備程序均透過執行下列命令進行：

```
admin@WF-500> show system software status
```

STEP 7 | 將 WildFire 分析設定檔附加至安全性原則規則。

根據附加的 WildFire 分析設定檔評估安全性原則規則允許的流量；防火牆轉送符合設定檔的流量進行 WildFire 分析。

1. 選取 **Policies**（原則） > **Security**（安全性），然後 **Add**（新增） 或修改原則規則。
2. 按一下原則規則內部的 **Actions**（動作）頁籤。
3. 在設定檔設定部分，選取做為 **Profile Type**（設定檔類型）的 **Profiles**（設定檔），然後選取附加至原則規則的 **WildFire Analysis**（**WildFire** 分析）設定檔



STEP 8 | 確保啟用防火牆以轉送解密 SSL 流量進行 WildFire 分析。

這是建議的 WildFire 最佳做法。

STEP 9 | 檢閱並實施 WildFire 最佳做法。

STEP 10 | 按一下 **Commit**（交付）以套用 WildFire 設定。

STEP 11 | (選用) 確認 WildFire 提交。

STEP 12 | 選擇下一步操作...

- 確認 WildFire 提交以確認防火牆已成功轉送檔案進行 WildFire 分析。
- 透過 WildFire 設備提交惡意軟體或報告。啟用此功能可將在 WildFire 私人雲端中識別的惡意軟體自動轉送至 WildFire 公共雲端。WildFire 公共雲端重新分析樣本，如果樣本為惡意軟體，則會產生特徵碼。特徵碼透過 Wildfire 特徵碼更新散佈至全球使用者。
- 監控 WildFire 設備活動 評估針對惡意軟體報告的警示和詳細資料。

透過 WildFire 設備提交惡意軟體或報告

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

啟用 WildFire 設備的雲端智慧功能，將在 WildFire 私人雲端中發現的惡意軟體樣本自動提交至 WildFire 公共雲端。WildFire 公共雲端進一步分析惡意軟體並產生特徵碼以識別該樣本。特徵碼隨後新增至 WildFire 特徵碼更新，並散佈至全球使用者，防禦未來威脅的攻擊。如果您不想轉送網路之外的惡意軟體樣本，可轉而選擇僅提交在網路上發現的惡意軟體的 WildFire 報告，這有助於收集 WildFire 統計資料及威脅情報。

提交惡意軟體至 WildFire 公共雲端

透過 WildFire 設備執行下列 CLI 命令，以讓設備自動提交惡意軟體樣本至 WildFire 公共雲端：

```
admin@WF-500admin@WF-500# set deviceconfig setting wildfire cloud-intelligence submit-sample yes
```

如果原本提交樣本進行 *WildFire* 私人雲端分析的防火牆啟用了封包擷取 *(PCAP)*，惡意軟體的 *PCAP* 也會轉送至 *WildFire* 公共雲端。

提交惡意軟體報告至 WildFire 公共雲端

如果啟用了 *WildFire* 設備來提交惡意軟體至 WildFire 公共雲端，您不需要也啟用設備來提交惡意軟體報告至公共雲端。當將惡意軟體提交至 *WildFire* 公共雲端時，公共雲端將產生該樣本的新惡意軟體報告。

若要啟用 WildFire 設備來自動提交惡意軟體報告至 WildFire 公共雲端（而非惡意軟體樣本），請在 WildFire 設備上執行下列 CLI 命令：

```
admin@WF-500# set deviceconfig setting wildfire cloud-intelligence
 submit-report yes
```

確認雲端智慧設定

檢查以確認已啟用雲端智慧，透過執行下列命令提交惡意軟體或提交惡意軟體報告至 WildFire 公共雲端：

```
admin@WF-500> show wildfire status
```

請參閱 `Submit sample` and `Submitreport` 欄位。

設定在獨立 WildFire 設備上使用自訂憑證進行驗證

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

依預設，WildFire 設備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。自訂憑證可讓您建立唯一的信任鏈，以確保 WildFire 設備與防火牆或 Panorama 之間的相互驗證。您可在 Panorama 或防火牆上本機產生這些憑證，從信任的協力廠商憑證簽發單位 (CA) 取得，或從企業私密金鑰基礎結構 (PKI) 取得。

下列主題說明如何設定並非由 Panorama 管理的獨立 WildFire 設備。有關如何設定由 Panorama 管理的 WildFire 設備和 WildFire 叢集的自訂憑證，請參閱 Panorama 管理指南。

- WildFire 設備相互 SSL 驗證
- 設定在 WildFire 設備上使用自訂憑證進行驗證

WildFire 設備相互 SSL 驗證

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

當防火牆或 Panorama 傳送樣本至 WildFire 設備進行分析時，防火牆充當用戶端，WildFire 設備充當伺服器。為了相互驗證，每個裝置都會出示憑證以向另一個裝置表明自己的身分。

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—WildFire 設備需要憑證和憑證設定檔才可向防火牆表明自己的身分。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 WildFire 設備管理介面的 IP 位址或 FQDN。防火牆會根據 WildFire 設備的 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 WildFire 設備的身分。

  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—每個防火牆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。

設定在 WildFire 設備上使用自訂憑證進行驗證

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

使用下列工作流程取代預先定義的憑證以自訂 WildFire 部署中的憑證。當防火牆或 Panorama 傳送樣本至 WildFire 設備進行分析時，防火牆充當用戶端，WildFire 設備充當伺服器。

STEP 1 | 取得 WildFire 設備和防火牆或 Panorama 的金鑰配對與憑證授權單位 (CA) 憑證。

STEP 2 | 匯入 CA 憑證以在防火牆上驗證憑證。

1. 在 WildFire 設備上登入 CLI 並進入設定模式。

```
admin@WF-500> configure
```

2. 使用 TFTP 或 SCP 匯入憑證。

```
admin@WF-500#{tftp | scp} import certificate from <value>
 file <value> remote-port <1-65535> source-ip <ip/netmask>
 certificate-name <value> passphrase <value> format {pkcs12 |
 pem}
```

STEP 3 | 使用 TFTP 或 SCP 匯入包含伺服器憑證與私密金鑰的 WildFire 設備金鑰配對。

```
admin@WF-500# {tftp | scp} import keypair from <value> file <value>
 remote-port <1-65535> source-ip <ip/netmask> certificate-
name <value> passphrase <value> format {pkcs12 | pem}
```

STEP 4 | 設定包含 root CA 和中繼 CA 的憑證設定檔。此憑證設定檔定義了 WildFire 設備與防火牆彼此相互驗證的方式。

1. 在 WildFire 設備的 CLI 中，進入設定模式。

```
admin@WF-500> configure
```

2. 為憑證設定檔命名。

```
admin@WF-500# set shared certificate-profile <name>
```

3. 設定 CA。

default-ocsp-url 與 *ocsp-verify-cert* 命令為選用。

```
admin@WF-500# set shared certificate-profile <name> CA <name>
```

```
admin@WF-500# set shared certificate-profile <name> CA <name>
 [default-ocsp-url <value>]
```

```
admin@WF-500# set shared certificate-profile <name> CA <name>
 [ocsp-verify-cert <value>]
```

STEP 5 | 設定 WildFire 設備的 SSL/TLS 設定檔。此設定檔定義了 WildFire 設備與防火牆用於 SSL/TLS 服務的憑證和 SSL/TLS 通訊協定範圍。

1. 識別 SSL/TLS 設定檔。

```
admin@WF-500# set shared ssl-tls-service-profile <name>
```

2. 選取憑證。

```
admin@WF-500# set shared ssl-tls-service-profile <name>
 certificate <value>
```

3. 定義 SSL/TLS 範圍。

   PAN-OS 8.0 和更新版本僅支援 *TLS 1.2* 和更新 *TLS* 版本。您必須將最高版本設定為 *TLS 1.2* 或最高。

```
admin@WF-500# set shared ssl-tls-service-profile <name>
 protocol-settings min-version {tls1-0 | tls1-1 | tls1-2}
```

```
admin@WF-500# set shared ssl-tls-service-profile <name>
 protocol-settings max-version {tls1-0 | tls1-1 | tls1-2 |
 max}
```

STEP 6 | 在 Wildfire 設備上設定安全伺服器通訊。

1. 設定 SSL/TLS 設定檔。此 SSL/TLS 服務設定檔適用於 WildFire 與用戶端裝置之間的所有 SSL 連線。

```
admin@WF-500# set deviceconfig setting management secure-conn-
server ssl-tls-service-profile <ssltls-profile>
```

2. 設定憑證設定檔。

```
admin@WF-500# set deviceconfig setting management secure-conn-
server certificate-profile <certificate-profile>
```

設定 WildFire 設備 VM 介面

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

虛擬電腦介面 (vm-interface) 可讓您從 WildFire 設備中的沙箱虛擬電腦連線至外部網路，以便觀察惡意行為，其中分析的檔案會尋找網路存取。下列各節說明虛擬電腦介面及設定此介面所需的步驟。您可以選擇性地透過虛擬電腦介面啟用 Tor 功能，如有任何源自 WildFire 設備，且經虛擬電腦介面傳送而來的惡意流量，此功能將予以遮罩，使得惡意網站即便收到該流量，亦無法偵測您的公開 IP 位址。

此節也說明將虛擬電腦介面連接到 Palo Alto Networks 防火牆專用連接埠以啟用網際網路連線所需的步驟。

- 虛擬電腦介面概要介紹
- 在 WildFire 設備上設定 VM 介面
- 將防火牆連接至 WildFire 設備 VM 介面

虛擬電腦介面概要介紹

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

WildFire 使用虛擬電腦介面 (在設備背面標示為 **1**) 來提升惡意軟體偵測功能。此介面允許 WildFire 虛擬電腦上執行的檔案樣本與網際網路進行通訊，並且讓 WildFire 設備更有效分析樣本檔案的行為，判斷檔案是否顯現惡意軟體的特徵。

- 雖然建議您啟用虛擬電腦介面，不過請勿將介面連接到允許存取任何伺服器/主機的網路，因為 *WildFire* 虛擬電腦中執行的惡意軟體可能使用此介面自行傳播。
- 此連線可以是專用的 *DSL* 線路，也可以是僅允許虛擬電腦介面直接存取網際網路並限制內部伺服器/用戶端主機進行任何存取的網路連線。
- 停用操作於 *FIPS/CC* 模式中的 *WildFire* 設備上的 *VM* 介面。

下圖顯示將虛擬電腦介面連接到網路的兩個選項。

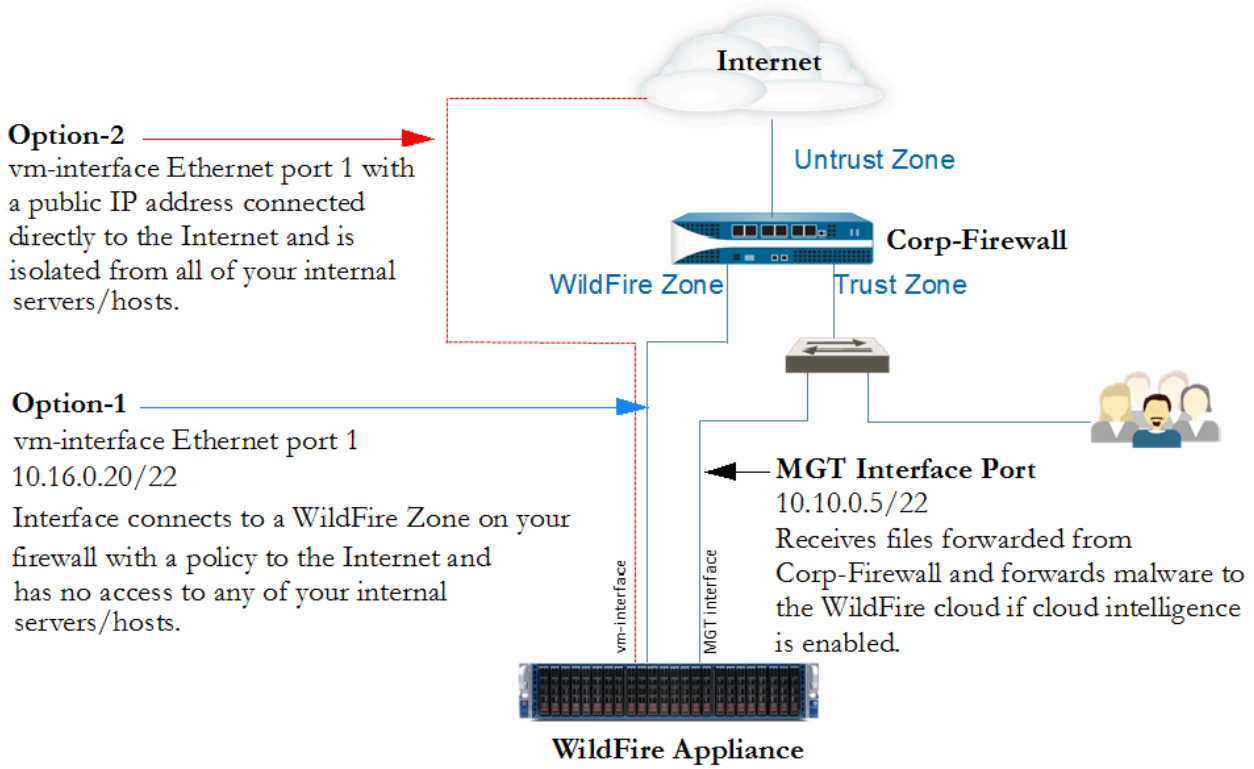


圖 **1:** 虛擬電腦介面範例

- 選項**-1**（建議）— 將虛擬電腦介面連接到原則僅允許網際網路連線的防火牆上專屬區域之中的介面。這相當重要，因為 WildFire 虛擬電腦中執行的惡意軟體可能用此介面自行傳播。這是建議的選項，因為防火牆日誌可用來掌握虛擬電腦介面產生的任何流量。
- 選項**-2**—使用 DSL 之類的專用網際網路供應商連線，將虛擬電腦介面連接到網際網路。確定此連線未存取內部伺服器/主機。雖然這是簡單的解決方案，不過不會記錄虛擬電腦介面之外惡意軟體產生的流量，除非您在 WildFire 設備與 DSL 連線之間設有防火牆或流量監控工具。

在 WildFire 設備上設定 VM 介面

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

本節說明使用先前在虛擬電腦介面範例中所述的選項 1 設定，在 WildFire 設備上設定 VM 介面所需的步驟。使用此選項設定虛擬電腦介面後，也必須在 Palo Alto Networks 防火牆設定介面，虛擬電腦介面的流量將透過此介面進行傳輸，如將防火牆連接至 WildFire 設備 VM 介面所述。

虛擬電腦介面預設包含下列設定：

- IP 位址：192.168.2.1
- 網路遮罩：255.255.255.0
- 預設閘道：192.168.2.254
- DNS：192.168.2.254

如果計劃啟用此介面，請使用網路適當的設定來設定此介面。如果不計劃使用此介面，請保留預設設定。請注意，此介面必須設定網路值，否則將發生交付失敗。

STEP 1 | 在 WildFire 設備上設定虛擬電腦介面的 IP 資訊。本範例中使用了以下 IPv4 值，但該設備也支援 IPv6 位址：

- IP 位址 - 10.16.0.20/22
- 子網路遮罩 - 255.255.252.0
- 預設閘道 - 10.16.0.1
- DNS 伺服器 - 10.0.0.246

虛擬電腦介面不可與管理介面 *(MGT)* 位於同一個網路。

1. 進入組態模式：

```
admin@WF-500> configure
```

2. 設定虛擬電腦介面的 IP 資訊：

```
admin@WF-500# set deviceconfig system vm-interface ip-address
 10.16.0.20 netmask 255.255.252.0 default-gateway 10.16.0.1
 dns-server 10.0.0.246
```

您僅可在虛擬電腦介面上設定一個 *DNS* 伺服器。最好使用 *ISP* 的 *DNS* 伺服器或開放 *DNS* 服務。

STEP 2 | 啟用虛擬電腦介面。

1. 啟用虛擬電腦介面：

```
admin@WF-500# set deviceconfig setting wildfire vm-network-
enable yes
```

2. 提交設定：

```
admin@WF-500# commit
```

STEP 3 | 測試虛擬電腦介面的連線能力。

偵測系統並指定虛擬電腦介面做為來源。例如，若虛擬電腦介面 IP 位址為 10.16.0.20，請執行下列命令，其中 *ip-or-hostname* 為啟用偵測伺服器/網路的 IP 或主機名稱：

```
admin@WF-500> ping source 10.16.0.20 host ip-or-hostname
```

例如：

```
admin@WF-500> ping source 10.16.0.20 host 10.16.0.1
```

STEP 4 | （選用）傳送惡意軟體產生的惡意流量至網際網路。Tor 網路會將您的公開 IP 位址加上遮罩，讓惡意網站的擁有人無法判定流量來源。

1. 啟用 Tor 網路：

```
admin@WF-500# set deviceconfig setting wildfire vm-network-use-tor
```

2. 提交設定：

```
admin@WF-500# commit
```

STEP 5 | （選用）確認 Tor 網路連線處於使用中且正常狀態。

1. 簽發下列 CLI 命令以在設備日誌中搜尋 Tor 事件 ID。正確設定及操作的 WildFire 設備不應產生任何事件 ID：
   - **admin@WF-500(active-controller)>showlog system direction equal backward | match anonymous-network-unhealthy**—Tor 服務已關閉或無法運作。請考慮重新啟動您的 Tor 服務且確認是否正常運作。
   - **admin@WF-500(active-controller)>show log systemdirection equal backward | match anonymous-network-unavailable**—Tor 服務正常運作，但是 WildFire 設備 VM 介面無法建立連線。確認您的網路連線及設定並且重新測試。

STEP 6 | 將防火牆連接至 WildFire 設備 VM 介面。

將防火牆連接至 WildFire 設備 VM 介面

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

下列範例工作流程說明如何將虛擬電腦介面連線到 Palo Alto Networks 防火牆的連接埠。將虛擬電腦介面連接到防火牆之前，防火牆必須已經有連接到網際網路的不信任區域。在此範例中，您將設定名稱為 wf-vm-zone 的新區域，它會包含用來將設備的虛擬電腦介面連線至防火牆的介面。與 wf-vm-zone 相關聯的原則將只允許虛擬電腦介面對不信任區域進行通訊。

STEP 1 | 設定虛擬電腦介面將連線的防火牆介面，並設定虛擬路由器。

wf-vm-zone 應僅包含用來將設備虛擬電腦介面連線至防火牆的介面（在此範例中為 *ethernet1/3*）。這是為了避免惡意軟體產生的任何流量散播至其他網路。

1. 從防火牆的 Web 介面，選取 **Network**（網路） > **Interfaces**（介面），然後選取介面，例如 **Ethernet1/3**。
2. 在 **Interface Type**（介面類型）下拉式清單中選取 **Layer3**。
3. 在 **Config**（設定）頁籤的 **Security Zone**（安全性地區）下拉式方塊中，選取**New Zone**（新增區域）。
4. 在區域對話方塊 **Name**（名稱）欄位中，輸入 wf-vm-zone，然後按一下 **OK**（確定）。
5. 在 **Virtual Router**（虛擬路由器）下拉式方塊中，選取 **default**（預設）。
6. 將 IP 位址指派給介面，選取 **IPv4** 或 **IPv6** 頁籤，按一下 IP 區段的 **Add**（新增），然後輸入要指派給介面的 IP 位址及網路遮罩，例如 10.16.0.0/22 (IPv4) 或 2001:db8:123:1::1/64 (IPv6)。
7. 若要儲存介面設定，請按一下 **OK**（確定）。

STEP 2 | 在防火牆上建立安全性原則，允許虛擬電腦介面存取網際網路，並封鎖所有連入的流量。在此範例中，原則名稱為 WildFire 虛擬電腦介面。由於您將不會建立從不信任區域到 wf-vm-interface 區域的安全性原則，因此預設將封鎖所有連入流量。

1. 選取 **Policies**（原則） > **Security**（安全性），然後按一下 **Add**（新增）
2. 在 **General**（一般）頁籤上，輸入閘道的 **Name**（名稱）。
3. 在 **Source**（來源）頁籤中，設定 **Source Zone**（來源地區）為 **wf-vm-zone**。
4. 在 **Destination**（目的地）頁籤中，設定 **Destination Zone**（目的地區域）為 **Untrust**（不信任）。
5. 在 **Application**（應用程式）及 **Service/ URL Category**（服務/**URL** 類別） 頁籤中，保留預設的 **Any**（任何）。
6. 在 **Actions**（動作）頁籤中，設定 **Action Setting**（動作設定）為 **Allow**（允許）。
7. 在 **Log Setting**（日誌設定）下，選取 **Log at Session End**（同時連線結束時的日誌）核取方塊。

如果擔心有人可能不慎將其他介面新增到 *wf-vm-zone*，請複製 *WildFire VM* 介面 安全性原則，然後在複製的規則相應的 ***Action***（動作）頁籤中，選取 ***Deny***（拒絕）。確定這個新的安全性原則列在 *WildFire VM* 介面原則下。這將覆寫允許同一個區域中的介面之間進行通訊的隱含內部區域允許規則，而拒絕/封鎖所有內部區域通訊。

STEP 3 | 連接纜線。

使用直通式 RJ-45 纜線，將 WildFire 設備的虛擬電腦介面直接連接到在防火牆上設定的連接埠（在此範例中為 Ethernet 1/3）。虛擬電腦介面在設備背面標示為 **1**。

啟用 WildFire 設備分析功能

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

- 設定 WildFire 設備內容更新
- 啟用本機特徵碼及 URL 類別產生
- 提交本機發現的惡意軟體或報告至 WildFire 公共雲端

設定 WildFire 設備內容更新

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

設定 WildFire 設備的每日內容更新。WildFire 內容更新為設備提供威脅情報功能，有助於準確偵測惡意軟體，提升設備從良性軟體樣本區分惡意軟體樣本的能力，以及確保設備擁有產生特徵碼所需的最新資訊。

- 直接從更新伺服器安裝 WildFire 內容更新
- 從啟用 SCP 的伺服器安裝 WildFire 內容更新

直接從更新伺服器安裝 **WildFire** 內容更新

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

STEP 1 | 驗證設備到更新伺服器之間的連線，並找出要安裝的內容更新。

1. 登入 WildFire 設備並執行下列命令以顯示目前的內容版本：

```
admin@WF-500> show system info | match wf-content-version
```

2. 確認設備可與 Palo Alto Networks 更新伺服器通訊，並檢視可用更新：

```
admin@WF-500> request wf-content upgrade check
```

命令會查詢 Palo Alto Networks 更新伺服器並提供可用更新的相關資訊，並識別設備目前安裝的版本。

```
Version Size  Released on      Downloaded Installed
 -------------------------------------------------
 2-253   57MB 2014/09/20 20:00:08 PDT no         no 2-39
 44MB 2014/02/12 14:04:27 PST yes     current
```

若設備無法連線至更新伺服器，您將必須允許設備連線至 Palo Alto Networks 更新伺服器 (updates.paloaltonetworks.com)，或如從啟用 SCP 的伺服器安裝 WildFire 內更新所述使用 SCP 來下載並安裝更新。

STEP 2 | 下載並安裝最新的內容更新。

1. 下載最新的內容更新：

```
admin@WF-500> request wf-content upgrade download latest
```

2. 檢視下載狀態：

```
admin@WF-500> show jobs all
```

您可執行 **show jobs pending**（顯示擱置中的工作）來檢視擱置中的工作。下列輸出顯示下載 (job id 5) 已完成下載（狀態為 FIN）：

```
Enqueued          ID  Type Status Result Completed
 ---------------------------------------------------
 2014/04/22 03:42:20  5  Downld  FIN   OK   03:42:23
```

3. 下載完成後，安裝更新：

```
admin@WF-500> request wf-content upgrade install version
 latest
```

再次執行 **show jobs all**（顯示所有工作）命令以監控安裝狀態。

STEP 3 | 驗證內容更新。

執行下列命令並參閱 `wf-content-version` 欄位：

```
admin@WF-500> show system info
```

以下顯示安裝 2-253 版本內容更新的範例輸出：

```
admin@WF-500> show system info hostname:WildFire ip-
address:10.5.164.245 netmask:255.255.255.0 default-
gateway:10.5.164.1 mac-address:00:25:90:c3:ed:56 vm-interface-
ip-address:192.168.2.2 vm-interface-netmask:255.255.255.0
 vm-interface-default-gateway:192.168.2.1 vm-interface-dns-
server:192.168.2.1 time:Mon Apr 21 09:59:07 2014 uptime:17
 days, 23:19:16 family: m model:WildFire serial: abcd3333 sw-
version:6.1.0 wf-content-version:2-253 wfm-release-date:2014/08/20
 20:00:08 logdb-version:6.1.2 platform-family: m
```

STEP 4 | （選用）每日或每週對安裝的內容更新排程。

1. 將設備排程為下載並安裝內容更新：

   ```
   admin@WF-500# set deviceconfig system update-schedule wf-
   content recurring [daily | weekly] action [download-and-
   install | download-only]
   ```

   例如，每天早上 8:00 下載並安裝更新：

   ```
   admin@WF-500# set deviceconfig system update-schedule wf-
   content recurring daily action download-and-install at 08:00
   ```

2. 提交設定

   ```
   admin@WF-500# commit
   ```

從啟用 SCP 的伺服器安裝 WildFire 內容更新

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

下列程序說明如何在無法直接連線至 Palo Alto Networks 更新伺服器的 WildFire 設備上安裝威脅情報內容更新。您將需要可暫存內容更新的已啟用安全複製 (SCP) 伺服器。

STEP 1 | 從更新伺服器擷取內容更新檔案。

1. 登入 Palo Alto Networks 支援入口網站，並按一下 **Dynamic Updates (**動態更新**)**。
2. 在 [WildFire 設備] 區段中，找到並下載最新的 WildFire 設備內容更新。
3. 將內容更新檔案複製到已啟用 SCP 的伺服器，並記下檔案名稱和目錄路徑。

STEP 2 | 在 WildFire 設備上安裝內容更新。

1. 登入 WildFire 設備並從 SCP 伺服器下載內容更新檔案：

```
admin@WF-500> scp import wf-content from username@host:path
```

例如：

```
admin@WF-500> scp import wf-content from bart@10.10.10.5:c:/
updates/panup-all-wfmeta-2-253.tgz
```

若您的 *SCP* 伺服器以非標準連接埠執行，或若您需要指定來源 *IP*。您也可以在 ***scp import*** 命令中定義這些選項。

2. 安裝更新：

```
admin@WF-500> request wf-content upgrade install file panup-
all-wfmeta-2-253.tgz
```

3. 檢視安裝狀態：

```
admin@WF-500> show jobs all
```

STEP 3 | 驗證內容更新。

驗證內容版本：

```
admin@WF-500> show system info | match wf-content-version
```

下列輸出現在顯示版本 2-253：

```
wf-content-version:2-253
```

啟用本機特徵碼及 URL 類別產生

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

WildFire 設備可根據從連接的防火牆及 WildFire API 接收的樣本在本機產生特徵碼，或將惡意軟體傳送到公共雲端進行特徵碼產生。設備可產生下列類型的防火牆特徵碼，用於封鎖惡意軟體及任何相關的命令及控制流量：

- **Antivirus signatures**（防毒特徵碼）—偵測並封鎖惡意檔案。WildFire 會將這些特徵碼新增至 WildFire 和防毒內容更新。
- **DNS signatures**（**DNS** 特徵碼）—偵測並封鎖命令的回撥網域並控制與惡意軟體相關聯的流量。WildFire 會將這些特徵碼新增至 WildFire 和防毒內容更新。
- **URL categories**（**URL** 類別）—將回撥網域分類為惡意軟體，並更新 PAN-DB 中的 URL 類別。

設定防火牆以五分鐘的頻率擷取 WildFire 設備產生的特徵碼。您也可以將惡意軟體樣本傳送至 WildFire 公共雲端，以便透過 Palo Alto Networks 內容發行在全球散佈特徵碼。

即使您使用 *WildFire* 設備進行本機檔案分析，您也可以 啟用連接的防火牆以接收 WildFire 公共雲端散佈的最新特徵碼 。

STEP 1 | 設定 WildFire 設備內容更新。

這使 WildFire 設備可以接收 Palo Alto Networks 的最新威脅情報。

STEP 2 | 啟用特徵碼及 URL 類別產生。

1. 登入設備並輸入 **configure** 以進入設定模式。
2. 啟用所有威脅防範選項：

```
admin@WF-500# set deviceconfig setting wildfire signature-
generation av yes dns yes url yes
```

3. 提交設定：

```
admin@WF-500# commit
```

您可以使用下列命令顯示在 *WildFire 8.0.1* 或更新環境中產生的特徵碼的狀態：

```
admin@WF-500# show wildfire global signature-status sha256
 equal <sha-256
value>
```

WildFire 設備無法顯示在 WildFire 8.0.1 以下版本中產生的特徵碼的狀態。

STEP 3 | 設定所連接防火牆的排程以擷取 WildFire 設備產生的特徵碼和 URL 類別。

最佳做法是設定防火牆同時從 *WildFire* 公共雲端及 *WildFire* 設備擷取內容更新。這可確保您的防火牆除接收從本機設備產生的特徵碼外，還接收根據全球偵測到的威脅產生的特徵碼。

- 對於 Panorama 管理的多個防火牆：

  啟動 Panorama 并選取 **Panorama** > **Device Deployment**（裝置部署） > **Dynamic Updates**（動態更新），按一下 **Schedules**（排程），然後 **Add**（新增）受管理的裝置的排定內容更新。

  如需使用 Panorama 設定受管理的防火墻以從 WildFire 設備接收特徵碼和 URL 類別的詳細資料，請參閱使用 Panorama 排定裝置的內容更新

  。

- 對於單一防火牆：

  1. 登入防火牆 Web 介面，選取 **Device**（裝置） > **Dynamic Updates**（動態更新）。

     對於設定為轉送檔案至 WildFire 設備的防火牆（在 WildFire 私人雲端或混合型雲端部署中），顯示 WF-Private 區段。

  2. 為防火牆設定 **Schedule**（排程），以從 WildFire 設備下載並安裝內容更新。

提交本機發現的惡意軟體或報告至 WildFire 公共雲端

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

讓 WildFire 設備自動提交惡意軟體樣本至 WildFire 公共雲端。WildFire 公共雲端進一步分析惡意軟體並產生特徵碼以識別該樣本。特徵碼隨後新增至 WildFire 特徵碼更新，並散佈至全球使用者，防禦未來威脅的攻擊。如果您不想轉送網路之外的惡意軟體樣本，可轉而選擇僅提交在網路上發現的惡意軟體的 WildFire 報告，這有助於收集和改善 WildFire 統計資料及威脅情報。

提交惡意軟體至 WildFire 公共雲端。

1. 透過 WildFire 設備執行下列 CLI 命令，以讓設備自動提交惡意軟體樣本至 WildFire 公共雲端：

   ```
   admin@WF-500# set deviceconfig setting wildfire cloud-
   intelligence submit-sample yes
   ```

   如果原本提交樣本進行 *WildFire* 私人雲端分析的防火牆啟用了封包擷取 *(PCAP)*，惡意軟體的 *PCAP* 也會轉送至 *WildFire* 公共雲端。

2. 前往 WildFire 入口網站檢視自動提交至 WildFire 公共雲端的惡意軟體的分析報告。當將惡意軟體提交至 WildFire 公共雲端時，公共雲端將產生該樣本的新分析報告。

提交分析報告至 WildFire 公共雲端

要自動提交惡意軟體報告至 WildFire 公共雲端（而非惡意軟體樣本），請在 WildFire 設備上執行下列 CLI 命令：

```
admin@WF-500# set deviceconfig setting wildfire cloud-intelligence
 submit-report yes
```

如果您已啟用 *WildFire* 設備為自動提交惡意軟體至 *WildFire* 公共雲端，則無需啟用此選項—*WildFire* 公共雲端將為樣本產生新的分析報告。

提交至 WildFire 公共雲端的報告無法在 WildFire 入口網站上檢視。WildFire 入口網站僅顯示 WildFire 公共雲端報告。

確認惡意軟體和報告提交設定

檢查以確認已啟用雲端智慧，透過執行下列命令提交惡意軟體或提交報告至 WildFire 公共雲端：

```
admin@WF-500> show wildfire status
```

請參閱 `Submit sample` and `Submitreport` 欄位。

升級 WildFire 設備

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

使用下列工作流程升級 WildFire 設備作業系統。如果您想要升級屬於 WildFire 叢集的設備，請參閱在叢集中升級 WildFire 設備。設備一次僅可使用一個環境來分析樣本，因此在更新設備之後，請檢閱可用 VM 影像檔清單，接著選擇最適合您環境的影像檔。在 Windows 7 的情況下，若您的環境混合 Windows 7 32 位元及 Windows 7 64 位元系統，建議您選擇 Windows 7 64 位元影像檔，讓 WildFire 可分析 32 位元及 64 位元的 PE 檔案。雖然您將設備設定為使用一個虛擬電腦影像檔設定，但設備會使用影像檔的多個執行個體以執行檔案分析。

視乎 WildFire 設備已分析和已儲存的樣本數量，升級設備軟體所需的時間有所不同；這是因為升級需要移轉所有惡意軟體樣本和 14 天內的良性軟體樣本。允許使用 30 至 60 分鐘升級您在生產環境中使用過的 WildFire 設備。

下列程序使用 PAN-OS 10.2.2 版本中的範例檔案名稱。您在 WildFire 設備上安裝的版本的確切檔案名稱可能會因特定版本而有所不同。

STEP 1 | 如果您是第一次設定 WildFire 設備，請參閱設定 WildFire 設備。

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**（裝置） > **Setup**（設定） > **WildFire** 並編輯 **General Settings**（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：

```
admin@WF-500> show wildfire latest samples
```

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 | 安裝最新 WildFire 設備內容更新。此更新為設備提供最新的威脅資訊以準確偵測惡意軟體。

在較舊的設備上，此程序可能需要長達 *6* 小時或更長時間。

1. 驗證您是否可在 WildFire 設備上執行最新的內容更新。

```
admin@WF-500> request wf-content upgrade check
```

2. 下載最新的 WildFire 內容更新套件。

```
admin@WF-500> request wf-content upgrade download latest
```

如果您未直接連線至 Palo Alto Networks 更新伺服器，可以下載並安裝來自啟用 SCP 的伺服器的 WildFire 內容更新。

3. 檢視下載狀態。

```
admin@WF-500> show jobs all
```

4. 下載完成後，安裝更新。

```
admin@WF-500> request wf-content upgrade install version latest
```

STEP 4 | （升級到 PAN-OS 10.2.2 時需要）升級 WildFire 設備上的 VM 映像。

1. 登入並存取 Palo Alto Networks 客戶支援入口網站軟體下載頁面。您也可以透過前往 **Updates**（更新） > **Software Updates**（軟體更新），手動從支援首頁導覽至軟體下載頁面。
2. 從軟體更新頁面中，選取 **WF-500 Guest VM Images**（**WF-500** 來賓 **VM** 映像）並下載下列 VM 映像檔案：

   Palo Alto Networks 會定期更新 *VM* 映像檔案；因此，特定檔案名稱會根據可用版本而變更。請務必下載最新版本，檔案名稱中的 *m-x.x.x* 表示版本號碼；此外，還有一個發佈日期，可以交叉參考以協助確定最新版本。

   - WFWinXpAddon3_m-1.0.1.xpaddon3
   - WFWinXpGf_m-1.0.1.xpgf
   - WFWin7_64Addon1_m-1.0.1.7_64addon1
   - WFWin10Base_m-1.0.1.10base
3. 將 VM 映像上傳到 WildFire 設備。
   1. 從 SCP 伺服器匯入 VM 映像：

      ```
      admin@WF-500>scp import wildfire-vm-image from
       <username@ip_address>/<folder_name>/<vm_image_filename>
      ```

      例如：

      ```
      admin@WF-500>scp import wildfire-vm-image from
       user1@10.0.3.4:/tmp/WFWin7_64Addon1_m-1.0.1.7_64addon1
      ```
   2. 若要檢查下載狀態，請使用下列命令：

      ```
      admin@WF-500>show jobs all
      ```
   3. 對剩餘的 VM 映像重複此動作。
4. 安裝 VM 映像。
   1. ```
      admin@WF-500>request system wildfire-vm-image upgrade
       install file <vm_image_filename>
      ```
   2. 對剩餘的 VM 映像重複此動作。
5. 確認 VM 映像已在 WildFire 設備上正確地安裝並啟用。
   1. （選用）檢視可用 VM 映像的清單：

      ```
      admin@WF-500> show wildfire vm-images
      ```
      ```

輸出顯示可用的 VM 映像。

2. 提交設定：

```
admin@WF-500# commit
```

3. 透過執行以下命令以檢視主動 VM 映像：

```
admin@WF-500> show wildfire status
```

STEP 5 | 下載 PAN-OS 10.2.2 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。

本程序中的範例說明了如何升級至 PAN-OS 10.2.2。升級時用合適的目標版本取代 10.2.2。

下載 10.2.2 軟體版本：

- 直接網際網路連線：
  1.
```
admin@WF-500> request system software download version 10.2.2
```
  2. 若要檢查下載狀態，請使用下列命令：

```
admin@WF-500> show jobs all
```

- 沒有網際網路連線：
  1. 導覽至 Palo Alto Networks 支援網站，然後在 [工具] 部分中按一下 **Software Updates**（軟體更新）。
  2. 將要安裝的 WildFire 設備軟體影像檔案下載到執行 SCP 伺服器軟體的電腦。
  3. 從 SCP 伺服器匯入軟體影像：

```
admin@WF-500> scp import software from <username@ip_address>/
<folder_name>/<imagefile_name>
```

例如：

```
admin@WF-500> scp import software from user1@10.0.3.4:/tmp/
WildFire_m-10.2.2
```

  4. 若要檢查下載狀態，請使用下列命令：

```
admin@WF-500> show jobs all
```

STEP 6 | 確認所有服務都在執行。

```
admin@WF-500> show system software status
```

STEP 7 | 安裝 10.2.2 軟體版本。

```
admin@WF-500> request system software install version 10.2.2
```

STEP 8 | 完成軟體升級。

1. 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> show jobs all Enqueued
 Dequeued ID Type Status Result Completed
 ------------------------------------------------- 02:42:36
 02:42:36 5 Install FIN OK 02:43:02
```

2. 重新啟動設備：

```
admin@WF-500> request restart system
```

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。

STEP 9 | 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 10.2.2：

```
admin@WF-500> show system info | match sw-version
```

2. 確認所有程序都在執行：

```
admin@WF-500> show system software status
```

3. 確認自動提交（`AutoCom`（自動提交））工作已完成：

```
admin@WF-500> show jobs all
```

STEP 10 | （選用）啟用 WildFire 設備用於執行分析的 VM 映像。每個可用的 VM 映像代表一個作業系統，並支援以該作業系統為基礎的若干個不同分析環境。

- 若您的網路環境混合 *Windows 7 32* 位元及 *Windows 7 64* 位元系統，建議您選擇 *Windows 7 64* 位元映像，讓 *WildFire* 可分析 *32* 位元及 *64* 位元的 *PE* 檔案。
- 目前可用的分析環境都是 *vm-3 (Windows XP)*、*vm-5 (Windows 7 64* 位元*)* 和 *vm-7 (Windows 10 64* 位元*)*。

- 請執行下列命令以檢視主動虛擬機器映像，並參閱 `Selected VM` 欄位：

```
admin@WF-500> show wildfire status
```

- 查看可用虛擬電腦影像檔清單：

```
admin@WF-500> show wildfire vm-images
```

下面的輸出顯示 `vm-5` 是 Windows 7 64 位元影像檔：

```
vm-5 Windows 7 64bit, Adobe Reader 11, Flash 11, Office 2010。支援
 PE、PDF、Office 2010 及更早版本
```

- 設定要用於分析的影像檔：

```
admin@WF-500# set deviceconfig setting wildfire active-vm <vm-
image-number>
```

例如，若要使用 vm-5，請執行下列命令：

```
admin@WF-500#set deviceconfig setting wildfire active-vm vm-5
```

並提交設定：

```
admin@WF-500#commit
```

STEP 11 | 接下來的步驟：

- （選用）升級防火牆至 PAN-OS 10.2.2。請參閱《PAN-OS 10.2 新功能指南》包含的防火牆升級指導。執行 PAN-OS 10.2.2 之前版本的防火牆仍可繼續轉送樣本至執行 10.2.2 的 WildFire 設備。
- （疑難排解）升級後，若您發現資料移轉問題或錯誤，可重新啟動 WildFire 設備以重新啟動升級程序—重新啟動 WildFire 設備不會導致資料遺失。

利用網際網路連線安裝 WildFire 設備裝置憑證

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權 ❑ 具有以下使用者角色之一的客戶支援入口網站 (CSP) 帳戶： 超級使用者、標準使用者、受限使用者、威脅研究員、AutoFocus 試用角色、群組超級使用者、群組標準使用者、群組受限使用者、群組威脅研究員、授權支援中心 (ASC) 使用者和 ASC 完整服務使用者。 ❑ 超級使用者存取 WildFire 設備

若要在網際網路連線可用時在 WF-500 設備上擷取裝置憑證，您必須登入 Palo Alto 網路支援入口網站，以產生用於存取憑證的一次性密碼。然後使用此 OTP 來擷取特定設備上的裝置憑證。

WF-500B 設備配備受信任平台模組 *(TPM)*，可用於安全地識別自身並自動擷取裝置憑證—無需使用者介入即可管理 *WF-500B* 裝置憑證。

如果您正在操作 WildFire 私人雲端 且未連線到任何 WildFire 服務，則不需要更新 WildFire 設備裝置憑證。相反的，WildFire 設備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，您也可以使用 設定在獨立 WildFire 設備上使用自訂憑證進行驗證。

如果您的 *WF-500B* 設備未連線到網際網路，您可能會發現因應設備重複嘗試擷取裝置憑證而導致的作業失敗。

要在防火牆上成功安裝裝置憑證，您的網路必須允許使用以下 FQDN 和連接埠。

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

FQDN	連接埠
• certificate.paloaltonetworks.com	
• *.gpcloudservice.com	TCP 444 和 TCP 443

STEP 1 | 確認您在 WildFire 設備上執行下列其中一個 PAN-OS 版本：

- PAN-OS 11.0.1 和更新版本
- PAN-OS 10.2.4 和更新版本
- PAN-OS 10.1.10 和更新版本（WF-500B 設備不支援）
- PAN-OS 10.0.12 和更新版本（WF-500B 設備不支援）
- PAN-OS 9.1.17 和更新版本（WF-500B 設備不支援）

STEP 2 | 產生一次性密碼 (OTP)。

1. 以具有權限可產生 OTP 的使用者角色登入客戶支援入口網站。
2. 選取 **Products**（產品） > **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 WF-500**（為 **WF-500** 產生 **OTP**）。
4. 選取您的 **WF-500 Device**（**WF-500** 裝置）序號。
5. **Generate OTP**（產生 **OTP**）且複製 OTP。

STEP 3 | 使用超級使用者管理權限存取 WF-500 設備 CLI。

STEP 4 | 將 WildFire 設備設定為與 NTP 伺服器同步：

```
admin@WF-500> configure admin@WF-500# set deviceconfig system ntp-servers primary-ntp-server ntp-server-address <NTP primary server IP address> admin@WF-500# set deviceconfig system ntp-servers secondary-ntp-server ntp-server-address <NTP secondary server IP address>
```

STEP 5 | 使用下列 CLI 命令下載並安裝 WF-500 設備憑證（記住使用您在客戶支援入口網站中所產生正確的**One-time Password**（一次性密碼））：

```
admin@WF-500> request certificate fetch otp <otp_value>
```

STEP 6 | 您的 WF-500 設備成功地擷取並安裝裝置憑證。

STEP 7 | （選用）使用下列 CLI 命令確認已成功下載和安裝裝置憑證：

```
admin@WF-500> show device-certificate status
```

成功安裝裝置憑證會顯示下列回應：

```
裝置憑證資訊：目前的裝置憑證狀態：有效，下列時間之前無效：2022/11/30
 15:17:47 PST 以下時間後無效：2023/02/28 15:17:47 PST 上次擷取的時間戳
記：2022/11/30 15:29:42 PST 上次擷取的狀態：成功，上次擷取的資訊：成功擷取裝
置憑證
```

STEP 8 | 使用下列 CLI 命令重新整理 WildFire 設備設定，以使用更新的裝置憑證建立與進階 WildFire 雲端的連線：

表 **1:**

在 **WildFire** 設備上執行的 **PAN-OS** 版本	**CLI** 命令
• PAN-OS 11.0.1 和更新版本 • PAN-OS 10.2.5 和更新版本 • PAN-OS 10.1.10 和更新版本	`admin@WF-500> test wildfire registration`
• PAN-OS 10.2.4 • PAN-OS 10.0.12 和更新版本 • PAN-OS 9.1.17 和更新版本	`admin@WF-500> request restart system` 此程序可能需要 *20* 分鐘才會完成。
設定為 WildFire 叢集節點的任何版本	`admin@WF-500(active-controller)> request cluster reboot-local-node`

在 **WildFire** 設備上執行的 **PAN-OS** 版本	**CLI** 命令

	您可以使用下列 *CLI* 命令檢視 *WildFire* 控制器節點上重新啟動工作的狀態：
	`admin@WF-500(active-controller)> show cluster task pending`
	當沒有剩餘待處理工作時，請使用下列 *CLI* 命令來驗證重新啟動是否成功：
	`admin@WF-500(active-controller)> show cluster task history`
	完成後，您應該會看到狀態已完成：於 *YYYY-MM-DD HH:MM:SS UTC* 成功，指示重新啟動程序完成的時間。

監控 WildFire 設備活動

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

您可以透過存取已提交範例的防火牆（如果您集中管理多個防火牆，請存取 Panorama）或 使用 WildFire API 檢視提交到 WildFire 設備的範例分析結果。

WildFire 已分析一個樣本並傳遞其為惡意軟體、網路釣魚、灰色或良性的裁定，並已產生該樣本的詳細分析報告。在提交樣本的防火牆上檢視的 WildFire 分析報告還包括偵測樣本期間的工作階段詳細資訊。對於識別為惡意軟體的樣本，WildFire 分析報告包括關於現有 WildFire 特徵碼（可能與新識別的惡意軟體相關）的詳細資訊，以及表明樣本為惡意軟體的檔案屬性、行為及活動的相關資訊。

請參閱下列主題獲得詳細資訊，來監控 WildFire 提交，檢視 WildFire 分析樣本的報告，以及根據提交及分析結果來設定警示及通知：

- 關於 WildFire 日誌記錄與報告
- 使用 WildFire CLI 監控 WildFire 設備
- 使用防火牆監控 WildFire 設備提交

關於 WildFire 日誌記錄與報告

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

您可以透過 WildFire 入口網站或 WildFire API，在防火牆上監控 WildFire 設備。

對於每個樣本 WildFire 分析，WildFire 在 WildFire 分析報告中，將樣本分類為惡意軟體、網路釣魚、灰色軟體或良性的 WildFire 分析報告，以及詳細說明樣本資訊及行為。在提交樣本的防火牆及分析樣本的 WildFire 雲端（公共或私人）上可找到 WildFire 分析報告，或者可使用 WildFire API 擷取：

- 在防火牆上—所有防火牆提交進行 WildFire 分析的樣本均記錄為 WildFire 提交項目（**Monitor**（監控） > **WildFire Submissions**（**WildFire** 提交））。WildFire 提交日誌中的 Action（動作）欄表示防火牆是否允許或封鎖檔案。對於每個 WildFire 提交項目，您可以開啟詳細日誌檢視，檢視樣本的 WildFire 分析報告或下載 PDF 格式的報告。
- 在 WildFire 入口網站上—監控 WildFire 活動，包括每個樣本的 WildFire 分析報告，也可下載 PDF 格式的報告。在 WildFire 私人部署中，WildFire 入口網站提供手動上載至入口網站的樣本詳細資訊以及由啟用雲端智慧的 WildFire 設備提交的樣本。

  在入口網站上檢視 *WildFire* 分析報告的選項，僅支援啟用了雲端智慧功能的 *WildFire* 設備。
- 帶 WildFire API—從 WildFire 設備或 WildFire 公共雲端擷取 WildFire 分析報告。

使用 WildFire 設備監控樣本分析狀態

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

在您的 WildFire 設備上使用 WildFire CLI（命令列介面）監控分析相關的詳細資訊。您可以檢視分析平台利用率資訊、目前的樣本佇列以及樣本處理詳細資訊。

請參閱下列章節，瞭解如何使用 WildFire 設備監控 WildFire 活動的詳細資訊：

- 檢視 WildFire 分析環境使用率
- 檢視 WildFire 樣本分析處理詳細資料

檢視 WildFire 分析環境使用率

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

WildFire 設備使用各種分析環境來偵測樣本內的惡意行為。您可以檢查使用中的分析環境、可用的數目，以及佇列中有多少待分析的檔案。如果特定分析環境的利用率一直處於（或接近）最大工作負載容量，請考慮卸載較不敏感的檔案分析至 Palo Alto Networks 代管的 WildFire 公共雲端、更新檔案轉送政策，或重新定義檔案轉送限制（Palo Alto Networks 建議所有的檔案類型皆使用預設的檔案轉送值）。

STEP 1 | 存取 CLI，並且依據您想要查看利用率統計的分析環境使用下列其中一個命令。

- 可攜式可執行檔分析環境利用率—**show wildfire wf-vm-pe-utilization**
- 文件分析環境利用率—**show wildfire wf-vm-doc-utilization**
- 電子郵件連結分析環境利用率—**show wildfire wf-vm-elinkda-utilization**
- 存檔分析環境利用率—**show wildfire wf-vm-archive-utilization**

設備會指示給定分析環境的使用中數目及可用數目：

```
{ available:2, in_use:1, }
```

STEP 2 | 檢視等待分析的 WildFire 設備樣本數目及詳細資訊。分析環境可供使用時處理樣本。

show wildfire wf-sample-queue-status

```
{ DW-ARCHIVE:4, DW-DOC:2, DW-ELINK:0, DW-PE:21, DW-
URL_UPLOAD_FILE:2, }
```

檢視 WildFire 樣本分析處理詳細資料

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

WildFire 設備會保留事件日誌內分析活動記錄。您可以檢視在您的網路中哪些連線的服務或設備分析特定樣本的詳細資訊，以及在給定時間範圍內分析的樣本數目。您可以使用此資訊來監控活動及定開發政策及對策，以抵禦惡意活動。不尋常的高負載活動可指示可疑活動。也請考慮威脅情報工具，例如 AutoFocus，以研究及判定威脅的本質。

STEP 1 | 檢視在指定時間範圍內本機處理的樣本數目或依據最大樣本數目。

show wildfire local sample-processed {time [last-12-hrs| last-15-minutes | last-1-hr | last-24-hrs | last-30-days | last-7-days| last-calender-day | last-calender-month] \ count <number_of_samples>}。

```
Latest samples information:
 +-------------------------------------------------------------------------
+---------------------+-----------+------------+-----------
+------------+--------------------+ | SHA256 | Create Time
 | File Name | File Type | File Size | Malicious | Status |
 +-------------------------------------------------------------------------
+---------------------+-----------+------------
+-----------+------------+--------------------+ |
 ce752b7b76ac2012bdff2b76b6c6af18e132ae8113172028b9e02c6647ee19bb |
 2018-12-09 16:55:53 | | Email Link | 31,522 | | download complete
 | |
 349e57e51e7407abcd6eccda81c8015298ff5d5ba4cedf09c7353c133ceaa74b |
 2018-12-09 16:53:40 | | Email Link | 39,679 | | download complete
 |
 +-------------------------------------------------------------------------
+---------------------+-----------+------------+-----------
+------------+--------------------+
```

STEP 2 | 識別提交特定樣本以進行 WildFire 分析的裝置。

show wildfire global sample-device-lookup sha256equal <SHA_256>。

```
 Sample
 1024609813c57fe174722c53b3167dc3cf5583d5c7abaf4a95f561c686a2116e
 last seen on following devices:
 +-------------------------------------------------------------------------
```

```
+-----------+-----------+---------------------+ |
 SHA256 | Device ID | Device IP | Submitted Time |
 +-------------------------------------------------------------------
+-----------+-----------+---------------------+ |
 1024609813c57fe174722c53b3167dc3cf5583d5c7abaf4a95f561c686a2116e
 | Manual | Manual | 2019-08-05 19:24:39 |
 +-------------------------------------------------------------------
+-----------+-----------+---------------------+
```

使用 WildFire CLI 監控 WildFire 設備

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

使用 WildFire™ CLI（命令列介面）檢視內部系統日誌。您可以檢閱記錄日誌事件，以監控 WildFire 組件的健康情況及狀態，例如叢集節點、核心與分析器服務，以及疑難排解，及確認系統設定。如需有關其他 PAN-OS 命令的資訊，請參閱《PAN-OS CLI 快速入門》。

- 檢視 WildFire 設備系統日誌

檢視 WildFire 設備系統日誌

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

使用終端機模擬器（例如 PuTTY），使用 Secure Shell（安全殼 - SSH）連線，或從您的管理電腦上的串列介面至裝置上的主控台連接埠的實體直接串列連接，連接至 WildFire 設備。

STEP 1 | 啟動終端機模擬軟體並且選擇連接類型（串列或 SSH）。

- 若要建立 SSH 連線，請輸入您想要連線的裝置的 WildFire 主機名稱或 IP 位址，並且將連接埠設定為 **22**。
- 若要建立串列連接，請連接管理電腦上的串列介面至裝置上的主控台連接埠。在終端機模擬軟體中設定串列連接設定，如下：
  - 資料範圍：**9600**
  - 資料位元：**8**
  - 同位檢查：無
  - 停止位元：**1**
  - 流量控制：無

STEP 2 | 出現登入提示時輸入您的管理認證。

STEP 3 | 在 WildFire 設備上輸入下列命令：

```
admin@WF-500>show log system subtype direction equal backward
```

此命令會從最舊至最近的順序，顯示分類為 wildfire-appliance 子類型的所有記錄事件。

- 您可以加入命令引數 `direction equal backward`，以最近至最舊的顛倒順序顯示日誌。
- WildFire 設備 CLI 所傳回的日誌訊息可包括各種子類型。您可以依據常見的關鍵字篩選日誌。使用下列的命令引數以依據特定字串進行篩選：`match queue < keyword>`

  下列 WildFire 設備日誌顯示啟動期間的系統初始化處理程序。

```
Time Severity Subtype Object EventID ID Description
 ================================================================================
 2017/03/29 12:04:33 medium general general 0 Hostname changed to
 WF-500 2017/03/29 12:04:40 info general general 0 VPN Disable mode
 = off 2017/03/29 12:04:41 info hw ps-inse 0 Power Supply #1 (top)
 inserted 2017/03/29 12:04:41 high general system- 1 The system
 is starting up.2017/03/29 12:04:41 info raid pair-de 0 New Disk
 Pair A detected.2017/03/29 12:04:41 info raid pair-de 0 New Disk
 Pair A detected.2017/03/29 12:04:41 info raid pair-de 0 New Disk
 Pair B detected.2017/03/29 12:04:41 info raid pair-de 0 New Disk
 Pair B detected.2017/03/29 12:04:41 info cluster cluster 0 Cluster
 daemon is initializing.2017/03/29 12:04:41 info port eth1 link-
ch 0 Port eth1:Up 1Gb/s Full duplex 2017/03/29 12:04:41 info port
 MGT link-ch 0 Port MGT:Up 1Gb/s Full duplex 2017/03/29 12:04:41
 info port eth3 link-ch 0 Port eth3:Up 1Gb/s Full duplex 2017/03/29
 12:04:41 info port eth2 link-ch 0 Port eth2:Up 1Gb/s Full duplex
 2017/03/29 12:04:41 info general general 0 Power Supply #1 (top)
 is not present on startup 2017/03/29 12:04:41 info general general
 0 Power Supply #2 (bottom) is not present on startup
```

使用防火牆監控 WildFire 設備提交

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

由防火牆轉送的範例（到 WildFire 私人雲端和/或公共雲端）將作為項目新增至 **WildFire Submissions**（**WildFire** 提交）日誌。詳細的 WildFire 分析報告顯示於每個 WildFire 提交項目的展開檢視中。如需使用防火牆監控惡意軟體的詳細資訊，請參閱監控 WildFire 活動。

檢視 WildFire 設備日誌和分析報告

這可在何處使用？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

WildFire 日誌包含有關 WildFire 分析的範例（檔案和電子郵件連結）的資訊。其中包括構件，也就是與日誌事件相關的屬性、活動或行為，例如攻擊者的應用程式類型或 IP 位址。除此之外也有 Wildfire 特定的品質，例如高層分析結果，包括將範例判別為惡意軟體、網路釣魚、灰色軟體或良性軟體，並詳述範例資訊。透過檢閱 WildFire 提交日誌，您也可瞭解您網路中的使用者是否下載可疑檔案。WildFire 分析報告會顯示詳細的範例資訊、目標使用者、電子郵件標頭資訊（若啟用）、傳遞檔案的應用程式，以及用於檔案命令和控制活動的所有 URL。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。

STEP 1 | 轉送檔案以進行 WildFire 設備分析.

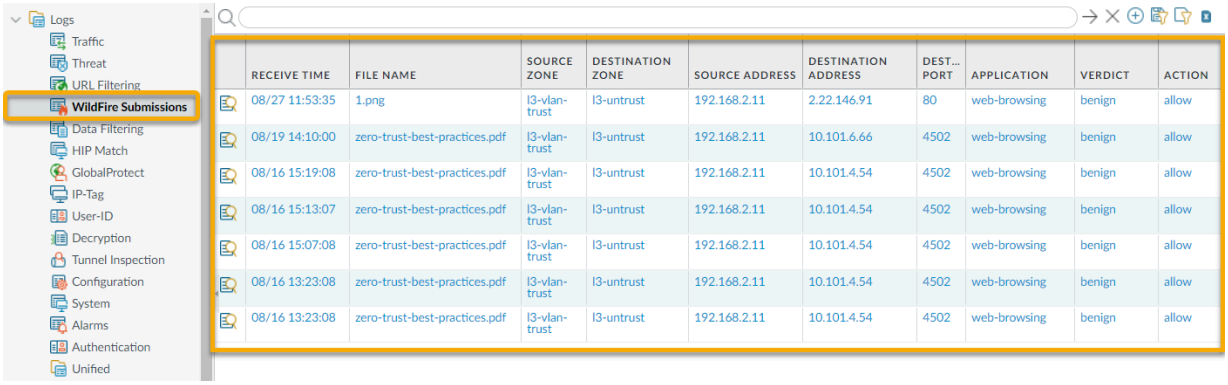
STEP 2 | 設定 WildFire 提交日誌設定。

STEP 3 | 若要檢視透過防火牆提交至 WildFire 公共、私人或混合型雲端的範別，請選取 **Monitor**（監控）> **Logs**（日誌）> **WildFire Submissions**（**WildFire** 提交）。WildFire 完成樣本分析後，結果將傳回提交該樣本防火牆，且可在 WildFire 提交日誌中存取。提交日誌包含指定樣本的詳細資料，包括下列資訊：

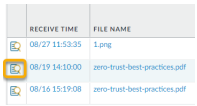
- 裁定列指明樣本為良性、惡意、網路釣魚或灰色。
- 動作列表示防火牆允許還是封鎖樣本。

- 「嚴重性」欄透過下列值表示樣本對組織的影響程度：重大、高、中、低及資訊。

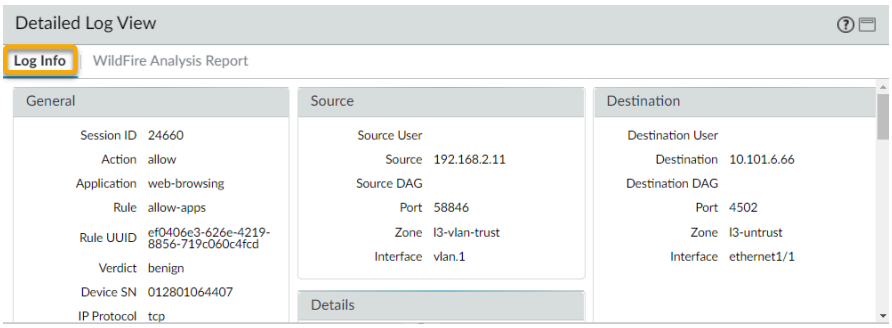
  下列嚴重性值由裁定值和動作值共同確定。
  - 低 - 動作設定為允許的灰色樣本。
  - 高 - 動作設定為允許的惡意樣本。
  - 資訊：
    - 動作設定為允許的良性樣本。
    - 動作設定為封鎖的任何裁定樣本。



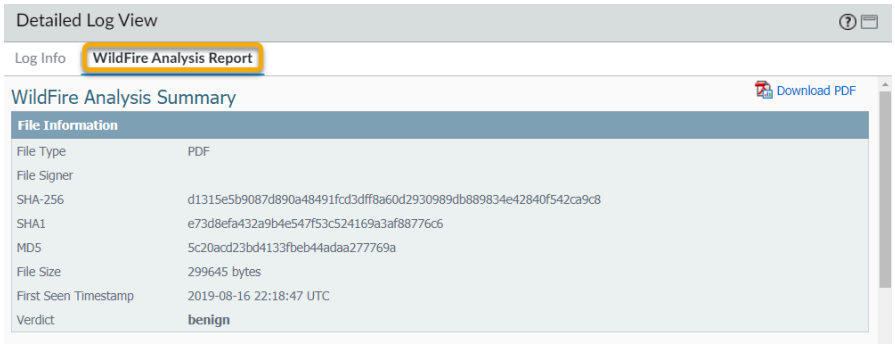
STEP 4 | 對於任何項目，選取 Log Details（日誌詳細資訊）圖示，即可開啟每個項目的詳細日誌檢視：



詳細日誌檢視顯示每個項目的 Log Info（日誌資訊）及 WildFire Analysis Report（WildFire 分析報告）。如果防火牆啟用了封包擷取 (PCAP)，亦會顯示樣本 PCAP。



對於所有樣本，WildFire 分析報告將顯示檔案及工作階段詳細資訊。對於惡意軟體樣本，WildFire 分析報告將會展開，包含表明檔案為惡意的檔案屬性及行為詳細資訊。



STEP 5 | （選用）**Download PDF**（下載 **PDF**） 版本的 WildFire 分析報告。

WildFire 裝置叢集

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

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。它在不允許存取 WildFire 公共雲端的環境下尤其有用。您可以在單一網路上將最多 20 個 WildFire 裝置作為一個 WildFire 裝置叢集管理。叢集還可以提供叢集散佈至所有連線防火牆的單一特徵碼包、高可用性 (HA) 架構以實現容錯，以及使用 Panorama 集中管理叢集的功能。您也可以使用 Panorama 管理獨立 WildFire 設備。

若要建立 WildFire 設備叢集，您想要放入叢集的所有 WildFire 設備都必須執行 PAN-OS 8.0.1 或更新版本。當您使用 Panorama 來管理 WildFire 設備叢集時，Panorama 也必須運行 PAN-OS 8.0.1 或更新版本。您無需獨立授權也能建立並管理 WildFire 設備叢集。

- WildFire 設備叢集復原能力與規模
- WildFire 裝置叢集管理
- 在 WildFire 設備上本機設定叢集
- 設定 WildFire 設備至設備加密
- 監控 WildFire 叢集
- 在叢集中升級 WildFire 設備
- 對 WildFire 叢集進行疑難排解

WildFire 設備叢集復原能力與規模

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

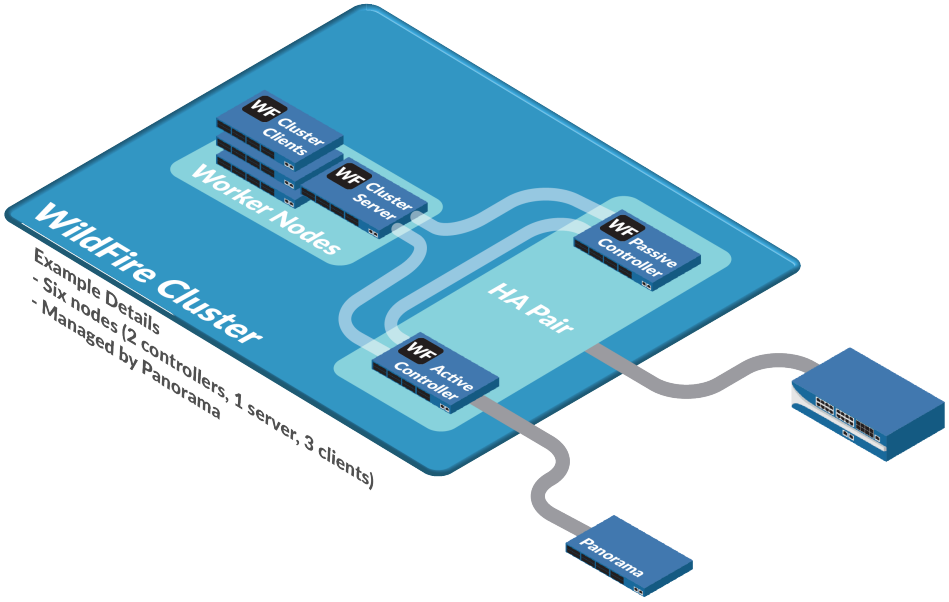
WildFire 設備叢集將多達二十個 WildFire 設備的樣本分析和儲存能力彙集在一起，以便您在單一網路上支援大型防火牆部署。您可以使用使用 CLI 在本機 WildFire 設備上靈活管理並設定叢集，或者在 Panorama M-Series 或虛擬設備伺服器上集中管理並設定叢集。WildFire 設備叢集環境包括：

- 您想要作為叢集分組並管理的 2 到 20 個 WildFire 設備。一個叢集必須在高可用性 (HA) 對中至少設定兩個 WildFire 設備。
- 轉送樣本至叢集進行流量分析和特徵碼產生的防火牆。
- （選用）一個或兩個 Panorama 設備以進行集中叢集管理（如果您選擇不在本地管理叢集）。若要提供 Ha，請使用設定為 HA 對的兩個 Panorama 設備。

新增至 WildFire 設備叢集的每個 WildFire 設備都會成為該叢集的一個節點（相對於獨立 WildFire 設備）。Panorama 最多可管理 10 個 WildFire 設備叢集，共包含 200 個 WildFire 叢集節點（10 個叢集，每個叢集最多包含 20 個節點）。

Panorama 可同時管理獨立 WildFire 設備和 *WildFire* 設備叢集。*Panorama* 可以管理的獨立 *WildFire* 設備和 *WildFire* 設備叢集節點的總和為 *200* 個。例如，如果 *Panorama* 管理共包含 *15* 個 *WildFire* 叢集節點的 *3* 個叢集和 *8* 個獨立 *WildFire* 設備，那麼 *Panorama* 共管理了 *23* 個 *WildFire* 設備，並可以再管理最多 *177* 個 *WildFire* 設備。

與 *Panorama* 連線的 *WildFire* 設備沒有註冊限制，即您可連線儘可能多的裝置而不影響容量授權。如需 *Panorama* 授權的詳細資訊，請參閱註冊 Panorama 並安裝授權。



叢集節點可以充當下列三種角色之一：

- 控制器節點—如果您未使用 Panorama M-Series 或虛擬設備管理叢集，兩個控制器節點將管理佇列服務和資料庫、產生特徵碼並在本機管理叢集。每個叢集最多可包含兩個控制器節點。若要具有容錯功能，每個 WildFire 設備叢集應至少將兩個節點設定為主要控制器節點和控制器備份節點 HA 對。除了在正常維護或故障情況下，每個叢集都應該有兩個控制器節點。
- 工作節點（叢集用戶端）—不是控制器節點的叢集節點即為工作節點。工作節點可以提高叢集的分析能力、儲存能力及資料復原能力。
- 伺服器節點（叢集伺服器）—WildFire 叢集中的第三個節點會自動設定為伺服器節點，它是一種特殊的工作節點，除標準工作節點的功能外，它還可提供資料庫和基礎結構冗餘等功能。

當防火牆在叢集節點上註冊，或您將已具有註冊防火牆的 WildFire 設備新增至叢集時，叢集會向連線的防火牆推送註冊清單。註冊清單包含叢集中的每個節點。如果叢集節點故障，已連線至該節點的防火牆將重新註冊至其他叢集節點。這樣的復原能力也是建立 WildFire 設備叢集的優勢之一。

優勢	說明
擴充	WildFire 設備叢集可以增加單一網路上的分析輸送量和儲存容量，讓您無需對網路分段也能為大型防火牆網路提供服務。
高可用性	如果一個叢集節點故障，HA 設定的容錯功能可以防止重要資料和服務遺失。如果您使用 Panorama 集中管理叢集，Panorama HA 設定可提供集中管理容錯功能。

優勢	說明
單一特徵碼包散佈	無論哪個叢集節點收到或分析了資料，所有連線至叢集的防火牆都會收到相同的特徵碼包。特徵碼包基於所有叢集成員的活動和分析結果建立，這表示每個連線的防火牆都會受益於叢集知識組合。
集中管理 (Panorama)	使用 Panorama 管理 WildFire 設備叢集可以節省時間並簡化管理程序。Panorama 沒有使用 CLI 和指令碼來管理 WildFire 設備或叢集，而是提供了網路裝置的單一虛擬管理平台 (single-pane-of-glass) 視圖。您還可以向多個 WildFire 設備叢集推送命令設定、設定更新及軟體升級，而且您可使用 Panorama Web 介面取代 WildFire 設備 CLI 執行所有這些操作。
負載平衡	當叢集有兩個或更多主動節點時，叢集會自動在節點之間對分析、報告產生、特徵碼建立、儲存及 WildFire 內容進行散佈和負載平衡。

WildFire 叢集高可用性

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

高可用性是 WildFire 設備叢集的一個重要優勢，因為 HA 可防止重要資料和服務遺失。HA 叢集能夠在節點之間複製並散佈重要資料，例如分析結果、報告和特徵碼，這樣，一個節點故障時不會導致資料遺失。HA 叢集還可以提供冗餘關鍵的服務，例如分析功能、WildFire API 和特徵碼產生，這樣，一個節點故障不會使服務中斷。一個叢集必須至少有兩個節點才能提供高可用性優勢。叢集節點故障不會影響防火牆，因為註冊至故障節點的防火牆可以使用叢集註冊清單註冊至其他叢集節點。

使用者會將 HA 對中的兩個裝置分別設定為主要和次要設備。基於此初始優先順序值設定，WildFire 還會將執行狀態「主動」指派給主要設備，將「被動」指派給次要裝置。此狀態決定哪個 WildFire 設備將被用作管理和基礎結構控制的接觸點。被動裝置總是與主動設備同步，並可在系統或網路發生故障時充當該角色。例如，當處於主動狀態的主要設備（主動—主要）發生故障時，容錯移轉事件將發生，並轉換為被動—主要狀態，而次要設備則轉換為主動—次要。無論設備處於何種狀態，最初指派的優先順序值都保持不變。

當 HA 對無法再彼此通訊時，會發生容錯移轉，因為無回應，或發生致命錯誤。雖然 WildFire HA 對會嘗試自動解決小問題，但重大事件需要使用者干預。當控制器被使用者暫停或解除時，容錯移轉也會觸發。

不要設定只有一個控制器節點的叢集。每個叢集應有一個 *HA* 控制器對。叢集應該只會在暫時情況下有單一的控制器節點，例如，當您交換控制器節點或控制器節點故障時。

在雙節點叢集 HA 對中，如果一個控制器節點故障，另一個控制器節點無法處理樣本。對於可處理樣本的剩餘叢集節點，您必須將其設定為獨立 WildFire 設備：在剩餘叢集節點上刪除 HA 與叢集設定並重新啟動節點。節點會作為獨立 WildFire 設備復原。

三節點叢集將利用第三個伺服器節點執行 HA 對，以提供額外的冗餘。伺服器會將相同的資料庫和伺服器基礎結構服務作為控制器執行，但不會產生特徵碼。這樣的部署可讓叢集在一個控制器節點故障時正常執行。

已新增至 WildFire 叢集的其他節點將作為工作或伺服器節點執行。第三個節點已自動設定為伺服器，而所有後續節點都會新增為工作節點。

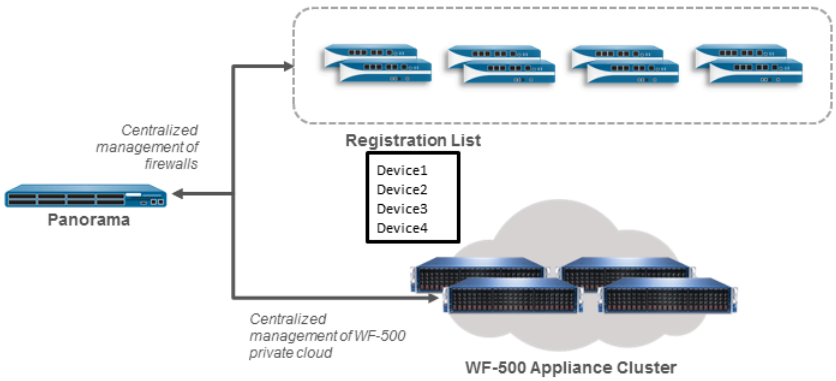
使用 Panorama 管理 WildFire 叢集的優勢

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

如果使用 Panorama 管理 WildFire 設備叢集，您可以將兩個 Panorama M-Series 或虛擬設備設定為一個 HA 對以提供管理冗餘。如果您未設定冗餘 Panorama 設備且 Panorama 設備故障，則您仍可從控制器節點在本機管理叢集。

如果您使用 Panorama HA 對管理叢集且一個 Panorama 設備故障，則另一個 Panorama 設備會接管對叢集的管理。如果 Panorama HA 端點故障，會儘快還原故障 Panorama 端點的服務以還原管理 HA。

提供分析、儲存功能和集中管理 HA 需要至少兩個設定為叢集控制器的 WildFire 設備和控制器備份節點，以及兩個 Panorama M-Series 或虛擬設備。



防火牆會收到包含屬於叢集的所有 WildFire 設備的註冊清單。防火牆可以註冊到叢集中的任意節點且叢集會自動平衡其節點之間的負載。

WildFire 裝置叢集管理

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

若要管理 WildFire 設備叢集，您需要瞭解叢集的功能及管理建議。

類別	說明
叢集操作和設定	對所有叢集節點進行相同設定，以確保分析和設備間通訊時的一致性： • 所有叢集節點必須執行相同版本的 PAN-OS（PAN-OS 8.0.1 或更新版本）。Panorama 執行的軟體版本必須與叢集節點相同或更新。防火牆可以執行相同的軟體版本，使其提交樣本至 WildFire 設備。防火牆無需特定的軟體版本也能提交樣本至 WildFire 設備叢集。 • 叢集節點可從控制器節點繼承除介面設定之外的設定。叢集成員會監控控制器節點設定，並在控制器節點交付更新的設定時更新自身設定。工作節點會繼承一些設定，例如內容更新伺服器設定、WildFire 雲端伺服器設定、樣本分析影像檔、樣本資料保留時間範圍、分析環境設定、特徵碼產生設定、日誌設定、驗證設定，及 Panorama 伺服器、DNS 伺服器和 NTP 伺服器設定。 • 當您使用 Panorama 管理叢集時，Panorama 設備會推送一致的設定至所有叢集節點。雖然您可以在 WildFire 設備節點上本機變更設定，但 Palo Alto Networks 不建議您這樣做，因為 Panorama 設備下次推送設定時，其會取代節點上正在執行的設定。對 Panorama 管理的叢集節點進行的本機變更常常會導致 Out of Sync（不同步）錯誤。 • 如果兩個控制器節點上的叢集節點成員清單不同，叢集會產生 Out of Sync（不同步）警告。為了避免兩個控制器節點不斷更新另一個節點的不同步成員清單，叢集成員執行會停止。在這種情況下，您可以透過執行操作命令 **`request high-availability sync-to-remote running-configuration`**，同步控制器和控制器備份節點上本機 CLI 的叢集成員清單。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。在每個控制器節點上，執行 **`show cluster all-peers`**，並比較和修正成員清單。 • 一個叢集只能包含兩個控制器節點（主要和備份）；嘗試在本機向叢集新增第三個控制器節點失敗。（Panorama Web 介面可自動防止您新增第三個控制器節點。）向叢集新增的第三個和所有後續節點必須都是工作節點。

類別	說明
	• HA 設定的特徵是，叢集會散佈並保留多個資料庫、佇列服務及樣本提交複本，以在叢集節點故障的情況下提供冗餘。執行為 HA 提供冗餘所需的額外服務對輸送量的影響非常小。 • 叢集將自動檢查用於分析環境網路的重複 IP 地址。 • 如果您想要將屬於一個叢集的節點移動到不同叢集，必須先將該節點從其目前叢集中移除。 • 請勿變更目前叢集中執行的 WildFire 設備之 IP 位址。否則，相關聯的防火牆會從節點取消註冊。
叢集資料保留原則	資料保留原則可以決定 WildFire 設備叢集儲存不同類型樣本的時間。 • 良性和灰色樣本—叢集可將良性和灰色樣本保留 1 至 90 天（預設值為 14）。 • 惡意樣本—叢集可將惡意樣本保留至少 1 天（預設值為無限，即永不刪除）。惡意樣本可能包括網路釣魚裁定樣本。 在整個叢集中設定相同的資料保留政策（在本機設定一般叢集設定中的 4 或在 Panorama 上設定一般叢集設定中的 4）。
網路	不允許 WildFire 設備叢集之間通訊。特定叢集內的節點可以彼此通訊，但不能與其他叢集中的節點通訊。 所有叢集成員必須： • 使用專用叢集管理介面進行叢集管理和通訊（在 Panorama 中執行）。 • 在相同子網路中具有靜態 IP 地址。 • 在叢集節點之間使用低延遲連線。連線的最大延遲不應超過 500 毫秒。
專用叢集管理介面	專用叢集管理介面讓控制器節點管理叢集，和標準管理介面 (Ethernet0) 不同。Panorama 將執行設定專用叢集管理介面。 在雙節點設定中，如果兩個控制器節點之間的叢集管理連結發生故障，即使與主要控制器節點沒有管理通訊，控制器備份節點服務和樣本分析也將繼續執行。這是因為當叢集管理連結發生故障時，控制器節點不知道主要控制器節點是否仍然正常運作，從而導致「腦分裂」狀況。控制器備份節點必須繼續提供叢集服務，以防主要控制器節點無法正常運作。當叢集管理連結還原後，來自各個控制器節點的資料將合併。

類別	說明
DNS	您可將 WildFire 設備叢集中的控制器節點用作叢集的授權 DNS 伺服器。（授權 DNS 伺服器用於叢集成員的實際 IP 地址，這與遞迴 DNS 伺服器不同，後者可查詢授權 DNS 伺服器，並將要求的資訊傳遞至發出初始要求的主機。） 提交樣本至 WildFire 設備叢集的防火牆應傳送 DNS 查詢至其常規 DNS 伺服器，例如企業內部 DNS 伺服器。內部 DNS 伺服器可轉送 DNS 查詢至 WildFire 設備叢集控制器（根據查詢的網域）。使用叢集控制器作為 DNS 伺服器可提供諸多優點： • 自動負載平衡—當叢集控制器解析服務廣告主機名稱時，主機叢集節點的順序是隨機的，它可有組織地平衡節點上的負載。 • 容錯—如果一個叢集節點故障，叢集控制器會自動將其從 DNS 回應移除，以便防火牆傳送新要求至正常執行的節點。 • 靈活性並易於管理—當您新增節點至叢集時，由於控制器會自動更新 DNS 回應，您無需在防火牆上進行任何變更，要求便可自動前往新節點以及之前存在的節點。 雖然 DNS 記錄不應被快取，但對於疑難排解，如果 DNS 查找成功，TTL 為 0。但是，當 DNS 查找返回 NXDOMAIN 時，TTL 和「最小 TTL」均為 0。
管理	您可以使用本機 WildFire CLI 或 Panorama 管理 WildFire 叢集。WildFire 叢集節點上有兩個可在本機使用的管理角色： • 超級讀取者—唯讀存取。 • 超級使用者—讀取及寫入存取權限。
防火牆註冊	WildFire 設備叢集會向連線至叢集節點的每個防火牆推送包含叢集所有節點的清單。當您在叢集中的設備上註冊防火牆時，防火牆會收到註冊清單。當您將已具有連線防火牆的獨立 WildFire 設備新增至叢集，以使其成為叢集節點時，這些防火牆將收到註冊清單。 如果節點故障，連線的防火牆將使用註冊清單在清單上的下一個節點註冊。
資料移轉	為了提供資料冗餘，叢集中的 WildFire 設備節點將共享資料庫、佇列服務及樣本提交內容，但該資料的精確位置取決於叢集拓撲。因此，每當拓撲變更時，叢集中的 WildFire 設備會進行資料移轉或資料重新排列。拓撲變更包括新增和移除節點，以及變更已存在節點角色的變更。當資料庫轉換為更新的版本時，也會發生資料移轉，例如從 WildFire 7.1 升級至 8.0。

類別	說明
	可以透過執行 WildFire CLI 狀態命令來檢視資料移轉狀態。此程序視乎 WildFire 設備上資料的數量，可能需要幾小時。

部署 WildFire 叢集

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

若要部署 WildFire 設備叢集，您必須升級所有將註冊至叢集的設備、建立 WildFire 叢集，然後最終設定最滿足您需要的設定。您可從 WildFire 設備 CLI 或通過 Panorama 在本機執行這些工作，這讓您能夠快速地將設定變更和升級套用至 WildFire 設備。

下列程序顯示了如何建立和設定 WildFire HA（高可用性）對及如何新增額外設備節點至叢集。

STEP 1 | 本機升級您的 WildFire 設備至 PAN-OS 8.0.1 或更新版本，PAN-OS 8.0.1 是運作叢集支援的最低版本。

STEP 2 | 建立、設定並新增節點至 WildFire 設備叢集。

- 本機設定叢集並新增節點
- 在 Panorama 上設定叢集並新增節點

STEP 3 | 設定一般 WildFire 設備叢集設定。

- 本機設定一般叢集設定
- 在 Panorama 上設定一般叢集設定

STEP 4 | （選用）加密 WildFire 叢集設備至設備通訊。

- 使用預先定義的憑證透過 CLI 設定設備至設備加密
- 使用自訂憑證透過 CLI 設定設備至設備加密
- 使用預先定義的憑證在 Panorama 上集中設定設備至設備加密
- 使用自訂憑證在 Panorama 上集中設定設備至設備加密

STEP 5 | 確認您的 WildFire 設備叢集運作正常。

- 使用 CLI 檢視 WildFire 叢集狀態
- 使用 Panorama 檢視 WildFire 叢集狀態

STEP 6 | （選用）升級已註冊至叢集的 WildFire 設備。

- 在有網際網路連線的情況下本機升級叢集
- 在沒有網際網路連線的情況下本機升級叢集
- 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

在 WildFire 設備上本機設定叢集

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

在本機設定 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。

如果您使用 Panorama 管理 WildFire 設備叢集，也可在 Panorama 上集中設定 WildFire 叢集。

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。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。

當 WildFire 設備可用時，請執行適當的工作：

- 本機設定叢集並新增節點
- 本機設定一般叢集設定
- 從本機叢集移除節點

本機設定叢集並新增節點

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

當您對叢集新增節點時，叢集將根據您設定的控制器節點介面，自動設定節點之間的通訊。

STEP 1 | 確保您想要新增至叢集的每個 WildFire 設備均運行 PAN-OS 8.0.1 或更新版本。

在每個 WildFire 設備上，運行：

```
admin@WF-500> show system info | match version
```

STEP 2 | 確認 WildFire 設備沒有在分析樣本並處於獨立狀態（不是其他叢集的成員）。

1. 在每個設備上，顯示設備是否在分析樣本：

```
admin@WF-500> show wildfire global sample-analysis
```

   沒有樣本應顯示為 `pending`。所有樣本均應處於完成狀態。如果樣本顯示為 `pending`，請等待其完成分析。`Pending` 樣本與惡意和非惡意樣本分開顯示。`Finish Date` 顯示分析完成的日期與時間。

2. 在每個設備上，確認所有程序都在執行：

```
admin@WF-500> show system software status
```

3. 在每個設備上，檢查以確保設備處於獨立狀態且不屬於叢集：

```
admin@WF-500> show cluster membership Service Summary:
 wfpc signature Cluster name:Address:10.10.10.100 Host
 name:WF-500 Node name: wfpc-000000000000-internal Serial
 number:000000000000 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.
```

   反白顯示的行表示節點處於獨立模式且可以從獨立設備轉換為叢集節點。

   這些範例中的 *12* 位序號 *(000000000000)* 為一般範例，不是真正的序號。您網路中的 *WildFire* 設備具有唯一的真正序號。

STEP 3 | 設定主要控制器節點。

這包括將節點設定為 HA 對的主要控制器、啟用 HA，定義設備用於 HA 控制連結和叢集通訊與管理的介面。

1. 啟用高可用性並設定到控制器備份節點的控制連結介面，例如，在介面 eth3 上：

```
admin@WF-500# set deviceconfig high-availability enabled yes
 interface ha1 port eth3 peer-ip-address <secondary-node-eth3-
ip-address>
```

2. 將設備設定為主要控制器節點：

```
admin@WF-500# set deviceconfig high-availability election-
option priority primary
```

3. （選用）設定控制器節點與控制器備份節點之間的備份高可用性介面，例如，在管理介面上：

```
admin@WF-500# set deviceconfig high-availability interface
 ha1-backup port management peer-ip-address <secondary-node-
management-ip-address>
```

4. 在叢集內設定通訊與管理的專用介面，包括指定叢集名稱與將節點角色設定為控制器節點：

```
admin@WF-500# set deviceconfig cluster cluster-name <name>
 interface eth2 mode controller
```

本範例將 eth2 用作專用的叢集通訊連接埠。

叢集名稱必須為有效的子域名，且長度最多為 63 個字元。僅可使用小寫字元與數字，如果不在叢集名稱的開頭或結尾，則可使用連字號與句點。

STEP 4 | 設定控制器備份節點。

這包括將節點設定為 HA 對的備份控制器、啟用 HA，定義設備用於 HA 控制連結和叢集通訊與管理的介面。

1. 啟用高可用性，並在與主要控制器節點使用的同一介面（本範例中為 eth3）上設定到主要控制器節點的控制連結介面連線：

```
admin@WF-500# set deviceconfig high-availability enabled yes
 interface ha1 port eth3 peer-ip-address <primary-node-eth3-
ip-address>
```

2. 將設備設定為控制器備份節點：

```
admin@WF-500# set deviceconfig high-availability election-
option priority secondary
```

3. （建議）設定控制器備份節點與控制器節點之間的備份高可用性介面，例如，在管理介面上：

```
admin@WF-500# set deviceconfig high-availability interface
 ha1-backup port management peer-ip-address <primary-node-
management-ip-address>
```

4. 在叢集內設定通訊與管理的專用介面，包括指定叢集名稱與將節點角色設定為控制器節點：

```
admin@WF-500# set deviceconfig cluster cluster-name <name>
 interface eth2 mode controller
```

STEP 5 | 交付兩個控制器節點上的設定。

在每個控制器節點上：

```
admin@WF-500# commit
```

交付兩個控制器節點上的設定會產生一個雙節點叢集。

STEP 6 | 驗證主要控制器節點上的設定。

在主要控制器節點上：

```
admin@WF-500(active-controller)> show cluster membership
 Service Summary: wfpc signature Cluster name: mycluster
 Address:10.10.10.100 Host name:WF-500 Node name:
 wfpc-000000000000-internal Serial number:000000000000 Node mode:
 controller Server role:True HA priority: primary Last changed:Sat,
 04 Mar 2017 12:52:38 -0800 Services: wfcore signature wfpc
 infra Monitor status:Serf Health Status: passing Agent alive and
 reachable Application status:  global-db-service:JoinedCluster
```

```
 wildfire-apps-service:Ready  global-queue-service:JoinedCluster
 wildfire-management-service:Done  siggen-db:ReadyMaster Diag
 report:10.10.10.110: reported leader '10.10.10.100', age 0.
 10.10.10.100: local node passed sanity check.
```

提示 (active-controller) 和突出顯示的 Application status 行表示節點處於控制器模式、已就緒，並為主要控制器節點。

STEP 7 | 驗證次要控制器節點上的設定。

在次要控制器節點上：

```
admin@WF-500(passive-controller)> show cluster membership
 Service Summary: wfpc signature Cluster name: mycluster
 Address:10.10.10.110 Host name:WF-500 Node name:
 wfpc-000000000000-internal Serial number:000000000000 Node
 mode: controller Server role:True HA priority: secondary
 Last changed:Fri, 02 Dec 2016 16:25:57 -0800 Services: wfcore
 signature wfpc infra Monitor status:Serf Health Status: passing
 Agent alive and reachable Application status:  global-db-
service:JoinedCluster  wildfire-apps-service:Ready  global-
queue-service:JoinedCluster  wildfire-management-service:Done
 siggen-db:ReadySlave Diag report:10.10.10.110: reported leader
 '10.10.10.100', age 0. 10.10.10.110: local node passed sanity
 check.
```

提示 (passive-controller) 和突出顯示的 Application status 行表示節點處於控制器模式、已就緒，並為備份控制器節點。

STEP 8 | 測試節點設定。

驗證控制器節點 API 金鑰可在全域檢視：

```
admin@WF-500(passive-controller)> show wildfire global api-keys
 allService Summary: wfpc signatureCluster name: mycluster
```

兩個設備的 API 金鑰均應可檢視。

STEP 9 | 手動同步控制器節點上的高可用性設定。

同步控制器節點可確保設定相符並應只需同步一次。高可用性設定同步完成後，控制器節點會保持設定同步，您無需再同步。

1. 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。

2. 提交設定：

```
admin@WF-500# commit
```

STEP 10 | 驗證叢集正常運作。

若要驗證與防火牆相關的資訊，您首先必須透過選取 ***Device***（裝置） > ***Setup***（設定） > ***WildFire*** 並編輯 ***General Settings***（一般設定），將至少一個防火牆連線至叢集節點來指向節點。

1. 顯示對等叢集以確保兩個控制器均為叢集成員：

```
admin@WF-500(active-controller)> show cluster all-peers
```

2. 顯示兩個節點或任一控制器節點的 API 金鑰（如果您建立了 API 金鑰）：

```
admin@WF-500(active-controller)> show wildfire global api-keys
 all
```

3. 存取任一控制器節點的任何樣本：

```
admin@WF-500(active-controller)> show wildfire global sample-
status sha256 equal <value>
```

4. 防火牆可以註冊並上載檔案至兩個節點。Confirm that the firewall is successfully forwarding samples.
5. 兩個節點可以下載並分析檔案。
6. 建立叢集後，所有已分析的檔案將顯示兩個儲存位置，每個節點上顯示一個。

STEP 11 | （選用）設定工作節點並將其新增至叢集。

工作節點會使用控制器節點的設定，以使設定一致。對於共包含 20 個節點的叢集，您最多可新增 18 個工作節點。

1. 在主要控制器節點上，將工作新增至控制器節點的工作清單：

```
admin@WF-500(active-controller)> configure
 admin@WF-500(active-controller)# set deviceconfig cluster
 mode controller worker-list <ip>
```

<*ip*> 為您想要新增至叢集的工作節點的叢集管理介面 IP 位址。使用獨立命令將每個工作節點新增至叢集。

2. 交付控制器節點的設定：

```
admin@WF-500(active-controller)# commit
```

3. 在 WildFire 設備上，您想要轉換為叢集工作節點、設定要加入的叢集、設定叢集通訊介面，以及使設備處於 `worker` 模式：

```
admin@WF-500> configure admin@WF-500# set deviceconfig cluster
 cluster-name <name> interface eth2 mode worker
```

叢集通訊介面必須為指定在控制器節點上進行叢集內通訊的同一介面。在本範例中，`eth2` 是在控制器節點上設定用於進行叢集通訊的介面。

4. 交付工作節點上的設定：

```
admin@WF-500# commit
```

5. 等待所有服務出現在工作節點上。執行 **`show cluster membership`** 並檢查 `Application status`，這會在所有服務出現時於 `Ready` 狀態中顯示所有服務和 `siggen-db`。
6. 在任一叢集控制器節點上，檢查以確保工作節點已新增：

```
admin@WF-500> show cluster all-peers
```

您新增的工作節點會出現在叢集節點清單中。如果您不小心將錯誤的 WildFire 設備新增至叢集，可以從本機叢集移除節點。

STEP 12 | 驗證工作節點上的設定。

1. 在工作節點上，檢查以確保 `Node mode` 欄位顯示節點處於工作模式：

```
admin@WF-500> show cluster membership
```

2. 驗證防火牆可在工作節點上註冊及工作節點可下載並分析檔案。

本機設定一般叢集設定

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

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。
- 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。

在叢集的主要控制器節點上使用 CLI 設定 WildFire 設定。其他叢集節點使用在叢集控制器上設定的設定。

STEP 1 | 設定 WildFire 叢集的一般設定。此程序與設定 WildFire 設備設定類似。

1. （建議）重設管理密碼。
2. 進行管理介面設定。設定 WildFire 設備叢集節點 IP 地址與預設閘道。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。同時設定 DNS 伺服器 IP 位址。
3. 設定 WildFire 設備時鐘。手動或透過指定 NTP 伺服器設定時鐘，並設定 NTP 伺服器驗證。
4. 選擇設備將用於分析檔案的虛擬電腦影像檔。
5. （選用）允許其他使用者管理 WildFire 設備。新增管理員帳戶並為其指派角色以管理叢集。
6. 設定 RADIUS 驗證供管理者存取。

STEP 2 | （選用）將叢集連線至 WildFire 公共雲端並設定叢集會使用的雲端服務。

如果沒有商業原因阻止您將 WildFire 設備叢集連線至公共 WildFire 雲端，將叢集連線至雲端具有諸多優勢，例如：

- 使用雲端的資源在多個環境中使用不同方法執行樣本分析。
- 執行本機分析前，自動查詢雲端進行裁定，以卸載叢集中的工作。（預設為停用。）
- 幫助蒐集全域 WildFire 社群的情報並從中受益。

本表格行所述的功能並不特定於叢集。您也可在獨立的 *WildFire* 設備上設定這些功能。

1. 從蒐集自所有連線的 WildFire 設備的情報受益：

```
admin@WF-500(active-controller)# set deviceconfig setting
 wildfire cloud-server <hostname-value>
```

WildFire 公共雲端伺服器主機名稱的預設值為 `wildfire-public-cloud`。您可向任何公共 WildFire 雲端轉送檔案至以進行 WildFire 分析。

2. 如果您將叢集邊線至 WildFire 公共雲端，請先設定是否自動查詢公共雲端進行裁定，然後再執行本機分析。先查詢公共雲端可減少本機 WildFire 叢集上的負載：

```
admin@WF-500(active-controller)# set deviceconfig setting
 wildfire cloud-intelligence cloud-query (no | yes)
```

3. 如果您將叢集連線至 WildFire 公共雲端，設定您想要提交本機發現的惡意軟體或報告至 WildFire 公共雲端的資訊類型（診斷資料、關於惡意軟體分析的 XML 報告、惡意樣本）。如果您傳送惡意樣本，叢集不會傳送報告。

```
admin@WF-500(active-controller)# set deviceconfig setting
 wildfire cloud-intelligence submit-diagnostics (no | yes)
 submit-report (no | yes) submit-sample (no | yes)
```

STEP 3 | （選用）設定控制器節點以使用 DNS 協定發佈服務狀態。

```
admin@WF-500(active-controller)# set deviceconfig cluster mode
 controller service-advertisement dns-service enabled yes
```

STEP 4 | （選用）設定惡意和良性或灰色樣本的資料保留原則。

1. 選取保留不同類型資料的時間長度：

```
admin@WF-500(active-controller)# set deviceconfig setting
 wildfire file-retention malicious <indefinite | 1-2000> non-
malicious <1-90>
```

保留惡意樣本的預設時間為無限（不刪除）。保留非惡意樣本（良性和灰色）樣本的預設時間為 14 天。

STEP 5 | （選用）設定偏好分析環境。

1. 如果您的分析環境主要分析可執行檔樣本或文件樣本，您可以配置大部分叢集資源來分析這些樣本類型：

```
admin@WF-500(active-controller)# set deviceconfig setting
 wildfire preferred-analysis-environment (Documents |
 Executables | default)
```

對於叢集中的每個 WildFire 設備：

- `Default` 選項可同時分析 16 個文件、10 個可攜式執行檔 (PE) 及 2 個電子郵件連結。
- Documents（文件）選項可同時分析 25 個文件、1 個 PE 及 2 個電子郵件連結。
- Executables（可執行檔）選項可同時分析 25 個 PE、1 個文件及 2 個電子郵件連結。

您可為叢集中的每個節點設定不同的偏好分析環境。（如果您使用 Panorama 管理叢集，Panorama 可以設定整個叢集的分析環境。）

STEP 6 | 設定節點分析設定。

1. （選用）設定內容更新以提高惡意軟體分析。
2. 設定虛擬電腦介面以使叢集在分析的樣本尋找網路存取時，觀察惡意軟體行為。
3. （選用）啟用本機特徵碼及 URL 類別產生，以產生 DNS、防毒特徵碼和 URL 類別。

STEP 7 | 設定日誌記錄。

1. 設定 WildFire 提交日誌設定。

從本機叢集移除節點

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

您可以使用本機 CLI 移除叢集中的節點。從雙節點叢集中移除節點的程序和三個或更多節點的叢集不同。

從三個或更多節點的叢集中移除工作節點。

1. 從工作節點的 CLI 解除工作節點：

```
admin@WF-500> request cluster decommission start
```

   Decommission 命令僅適用於包含三個或更多節點的叢集。請勿使用 *decommission* 移除雙節點叢集中的節點。

2. 確認解除節點成功：

```
admin@WF-500> show cluster membership
```

   此命令會在工作節點從叢集中移除後報告 `decommission: success`。如果命令未顯示成功解除，請等待幾分鐘以讓解除完成，然後再次執行命令。

3. 從工作節點的 CLI 刪除叢集設定：

```
admin@WF-500># delete deviceconfig cluster
```

4. 提交設定：

```
admin@WF-500># commit
```

5. 確認所有程序都在執行：

```
admin@WF-500> show system software status
```

6. 從控制器節點的工作清單中移除工作節點：

```
admin@WF-500(active-controller)# delete deviceconfig cluster
 mode controller worker-list <worker-node-ip>
```

7. 提交設定：

```
admin@WF-500(active-controller)# commit
```

8. 在控制器節點上，檢查以確保工作節點已移除：

```
admin@WF-500(active-controller)> show cluster all-peers
```

   您已移除的工作節點不會出現在叢集節點清單中。

從雙節點叢集中移除控制器節點。

正常情況下，每個叢集在使用高可用性設定時必須有兩個控制器節點。但是，維護或交換出控制器節點可能需要使用 CLI 從叢集移除控制器節點：

1. 暫停您想要移除的控制器節點：

```
admin@WF-500(passive-controller)> debug cluster suspend on
```

2. 在您想要移除的控制器節點上，刪除高可用性設定。本範例顯示了移除控制器備份節點：

```
admin@WF-500(passive-controller)> configure
 admin@WF-500(passive-controller)# delete deviceconfig high-availability
```

3. 刪除叢集設定：

```
admin@WF-500(passive-controller)# delete deviceconfig cluster
```

4. 提交設定：

```
admin@WF-500(passive-controller)# commit
```

5. 等待服務復原。執行 **show cluster membership** 並檢查 `Application status`，這會在所有服務出現時於 `Ready` 狀態中顯示所有服務和 `siggen-db`。`Node mode` 應該為 `stand_alone`。
6. 在剩餘叢集節點上，檢查以確保此節點已移除：

```
admin@WF-500(active-controller)> show cluster all-peers
```

您已移除的控制器節點不會出現在叢集節點清單中。

7. 如果您準備了其他 WildFire 設備，儘快將其新增至叢集，以還原高可用性（本機設定叢集並新增節點）。

如果您沒有準備其他 WildFire 設備以取代移除的叢集節點，應從剩餘叢集節點移除高可用性與叢集設定，因為不建立使用單節點叢集，且其不具備高可用性。最好將單一 WildFire 設備作為獨立設備，而不是單節點叢集管理。

若要從剩餘節點（在本範例中，為主要控制器節點）移除高可用性和叢集設定：

```
admin@WF-500(active-controller)> configure
 admin@WF-500(active-controller)# delete deviceconfig
```

```
high-availability admin@WF-500(active-controller)# delete
deviceconfig cluster admin@WF-500(active-controller)# commit
```

等待服務復原。執行 **show cluster membership** 並檢查 Application status，這會在所有服務出現時於 Ready 狀態中顯示所有服務和 siggen-db。Node mode 應該為 stand_alone。

設定 WildFire 設備至設備加密

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

您可加密在叢集中所部署設備之間的 WildFire 通訊。依預設，當 WildFire 設備與管理設備以及 WildFire 對等叢集通訊時，會使用純文字傳送資料。您可使用預先定義的憑證或自訂憑證驗證使用 IKE/IPsec 通訊協定的 WildFire 對等設備之間的連線。預先定義的憑證符合目前經 FIPS/CC/UCAPL 核准的憑證與合規要求。如果您要改為使用自訂憑證，則必須選取符合 FIPS/CC/UCAP 標準的憑證，否則將無法匯入憑證。

您可使用 WildFire CLI 在本機設定 WildFire CLI 設備至設備加密，或透過 Panorama 集中設定。記住，特定叢集內的所有 WildFire 設備必須執行支援加密通訊的 PAN-OS 版本。

如果叢集中的 *WildFire* 設備使用 *FIPS/CC* 模式，則加密會使用預先定義的憑證自動啟用。

根據您要部署設備至設備加密的方式，執行下列其中一項工作：

- 使用預先定義的憑證在 Panorama 上集中設定設備至設備加密
- 使用自訂憑證在 Panorama 上集中設定設備至設備加密
- 使用預先定義的憑證透過 CLI 設定設備至設備加密
- 使用自訂憑證透過 CLI 設定設備至設備加密

使用預先定義的憑證透過 CLI 設定設備至設備加密

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

使用 CLI 設定設備至設備加密時，您必須從被指定為主動控制器的 WildFire 設備發出所有命令。設定變更將自動散佈至被動控制器。如果您執行包含 3 個或更多節點的叢集，還必須將用作伺服器節點的 WildFire 叢集設備與主動控制器進行相同的設定。

STEP 1 | 將每個受管理的 WildFire 設備 升級 至 PAN-OS 9.0。

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 | 在被指定為主動控制器的 WildFire 設備上啟用安全叢集通訊。

```
set deviceconfig cluster encryption enabled yes
```

STEP 4 | （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。

```
set deviceconfig high availability encryption enabled yes
```

STEP 5 | （僅限包含 3 個或更多節點的設備叢集）針對已在叢集中註冊的第三個 WildFire 設備伺服器節點重複步驟 2-4。

使用自訂憑證透過 CLI 設定設備至設備加密

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

使用 CLI 設定設備至設備加密時，您必須從被指定為主動控制器的 WildFire 設備發出所有命令。設定變更將自動散佈至被動控制器。如果您執行包含 3 個或更多節點的叢集，還必須將用作伺服器節點的 WildFire 叢集設備與主動控制器進行相同的設定。

STEP 1 | 將每個受管理的 WildFire 設備 升級 至 PAN-OS 9.0。

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 | 匯入（或者產生）含有私密金鑰的憑證及其 CA 憑證。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. 要匯入自訂憑證，請從 WildFire 設備 CLI 中輸入下列命令：**scp import certificate from <value> file <value> remote-port <1-65535> source-ip <ip/netmask> certificate-name <value> passphrase <value> format <value>**
2. 若要產生自訂憑證，請從 WildFire 設備 CLI 輸入下列命令：**request certificate generate certificate-name name digest country-code state locality organization email filename ca signed-by | ocsp-responder-url days-till-expiry hostname [...] request certificate generate certificate-name name digest country-code state locality organization email filename ca signed-by | ocsp-responder-url days-till-expiry ip [...] request certificate generate certificate-name name**

STEP 4 | 匯入包含伺服器憑證和私密金鑰的 WildFire 設備金鑰配對。

```
scp import keypair from <value> file <value> remote-port <1-65535>
 source-ip <ip/netmask> certificate-name <value> passphrase <value>
 format <pkcs12|pem>
```

STEP 5 | 設定並指定 SSL/TLS 設定檔，以定義憑證和通訊協定供 WildFire 設備用於 SSL/TLS 服務。

set deviceconfig setting management secure-conn-server ssl-tls-service-profile <profile name>

1. 建立 SSL/TLS 設定檔。

   ```
   set shared ssl-tls-service-profile <name>
   ```

2. 指定自訂憑證。

   ```
   set shared ssl-tls-service-profile <name> certificate <value>
   ```

3. 定義 SSL/TLS 範圍。

   ```
   set shared ssl-tls-service-profile <name> protocol-settings
    min-version <tls1-0|tls1-1|tls1-2>
   ```

   ```
   set shared ssl-tls-service-profile <name> protocol-settings
    max-version <tls1-0|tls1-1|tls1-2|max>
   ```

4. 指定 SSL/TLS 設定檔。此 SSL/TLS 服務設定檔適用於 WildFire 設備和防火牆以及 WildFire 對等設備之間的所有連線。

   ```
   set deviceconfig setting management secure-conn-server ssl-
   tls-service-profile <ssltls-profile>
   ```

STEP 6 | 設定並指定憑證設定檔，以定義憑證和通訊協定供 WildFire 設備用於 SSL/TLS 服務。

1. 建立憑證設定檔。

```
set shared certificate-profile <name>
```

2. （選用）設定主體（通用名稱）或主體別名。

```
set shared certificate-profile <name> username-field subject
 <common-name>
```

```
set shared certificate-profile <name> username-field subject-
alt <email|principal-name>
```

3. (Optional) Set the user domain.

```
set shared certificate-profile <name> domain <value>
```

4. 設定 CA。

```
set shared certificate-profile <name> CA <name>
```

```
set shared certificate-profile <name> CA <name> default-ocsp-
url <value>
```

```
set shared certificate-profile <name> CA <name> ocsp-verify-
cert <value>
```

5. 指定憑證設定檔。

```
set deviceconfig setting management secure-conn-server
 certificate-profile <certificate-profile>
```

STEP 7 | 匯入憑證和私密金鑰配對。

STEP 8 | 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，則執行步驟 9。

1. 選取 **Device**（裝置） > **Certificates Management**（憑證管理） > **Certificate Profile**（憑證設定檔）。
2. 設定憑證設定檔。
3. 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。
4. 從各自的下拉式清單中選取 **Certificate Type**（憑證類型）、**Certificate**（憑證）及 **Certificate Profile**（憑證設定檔）並進行設定，以使用步驟 2 建立的自訂憑證。
5. 在自訂通訊下，選取 **WildFire Communication**（**WildFire** 通訊）。
6. 按一下 **OK**（確定）。

STEP 9 | 停用預先定義的憑證。

```
set deviceconfig setting management secure-conn-server disable-pre-defined-cert yes
```

STEP 10 | 指定用於在自訂憑證中進行驗證的 DNS 名稱（通常為主體名稱或主體別名）。例如，預設網域名稱是 **wfpc.service.mycluster.paloaltonetworks.com**

```
set deviceconfig setting wildfire custom-dns-name <custom_dns_name>.
```

STEP 11 | （僅限包含 3 個或更多節點的設備叢集）針對已在叢集中註冊的第三個 WildFire 設備伺服器節點重複步驟 2-10。

監控 WildFire 叢集

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

您可使用 CLI 或 Panorama 查看 WildFire 叢集的操作狀態。這讓您可以確認在給定節點上執行的應用程式和服務是否正常運作。若要 WildFire 叢集正常執行，適當的服務和應用程式在每個節點上必須為主動，且所有狀態都必須處於健康狀態。在這些參數之外執行的叢集可能未處於最佳狀態，或者會顯示其他問題及設定問題。

CLI 可以顯示 *Panorama* 未提供的資訊。對與叢集相關的問題進行疑難排解時，強烈建議使用 *WildFire CLI*。

透過執行一系列 WildFire CLI 顯示命令，您可以檢視 WildFire 控制器節點的目前狀態。這些命令會顯示設定詳情、目前在設備上執行的應用程式和服務，以及狀態/錯誤訊息。然後您可以使用這些詳細資訊判斷叢集的狀態。檢視狀態不會中斷任何 WildFire 服務，並可隨時執行。

請參閱下列章節，瞭解如何監控 WildFire 設備的詳細資訊：

- 使用 CLI 檢視 WildFire 叢集狀態
- 使用 Panorama 檢視 WildFire 叢集狀態
- WildFire 應用程式狀態
- WildFire 服務狀態

使用 CLI 檢視 WildFire 叢集狀態

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

若要確認 WildFire 叢集在正常操作參數之內執行，您必須執行下列命令：

- **show cluster controller**— 顯示主動/被動 WildFire 叢集節點的狀態。
- **show cluster all-peers**— 顯示有關特定 WildFire 叢集中所有成員的資訊。
- **show cluster membership**— 顯示叢集和獨立節點的 WildFire 設備資訊。
- **show cluster data-migration-status**—顯示資料移轉程序的目前狀態。
- **show log system**—顯示 WildFire 事件日誌，包括系統狀態詳細資訊。

STEP 1 | 在 WildFire 設備控制器節點上，執行：

```
admin@WF-500(active-controller)>show clustercontroller
```

健康的 WildFire 叢集會顯示下列詳細資訊：

- 設備註冊的叢集名稱及其設定角色。
- 當內部叢集介面正常運作時，`K/V API online status` 顯示為 `True`。狀態 `False` 可以表示節點設定不正確或網路問題。
- `Task processing` 在主動（主要）控制器上顯示為 `True`，在被動（備份）控制器上顯示為 `False`。
- 叢集中所有 WildFire 節點的 IP 地址均列示在 `App Service Avail` 下方。
- 最多三個 `Good Core Servers`。`Good Core Servers` 的數量取決於叢集中執行的節點數量。如果叢集內有第三個節點在執行，它會自動設定為伺服器節點，以最大化叢集完整性。
- 無 `Suspended Nodes`。
- `Current Task` 可提供有關叢集級別操作（例如重新啟動、解除及暫停工作）的背景資訊。

下列範例顯示了在雙節點 WildFire 叢集中設定的主動控制器，處於健康狀態時的輸出：

```
Cluster name:WildFire_Cluster K/V API online:True Task
 processing: on Active Controller:True DNS Advertisement:App
 Service DNS Name:App Service Avail:2.2.2.14, 2.2.2.15 Core
 Servers:009701000026:2.2.2.15 009701000043:2.2.2.14 Good Core
 Servers:2 Suspended Nodes:Current Task: * Showing latest completed
 task Request: startup from qa14 (009701000043/80025) at 2017-09-18
 21:43:34 UTC null Response: permit by qa15 at 2017-09-18 21:45:15
 UTC 1/2 core servers available.Finished: success at 2017-09-18
 21:43:47 UTC
```

STEP 2 | 在 WildFire 設備控制器節點上，執行：

```
admin@WF-500>show cluster all-peers
```

健康的 WildFire 叢集會顯示下列詳細資訊：

- 有關叢集中 WildFire 節點的一般資訊列示在 `Address`、`Mode`、`Server`、`Node` 及 `Name` 下。
- 所有 WildFire 叢集節點都在執行 `wfpc` 服務，它是一個內部檔案樣本分析服務。
- 作為主動、被動或伺服器執行的節點會在 `Status` 旁邊顯示 `Serverrole applied`。如果節點已設定為伺服器，但沒有作為伺服器執行，`status` 會顯示 `Serverrole assigned`。

  在 *3* 節點部署中，第三個伺服器節點將被分類為工作節點。

- 最近移除的節點可能會出現，但顯示為 `Disconnected`。從叢集節點清單中移除已中斷連線的節點可能需要幾天時間。
- 主動控制器節點顯示 `siggen-db:ReadyMaster`。
- 被動控制器節點顯示 `siggen-db:ReadySlave`。

  如需有關一般 *WildFire* 應用及服務狀態的詳細資訊，請參閱 WildFire 應用狀態及 WildFire 服務狀態。

- `Diag report` 顯示叢集系統事件和錯誤訊息：

錯誤訊息	說明
`Unreachable`	該節點無法從叢集控制器存取。
`Unexpected member`	該節點不屬於叢集設定。該節點最近可能已被從叢集設定中刪除或設定錯誤。
`Left cluster`	該節點無法再從叢集控制器存取。
`Incorrect cluster name`	該節點設定的叢集名稱不正確。
`Connectivity unstable`	該節點與叢集控制器的連線不穩定。
`Connectivity lost`	該節點與叢集控制器的連線已中斷。

錯誤訊息	說明
`Unexpected server serial number`	偵測到意外出現的伺服器節點。

下列範例顯示了在健康狀態下執行的 3 節點 WildFire 叢集：

```
Address Mode Server Node Name ------- ---- ------ ---------
 2.2.2.15 controller Self True qa15 Service: infra signature
 wfcore wfpc Status:Connected, Server role applied Changed:Mon, 18
 Sep 2017 15:37:40 -0700 WF App: global-db-service:JoinedCluster
 wildfire-apps-service:Stopped global-queue-service:JoinedCluster
 wildfire-management-service:Done siggen-db:ReadySlave 2.2.2.14
 controller Peer True qa14 Service: infra signature wfcore wfpc
 Status:Connected, Server role applied Changed:Mon, 18 Sep 2017
 15:37:40 -0700 WF App: global-db-service: commit-lock wildfire-
apps-service:Stopped global-queue-service:ReadyStandalone wildfire-
management-service:Done siggen-db:ReadyMaster 2.2.2.16 worker True
 wf6240 Service: infra wfcore wfpc Status:Connected, Server role
 applied Changed:Wed, 22 Feb 2017 11:11:15 -0800 WF App: wildfire-
apps-service:Ready global-db-service:JoinedCluster global-queue-
service:JoinedCluster local-db-service:DataMigrationFailed Diag
 report:2.2.2.14: reported leader '2.2.2.15', age 0. 2.2.2.15:
 local node passed sanity check.
```

STEP 3 | 在 WildFire 設備控制器節點上，執行：

```
admin@WF-500>show cluster membership
```

健康的 WildFire 叢集會顯示下列詳細資訊：

- 一般 WildFire 設備設定詳細資訊，例如叢集名稱、設備的 IP 地址、序號等。
- `Server role` 表示 WildFire 設備是否作為叢集伺服器執行。叢集伺服器操作其他基礎結構應用和服務。每個叢集最多可包含三個伺服器。
- `Node mode` 描述 WildFire 設備的角色。根據您的設定和部署中的節點數量，已在叢集中註冊的 WildFire 設備可以是 `controller` 或 `worker` 節點。不屬於叢集的設備將顯示 `stand_alone`。
- 根據叢集節點角色操作下列 `Services`：

節點類型	在節點上執行的服務
控制器節點（主動或被動）	• `infra` • `wfpc` • 特徵碼 • `wfcore`
伺服器節點	• `infra`

節點類型	在節點上執行的服務
	• wfpc • wfcore
工作節點	• infra • wfpc

- `HA priority` 根據其設定的角色顯示主要或次要，但此設定與目前設備的 HA 狀態無關。
- `Work queue status` 顯示待分析樣本和目前正在分析的樣本。還顯示特定 WildFire 設備接收的負載數量。

如需有關 *WildFire* 應用及服務狀態的詳細資訊，請參閱 WildFire 應用狀態及 WildFire 服務狀態。

下列範例顯示了在健康狀態下執行的 WildFire 控制器：

```
Service Summary: wfpc signature Cluster name: qa-auto-0ut1
 Address:2.2.2.15 Host name: qa15 Node name: wfpc-009701000026-
internal Serial number:009701000026 Node mode: controller Server
 role:True HA priority: secondary Last changed:Fri, 22 Sep 2017
 11:30:47 -0700 Services: wfcore signature wfpc infra Monitor
 status:Serf Health Status: passing Agent alive and reachable
 Service 'infra' check: passing Application status: global-db-
service:ReadyLeader wildfire-apps-service:Ready global-queue-
service:ReadyLeader wildfire-management-service:Done siggen-
db:Ready Work queue status: sample anaysis queued:0 sample
 anaysis running:0 sample copy queued:0 sample copy running:0 Diag
 report:2.2.2.14: reported leader '2.2.2.15', age 0. 2.2.2.15:
 local node passed sanity check.
```

STEP 4 | 在 WildFire 設備控制器節點上，執行：

admin@WF-500(active-controller)>show clusterdata-migration-status

WildFire 設備顯示下列資料移轉詳細資訊：

- 資料移轉進行中時，切勿轉送檔案至 WildFire 設備叢集。資料移轉完成時，會顯示完成時間戳記。
- 變更 WildFire 叢集拓撲（例如，新增或移除節點，及變更節點角色）會觸發資料移轉事件。
- 資料移轉會發生在升級至新版 WildFire 之後。升級之後，務必檢查 WildFire 叢集的操作狀態，以確認功能是否正常。

下列範例顯示 WildFire 設備叢集中的資料移轉進度：

```
admin@WF-500(active-controller)>: show data-migration-status 100%
 completed on Mon Sep 9 21:44:48 PDT 2019
```

STEP 5 | 在 WildFire 設備主動、被動及伺服器節點上，執行：

admin@WF-500(active-controller)>show log systemsubtype direction equal backward

此命令會從最近至最舊的順序，顯示分類為 wildfire-appliance 子類型的所有記錄事件。

- 您必須簽發此命令至叢集中的所有節點。例如，如果您正在操作 3 節點叢集，則必須確認主動控制器、被動控制器及伺服器節點上的狀態。
- WildFire 設備 CLI 所傳回的日誌訊息可包括各種子類型。您可以依據常見的子類型關鍵字篩選日誌。依據特定元件，使用下列的命令引數進行篩選：
  - global-queue—**matchqueue**，例如 **show log system directionequal backward | match queue**
  - global-database—**match global**，例如 **show log system direction equal backward | matchglobal**
  - signature-generation—**match signature**，例如 **show log system direction equal backward| match signature**
- WildFire 設備叢集在正常操作時會傳回 2 節點叢集中每個節點的狀態讀取結果。正常運作的 WildFire 叢集節點會依據設備角色而具有不同的狀態讀取結果。

  使用下列檢查清單確認 WildFire 設備服務在您的叢集部署中正確執行。

  - 主動控制器

元件	主動控制器狀態
global-queue	❑ infowildfire cluster 0 Global queue (rabbitmq) cluster formation succeeded withstatus ReadyLeader ❑ info general general 0 Setup policy for global-queue service
global-database	❑ infogeneral general 0 I'm cluster leader, bootstrap for global-db service ❑ info general general 0 Setup policy for global-queue service
signature-generation	❑ infowildfir cluster 0 Signature generation service status set to ReadyMaster ❑ info wildfir cluster 0 Signature generationservice status set to ReadyMaster

元件	主動控制器狀態
	從最近至最舊的順序顯示 *WildFire* 設備所傳回的日誌訊息。如上述程序所示，如果您未使用 ***direction equal backward*** 命令引數，*WildFire* 設備 *CLI* 會以從最舊至最近的順序傳回日誌訊息。

- 被動控制器

元件	被動控制器狀態範例
global-queue	infogeneral general 0 Setup policy for global-queue service info wildfire cluster 0 Global queue (rabbitmq)cluster formation succeeded with status JoinedCluster info general general 0 Join cluster for global-queueservice - succeeded info general general 0 Setup policy for global-queue service
global-database	infogeneral general 0 Setup policy for global-queue service info general general 0 Restore applications:done, For global-db bootstrap and join cluster info general general 0 Start vm_mgr, For global-dbbootstrap and join cluster info general general 0 Start uwsgi, For global-dbbootstrap and join cluster info general general 0 Start wf_services, Forglobal-db bootstrap and join cluster info general general 0 Suspend applications:done, For global-db bootstrap and join cluster info general general 0 Stop vm_mgr, For global-dbbootstrap and join cluster info general general 0 Stop uwsgi, For global-dbbootstrap and join cluster info general general 0 Stop wf_services, Forglobal-db bootstrap and join cluster

元件	被動控制器狀態範例
	❑ info general general 0 Bootstrap and join clusterfor global-db service
signature-generation	❑ infowildfir cluster 0 Signature generation service status set to ReadySlave ❑ info wildfir cluster 0 Signature generationservice status set to ReadySlave

從最近至最舊的順序顯示 *WildFire* 設備所傳回的日誌訊息。如上述程序所示，如果您未使用 ***direction equal backward*** 命令引數，*WildFire* 設備 *CLI* 會傳回從最舊至最近順序的日誌訊息。

- WildFire 設備叢集在正常操作時會傳回 3 節點叢集中每個節點的狀態讀取結果。正常運作的 WildFire 叢集節點會依據設備角色而具有不同的狀態讀取結果。

  使用下列檢查清單確認 WildFire 設備服務在您的叢集部署中正確執行。

  - 主動控制器

元件	主動控制器狀態
global-queue	❑ infowildfire cluster 0 Global queue (rabbitmq) cluster formation succeeded withstatus JoinedCluster ❑ info general general 0 Join cluster for global-queueservice - succeeded ❑ info general general 0 Setup policy for global-queue service
global-database	❑ infogeneral general 0 Restore applications: done, For global-db bootstrap andjoin cluster ❑ info general general 0 Start vm_mgr, For global-dbbootstrap and join cluster ❑ info general general 0 Start uwsgi, For global-dbbootstrap and join cluster ❑ info general general 0 Start wf_services, Forglobal-db bootstrap and join cluster ❑ info general general 0 Suspend applications:done, For global-db bootstrap and join cluster ❑ info general general 0 Stop vm_mgr, For global-dbbootstrap and join cluster

元件	主動控制器狀態
	❑ info general general 0 Stop uwsgi, For global-dbbootstrap and join cluster ❑ info general general 0 Stop wf_services, Forglobal-db bootstrap and join cluster ❑ 2019/07/19 14:40:19 info general general 0Bootstrap and join cluster for global-db service
signature-generation	❑ infowildfire cluster 0 Signature generation service status set to ReadyMaster

從最近至最舊的順序顯示 *WildFire* 設備所傳回的日誌訊息。如上述程序所示，如果您未使用 ***direction equal backward*** 命令引數，*WildFire* 設備 *CLI* 會以從最舊至最近的順序傳回日誌訊息。

- 被動控制器

元件	被動控制器狀態
global-queue	❑ infogeneral general 0 Setup policy for global-queue service ❑ info general general 0 Setup policy for global-queue service ❑ info wildfire cluster 0 Global queue (rabbitmq)cluster formation succeeded with status ReadyLeader ❑ info general general 0 Setup policy for global-queue service
global-database	❑ infogeneral general 0 I'm cluster leader, bootstrap for global-db service ❑ info general general 0 Setup policy for global-queue service
signature-generation	❑ infowildfire cluster 0 Signature generation service status set to ReadySlave ❑ info wildfire cluster 0 Signature generationservice status set to ReadySlave

元件	被動控制器狀態
	從最近至最舊的順序顯示 *WildFire* 設備所傳回的日誌訊息。如上述程序所示，如果您未使用 ***direction equal backward*** 命令引數，*WildFire* 設備 *CLI* 會以從最舊至最近的順序傳回日誌訊息。

- 伺服器節點

元件	伺服器節點狀態
global-queue	❑ infowildfire cluster 0 Global queue (rabbitmq) cluster formation succeeded withstatus JoinedCluster ❑ info general general 0 Join cluster for global-queueservice - succeeded ❑ info general general 0 Setup policy for global-queue service ❑ info wildfire cluster 0 Global queue (rabbitmq)cluster formation succeeded with status StandbyAsWorker
global-database	❑ infogeneral general 0 Restore applications: done, For global-db bootstrap andjoin cluster ❑ info general general 0 Start vm_mgr, For global-dbbootstrap and join cluster ❑ info general general 0 Start uwsgi, For global-dbbootstrap and join cluster ❑ info general general 0 Start wf_services, Forglobal-db bootstrap and join cluster ❑ info general general 0 Suspend applications:done, For global-db bootstrap and join cluster ❑ info general general 0 Stop vm_mgr, For global-dbbootstrap and join cluster ❑ info general general 0 Stop uwsgi, For global-dbbootstrap and join cluster ❑ info general general 0 Stop wf_services, Forglobal-db bootstrap and join cluster ❑ 2019/07/19 14:32:50 info general general 0Promote worker node and join cluster for global-db service

元件	伺服器節點狀態
signature-generation	❑ infowildfire cluster 0 Signature generation service status set to Stopped ❑ critical wildfire cluster 0 Signature DataMigrationDone

從最近至最舊的順序顯示 *WildFire* 設備所傳回的日誌訊息。如上述程序所示，如果您未使用 ***direction equal backward*** 命令引數，*WildFire* 設備 *CLI* 會傳回從最舊至最近順序的日誌訊息。

WildFire 應用程式狀態

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

WildFire 設備操作一系列內部應用程式來管理和協調樣本資料的處理。檢視 WildFire 設備叢集的狀態時，這些應用程式及其必要的狀態將顯示。

下列清單顯示了叢集組件、用途及狀態情況：

名稱	說明	可能的狀態情況	定義
global-db-service	此應用程式資料庫用於儲存 WildFire 分析資料。	AcquiringSessionSpinLock	等待工作階段旋轉鎖，直到擷取該旋轉鎖或逾時。
		啟動載入	樣本資料庫應用程式目前處於啟動載入狀態。
		BootstrappingNoMeet	本機樣本資料庫服務在沒有與其他 WildFire 設備形成叢集的情況下啟動。
		FailedToBecomeWorker	作為工作節點加入叢集失敗。
		FailedToBootstrap	啟動載入程序失敗。
		FailedToJoinCluster	加入叢集失敗。
		FailedToStartServices	內部資料庫服務啟動失敗。

名稱	說明	可能的狀態情況	定義
		MaintenanceDecommission	啟動資料庫服務的解除程序。
		MaintenanceDecommissionDone	資料庫服務已被解除。
		MaintenanceFailover	開始降階本機服務和容錯移轉備份複本。
		MaintenanceFailed	服務容錯移轉失敗。
		MaintenanceFailoverDone	服務容錯移轉完成。
		MaintenanceRecoverFromSplitbrain	WildFire 設備目前處於「腦分裂」模式，資料庫服務狀態將在服務啟動時設定為 MaintenanceRecoverFromSplitbrain。
		MaintenanceSuspend	資料庫服務正在暫停中，因為使用者發出了下列命令之一：debug cluster suspend 或 request cluster decommission。
		MaintenanceSuspendDone	資料庫服務已完成暫停程序。
		DataMigration	本機資料庫的內容正在與主要資料庫合併。當 WildFire 設備加入叢集時會發生此情況。
		DataMigrationDone	資料移轉程序完成。
		DataMigrationFailed	資料移轉程序失敗。
		JoinedCluster	本機資料庫服務已加入叢集。
		準備就緒	資料庫服務處於準備就緒狀態。

名稱	說明	可能的狀態情況	定義
		ReadyLeader	資料庫服務處於準備就緒狀態，且設備已設定為領導者。
		ReadyStandalone	資料庫服務處於準備就緒狀態，且設備正在作為獨立設備執行。
		腦分裂	偵測到「腦分裂」狀況且資料庫服務已進入「腦分裂」模式。服務將很快轉換至 ReadyStandalone。
		StandbyAsWorker	工作節點資料庫服務處於待命狀態。
		WaitingforLeaderReady	本機節點正在等待加入領導者節點。

名稱	說明	可能的狀態情況	定義
global-queue-service	處理已傳送進行 WildFire 分析的樣本的管理和優先順序。	啟動載入	佇列服務應用程式目前處於啟動載入狀態。
		FailedToBecomeWorker	作為工作節點加入叢集失敗。
		FailedToBootstrap	啟動載入程序失敗。
		FailedToJoinCluster	加入叢集失敗。
		FailedToStartServices	內部佇列服務啟動失敗。
		MaintenanceDecommission	啟動佇列服務的解除程序。
		MaintenanceDecommissionDone	佇列服務已被解除。
		MaintenanceFailover	開始降階本機服務和容錯移轉備份複本。
		MaintenanceFailed	服務容錯移轉失敗。

名稱	說明	可能的狀態情況	定義
		MaintenanceFailoverDone	服務容錯移轉完成。
		MaintenanceRecoverFromSplitbrain	WildFire 設備目前處於「腦分裂」模式，佇列服務狀態將在服務啟動時設定為
		MaintenanceSuspend	佇列服務正在暫停中，因為使用者發出了下列命令之一：debug cluster suspend 或 request cluster decommission。
		MaintenanceSuspendDone	佇列服務已完成暫停程序。
		JoinedCluster	佇列服務已加入叢集。
		準備就緒	佇列服務處於準備就緒狀態。
		ReadyLeader	佇列服務處於準備就緒狀態，且設備已設定為領導者。
		ReadyStandalone	佇列服務處於準備就緒狀態，且設備正在作為獨立設備執行。
		腦分裂	偵測到「腦分裂」狀況且佇列服務已進入「腦分裂」模式。服務將很快轉換至 ReadyStandalone。
		StandbyAsWorker	工作節點佇列服務處於待命狀態。

名稱	說明	可能的狀態情況	定義
siggen-db	產生 WildFire 私人特徵碼和分析樣本。	DatabaseFailover	進行 HA 容錯移轉時，被動控制器會變成主動控制器。被動控制器中的特徵碼服務會變成主要，且狀態會設定為 DatabaseFailover。

名稱	說明	可能的狀態情況	定義
		DatabaseFailoverFaild	特徵碼資料庫容錯移轉失敗。
		DataMigration	本機特徵碼資料庫的內容正在與主要資料庫合併。當 WildFire 設備加入叢集時會發生此情況。
		DataMigrationDone	資料移轉程序完成。
		DataMigrationFailed	資料移轉程序失敗。
		已取消註冊	特徵碼資料庫服務已取消註冊。
		MaintenanceDecommission	啟動特徵碼資料庫服務的解除程序。
		MaintenanceDecommissionDone	佇列服務已被解除。
		MaintenanceFailover	開始降階本機服務和容錯移轉備份複本。
		MaintenanceFailoverDone	服務容錯移轉完成。
		MaintenanceSuspend	特徵碼資料庫服務正在暫停中，因為使用者發出了下列命令之一：debug cluster suspend 或 request cluster decommission。
		MaintenanceSuspendDone	特徵碼資料庫服務已完成暫停程序。
		MigrateMalwareDatabase	將 PAN-OS 從版本 7.1 升級至 8.0 時，樣本資料將轉換為不同格式。這些狀態表示資料移轉程序的進度。
		MigrateSiggenDatabaseStage1	
		MigrateSiggenDatabaseStage2	
		MigrateSiggenDatabaseStage3	

名稱	說明	可能的狀態情況	定義
		準備就緒	特徵碼資料庫服務處於準備就緒狀態。
		ReadyMaster	特徵碼資料庫服務處於主要模式，且正在主動控制器上執行。
		ReadySlave	特徵碼資料庫服務處於備份模式，且正在被動控制器上執行。
		ReadyStandalone	特徵碼資料庫服務處於準備就緒狀態，且設備正在作為獨立設備執行。
		腦分裂	偵測到「腦分裂」狀況且特徵碼資料庫服務已進入「腦分裂」模式。服務將很快轉換至 ReadyStandalone。
		已停止	特徵碼資料庫服務已在設備上停止。

名稱	說明	可能的狀態情況	定義
wildfire-management-service	WildFire 工作模式管理服務。	執行	WildFire 管理服務處於執行狀態。
		完成	WildFire 管理服務執行已完成。

名稱	說明	可能的狀態情況	定義
wildfire-apps-service	WildFire 基礎結構應用程式。	已取消註冊	WildFire 應用程式服務已取消註冊。
		準備就緒	WildFire 應用程式服務處於準備就緒狀態。
		已還原	WildFire 應用程式服務已完成維護程序。

名稱	說明	可能的狀態情況	定義
		排程	WildFire 應用程式服務處於排程狀態。
		SetupSampleStorage	當 WildFire 正在從 7.1 升級至 8.0 時，此 WildFire 應用程式服務將執行。
		已停止	WildFire 應用程式服務已設備上停止。
		已暫停	由於維護，WildFire 應用程式服務已暫停。

WildFire 服務狀態

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

WildFire 設備操作一系列內部服務來管理和協調樣本資料的處理。檢視 WildFire 設備叢集的狀態時，這些服務及其必要的狀態將顯示。

下列清單顯示了 WildFire 服務組件、用途、狀態情況及其他相關詳細資訊：

名稱	用途	受影片的節點	**STATUS (狀態)**
`infra`	表示 WildFire 叢集基礎結構服務正在特定節點上執行。	所有節點	當服務正在執行時顯示在 CLI 狀態螢幕中。如果這些服務沒有在特定節點上出現，請驗證設備的設定。
`wfpc`	表示檔案樣本分析服務（WildFire 私人雲端）能夠進行檔案分析和報告產生。		
特徵碼	產生 WildFire 私人特徵碼和分析樣本。	主動（主要）/被動（備份）控制器	
`wfcore`	表示節點正在作為 WildFire 叢集基礎結構服務的伺服器執行。	伺服器節點	

在叢集中升級 WildFire 設備

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

您可以使用 CLI 個別升級已在叢集中註冊的 WildFire 設備，或使用 Panorama 作為群組升級叢集。

視乎 WildFire 設備已分析和已儲存的樣本數量，升級設備軟體所需的時間有所不同；這是因為升級需要移轉所有惡意軟體樣本和 14 天內的良性軟體樣本。允許使用 30 至 60 分鐘升級您在生產環境中使用過的每個 WildFire 設備。

- 叢集中的所有節點必須執行相同版本的作業系統。
- *Panorama* 可以管理執行 *PAN-OS* 軟體版本 *8.0.1* 或更新版本的 *WildFire* 設備及設備叢集。
- 確保裝置連線至可靠的電源。升級過程中的電力損耗會使裝置無法使用。

根據您的部署，執行下列工作之一以升級您的 WildFire 叢集：

- 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
- 在有網際網路連線的情況下本機升級叢集
- 在沒有網際網路連線的情況下本機升級叢集

在有網際網路連線的情況下本機升級叢集

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

若要在本機升級叢集，您必須個別升級已在叢集中註冊的每個 WildFire 設備。當設備完成升級時，其將自動重新註冊至原本指定給的叢集。

STEP 1 | 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：

```
admin@WF-500(passive-controller)> show wildfire latest samples
```

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 2 | 安裝最新 WildFire 設備內容更新。此更新為設備提供最新的威脅資訊以準確偵測惡意軟體。

在較舊的設備上，此程序可能需要長達 *6* 小時或更長時間。

1. 驗證您是否可在 WildFire 設備上執行最新的內容更新。

```
admin@WF-500> request wf-content upgrade check
```

2. 下載最新的 WildFire 內容更新套件。

```
admin@WF-500> request wf-content upgrade download latest
```

如果您未直接連線至 Palo Alto Networks 更新伺服器，可以下載並安裝來自啟用 SCP 的伺服器的 WildFire 內容更新。

3. 檢視下載狀態。

```
admin@WF-500> show jobs all
```

4. 下載完成後，安裝更新。

```
admin@WF-500> request wf-content upgrade install version latest
```

STEP 3 | （升級到 PAN-OS 10.2.2 時需要）升級 WildFire 設備上的 VM 映像。

1. 登入並存取 Palo Alto Networks 客戶支援入口網站軟體下載頁面。您也可以透過前往 **Updates**（更新） > **Software Updates**（軟體更新），手動從支援首頁導覽至軟體下載頁面。
2. 從軟體更新頁面中，選取 **WF-500 Guest VM Images**（**WF-500** 來賓 **VM** 映像）並下載下列 VM 映像檔案：

   Palo Alto Networks 會定期更新 *VM* 映像檔案；因此，特定檔案名稱會根據可用版本而變更。請務必下載最新版本，檔案名稱中的 *m-x.x.x* 表示版本號碼；此外，還有一個發佈日期，可以交叉參考以協助確定最新版本。

   - WFWinXpAddon3_m-1.0.1.xpaddon3
   - WFWinXpGf_m-1.0.1.xpgf
   - WFWin7_64Addon1_m-1.0.1.7_64addon1
   - WFWin10Base_m-1.0.1.10base
3. 將 VM 映像上傳到 WildFire 設備。
   1. 從 SCP 伺服器匯入 VM 映像：

      ```
      admin@WF-500>scp import wildfire-vm-image from
       <username@ip_address>/<folder_name>/<vm_image_filename>
      ```

      例如：

      ```
      admin@WF-500>scp import wildfire-vm-image from
       user1@10.0.3.4:/tmp/WFWin7_64Addon1_m-1.0.1.7_64addon1
      ```
   2. 若要檢查下載狀態，請使用下列命令：

      ```
      admin@WF-500>show jobs all
      ```
   3. 對剩餘的 VM 映像重複此動作。
4. 安裝 VM 映像。
   1. ```
      admin@WF-500>request system wildfire-vm-image upgrade
       install file <vm_image_filename>
      ```
   2. 對剩餘的 VM 映像重複此動作。
5. 確認 VM 映像已在 WildFire 設備上正確地安裝並啟用。
   1. （選用）檢視可用 VM 映像的清單：

      ```
      admin@WF-500> show wildfire vm-images
      ```
      ```

輸出顯示可用的 VM 映像。

2. 提交設定：

```
admin@WF-500# commit
```

3. 透過執行以下命令以檢視主動 VM 映像：

```
admin@WF-500> show wildfire status
```

STEP 4 | 確認您要安裝的 WildFire 設備軟體版本可用。

```
admin@WF-500(passive-controller)> request system software check
```

STEP 5 | 下載 PAN-OS 10.2.2 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。本程序中的範例說明了如何升級至 PAN-OS 10.2.2。升級時用合適的目標版本取代 10.2.2。

下載 10.2.2 軟體版本。

```
admin@WF-500(passive-controller)> request system software download
 version 10.2.2
```

若要檢查下載狀態，請使用下列命令

```
admin@WF-500(passive-controller)> show jobs all
```

STEP 6 | 確認所有服務都在執行。

```
admin@WF-500(passive-controller)> show system software status
```

STEP 7 | 安裝 10.2.2 軟體版本。

```
admin@WF-500(passive-controller)> request system software install
 version 10.2
```

STEP 8 | 完成軟體升級。

1. 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
```

2. 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。

STEP 9 | 對於叢集中的每個 WildFire 工作節點，重複第 1-8 步。

STEP 10 | （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 11 | 確認 WildFire 設備已可以繼續進行樣本分析。

1. 驗證 sw-version 欄位是否顯示升級後的發行版本：

```
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
```

4. 確認資料移轉已成功完成。執行 `show cluster data-migration-status` 以檢視資料庫合併進度。資料合併完成後，完成時間戳記顯示：

```
100% completed on Mon Sep 9 21:44:48 PDT 2019
```

資料合併的持續時間取決於 *WildFire* 設備上儲存的資料數量。必須分配至少若干小時來復原，因為資料合併的過程可能比較漫長。

在沒有網際網路連線的情況下本機升級叢集

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

若要在本機升級叢集，您必須個別升級已在叢集中註冊的每個 WildFire 設備。當設備完成升級時，其將自動重新註冊至原本指定給的叢集。

STEP 1 | 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：

```
admin@WF-500(passive-controller)> show wildfire latest samples
```

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 2 | 從更新伺服器擷取內容更新檔案。

1. 登入 Palo Alto Networks 支援入口網站，並按一下 **Dynamic Updates (**動態更新**)**。
2. 在 [WildFire 設備] 區段中，找到並下載最新的 WildFire 設備內容更新。
3. 將內容更新檔案複製到已啟用 SCP 的伺服器，並記下檔案名稱和目錄路徑。

STEP 3 | 在 WildFire 設備上安裝內容更新。

1. 登入 WildFire 設備並從 SCP 伺服器下載內容更新檔案：

```
admin@WF-500> scp import wf-content from username@host:path
```

例如：

```
admin@WF-500> scp import wf-content from bart@10.10.10.5:c:/
updates/panup-all-wfmeta-2-253.tgz
```

若您的 *SCP* 伺服器以非標準連接埠執行，或若您需要指定來源 *IP*。您也可以在 ***scp import*** 命令中定義這些選項。

2. 安裝更新：

```
admin@WF-500> request wf-content upgrade install file panup-
all-wfmeta-2-253.tgz
```

3. 檢視安裝狀態：

```
admin@WF-500> show jobs all
```

STEP 4 | 驗證內容更新。

驗證內容版本：

```
admin@WF-500> show system info | match wf-content-version
```

下列輸出現在顯示版本 2-253：

```
wf-content-version:2-253
```

STEP 5 | （升級到 PAN-OS 10.2.2 時需要）升級 WildFire 設備上的 VM 映像。

1. 登入並存取 Palo Alto Networks 客戶支援入口網站軟體下載頁面。您也可以透過前往 **Updates**（更新） > **Software Updates**（軟體更新），手動從支援首頁導覽至軟體下載頁面。
2. 從軟體更新頁面中，選取 **WF-500 Guest VM Images**（**WF-500** 來賓 **VM** 映像）並下載下列 VM 映像檔案：

   Palo Alto Networks 會定期更新 *VM* 映像檔案；因此，特定檔案名稱會根據可用版本而變更。請務必下載最新版本，檔案名稱中的 *m-x.x.x* 表示版本號碼；此外，還有一個發佈日期，可以交叉參考以協助確定最新版本。

   - WFWinXpAddon3_m-1.0.1.xpaddon3
   - WFWinXpGf_m-1.0.1.xpgf
   - WFWin7_64Addon1_m-1.0.1.7_64addon1
   - WFWin10Base_m-1.0.1.10base
3. 將 VM 映像上傳到 WildFire 設備。
   1. 從 SCP 伺服器匯入 VM 映像：

      ```
      admin@WF-500>scp import wildfire-vm-image from
       <username@ip_address>/<folder_name>/<vm_image_filename>
      ```

      例如：

      ```
      admin@WF-500>scp import wildfire-vm-image from
       user1@10.0.3.4:/tmp/WFWin7_64Addon1_m-1.0.1.7_64addon1
      ```
   2. 若要檢查下載狀態，請使用下列命令：

      ```
      admin@WF-500>show jobs all
      ```
   3. 對剩餘的 VM 映像重複此動作。
4. 安裝 VM 映像。
   1. ```
      admin@WF-500>request system wildfire-vm-image upgrade
       install file <vm_image_filename>
      ```
   2. 對剩餘的 VM 映像重複此動作。
5. 確認 VM 映像已在 WildFire 設備上正確地安裝並啟用。
   1. （選用）檢視可用 VM 映像的清單：

      ```
      admin@WF-500> show wildfire vm-images
      ```
      ```

輸出顯示可用的 VM 映像。

2. 提交設定：

```
admin@WF-500# commit
```

3. 透過執行以下命令以檢視主動 VM 映像：

```
admin@WF-500> show wildfire status
```

STEP 6 | 確認您要安裝的 WildFire 設備軟體版本可用。

```
admin@WF-500(passive-controller)> request system software check
```

STEP 7 | 下載 PAN-OS 10.2.2 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。本程序中的範例說明了如何升級至 PAN-OS 10.2.2。升級時用合適的目標版本取代 10.2.2。

下載 10.2.2 軟體版本：

1. 導覽至 Palo Alto Networks 支援網站，然後在 [工具] 部分中按一下 **Software Updates**（軟體更新）。
2. 將要安裝的 WildFire 設備軟體影像檔案下載到執行 SCP 伺服器軟體的電腦。
3. 從 SCP 伺服器匯入軟體影像：

```
admin@WF-500> scp import software from <username@ip_address>/
<folder_name>/<imagefile_name>
```

例如：

```
admin@WF-500> scp import software from user1@10.0.3.4:/tmp/
WildFire_m-10.2.2
```

4. 若要檢查下載狀態，請使用下列命令：

```
admin@WF-500> show jobs all
```

STEP 8 | 確認所有服務都在執行。

```
admin@WF-500(passive-controller)> show system software status
```

STEP 9 | 安裝 10.2.2 軟體版本。

```
admin@WF-500(passive-controller)> request system software install
 version 10.2.2
```

STEP 10 | 完成軟體升級。

1. 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
```

2. 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。

STEP 11 | 對於叢集中的每個 WildFire 工作節點，重複第 1-10 步。

STEP 12 | （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 13 | 確認 WildFire 設備已可以繼續進行樣本分析。

1. 驗證 sw-version 欄位是否顯示升級後的發行版本：

   ```
   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
   ```

4. 確認資料移轉已成功完成。執行 `show cluster data-migration-status` 以檢視資料庫合併進度。資料合併完成後，完成時間戳記顯示：

   ```
   100% completed on Mon Sep 9 21:44:48 PDT 2019
   ```

   資料合併的持續時間取決於 *WildFire* 設備上儲存的資料數量。必須分配至少若干小時來復原，因為資料合併的過程可能比較漫長。

對 WildFire 叢集進行疑難排解

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

請參閱下列主題以診斷 WildFire 叢集問題並進行疑難排解：

- 對 WildFire 「腦分裂」狀況進行疑難排解

對 WildFire 「腦分裂」狀況進行疑難排解

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

當一個節點（或兩個 HA 對等體）認為另一個節點不再操作時，WildFire 雙節點 HA（高可用性）叢集將出現「腦分裂」狀況。當網路連線或設定問題導致兩個 HA 和叢集連線失敗時，會發生這種情況，但允許設備繼續處理樣本。此問題發生時，兩個 WildFire 設備都假定為主動（或主要）控制器，而無需備份，從而失去了 HA 部署的優點，例如備援和負載平衡。此外，這會使 WildFire 設備無法高效利用分析資源。當 WildFire 叢集發生輕微的分裂時，會自動嘗試從「腦分裂」狀況復原。較嚴重的分裂則需要人工干預。

下列狀況會隨著「腦分裂」一同發生：

- 兩個 WildFire 對等節點無法感知彼此的狀態或 HA 角色。
- 兩個 WildFire 對等節點會變成主要伺服器，並將繼續從防火牆接收樣本，但會作為獨立設備運作。
- 當 HA 不可用時，與叢集相關的工作將暫停。

正確設定的 *3* 節點 *WildFire* 設備叢集不會發生「腦分裂」狀況，因為第三個伺服器節點會提供額外的冗餘。

「腦分裂」狀況行發生的原因是什麼？

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

「腦分裂」狀況是對雙節點叢集中一個節點發生故障時的修正回應，這種情況下，WildFire 高可用性節點對無法彼此通訊，但仍可提供有限的功能。雖然高可用性和負載平衡功能不再可用，但您仍可轉送樣本至 WildFire 進行分析。「腦分裂」由下列原因之一導致：

- 硬體問題或斷電。
- 網路連線問題，例如交換器/路由器故障、網路不穩定或網路分割。
- WildFire 設備設定和連線問題。

  Palo Alto Networks 建議使用 *HA1* 和叢集介面連結的直接纜線連線。

- WildFire 節點不健康。

判斷 **WildFire** 叢集是否處於「腦分裂」狀況中

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

當 WildFire 雙節點叢集中的設備進入「腦分裂」狀況時，服務故障會在 WildFire CLI 中產生警告並管理 Panorama（如果有）。

STEP 1 | （僅限 WildFire 設備 CLI）在 WildFire 設備控制器上，執行：

```
admin@WF-500>show cluster membership
```

受影響的 WildFire 叢集節點會在 `Service Summary` 旁邊顯示 `Cluster:splitbrain`。

下列範例顯示了處於「腦分裂」狀況的雙節點 WildFire 叢集的一個節點：

```
Service Summary:Cluster:splitbrain Cluster name:WF_Cluster_1
 Address:2.2.2.114 Host name: wf1 Node name: wfpc-009707000380-
internal Serial number:009707000380 Node mode: controller Server
 role:True HA priority: secondary Last changed:Tue, 24 Oct 2017
 15:13:18 -0700 Services: wfcore signature wfpc infra Monitor
 status:Serf Health Status: passing Agent alive and reachable
 Service 'infra' check: passing Application status: global-db-
service:ReadyLeader wildfire-apps-service:Ready global-queue-
service:ReadyLeader wildfire-management-service:Done siggen-
db:ReadyMaster Work queue status: sample anaysis queued:0 sample
 anaysis running:0 sample copy queued:0 sample copy running:0 Diag
 report:2.2.2.114: reported leader '2.2.2.114', age 0. 2.2.2.114:
 local node passed sanity check.
```

STEP 2 | （僅限 Panorama）在管理 WildFire 叢集的 Panorama 設備上：

1. 選取 **Panorama > Managed WildFire Clusters**（受管理的 **WildFire** 叢集）。
2. 在 **Cluster Status**（叢集狀態）欄中，查看是否存在 **cluster [splitbrain]**（叢集 **[**腦分裂**]**）。這表示設備處於「腦分裂」模式。

APPLIANCE	SOFTWARE VERSION	IP ADDRESS	CONNECTED	CLUSTER NAME	ANALYSIS ENVIRONM...	CONTENT	ROLE	CONFIG STATUS	CLUSTER STATUS	LAST COMMIT STATE	UTILIZATION	FIREWALLS CONNECTED
wfcluster1 (2/3 Nodes Connected)											View	View
qa19	10.0.2-c12		Connected	WF_Cluster1	vm-5	4033-4496	Controller		cluster [splitbrain]			
qa18			Connected		vm-5		Controller Backup					
qa17	10.0.2-c12		Connected		vm-5	4033-4496	Worker					

從「腦分裂」狀況中復原

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

若要解決 「腦分裂」問題，請為您的網路問題偵錯，並還原 WildFire HA 對之間的連線。WildFire 設備叢集會自動嘗試從「腦分裂」狀況中復原，但如果這些措施失敗，您必須手動啟動復原程序。

STEP 1 | 確認您的網路正常運作，且 WildFire 設備正在傳輸和接收流量。

1. 在 WildFire 設備介面上啟用偵測功能。
   - 在特定設備介面上啟用 Ping—`setdeviceconfig system <interface_number> service disable-icmp no`
   - 在所有設備介面上啟用 Ping—`setdeviceconfig system service disable-icmp no`
2. 從 WildFire 介面產生偵測流量至外部裝置。確認接收和傳輸計數器確實增加。

   ```
   ping source <wildfire-interface-ip> host<destination-ip-address>
   ```

STEP 2 | 判斷哪個 WildFire 設備不健康。參閱使用 CLI 檢視 WildFire 叢集狀態或使用 Panorama 檢視 WildFire 叢集狀態以檢視設備的狀態。

STEP 3 | 使用下列命令慢慢重新啟動不安全的節點：

```
request cluster reboot-local-node
```

已重新啟動的 WildFire 設備應自動註冊至為其設定的 WildFire 叢集。

處於「腦分裂」模式的剩餘控制器節點必須健康狀態。

STEP 4 | 等待資料移轉完成。執行 `show cluster data-migration-status` 以檢視資料庫合併進度。資料合併完成後，完成時間戳記顯示：

```
100% completed on Mon Sep 9 21:44:48 PDT 2019
```

資料合併的持續時間取決於 *WildFire* 設備上儲存的資料數量。必須分配至少若干小時來復原，因為資料合併的過程可能比較漫長。

STEP 5 | 在 Panorama 上或透過 WildFire 設備 CLI 確認叢集的狀態。

使用 WildFire 設備 CLI

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

下列主題說明 WildFire™ 設備軟體特有的 CLI 命令。所有其他的命令（例如設定介面、交付設定及設定系統資訊等）與 PAN-OS 相同，也以階層方式顯示。如需有關 PAN-OS 命令的資訊，請參閱《PAN-OS CLI 快速入門》。

- WildFire 設備軟體 CLI 概念
- WildFire CLI 命令模式
- 存取 WildFire 設備 CLI
- WildFire 設備 CLI 操作
- WildFire 設備設定模式命令參考
- WildFire 設備操作模式命令參考

WildFire 設備軟體 CLI 概念

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

本節介紹與說明如何使用 WildFire 設備軟體命令列介面 (CLI)：

- WildFire 設備軟體 CLI 結構
- WildFire 設備軟體　CLI 命令慣例
- WildFire 設備 CLI 命令訊息
- WildFire 設備命令選項符號
- WildFire 設備權限等級

WildFire 設備軟體 CLI 結構

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

WildFire 設備軟體　CLI 用於管理設備。CLI 是設備的唯一介面，可用來檢視狀態與設定資訊，以及修改設備設定。透過 SSH 或直接使用主控台連接埠存取主控台，即可存取 WildFire 設備軟體 CLI。

WildFire 設備軟體　CLI 以兩種模式運作：

- 操作模式—檢視系統狀態、導覽至　WildFire 設備軟體　CLI，及進入設定模式。
- **Configuration mode**（設定模式）—檢視與修改設定階層。

WildFire 設備軟體　CLI 命令慣例

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

基本的命令提示併入設備的使用者名稱與主機：

```
username@hostname>
```

範例：

```
admin@WF-500>
```

進入設定模式後，提示會從 > 變更為 #：

```
username@hostname> (Operational mode) username@hostname> configure
 Entering configuration mode [edit] username@hostname# (Configuration
 mode)
```

在設定模式中，目前的階層內容會顯示在命令發出時以方括號所顯示的 [edit...] 橫幅旁。

WildFire 設備 CLI 命令訊息

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

訊息會在命令發出時顯示。訊息會提供內容資訊，並協助更正無效的命令。在下列範例中，訊息以粗體顯示。

範例：未知命令

```
username@hostname# application-group Unknown command: application-
group [edit network] username@hostname#
```

範例：變更模式

```
username@hostname# exit Exiting configuration mode
 username@hostname>
```

範例：無效的語法

```
username@hostname> debug 17 Unrecognized command Invalid syntax.
 username@hostname>
```

CLI 會檢查每個命令的語法。如果語法正確，它會執行命令，候選階層的變更則會記錄下來。如果語法不正確，便會顯示無效的語法訊息，如以下範例所示：

```
username@hostname# set deviceconfig setting wildfire cloud-
intelligence submit-sample yes Unrecognized command Invalid syntax.
 [edit] username@hostname#
```

WildFire 設備命令選項符號

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

選項前面的符號可提供有關命令語法的額外資訊。

符號	說明
*	此選項為必要。
>	此命令有額外的巢狀選項。
+	此命令在此層級有額外的命令選項。
|	有選項可指定以「例外值」或「符合值」限制命令。
“ “	雖然雙引號不是命令選項符號，但在 CLI 命令中輸入多字詞時仍必須使用。例如，若要建立名為 Test Group 的位址群組，並將名稱為 user1 的使用者新增至此群組，您必須在群組名稱前後加上雙引號，如下所示： set address-group “Test Group” user1. 如果您沒有在群組名稱前後加上雙引號，則 CLI 會將 Test 這個字解譯為群組名稱，將 Group 解譯為使用者名稱，並會顯示如下的錯誤：`testis not a valid name`。 單引號在此範例中也為無效。

下列範例顯示如何使用這些符號。

範例：在下列命令中，`from` 為必要關鍵字：

```
username@hostname> scp import configuration ? + remote-port SSH
 port number on remote host * from Source (username@host:path)
 username@hostname> scp import configuration Example:此命令輸出顯示使
用 + 和 > 指定的選項。username@hostname# set rulebase security rules
 rule1 ? + action action + application application + destination
 destination + disabled disabled + from from + log-end log-end +
 log-setting log-setting + log-start log-start + negate-destination
 negate-destination + negate-source negate-source + schedule schedule
 + service service + source source + to to > profiles profiles
```

```
<Enter> Finish input [edit] username@hostname# set rulebase security
rules rule1
```

每個有 + 的選項皆可新增至此命令。

設定檔關鍵字（有 >）有額外的選項：

```
username@hostname# set rulebase security rules rule1 profiles ? +
 virus Help string for virus + spyware Help string for spyware +
 vulnerability Help string for vulnerability + group Help string for
 group <Enter> Finish input [edit] username@hostname# set rulebase
 security rules rule1 profiles
```

WildFire 設備權限等級

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

權限等級將決定使用者所能排除的命令以及所能檢視的資訊。

層級	說明
superreader	具備設備的完整唯讀存取權。
超級使用者	具備設備的完整讀寫存取權。

WildFire CLI 命令模式

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

下列主題說明用於與 WildFire 設備軟體 CLI 互動的模式：

- WildFire 設備 CLI 設定模式
- WildFire 設備 CLI 操作模式

WildFire 設備 CLI 設定模式

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

在設定模式中輸入命令以修改候選設定。修改後的候選設定會儲存於設備記憶體，並在設備執行時予以維護。

每個設定命令皆與動作有關，並也包含關鍵字、選項與值。

本節說明設定模式與設定階層：

- 設定模式命令用法
- 設定階層
- 階層路徑
- 導覽階層

設定模式命令用法

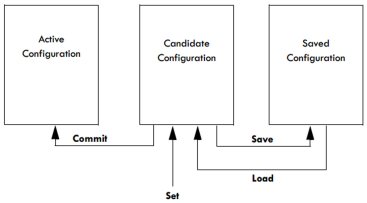
我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

使用下列命令可儲存與套用設定變更：

- `save`—將候選設定儲存在設備上的非揮發性儲存體。所儲存的設定會予以保留，直到遭到後續的 **save** 命令覆寫為止。請注意，此命令不會讓設定生效。
- `commit`—將候選設定套用至設備。交付的設定會變成設備的使用中設定。
- `set`—變更候選設定中的值。

- `load`—將最後儲存的設定或指定的設定指定為候選設定。

  若現有設定模式尚未發出 ***save*** 或 ***commit*** 命令，設備斷電時可能失去所變更的設定。



與傳統的 CLI 架構相比，維護候選設定並將儲存步驟與交付步驟分開，可提供數項重要的優點：

- 區分儲存與交付概念可同時進行多項變更，並減少系統弱點。
- 可針對類似的功能調整命令。例如，設定兩個 Ethernet 介面時，每個介面的 IP 位址不同，您可以先編輯第一個介面的設定、複製命令、僅修改介面與 IP 位址，然後將變更套用到第二個介面。
- 命令結構始終一致。

由於候選設定始終是唯一的設定，因此對候選設定的所有授權變更將與彼此一致。

設定階層

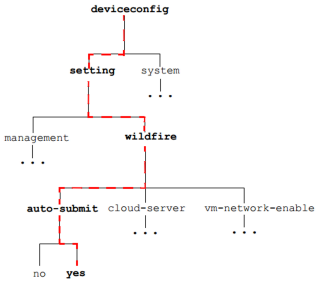
我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

設備的設定是以階層式結構加以組織。若要顯示目前層級的區段，請使用 `show` 命令。輸入 show 可顯示完整的階層，輸入 `show` 與關鍵字則可顯示階層的區段。例如，從設定模式的最上層執行 `show` 命令時，會顯示完整的設定。執行 `edit mgt-config` 命令並輸入 `show`，或者僅執行 **`showmgt-config`**，均只會顯示階層的 mgt-config 部分。

階層路徑

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

輸入命令時，會透過階層追蹤路徑，如下所示：

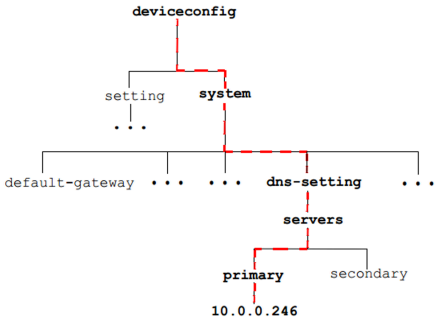


例如，下列命令會為設備指定主要 DNS 伺服器 10.0.0.246：

```
[edit] username@hostname# set deviceconfig system dns-setting servers
 primary 10.0.0.246
```

此命令會在階層中及下列 show 命令的輸出中產生新的元素：

```
[edit] username@hostname# show deviceconfig system dns-settings dns-
setting { servers { primary 10.0.0.246 } } [edit] username@hostname#
```



導覽階層

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

設定模式命令提示列下方顯示的 [edit...] 橫幅會顯示目前的階層內容。

```
[edit]
```

表示相關內容為階層的最上層，而

```
[edit deviceconfig]
```


表示相關內容在 deviceconfig 層級。

使用所列的命令在整個設定階層內導覽。

層級	說明
編輯	設定命令階層內的設定內容。
向上	將內容變更為階層中的上一層。
最前面	將內容變更為階層中的最高層。

使用 ***up*** 命令與 ***top*** 命令後所發出的 ***set*** 命令會從新的內容開始。

WildFire 設備 CLI 操作模式

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

首次登入裝置時，WildFire 設備軟體 CLI 會以操作模式開啟。操作模式命令與立即執行的動作有關，不涉及變更設定，也不需要儲存或交付。

操作模式命令有數種類型：

- **Network access**（網路存取）—對另一個主機開啟視窗。支援 SSH。
- **Monitoring and troubleshooting**（監控與疑難排解）—執行診斷與分析。包含 `debug` 與 `ping` 命令。
- **Display commands**（顯示命令）—顯示或清除目前資訊。包含 `clear` 與 `show` 命令。
- **WildFire** 設備軟體 **CLI** 導覽命令—進入設定模式或離開 WildFire 設備軟體 CLI。包含 `configure`、`exit` 及 `quit` 命令。
- **System commands**（系統命令）—提出系統層級要求或重新啟動。包含 `set` 與 `request` 命令。

存取 WildFire 設備 CLI

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

本節說明如何存取 WildFire 設備軟體 CLI：

- 建立直接主控台連線
- 建立 SSH 連線

建立直接主控台連線

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

如需直接連線主控台，請使用下列設定：

- 資料範圍：9600
- 資料位元：8
- 同位檢查：無
- 停止位元：1
- 流量控制：無

建立 SSH 連線

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

若要存取 WildFire 設備軟體 CLI：

STEP 1 | 使用終端機模擬軟體建立與 WildFire 設備的 SSH 主控台連線。

STEP 2 | 輸入管理使用者名稱。預設值為 admin。

STEP 3 | 輸入管理密碼。預設值為 admin。

WildFire 設備軟體 CLI 以操作模式開啟，並顯示 CLI 提示：

```
username@hostname>
```

WildFire 設備 CLI 操作

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

- 存取 WildFire 設備操作與設定模式
- 顯示　WildFire 設備軟體　CLI 命令選項
- 限制 WildFire 設備 CLI 命令輸出
- 為 WildFire 設備設定命令設定輸出格式

存取 WildFire 設備操作與設定模式

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

登入時，WildFire 設備軟體　CLI 會以操作模式開啟。您可以隨時在操作模式與設定模式之間導覽。

- 若要從操作模式進入設定模式，請使用 **configure** 命令：

```
username@hostname> configure Entering configuration mode [edit]
 username@hostname#
```

- 若要離開設定模式並返回操作模式，請使用 **quit** 或 **exit** 命令：

```
username@hostname# quit Exiting configuration mode
 username@hostname>
```

若要在設定模式進行時進入操作模式，請使用 **run** 命令。例如，若要顯示設定模式的系統資源，請使用 **run show system resources**。

顯示　WildFire 設備軟體　CLI 命令選項

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

根據上下文使用 **?**（或 Meta-H）以根據內容顯示命令選項清單：

- 若要顯示操作命令清單，請在命令提示中輸入 **?**。

```
username@hostname> ? clear Clear runtime parameters configure
 Manipulate software configuration information create create commands
 debug Debug and diagnose delete Remove files from hard disk disable
 disable commands edit edit commands exit Exit this session find Find
 CLI commands with keyword grep Searches file for lines containing
 a pattern match less Examine debug file content ping Ping hosts and
 networks quit Exit this session request Make system-level requests
 scp Use scp to import / export files set Set operational parameters
 show Show operational parameters ssh Start a secure shell to another
 host submit submit commands tail Print the last 10 lines of debug
 file content telnet Start a telnet session to another host test
 verify system settings with test cases tftp Use tftp to import /
 export files traceroute Print the route packets take to network host
 username@hostname>
```

- 若要顯示所指定命令的可用選項，請在該命令後加上 **?**。

範例：

```
username@hostname> ping ? + bypass-routing Bypass routing table,
 use specified interface + count Number of requests to send
 (1..2000000000 packets) + do-not-fragment Don't fragment echo
 request packets (IPv4) + interval Delay between requests (seconds)
 + no-resolve Don't attempt to print addresses symbolically + pattern
 Hexadecimal fill pattern + size Size of request packets (0..65468
 bytes) + source Source address of echo request + tos IP type-of-
service value (0..255) + ttl IP time-to-live value (IPv6 hop-limit
 value) (0..255 hops) + verbose Display detailed output * host
 Hostname or IP address of remote host
```

限制 WildFire 設備 CLI 命令輸出

某些操作命令包含可限制顯示輸出的選項。若要限制輸出，請輸入直立線符號，後面加上 **except** 或 **match** 及要排除或包含的值：

範例：

以下為 show system info 命令輸出範例：

```
username@hostname> show system info hostname:WildFire
 ip-address:192.168.2.20 netmask:255.255.255.0 default-
gateway:192.168.2.1 mac-address:00:25:90:95:84:76 vm-interface-ip-
address:10.16.0.20 vm-interface-netmask:255.255.252.0 vm-interface-
default-gateway:10.16.0.1 vm-interface-dns-server:10.0.0.247 time:Mon
 Apr 15 13:31:39 2013 uptime:0 days, 0:02:35 family: m model:WF-500
 serial:009707000118 sw-version:8.0.1 wf-content-version:702-283 wf-
content-release-date: unknown logdb-version:8.0.15 platform-family:
 m operational-mode: normal username@hostname> The following sample
 displays only the system model information: username@hostname> show
 system info | match model model:WF-500 username@hostname>
```

為 WildFire 設備設定命令設定輸出格式

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

在操作模式中使用 **`set cli config-output-format`** 命令變更設定命令的輸出格式。選項包括預設格式 json (JavaScript Object Notation)、集格式及 XML 格式。預設格式是階層格式，設定區段在此格式中會縮排，並以大括號括住。

WildFire 設備設定模式命令參考

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

本節包含下列 WildFire 設備軟體所特有設定模式命令參考資訊。為 WildFire 設備軟體一部分的所有其他命令則與 PAN-OS 相同，如 PAN-OS 11.0 CLI 快速入門中所述。

- set deviceconfig cluster
- set deviceconfig high-availability
- set deviceconfig setting management
- set deviceconfig setting wildfire
- set deviceconfig system eth2
- set deviceconfig system eth3
- set deviceconfig system panorama local-panorama panorama-server
- set deviceconfig system panorama local-panorama panorama-server-2
- set deviceconfig system update-schedule
- set deviceconfig system vm-interface

set deviceconfig cluster

說明

在 WildFire 設備上設定 WildFire 設備叢集設定。您可以設定叢集名稱、用於進行叢集通訊的介面，以及叢集中設備的模式（角色）—控制器或工作。在您設定為叢集控制器的 WildFire 設備上，您可新增 WildFire 設備至該叢集，並設定控制器是否在其管理介面上提供 DNS 服務。

階層位置

```
set deviceconfig
```

語法

```
cluster { cluster-name <name>; interface {eth2 | eth3}; mode
 { controller { service-advertisement dns-service enabled {no | yes};
 worker-list {ip-address} } worker; } }
```

選項

+ `cluster-name` — 為叢集命名。叢集名稱必須為有效的域名區段。

+ `interface` — 設定介面以用於叢集通訊。叢集通訊介面在所有叢集成員上必須相同。

> `mode` — 將 WildFire 設備設定為控制器節點或工作節點。如果是控制器節點，設定控制器是否在管理介面上提供 DNS 服務 (`service-advertisement`)，並新增工作節點至叢集 (`worker-list`)。每個 WildFire 設備叢集應該有兩個控制器節點以提供高可用性。您可新增 2 個控制器節點和最多 18 個工作節點至叢集，叢集最多可包含 20 個節點。

範例輸出

```
admin@wf-500(active-controller)# show deviceconfig cluster cluster
 { cluster-name sid-6; interface eth2; mode { controller { worker-
list { 2.2.2.115; } } } }
```

需要權限層級

superuser, deviceadmin

set deviceconfig high-availability

說明

設定 Wildfire 設備叢集高可用性 (HA) 設定。

階層位置

```
set deviceconfig
```

語法

```
high-availability { enabled {no | yes}; election-option { preemptive
 {no | yes}; priority {primary | secondary}; timers { advanced
 {heartbeat interval <value> | hello-interval <value> | preemption-
hold-time <value> | promotion-hold-time <value>} aggressive;
 recommended; } } interface { ha1 { peer-ip-address <ip-address>;
 port {eth2 | eth3 | management}; encryption enabled {no | yes}; }
 ha1-backup { peer-ip-address <ip-address>; port {eth2 | eth3 |
 management}; } } }
```

選項

+ `enabled` — 啟用兩個控制器節點上的 HA，為叢集提供容錯功能。每個 WildFire 設備叢集應該有兩個設定為 HA 對的控制器節點。

> `election-option` — 設定先佔、優先順序及計時器 HA 選項值。

+ preemptive — 選取選項，用於根據 HA priority 設定，使被動 HA 對等體（控制器備份節點）先佔主動 HA 對等體（主要控制器節點）。例如，如果主要控制器節點出現問題，次要（被動）控制器節點會接管叢集控制。當主要控制器節點復原後，如果您不想設定先佔，次要控制器會繼續控制叢集，而主要控制器便會充當控制器備份節點。但是，如果您在兩個 HA 對等體上都設定了先佔，當主要控制器復原後，會先佔次要控制器，並重新控制叢集。次要控制器會繼續充當之前的控制器備份節點。您必須在兩個 HA 對等體上設定先佔設定，先佔機制才會發揮作用。

+ priority — 選取選項，用於設定 HA 對中每個控制器的先佔優先順序。同時在 HA 控制器對的兩個成員上設定先佔。

> timers — 設定 HA 選取選項的計時器。WildFire 設備提供了兩個預先設定的計時器選項（aggressive 和 recommended 設定），或者您也可以個別設定每個計時器。Advanced 計時器讓您可個別設定不同值：

- Heartbeat-interval 用於設定傳送活動訊號偵測的時間（單位：毫秒）。該值範圍是 1000 至 60,000 ms，預設值為 2000 ms。
- Hello-interval 用於設定傳送「Hello」訊息的時間（單位：毫秒）。該值範圍是 8000 至 60,000 ms，預設值為 8000 ms。
- Preemption-hold-time 用於設定先佔主動（主要）控制器節點之前保持在被動（控制器備份）模式的時間（單位：分鐘）。該值範圍是 1 至 60 分鐘，預設值為 1 分鐘。
- Promtion-hold-time 用於設定從被動（控制器備份）變更至主動（主要）狀態的時間（單位：毫秒）。該值範圍是 0 至 60,000 ms，預設值為 2000 ms。

> interface — 設定主要 (ha1) 和備份 (ha1-backup) 控制連結介面的 HA 介面設定。控制連結介面可讓 HA 控制器對保持同步，並準備好進行故障轉移，以防主要控制器節點出現問題。同時設定 ha1 介面和 ha1-backup 介面可在連結失敗的情況下，在控制器之間提供備援連線。設定：

- peer-ip-address。對於每個介面，設定 HA 對等體的 IP 位址。在 HA 對的另一個控制器節點上，Ha1 介面對等體為 ha1 介面 IP 地址。在 HA 對的另一個控制器節點上，ha1-backup 介面對等體為 ha1-backup 介面 IP 地址。
- port。在每個控制器節點上，設定要用於 ha1 介面的連接埠和要用於 ha-backup 介面的連接埠。您可以將 eth2、eth3 或 management 連接埠 (eth0) 用於 HA 控制連貫介面。您無法將分析環境網路介面 (eth1) 用作 ha1 或 ha1-backup 控制連結介面。在兩個 HA 對等體上使用相同介面作為 ha1 介面，並使用相同介面（不是 ha1 介面）作為 ha1-backup 介面。例如，在兩個控制器節點上將 eth3 設定為 ha1 介面，並將 management 介面設定為 ha1-backup 介面。

範例輸出

```
admin@wf-500(active-controller)# show deviceconfig high-availability
 high-availability { election-option { priority primary; } enabled
 no; interface { ha1 { peer-ip-address 10.10.10.150; port eth2 } ha1-
backup { peer-ip-address 10.10.10.160; port management } } }
```

需要權限層級

superuser, deviceadmin

set deviceconfig setting management

說明

在 WildFire 設備上設定系統管理工作階段設定。您可以設定逾時以結束閒置太久的管理工作階段及其鎖定管理員需要的登入重試次數（失敗的登入嘗試次數）。

階層位置

```
set deviceconfig setting
```

語法

```
management { idle-timeout {0 | <value>} admin-lockout { failed-
attempts <value> lockout-time <value> } }
```

選項

`+ idle-timeout` — 預設管理工作階段閒置逾時分鐘數。設定閒置逾時（1 至 1440 分鐘），或將逾時值設定為 0（零）以使工作階段永不逾時。

`> admin-lockout` — 設定 `failed-attempts` 次數 (0-10)，以在管理員被鎖定在系統外之前登入設備，以及 `lockout-time` 分鐘數 (0-60)，以在管理員超過 `failed-attempts` 閾值時鎖定管理員。

範例輸出

```
management { idle-timeout 0; admin-lockout { failed-attempts 3;
 lockout-time 5; } }
```

set deviceconfig setting wildfire

說明

在 Wildfire 設備上進行 WildFire 設定。您可以設定轉送惡意軟體檔案、定義接收遭惡意軟體感染檔案的雲端伺服器，以及啟用或停用 vm-interface。

階層位置

```
set deviceconfig setting
```

語法

```
wildfire { active-vm {vm-1 | vm-2 | vm-3 | vm-4 | vm-5 | <value>};
 cloud-server <value>; custom-dns-name <value>; preferred-analysis-
environment {Documents | Executables | default}; vm-network-
enable {no | yes}; vm-network-use-tor {enable | disable}; cloud-
intelligence { cloud-query {no | yes};submit-diagnostics {no |
 yes}; submit-report {no | yes}; submit-sample {no | yes}; } file-
retention { malicious {indefinite | <1-2000>}; non-malicious <1-90> }
 signature-generation { av {no | yes}; dns {no | yes}; url {no |
 yes}; } }
```

選項

+ `active-vm` — 選取 WildFire 將用於分析樣本的虛擬電腦環境。每個 vm 具備不同設定，例如 Windows XP、特定版本的 Flash、Adobe reader 等。若要檢視所選取的 VM，請執行下列命令：**`show wildfire status`** 並檢視 [選取的 VM] 欄位。若要檢視 VM 環境資訊，請執行下列命令：**`show wildfire vm-images`**。

+ `cloud-server` — 設備將轉送惡意樣本/報告到該處以重新分析的雲端伺服器主機名稱。預設的雲端伺服器是 wildfire-public-cloud。若要設定轉送，請使用下列命令：**`set deviceconfig setting wildfire cloud-intelligence`**。

+ `custom-dns-name` — 設定自訂 DNS 名稱以在伺服器憑證和 WildFire 伺服器清單中使用，取代預設 DNS 名稱 `wfpc.sevice.<clustername>.<domain>`。

+ `preferred-analysis-environment` —根據環境中最常分析的樣本類型，配置大部分資源進行文件分析或可執行檔分析。預設配置會平衡文件和可執行檔樣本之間的資源。例如，若要配置大部分分析資源至文件：**`set deviceconfig setting wildfire preferred-analysis-environment Documents`**。

+ `vm-network-enable` — Enable or disable the vm-network.啟用之後，在虛擬電腦沙箱中執行的樣本檔案即可存取網際網路。這可協助 WildFire 進一步分析惡意軟體的行為以尋找秘密回報活動之類的情況。

+ `vm-network-use-tor` — 啟用或停用 vm-interface 的 Tor 網路。此選項啟用時，任何來自 WildFire 沙箱系統的惡意流量會在樣本分析期間透過 Tor 網路傳送。Tor 網路會將您的公開 IP 位址加上遮罩，讓惡意網站的擁有人無法判定流量來源。

> `cloud-intelligence` — 設定設備以提交 WildFire 診斷資料、報告或樣本至 Palo Alto Networks WildFire 雲端，或自動查詢公共 WildFire 雲端，然後再執行本機分析以節約 WildFire 設備資源。提交報告選項將會傳送惡意樣本的報告到雲端以進行統計收集。提交樣本選項將會傳送惡意樣本到雲端。若已啟用 submit-sample，則無須啟用 submit-report，因為樣本會在雲端重新分析，且會在樣本為惡意的情況下收集新報告和特徵碼。

> `file-retention` — 設定儲存惡意（惡意軟體和網路釣魚）樣本和非惡意（灰色和良性）樣本的時間。保留惡意樣本的預設時間為無限（永不刪除）。保留非惡意樣本的預設時間為 14 天。例如，若要將非惡意樣本保留 30 天：**`set deviceconfig setting wildfire file-retention non-malicious 30`**。

`> signature-generation` — 讓設備在本機產生特徵碼，不需再將資料傳送至公共雲端，也能封鎖惡意內容。WildFire 設備將針對由 Palo Alto Networks 防火牆或 WildFire API 轉送而來的檔案進行分析，並產生能夠封鎖惡意檔案、相關命令和控制流量的防毒特徵碼及 DNS 特徵碼。當設備偵測到惡意 URL 時，它會傳送 URL 至 PAN-DB，而 PAN-DB 會將其指派至惡意軟體類別。

範例輸出

以下為 WildFire 設定的輸出範例。

```
admin@WF-500# show deviceconfig setting wildfire wildfire
 { signature-generation { av yes; dns yes; url yes; } cloud-
intelligence { submit-report no; submit-sample yes; submit-
diagnostics yes; cloud-query yes; } file-retention { non-malicious
 30; malicious 1000; { active-vm vm-5; cloud-server wildfire-public-
cloud; vm-network-enable yes; }
```

set deviceconfig system eth2

說明

設定 eth2 介面。

階層位置

```
set deviceconfig system
```

語法

```
eth2 { default-gateway <ip-address>; ip-address <ip-address>; mtu
 <value>; netmask <ip-netmask>; speed-duplex {100Mbps-full-duplex
 | 100Mbps-half-duplex | 10Mbps-full-duplex | 10Mbps-half-duplex |
 1Gbps-full-duplex | 1Gbps-half-duplex | auto-negotiate}; permitted-
ip <ip-address/netmask>; service disable-icmp {no | yes}; }
```

選項

+ `default-gateway` — eth2 介面之預設閘道的 IP 地址。
+ `ip-address` — eth2 介面的 IP 地址。
+ `mtu` — eth2 介面的最大傳輸單位 (MTU)。
+ `netmask` — eth2 介面的網路遮罩。
+ `speed-duplex` — eth2 介面的介面速度（10Mbps、100Mbps、1Gbps 或自動交涉）和雙工模式（全雙工或半雙工）。

`> permitted-ip` — 允許存取 eth2 介面的 IP 地址。如果您使用 IP 地址指定網路遮罩，網路遮罩必須採用斜線標記法。例如，若要指定 C 類地址，請輸入：10.10.10.100/24（不是 10.10.10.100 255.255.255.0）。

`> service-disable` — 停用 eth2 介面的 ICMP。

範例輸出

```
admin@wf-500(active-controller)# show deviceconfig system eth2 eth2
 { ip-address 10.10.10.120; netmask 255.255.255.0; service { disable-
icmp no; } speed-duplex auto-negotiate; mtu 1500; }
```

需要權限層級

superuser, deviceadmin

set deviceconfig system eth3

說明

設定 eth3 介面。

階層位置

```
set deviceconfig system
```

語法

```
eth3 { default-gateway <ip-address>; ip-address <ip-address>; mtu
 <value>; netmask <ip-netmask>; speed-duplex {100Mbps-full-duplex
 | 100Mbps-half-duplex | 10Mbps-full-duplex | 10Mbps-half-duplex |
 1Gbps-full-duplex | 1Gbps-half-duplex | auto-negotiate}; permitted-
ip <ip-address/netmask>; service disable-icmp {no | yes}; }
```

選項

`+ default-gateway` — eth3 介面之預設閘道的 IP 位址。

`+ ip-address` — eth3 介面的 IP 位址。

`+ mtu` — eth3 介面的最大傳輸單位 (MTU)。

`+ netmask` — eth3 介面的網路遮罩。

`+ speed-duplex` — eth3 介面的介面速度（10Mbps、100Mbps、1Gbps 或自動交涉）和雙工模式（全雙工或半雙工）。

`> permitted-ip` — 允許存取 eth3 介面的 IP 位址。如果您使用 IP 地址指定網路遮罩，網路遮罩必須採用斜線標記法。例如，若要指定 C 類地址，請輸入：10.10.10.100/24（不是 10.10.10.100 255.255.255.0）。

`> service-disable` — 停用 eth3 介面的 ICMP。

範例輸出

```
admin@wf-500(active-controller)# show deviceconfig system eth3 eth3
 { ip-address 10.10.20.120; netmask 255.255.255.0; service { disable-
icmp no; } speed-duplex auto-negotiate; mtu 1500; }
```

需要權限層級

superuser, deviceadmin

set deviceconfig system panorama local-panorama panorama-server

說明

設定主要 Panorama 伺服器以管理 WildFire 設備或設備叢集。

階層位置

```
set deviceconfig system panorama local-panorama
```

語法

```
panorama-server {IP address | FQDN};
```

選項

`+ panorama-server` — 設定主要 Panorama 伺服器的 IP 地址或完整網域名稱 (FQDN)，以用於管理 WildFire 設備或設備叢集。

範例輸出

輸出會被截斷，只會顯示包含 Panorama 伺服器設定的輸出片段。

```
admin@wf-500(active-controller)# show deviceconfig system
 system { panorama-server 10.10.10.100; panorama-server-2
 10.10.10.110 hostname myhost; ip-address 10.10.20.120; netmask
 255.255.255.0; default-gateway 10.10.10.1; update-server
 updates.paloaltonetworks.com; service { disable-icmp no; disable-ssh
 no; disable-snmp yes; } ...
```

需要權限層級

superuser, deviceadmin

set deviceconfig system panorama local-panorama panorama-server-2

說明

設定備份 Panorama 伺服器以管理 WildFire 設備或設備叢集。設定備份 Panorama 伺服器可為叢集或個別設備管理提供高可用性。

階層位置

```
set deviceconfig system panorama local-panorama
```

語法

```
panorama-server-2 {IP address | FQDN};
```

選項

`+ panorama-server-2` — 設定備份 Panorama 伺服器的 IP 地址或完整網域名稱 (FQDN)，以用於管理 WildFire 設備或設備叢集。

範例輸出

輸出會被截斷，只會顯示包含 Panorama 伺服器設定的輸出片段。

```
admin@wf-500(active-controller)# show deviceconfig system
 system { panorama-server 10.10.10.100; panorama-server-2
 10.10.10.110 hostname myhost; ip-address 10.10.20.120; netmask
 255.255.255.0; default-gateway 10.10.10.1; update-server
 updates.paloaltonetworks.com; service { disable-icmp no; disable-ssh
 no; disable-snmp yes; } ...
```

需要權限層級

superuser, deviceadmin

set deviceconfig system update-schedule

說明

在 WildFire 設備上排程內容更新。這些內容更新會為設備配備最新的威脅資訊，以精確偵測惡意軟體並提升設備區分惡意及良性軟體的能力。

階層位置

```
set deviceconfig system update-schedule
```

語法

```
wf-content recurring { daily at <value> action {download-and-install
 | download-only}; weekly { action {download-and-install | download-
only}; at <value>; day-of-week {friday | monday | saturday | sunday |
 thursday | tuesday | wednesday}; } }
```

選項

> `wf-content` — WildFire 內容更新。

> `daily` — 每天排程更新。

+ `action` — 指定要採取的動作。您可以為設備排定下載並安裝更新，或者下載後手動安裝。

+ `at` — 時間規格 hh:mm（例如 20:10）。

> `hourly` — 每小時排程更新。

+ `action` — 指定要採取的動作。您可以為設備排定下載並安裝更新，或者下載後手動安裝。

+ `at` — 小時之後的分鐘數。

> `weekly` — 每週排程更新。

+ `action` — 指定要採取的動作。您可以為設備排定下載並安裝更新，或者下載後手動安裝。

+ `at` — 時間規格 hh:mm（例如 20:10）。

+ `day-of-week` — 每週的某日（星期五、星期一、星期六、星期日、星期四、星期二、星期三）。

範例輸出

```
admin@WF-500# show update-schedule { wf-content { recurring
 { weekly { at 19:00; action download-and-install; day-of-week
 friday; } } } }
```

需要權限層級

superuser, deviceadmin

set deviceconfig system vm-interface

說明

在 WildFire 設備虛擬電腦沙箱上執行的惡意軟體使用 vm-interface 來存取網際網路。建議啟動此連接埠，這可在惡意軟體存取網際網路以從事回撥或其他活動時，幫助 WildFire 進一步識別惡意活動。此介面具備網際網路的隔離連線是相當重要的。若 WildFire 設備於 FIPS/CC 模式中操作，則會停用 VM 介面。如需詳細資訊，請參閱設定 WildFire 設備 VM 介面。

設定 vm-interface 後，可透過執行下列命令予以啟用：

```
set deviceconfig setting wildfire vm-network-enable yes
```

階層位置

```
set deviceconfig system
```

語法

```
set vm-interface { default-gateway <ip_address>; dns-server
 <ip_address>; ip-address <ip_address>; link-state; mtu; netmask
 <ip_address>; speed-duplex; {
```

選項

+ `default-gateway` — VM 介面的預設閘道。
+ `dns-server` — VM 介面的 DNS 伺服器。
+ `ip-address` — VM 介面的 IP 地址。
+ `link-state` — 將連結狀態設定為正常或失效。
+ `mtu` — VM 介面的最大傳輸單位。
+ `netmask` — VM 介面的 IP 網路遮罩。
+ `speed-duplex` — VM 介面的速度和雙工。

範例輸出

下列為設定的 vm-interface。

```
vm-interface { ip-address 10.16.0.20; netmask 255.255.252.0; default-
gateway 10.16.0.1; dns-server 10.0.0.246; }
```

需要權限層級

superuser, deviceadmin

WildFire 設備操作模式命令參考

我可以在哪裡使用這個？	我需要什麼？
• WildFire 設備	❑ WildFire 授權

本節包含下列 WildFire 設備軟體所特有操作模式命令的命令參考資訊。為 WildFire 設備軟體一部分的所有其他命令則與 PAN-OS 相同；請參閱 PAN-OS 11.0 CLI 快速入門 以取得這些命令的資訊。

- clear high-availability
- create wildfire api-key
- delete high-availability-key
- delete wildfire api-key
- delete wildfire-metadata
- disable wildfire
- edit wildfire api-key
- load wildfire api-key
- request cluster decommission
- request cluster reboot-local-node
- request high-availability state
- request high-availability sync-to-remote
- request system raid
- request wildfire sample redistribution
- request system wildfire-vm-image
- request wf-content
- save wildfire api-key
- set wildfire portal-admin
- show cluster all-peers
- show cluster controller
- show cluster membership
- show cluster task
- show cluster data migration status
- show high-availability all

- show high-availability control-link
- show high-availability state
- show high-availability transitions
- show system raid
- show wildfire
- show wildfire global
- show wildfire local
- submit wildfire local-verdict-change
- 測試 wildfire 登錄

clear high-availability

說明

在 WildFire 設備叢集的控制器節點上清除高可用性 (HA) 控制連結統計資訊與轉換統計資料。

語法

```
create { high-availability { control-link { statistics; }
 transitions; } }
```

選項

`> control-link>` —清除 HA 控制連結統計資料。

`> transitions>` —清除 HA 轉換統計資料（HA 轉換過程中發生的事件）。

範例輸出

清除控制連結或轉換統計資料後，WildFire 叢集會將所有值重設為零 (0)。

```
admin@wf-500(active-controller)> show high-availability control-link
 statistics High-Availability:Control Link Statistics:HA1: Messages-
TX :0 Messages-RX :0 Capability-Msg-TX :0 Capability-Msg-RX :0
 Error-Msg-TX :0 Error-Msg-RX :0 Preempt-Msg-TX :0 Preempt-Msg-
RX :0 Preempt-Ack-Msg-TX :0 Preempt-Ack-Msg-RX :0 Primary-Msg-
TX :0 Primary-Msg-RX :0 Primary-Ack-Msg-TX :0 Primary-Ack-Msg-
RX :0 Hello-Msg-TX :0 Hello-Msg-RX :0 Hello-Timeouts :0 Hello-
Failures :0 MasterKey-Msg-TX :0 MasterKey-Msg-RX :0 MasterKey-Ack-
Msg-TX :0 MasterKey-Ack-Msg-RX :0 Connection-Failures :0 Connection-
Tries-Failures :0 Connection-Listener-Tries :0 Connection-Active-
Tries :0 Ping-TX :0 Ping-Fail-TX :0 Ping-RX :0 Ping-Timeouts :0 Ping-
Failures :0 Ping-Error-Msgs :0 Ping-Other-Msgs :0 Ping-Last-Rsp :0
 admin@wf-500(active-controller)> show high-availability transitions
 High-Availability:Transition Statistics:Unknown :0 Suspended :0
 Initial :0 Non-Functional :0 Passive :0 Active :0
```

需要權限層級

superuser, deviceadmin

create wildfire api-key

說明

在您將在外部系統上使用的 WildFire 設備上建立 API 金鑰，以提交樣本至設備、查詢報告，或從設備擷取樣本及封包擷取 (PCAPS)。

語法

```
create { wildfire { api-key { key <value>; name <value>; { { {
```

選項

+ `key` —手動輸入金鑰值來建立 API 金鑰。金鑰值必須為 64 個字母字元 (a-z) 或數字 (0-9)。如果您未指定金鑰選項，則設備會自動產生金鑰。

+ `name` — 選擇性輸入 API 金鑰的名稱。API 金鑰名稱僅會用來標示金鑰，以便輕鬆找到針對特定用途指派的金鑰，且不會影響金鑰的功能。

範例輸出

下列輸入顯示設備擁有三個 API 金鑰，而其中一個金鑰名為 `my-api-key`。

```
admin@WF-500> show wildfire global api-keys all
 +-----------------------------------------------------+------------+
 | Apikey | Name |
 +-----------------------------------------------------
+------------+ | <API KEY> | my-api-key | | <API
 KEY> | my-api-key | | <API KEY> | my-api-key |
 +-----------------------------------------------------+------------
+ +---------+---------------------+---------------------+ | Status
 | Create Time | Last Used Time | +---------+---------------------
+---------------------+ | Enabled | 2017-03-02 19:14:36 | 2017-03-02
 19:14:36 | | Enabled | 2016-02-06 12:13:22 | 2017-03-01 12:10:20 |
 | Enabled | 2014-08-04 17:00:42 | 2017-03-01 11:12:52 | +---------
+---------------------+---------------------+
```

需要權限層級

superuser, deviceadmin

delete high-availability-key

說明

在 WildFire 設備叢集控制器節點的叢集控制連結上刪除用於實現高可用性 (HA) 的端點加密金鑰。

語法

```
delete { high-availability-key; }
```

選項

無額外的選項。

範例輸出

輸出中反白顯示的行表示 HA 控制連結上未啟用加密。

```
admin@wf-500(active-controller)> show high-availability state High-
Availability:Local Information:版本：1 State: active-controller (last
 1 days) Device Information:Management IPv4 Address:10.10.10.14/24
 Management IPv6 Address:HA1 Control Links Joint Configuration:
 Encryption Enabled: no Election Option Information:Priority:
 primary Preemptive: no Version Compatibility:Software
 Version:Match Application Content Compatibility:Match Anti-
Virus Compatibility:Match Peer Information:Connection status:
 up Version:1 State: passive-controller (last 1 days) Device
 Information:Management IPv4 Address:10.10.20.112/24 Management
 IPv6 Address:Connection up; Primary HA1 link Election Option
 Information:Priority: secondary Preemptive: no Configuration
 Synchronization:Enabled: yes Running Configuration: synchronized
```

需要權限層級

superuser, deviceadmin

delete wildfire api-key

說明

將 API 金鑰從 WildFire 設備刪除。當您刪除金鑰之後，設定為使用 API 在設備上執行 API 功能的系統將無法再存取設備。

語法

```
delete { wildfire { api-key { key <value>; { { {
```

選項

`+ key <value>` — The key value for the key that you want to delete.若要檢視 API 金鑰清單，請執行下列命令：

```
admin@WF-500> show wildfire global api-keys all
```

範例輸出

```
admin@WF-500> delete wildfire api-key key <API KEY> APIKey <API Key>
 deleted
```

需要權限層級

superuser, deviceadmin

delete wildfire-metadata

說明

在 WildFire 設備上刪除內容更新。如需內容更新及如何安裝的詳細資訊，請參閱 request wf-content。

語法

```
delete { wildfire-metadata update <value>; {
```

選項

`+ update <value>` — 定義您想刪除的內容更新。

範例輸出

接下來的輸出顯示刪除下列名稱的更新：

```
panup-all-wfmeta-2-181.candidate.tgz. admin@WF-500> delete wildfire-
metadata update panup-all-wfmeta-2-181.candidate.tgz successfully
 removed panup-all-wfmeta-2-181.candidate.tgz
```

需要權限層級

superuser, deviceadmin

disable wildfire

說明

停用網域特徵碼或樣本特徵碼，以便其從下一個 WildFire 內容套件版本中排除。

語法

```
disable wildfire { domain-signature { domain <value>; } OR... sample-
signature { sha256 { equal <value>; } }
```

選項

`> domain-signature`—將網域特徵碼的狀態設定為停用，以便其從下一個 WildFire 內容版本中排除。

`> sample-signature`—將樣本特徵碼的狀態設定為停用，以便其從下一個 WildFire 內容版本中排除。

範例輸出

已成功停用的樣本或網域不會顯示任何輸出。

```
admin@WF-500> disable wildfire sample-signature sha256 equal
 d1378bda0672de58d95f3bff3cb42385f2d806a4a15b89cdecfedbdb1ec08228
```

需要權限層級

superuser, deviceadmin

edit wildfire api-key

說明

在 WildFire 設備上修改 API 金鑰名稱或金鑰狀態（已啟用/已停用）。

語法

```
edit { wildfire { api-key [name | status] key <value>; { {
```

選項

`+ name`—變更 API 金鑰名稱。

`+ status`— 啟用或停用 API 金鑰。

`* key`—指定要修改的金鑰。

範例輸出

此命令中的金鑰值為必要。例如，若要將名為 `stu` 的金鑰名稱變更為 `stu-key1`，請輸入下列命令：

在下列命令中，您無須輸入舊的金鑰名稱；輸入新的金鑰名稱即可。

```
admin@WF-500> edit wildfire api-key name stu-key1 key <API
 KEY> To change the status of stu-key1 to disabled, enter the
 following command: admin@WF-500> edit wildfire api-key status
 disable key <API KEY> Example output that shows that stu-key1
 is disabled: admin@WF-500> show wildfire global api-keys all
```

```
 +-------------------------------------------------+------------+
 | Apikey | Name |
 +-------------------------------------------------+------------+
 | <API KEY> | stu-key1 |
 +-------------------------------------------------+------------
+ +----------+---------------------+---------------------+ | Status
 | Create Time | Last Used Time | +----------+---------------------
+---------------------+ | Disabled | 2017-03-02 19:14:36 | 2017-03-02
 19:14:36 | +----------+---------------------+---------------------+
```

需要權限層級

superuser, deviceadmin

load wildfire api-key

說明

將 API 金鑰匯入 WildFire 設備之後，您必須使用載入命令，讓此金鑰可供使用。使用此命令來取代所有現有的 API 金鑰，或者您可將匯入檔案中的金鑰與現有的金鑰資料庫合併。

語法

```
load { wildfire { from <value> mode [merge | replace]; { {
```

選項

* `from` — 指定您想匯入的 API 金鑰檔案名稱。金鑰檔案使用 .keys 副檔名。例如 my-api-keys.keys。若要檢視可匯入的金鑰清單，請輸入下列命令：

```
admin@WF-500> load wildfire api-key from ?
```

+ `mode` — 選擇性輸入匯入模式（合併/取代）。例如，若要以新金鑰檔案的內容取代設備上的金鑰資料庫，請輸入下列命令：

```
admin@WF-500> load wildfire api-key mode replace from my-api-
keys.keys
```

若您不指定 **mode** 選項，預設動作將合併金鑰。

需要權限層級

superuser, deviceadmin

request cluster decommission

說明

從具有三個或更多成員節點的叢集中移除 WildFire 設備叢集節點。請勿使用此命令移除雙節點叢集中的節點。而要使用 `delete deviceconfig high-availability` 和 `delete deviceconfig cluster` 命令從本機叢集移除節點。

階層位置

request cluster

語法

```
request { cluster { decommission { show; start; stop; } } }
```

選項

`show`—顯示節點解除工作的狀態。

`start`—開始節點解除工作。

`stop`—中止節點解除工作。

範例輸出

`Node mode` 欄位確認叢集節點解除已成功，因為模式為 `stand_alone`，而不是 `controller` 或 `worker`。

```
admin@wf-500> show cluster membership Service Summary: wfpc signature
 Cluster name:Address:10.10.10.86 Host name: wf-500 Node name:
 wfpc-009707000xxx-internal Serial number:009707000xxx Node mode:
 stand_alone Server role:True HA priority:Last changed:Wed, 15
 Feb 2017 00:05:11 -0800 Services: wfcore signature wfpc infra
 Monitor status:Serf Health Status: passing Agent alive and
 reachable Application status: wildfire-apps-service:Ready global-db-
service:ReadyStandalone global-queue-service:ReadyStandalone local-
db-service:ReadyMaster
```

需要權限層級

superuser, deviceadmin

request cluster reboot-local-node

說明

慢慢重新啟動本機 WildFire 叢集節點。

階層位置

```
request cluster
```

語法

```
request { cluster { reboot-local-node; } }
```

選項

無額外的選項。

範例輸出

您可以透過下列幾種方式來確認本機叢集節點已重新啟動還是正在重新啟動：

- `show cluster task local`—顯示本機節點要求的工作。
- `show cluster task current`—顯示目前在本機節點上執行的工作或最後完成的工作（僅限控制器節點）。
- `show cluster task pending`—顯示本機節點上已排入佇列但尚未執行的工作（僅限控制器節點）。
- `show cluster task history`—display tasks that have been run on the local node (controller nodes only).

例如，下列命令顯示了兩個叢集節點重新啟動工作已成功完成：

```
admin@qa15(passive-controller)> show cluster task history
 Request:        reboot from qa16 (009701000044/35533) at
 2017-02-17 19:21:53 UTC                 Reboot requested
 by admin Response:       permit by qa15 at 2017-02-17
 22:11:31 UTC                request not affecting
 healthy core server.Progress:       Wait for kv store
 ready for query...               KV store is ready, wait
 for cluster leader available...                Cluster
 leader is 2.2.2.16...                Checking is sysd and
 clusterd are alive...                Checking if cluster-
mgr is ready...               Checking global-db-cluster
 readiness...               Stopping global-queue server and
 leaving cluster...               Stopping global-db servers
 and doing failover...                rebooting...Finished:
  success at 2017-02-17 22:17:56 UTC Request:        reboot
 from qa16 (009701000044/35535) at 2017-02-17 22:45:50 UTC
                Reboot requested by admin Response:
 permit by qa15 at 2017-02-17 23:06:44 UTC
 request not affecting healthy core server.Progress:       Wait
 for kv store ready for query...                KV store is
 ready, wait for cluster leader available...
 Cluster leader is 2.2.2.15...                Checking is sysd
 and clusterd are alive...              Checking if cluster-
```

```
mgr is ready...                  Checking global-db-cluster
 readiness...                  Stopping global-queue server and leaving
 cluster...                  Stopping global-db servers and doing
 failover...                   rebooting...Finished:       success at
 2017-02-17 23:12:53 UTC
```

需要權限層級

superuser, deviceadmin

request high-availability state

說明

在 WildFire 設備叢集上，使本機控制器節點或對等控制器節點的高可用性 (HA) 狀態正常。

階層位置

```
request high-availability
```

語法

```
request { high-availability { state { functional; } peer
 {    functional; } } }
```

選項

> `functional`—使本機控制器節點的 HA 狀態正常。

> `peer`—使對等控制器節點的 HA 狀態正常。

範例輸出

輸出中反白顯示的行表示，本機控制器節點的 HA 狀態在主動（主要）控制器角色中正常，且對等控制器節點的 HA 狀態在被動（備份）控制器角色中正常。

```
admin@wf-500(active-controller)> show high-availability state
 High-Availability:Local Information:版本：1 State: active-
controller (last 1 days) Device Information:Management IPv4
 Address:10.10.10.14/24 Management IPv6 Address:HA1 Control
 Links Joint Configuration:Encryption Enabled: no Election
 Option Information:Priority: primary Preemptive: no Version
 Compatibility:Software Version:Match Application Content
 Compatibility:Match Anti-Virus Compatibility:Match Peer
 Information:Connection status: up Version:1 State: passive-
controller (last 1 days) Device Information:Management IPv4
 Address:10.10.20.112/24 Management IPv6 Address:Connection up;
 Primary HA1 link Election Option Information:Priority: secondary
```

```
 Preemptive: no Configuration Synchronization:Enabled: yes Running
 Configuration: synchronized
```

需要權限層級

superuser, deviceadmin

request high-availability sync-to-remote

說明

在 WildFire 設備叢集上，同步本機控制器節點的候選設定或執行中的設定，或本機控制器節點的時鐘（時間和日期）至遠端高可用性 (HA) 對等控制器節點。

階層位置

request high-availability

語法

```
request { high-availability { sync-to-remote { candidate-config;
 clock; running-config; } } }
```

選項

> `candidate-config`—同步本機對等控制器節點上的候選設定至遠端 HA 對等控制器節點。

> `clock`—同步本機對等控制器節點上的時鐘（時間與日期）至遠端 HA 對等控制器節點。

> `running-config`—同步本機對等控制器節點上執行中的設定至遠端 HA 對等控制器節點。

範例輸出

輸出中反白顯示的行表示 HA 設定狀態已在 HA 對等控制器節點上同步。

```
admin@wf-500(active-controller)> show high-availability state
 High-Availability:Local Information:版本：1 State: active-
controller (last 1 days) Device Information:Management IPv4
 Address:10.10.10.14/24 Management IPv6 Address:HA1 Control
 Links Joint Configuration:Encryption Enabled: no Election
 Option Information:Priority: primary Preemptive: no Version
 Compatibility:Software Version:Match Application Content
 Compatibility:Match Anti-Virus Compatibility:Match Peer
 Information:Connection status: up Version:1 State: passive-
controller (last 1 days) Device Information:Management IPv4
 Address:10.10.20.112/24 Management IPv6 Address:Connection up;
 Primary HA1 link Election Option Information:Priority: secondary
 Preemptive: no Configuration Synchronization:Enabled: yes Running
 Configuration: synchronized
```

需要權限層級

superuser, deviceadmin

request system raid

說明

使用此選項可管理安裝在 WildFire 設備中的 RAID 配對。WF-500 設備在前四個磁碟機擴充插槽 (A1、A2、B1、B2) 中隨附四個磁碟機。磁碟機 A1 與 A2 是 RAID 1 配對，磁碟機 B1 與 B2 是第二個 RAID 1 配對。

階層位置

request system

語法

```
raid { remove <value>; OR... copy { from <value>; to <value>; } OR...
 add {
```

選項

> `add`—新增磁碟至相應 RAID 磁碟組中

> `copy`—將磁碟機擴充插槽中的一個磁碟複製並移轉至另一個磁碟

> `remove`—從 RAID 磁碟組中移除磁碟

範例輸出

以下輸出為 RAID 設定正確的 WF-500 設備。

```
admin@WF-500> show system raid Disk Pair A Available Disk id A1
 Present Disk id A2 Present Disk Pair B Available Disk id B1 Present
 Disk id B2 Present
```

需要權限層級

superuser, deviceadmin

request wildfire sample redistribution

說明

重新分配本機 WildFire 設備叢集節點中的樣本，並選擇性地將樣本保留在本機節點上。

階層位置

```
request system
```

語法

```
request { wildfire { sample { redistribution {     keep-local-copy {no
 | yes};     serial-number <value>; } } } }
```

選項

* keep-local-copy—在本機 WildFire 設備節點上保留或不保留重新分配的樣本複本。
* serial-number—您重新分配樣本至的節點的序號。

範例輸出

Storage Nodes 顯示本機節點重新分配樣本至的其他節點。如果本機節點沒有在重新分配樣本，則只會顯示一個儲存節點位置。如果本機節點正在重新分配樣本，Storage Nodes 會顯示兩個儲存節點位置。反白顯示的輸出顯示儲存樣本的兩個儲存節點（本機節點和本機節點重新分配樣本至的節點），並確認樣本重新分配正在進行。

```
admin@WF-500> show wildfire global sample-
analysis Last Created 100 Malicious Samples
 +-------------------------------------------------------------------------
+ | SHA256 | Finish Date | Create Date | Malicious |
 +-------------------------------------------------------------------------
+ | <HASH VALUE> | 2017-03-24 17:27:40 | 2017-03-24 15:41:47 | Yes |
  | <HASH VALUE> | 2017-03-24 17:26:46 | 2017-03-24 15:41:45 | Yes |
  | <HASH VALUE> | 2017-03-24 17:26:54 | 2017-03-24 15:41:45 | Yes |
  | <HASH VALUE> | 2017-03-24 17:25:12 | 2017-03-24 15:41:44 | Yes |
  | <HASH VALUE> | 2017-03-24 17:24:28 | 2017-03-24 15:41:44 | Yes |
  | <HASH VALUE> | 2017-03-24 17:23:58 | 2017-03-24 15:41:44 | Yes |
  | <HASH VALUE> | 2017-03-24 17:26:52 | 2017-03-24 14:55:23 | Yes |
  | <HASH VALUE> | 2017-03-24 17:23:32 | 2017-03-24 14:55:23 | Yes |
  | <HASH VALUE> | 2017-03-24 17:24:58 | 2017-03-24 14:55:23 | Yes |
  | <HASH VALUE> | 2017-03-24 17:22:02 | 2017-03-24 14:55:23 | Yes |
 +-------------------------------------------------------------------------
+
 +-----------------------------------------------------------------------
+ | Storage Nodes | Analysis Nodes | Status | File Type |
 +-----------------------------------------------------------------------
+ | 0907:ld2_2,065:ld2_2 | qa116 | Notify Finish | Java JAR |
  | 0097:ld2_2,004:ld2_2 | qa117 | Notify Finish | Java Class
  | | 0524:ld2_2,006:ld2_2 | qa117 | Notify Finish | Java
 Class | | 0656:ld2_2,524:ld2_2 | qa117 | Notify Finish |
 Java Class | | 0024:ld2_2,056:ld2_2 | qa117 | Notify Finish
 | DLL | | 0324:ld2_2,006:ld2_2 | qa117 | Notify Finish |
 Java JAR | | 0682:ld2_2,006:ld2_2 | qa116 | Notify Finish |
 Java JAR | | 0092:ld2_2,016:ld2_2 | qa116 | Notify Finish |
 DLL | | 0682:ld2_2,002:ld2_2 | qa116 | Notify Finish | DLL
```

```
 | | 0056:ld2_2,824:ld2_2 | qa117 | Notify Finish | DLL |
 +-------------------------------------------------------------------
* lines 1-10
```

需要權限層級

superuser, deviceadmin

request system wildfire-vm-image

在用來分析檔案的 WildFire 設備虛擬電腦 (VM) 沙箱影像檔上執行升級。若要從 Palo Alto Networks 更新伺服器擷取新的 VM 影像檔，您必須先手動下載影像檔，將它放在啟用 SCP 的伺服器上，接著使用 SCP 用戶端從設備擷取影像檔。將影像檔下載到設備之後，您可以使用此命令來安裝。

階層位置

request system

語法

```
request { system { wildfire-vm-image { upgrade install file
 <value>; } } }
```

選項

`> wildfire-vm-image`—安裝虛擬電腦 (VM) 影像檔。

`+ upgrade install file`—執行 VM 影像檔升級。在檔案選項後輸入 **?** 來檢視可用的 VM 影像檔清單。例如，執行下列命令以列出可用的影像檔：

```
admin@WF-500> request system wildfire-vm-image upgrade install file ?
```

範例輸出

若要列出可用的 VM 影像檔，請執行下列命令：

```
admin@WF-500> request system wildfire-vm-image upgrade install
 file ?若要安裝 VM 影像檔（在此範例中為 Windows 7 64 位元），請執行下列命
令：admin@WF-500> request system wildfire-vm-image upgrade install
 file WFWin7_64Base_m-1.0.0_64base
```

需要權限層級

superuser, deviceadmin

request wf-content

在 WildFire 設備上執行內容更新。這些內容更新會為設備配備最新的威脅資訊，以精確偵測惡意軟體並提升設備區分惡意及良性軟體的能力。若要排程內容更新以自動安裝，請參閱設定裝置設定系統更新排程，若要在 WildFire 設備上刪除內容更新，請參閱刪除 Wildfire 中繼資料。

階層位置

```
request
```

語法

```
request wf-content { downgrade install {previous | <value>}; upgrade
 { check download latest info install { file <filename> version
 latest; } } }
```

選項

`> downgrade` — 安裝先前的內容版本。使用先前的選項來安裝之前安裝的內容套件，或輸入值以降級為特定內容套件號碼。

`> upgrade` — 執行內容升級功能

`> check` — 從 Palo Alto Networks 更新伺服器上取得可用內容套件的資訊

`> download` — 下載內容套件

`> info` — 顯示可用內容套件的相關資訊

`> install` — 安裝內容套件

`> file` — 指定包含內容套件的檔案名稱

`> version` — 根據內容套件的版本號碼下載或升級

範例輸出

若要列出可用的內容更新，請執行下列命令：

```
admin@WF-500> request wf-content upgrade check
 Version Size Released on Downloaded Installed
 ---------------------------------------------------------------------------
 2-217 58MB 2014/07/29 13:04:55 PDT yes current 2-188 58MB 2014/07/01
 13:04:48 PDT yes previous 2-221 59MB 2014/08/02 13:04:55 PDT no no
```

需要權限層級

superuser, deviceadmin

save wildfire api-key

說明

使用儲存命令將 WildFire 設備上的所有 API 金鑰儲存至檔案。您接著可以匯出金鑰檔案以進行備份，或大量修改金鑰。如需在 WildFire 設備上使用 WildFire API 的詳細資料，請參閱 WildFire API 參考。

階層位置

```
save
```

語法

```
save { wildfire { api-key to <value>; { {
```

選項

`* to` — 輸入金鑰匯出的檔案名稱。例如，若要將 WildFire 上的所有 API 金鑰匯出到名為 my-wf-keys 的檔案，請輸入下列命令：

```
admin@WF-500> save wildfire api-key to my-wf-keys
```

需要權限層級

superuser, deviceadmin

set wildfire portal-admin

說明

設定入口網站管理帳戶密碼，管理員將使用此密碼來檢視由 WildFire 設備產生的 WildFire 分析報告。在防火牆上檢視報告或從 Panorama **Monitor**（監控） > **WildFire Submissions**（**WildFire** 提交） > **View WildFire Report**（檢視 **WildFire** 報告） 中檢視報告時需要帳戶名稱（管理員）及密碼。預設的使用者名稱和密碼是 admin/admin。

入口網站管理員帳戶是您在設備上設定以從防火牆或 *Panorama* 檢視報告的唯一一個帳戶。您無法建立新帳戶或變更帳戶名稱。這是用來管理設備所用的同一個管理員帳戶。

階層位置

```
set wildfire
```

語法

```
set { wildfire { portal-admin { password <value>; } }
```

範例輸出

以下為此命令的輸出。

```
admin@WF-500> set wildfire portal-admin password Enter
 password:Confirm password:
```

需要權限層級

superuser, deviceadmin

show cluster all-peers

說明

在 WildFire 設備叢集控制器節點上，顯示所有 WildFire 設備叢集成員的狀態，包括 WildFire 設備模式（控制器或工作）、連線狀態及應用程式服務狀態。

階層位置

```
show cluster
```

語法

```
all-peers;
```

選項

無額外的選項。

範例輸出

```
admin@thing1(active-controller)> show cluster all-peers Address Mode
 Server Node Name ------- ---- ------ --------- 10.10.10.14
 controller Self True thing1 Service: infra signature wfcore wfpc
 Status:Connected, Server role applied Changed:Wed, 15 Feb 2017
 09:12:01 -0800 WF App: wildfire-apps-service:Ready global-db-
service:JoinedCluster global-queue-service:JoinedCluster siggen-
db:ReadyMaster 10.10.10.112     controller Peer True thing2
 Service: infra signature wfcore wfpc Status:Connected, Server role
 applied Changed:Wed, 15 Feb 2017 09:13:00 -0800 WF App: wildfire-
apps-service:Ready global-db-service:ReadyLeader global-queue-
service:ReadyLeader siggen-db:ReadySlave Diag report:10.10.10.112:
```

```
 reported leader '10.10.10.112', age 0. 10.10.10.14: local node
 passed sanity check.
```

需要權限層級

superuser, deviceadmin

show cluster controller

說明

在 WildFire 設備叢集控制器節點上，顯示 WildFire 設備叢集控制器的狀態，包括叢集名稱和本機控制器節點的角色（如果 `Active Controller` 欄位顯示 `True`，表示本機控制器為主要控制器，如果 `Active Controller` 欄位顯示 `False`，表示本機控制器為備份控制器）。

階層位置

```
show cluster
```

語法

```
controller;
```

選項

無額外的選項。

範例輸出

```
admin@thing1(active-controller)> show cluster controller
 Cluster name: satriani1 K/V API online:True Task processing:
 on Active Controller:True DNS Advertisement:App Service
 DNS Name:App Service Avail:10.10.10.112, 10.10.10.14 Core
 Servers:009707000742:10.10.10.112 009701000043:10.10.10.14 Good Core
 Servers:2 Suspended Nodes:Current Task: no tasks found
```

需要權限層級

superuser, deviceadmin

show cluster data migration status

說明

從 WildFire 設備叢集控制器節點使用此命令以顯示目前的資料移轉狀態。此命令顯示資料移轉於何時開始及進度。資料移轉完成時，此命令顯示完成時間戳記。如果資料移轉失敗，狀態將顯示 `0%` 完成。

階層位置

```
show cluster
```

語法

```
data-migration-status;
```

選項

無額外的選項。

範例輸出

```
adminWF-500(active-controller)> show cluster data-migration-status
 100% completed on Mon Sep 9 21:44:48 PDT 2019
```

需要權限層級

superuser, deviceadmin

show cluster membership

說明

針對叢集節點或獨立 WildFire 設備，顯示 WildFire 設備叢集成員資訊，包括 IP 地址、主機名稱、WildFire 設備序號、設備的角色 (`Node mode`)、高可用性優先順序及應用狀態。

階層位置

```
show cluster
```

語法

```
membership;
```

選項

無額外的選項。

範例輸出

您可以針對 WildFire 設備叢集節點成員（控制器和工作節點）與獨立 WildFire 設備，顯示叢集成員資訊，以確認其是否屬於叢集、其應用狀態及其他本機主機資訊。輸出視乎 WildFire 設備的角色而稍有不同。區別在於：

- 提示表示主動（主要）控制器節點和被動（備份）控制器節點，不表示工作節點或獨立節點。
- `Node mode` 表示 WildFire 設備是否為 `controller node`、`worker node` 或 `stand_alone` WildFire 設備。
- 對於主動控制器節點，`HA priority` 顯示 `primary`，對於被動（備份）控制器節點顯示 `secondary`，而對於工作節點和獨立 WildFire 設備，此欄位為空。
- `Application status` 欄位在部分欄位顯示不同值。對於 `global-db-service` 和 `global-queue-service`，叢集成員顯示 `ReadyLeader` 中 `JoinedCluster`，而獨立設備顯示 `ReadyStandalone`。

  對於 `siggen-db`，WildFire 設備叢集的主要控制器節點顯示 `ReadyMaster`，WildFire 設備叢集的次要控制器節點顯示 `ReadySlave`，WildFire 設備叢集工作節點顯示 `Ready`，且獨立 WildFire 設備顯示 `ReadyMaster`。

  所顯示每個 *WildFire* 設備序號的最後四位數會變更為「*xxxx*」，防止洩露真正序號。

WildFire 設備叢集中主要控制器節點上的輸出為：

```
admin@thing1(active-controller)> show cluster membership Service
 Summary: wfpc signature Cluster name: satriani1 Address:10.10.10.14
 Host name: thing1 Node name: wfpc-00970100xxxx-internal Serial
 number:00970100xxxx Node mode: controller Server role:True HA
 priority: primary Last changed:Wed, 15 Feb 2017 09:12:01 -0800
 Services: wfcore signature wfpc infra Monitor status:Serf Health
 Status: passing Agent alive and reachable Application status:
 wildfire-apps-service:Ready global-db-service:JoinedCluster global-
queue-service:JoinedCluster siggen-db:ReadyMaster
```

WildFire 設備叢集中控制器備份節點上的輸出為：

```
admin@thing2(passive-controller)> show cluster membership Service
 Summary: wfpc signature Cluster name: satriani1 Address:10.10.10.112
 Host name: thing2 Node name: wfpc-00970700xxxx-internal Serial
 number:009707000xxxx Node mode: controller Server role:True HA
 priority: secondary Last changed:Wed, 15 Feb 2017 09:13:10 -0800
 Services: wfcore signature wfpc infra Monitor status:Serf Health
 Status: passing Agent alive and reachable Application status:
 wildfire-apps-service:Ready global-db-service:ReadyLeader global-
queue-service:ReadyLeader siggen-db:ReadySlave
```

WildFire 設備叢集中工作節點上的輸出為：

```
admin@grinch> show cluster membership Service Summary: wfpc Cluster
 name: satriani1 Address:10.10.10.19 Host name: grinch Node name:
 wfpc-00970100xxxx-internal Serial number:00970100xxxx Node mode:
 worker Server role:True HA priority:Last changed:Thu, 09 Feb 2017
 15:55:55 -0800 Services: wfcore wfpc infra Monitor status:Serf
 Health Status: passing Agent alive and reachable Application status:
 wildfire-apps-service:Ready global-db-service:JoinedCluster global-
queue-service:JoinedCluster siggen-db:準備就緒
```

獨立 WildFire 設備（不是 WildFire 設備叢集成員）的輸出為：

```
admin@max> show cluster membership Service Summary: wfpc signature
 Cluster name:Address:10.10.10.90 Host name: max Node name:
 wfpc-00970700xxxx-internal Serial number:00970700xxxx Node mode:
 stand_alone Server role:True HA priority:Last changed:Mon, 13
 Feb 2017 02:54:52 -0800 Services: wfcore signature wfpc infra
 Monitor status:Serf Health Status: passing Agent alive and
 reachable Application status: wildfire-apps-service:Ready global-db-
service:ReadyStandalone global-queue-service:ReadyStandalone siggen-
db:ReadyMaster
```

需要權限層級

superuser, deviceadmin

show cluster task

說明

針對本機叢集節點或所有叢集節點，顯示 WildFire 設備叢集工作資訊，或顯示已完成的叢集工作歷程記錄或擱置中的叢集工作。

階層位置

```
show cluster
```

語法

```
task { current; history; local; pending; }
```

選項

> `current`— 顯示 WildFire 設備叢集上目前允許的工作。僅適用於叢集控制器節點。

> `history`— 顯示已完成的叢集工作。僅適用於叢集控制器節點。

> `local`— 顯示本機 WildFire 設備叢集節點上擱置中的工作。

> `pending`— 顯示整個 WildFire 設備叢集擱置中的工作。僅適用於叢集控制器節點。

範例輸出

```
admin@WF-500(active-controller)> show cluster task local
 Request:        reboot from WF-500 (009701000034/74702) at
 2017-02-21 03:06:45 UTC                Reboot requested by
 admin Queued:         by WF-500                2/3 core servers
 available. reboot not allowed to maintain quorum Request:
 reboot from WF-500 (009701000034/74704) at 2017-02-21 03:10:27 UTC
                 Reboot requested by admin Queued:         by WF-500
                 2/3 core servers available. reboot not allowed to
 maintain quorum admin@WF-500(active-controller)> show cluster task
 current no tasks found admin@WF-500(active-controller)> show cluster
 task pending Request:        reboot from WF-500 (009701000034/74702)
 at 2017-02-21 03:06:45 UTC                Reboot requested by
 admin Queued:         by WF-500                2/3 core servers
 available. reboot not allowed to maintain quorum Request:
  reboot from WF-500 (009701000034/74704) at 2017-02-21 03:10:27
 UTC                Reboot requested by admin Queued:
  by WF-500                2/3 core servers available.
 reboot not allowed to maintain quorum admin@WF-500B(passive-
controller)> show cluster task history Request:        reboot
 from WF-500 (009701000044/35533) at 2017-02-17 19:21:53 UTC
                 Reboot requested by admin Response:
 permit by WF-500B at 2017-02-17 22:11:31 UTC
  request not affecting healthy core server.Progress:
 Wait for kv store ready for query...                KV store
 is ready, wait for cluster leader available...
  Cluster leader is 10.10.10.100...                Checking
 is sysd and clusterd are alive...               Checking if
 cluster-mgr is ready...               Checking global-db-cluster
 readiness...              Stopping global-queue server and leaving
 cluster...               Stopping global-db servers and doing
 failover...                rebooting...Finished:       success at
 2017-02-17 22:17:56 UTC
```

需要權限層級

superuser, deviceadmin

show high-availability all

說明

顯示所有 WildFire 設備叢集高可用性 (HA) 資訊，包括 HA 控制連結、HA 狀態、HA 轉換資訊、對等軟體、內容更新、防毒軟體相容性資訊及對等連線和角色資訊。

階層位置

```
show high-availability
```

語法

```
all;
```

選項

無額外的選項。

範例輸出

```
admin@thing1(active-controller)> show high-availability all High-
Availability:Local Information:版本：1 State: active-controller (last
 1 days) Device Information:Management IPv4 Address:10.10.10.14/24
 Management IPv6 Address:HA1 Control Links Joint Configuration:Link
 Monitor Interval:3000 ms Encryption Enabled: no HA1 Control Link
 Information:IP 位址：10.10.10.140/24 MAC Address:00:00:5e:00:53:ff
 Interface: eth3 Link State:Up; Setting:1Gb/s-full Key
 Imported : no Election Option Information:Priority: primary
 Preemptive: no Promotion Hold Interval:2000 ms Hello Message
 Interval:8000 ms Heartbeat Ping Interval:2000 ms Preemption
 Hold Interval:1 min Monitor Fail Hold Up Interval:0 ms Addon
 Master Hold Up Interval:500 ms Version Information:Build
 Release:8.0.1-c31 URL Database:Not Installed Application
 Content:497-2688 Anti-Virus:0 Version Compatibility:Software
 Version:Match Application Content Compatibility:Match Anti-
Virus Compatibility:Match Peer Information:Connection status:
 up Version:1 State: passive-controller (last 1 days) Device
 Information:Management IPv4 Address:10.10.10.30/24 Management
 IPv6 Address:HA1 Control Link Information:IP 位址：10.10.10.130 MAC
 Address:00:00:5e:00:53:00 Connection up; Primary HA1 link Election
 Option Information:Priority: secondary Preemptive: no Version
 Information:Build Release:8.0.1-c31 URL Database:Not Installed
 Application Content:497-2688 Anti-Virus:0 Initial Monitor Hold
 inactive; Allow Network/Links to Settle:Link and path monitoring
 failures honored Configuration Synchronization:Enabled: yes Running
 Configuration: synchronized
```

需要權限層級

superuser, deviceadmin

show high-availability control-link

說明

針對主要和備份控制器節點之間的 HA 控制連結，顯示 WildFire 設備叢集高可用性 (HA) 統計資料，包括 HA 控制連結上傳輸和接收的各種訊息的數量、邊線失敗次數及偵測活動數量。

階層位置

```
show high-availability
```

語法

```
control-link { statistics; }
```

選項

`> statistics`— 顯示 WildFire 設備叢集控制器節點 HA 控制連結統計資料。

範例輸出

```
admin@thing1(active-controller)> show high-availability control-link
 statistics High-Availability:Control Link Statistics:HA1: Messages-
TX :13408 Messages-RX :13408 Capability-Msg-TX :2 Capability-Msg-
RX :2 Error-Msg-TX :0 Error-Msg-RX :0 Preempt-Msg-TX :0 Preempt-Msg-
RX :0 Preempt-Ack-Msg-TX :0 Preempt-Ack-Msg-RX :0 Primary-Msg-TX :1
 Primary-Msg-RX :1 Primary-Ack-Msg-TX :1 Primary-Ack-Msg-RX :1 Hello-
Msg-TX :13402 Hello-Msg-RX :13402 Hello-Timeouts :0 Hello-Failures :0
 MasterKey-Msg-TX :1 MasterKey-Msg-RX :1 MasterKey-Ack-Msg-TX :1
 MasterKey-Ack-Msg-RX :1 Connection-Failures :0 Connection-Tries-
Failures :12 Connection-Listener-Tries :1 Connection-Active-Tries :12
 Ping-TX :53614 Ping-Fail-TX :0 Ping-RX :53613 Ping-Timeouts :0 Ping-
Failures :0 Ping-Error-Msgs :0 Ping-Other-Msgs :0 Ping-Last-Rsp :1
```

需要權限層級

superuser, deviceadmin

show high-availability state

說明

針對本機和對等叢集控制器節點，顯示 WildFire 設備叢集高可用性 (HA) 狀態資訊，包括控制器節點為主動（主要）還是被動（備份）節點、控制器節點處於 HA 設定狀態已有多長時間、本機和對等控制器節點設定是否已同步，以及軟體、內容更新及防毒軟體版本在對等控制器節點之間是否相容。

階層位置

```
show high-availability
```

語法

```
state;
```

選項

無額外的選項。

範例輸出

```
admin@thing1(active-controller)> show high-availability state
 High-Availability:Local Information:版本：1 State: active-
controller (last 1 days) Device Information:Management IPv4
 Address:10.10.10.14/24 Management IPv6 Address:HA1 Control
 Links Joint Configuration:Encryption Enabled: no Election
 Option Information:Priority: primary Preemptive: no Version
 Compatibility:Software Version:Match Application Content
 Compatibility:Match Anti-Virus Compatibility:Match Peer
 Information:Connection status: up Version:1 State: passive-
controller (last 1 days) Device Information:Management IPv4
 Address:10.10.10.30/24 Management IPv6 Address:Connection up;
 Primary HA1 link Election Option Information:Priority: secondary
 Preemptive: no Configuration Synchronization:Enabled: yes Running
 Configuration: synchronized
```

需要權限層級

superuser, deviceadmin

show high-availability transitions

說明

針對叢集控制器節點，顯示 HA 轉換過程中所發生事件的 WildFire 設備叢集高可用性 (HA) 轉換資訊。

階層位置

```
show high-availability
```

語法

```
transitions;
```

選項

無額外的選項。

範例輸出

```
admin@thing1(active-controller)> show high-availability transitions
 High-Availability:Transition Statistics:Unknown :1 Suspended :0
 Initial :0 Non-Functional :0 Passive :0 Active :3
```

需要權限層級

superuser, deviceadmin

show system raid

說明

顯示 WildFire 設備的 RAID 設定。WF-500 設備在前四個磁碟機擴充插槽 (A1、A2、B1、B2) 中隨附四個磁碟機。磁碟機 A1 與 A2 是 RAID 1 配對，磁碟機 B1 與 B2 是第二個 RAID 1 配對。

階層位置

```
show system
```

語法

```
raid { detail; {
```

選項

無額外的選項。

範例輸出

以下顯示運作中 WF-500 設備的 RAID 設定。

```
admin@WF-500> show system raid detail Disk Pair A Available Status
 clean Disk id A1 Present model :ST91000640NS size :953869 MB
 partition_1 : active sync partition_2 : active sync Disk id A2
 Present model :ST91000640NS size :953869 MB partition_1 : active
 sync partition_2 : active sync Disk Pair B Available Status
 clean Disk id B1 Present model :ST91000640NS size :953869 MB
 partition_1 : active sync partition_2 : active sync Disk id B2
 Present model :ST91000640NS size :953869 MB partition_1 : active
 sync partition_2 : active sync
```

需要權限層級

superuser, superreader

submit wildfire local-verdict-change

說明

針對防火牆已提交的樣本，變更本機產生的 WildFire 裁定。裁定變更僅套用至已提交到 WildFire 設備的樣本，且相同樣本的裁定在 WildFire 公共雲端中保持不變。您可以使用 show wildfire global 命令檢視裁定已變更的樣本。

WildFire 私人雲端內容套件已更新，以反映您做出的任何裁定變更（在防火牆上，選取 **Device**（裝置）> **Dynamic Updates**（動態更新）> **WF-Private**（**WF**-私人）以啟用 WildFire 私人雲端內容更新）。當您將樣本裁定變更為惡意時，WildFire 設備會產生新的特徵碼以偵測惡意軟體，並將該特徵碼新增至 WildFire 私人雲端內容套件。當您將樣本裁定變更為良性時，WildFire 設備會從 WildFire 私人雲端內容套件移除特徵碼。

還可以使用 API 呼叫來變更本機樣本的裁定。如需詳細資訊，請參閱 WildFire API 參考。

階層位置

```
submit wildfire
```

語法

```
submit { wildfire { local-verdict-change { hash <value>; verdict
 <value>; comment <value>; } }
```

選項

* `hash` — 為您要變更裁定的檔案指定 SHA-256 雜湊算法。
* `verdict` — 輸入新檔案裁定：0 表示良性樣本；1 表示惡意樣本；2 表示灰色樣本。
* `comment` — 包含描述裁定變更的註解。

範例輸出

以下為此命令的輸出。

```
admin@WF-500> submit wildfire local-verdict-change comment test hash
 c323891a87a8c43780b0f2377de2efc8bf856f02dd6b9e46e97f4a9652814b5c
 verdict 2 Please enter 'Y' to commit: (y or n) verdict is changed
 (old verdict:1, new verdict:2)
```

需要權限層級

superuser, deviceadmin

show wildfire

說明

顯示關於 WildFire 設備的各種資訊，例如全球和本機裝置、與樣本相關的詳細資訊、設備狀態，及選取執行分析的虛擬電腦。

階層位置

```
show wildfire
```

語法

```
status | vm-images | wf-vm-pe-utilization | wf-vm-doc-utilization
 | wf-vm-email-link-utilization | wf-vm-archive-utilization | wf-
sample-queue-status }
```

選項

`> status` — 顯示設備狀態以及設定資訊，例如用於分析樣本的虛擬電腦 (VM)、樣本/報告是否傳送至雲端、VM 網路以及註冊資訊。

`> vm-images` — 顯示用來分析樣本的可用虛擬電腦影像檔的屬性。若要檢視目前使用中的影像檔，請執行下列命令：

```
admin@WF-500> show wildfire status
```

and view the `VM field`。

`> wf-sample-queue-status` — 顯示等待分析的 WildFire 設備樣本數目及詳細資訊。

`> wf-vm-doc-utilization` — 顯示用於處理文件的可供使用及使用中的分析環境數目。

`> wf-vm-elinkda-utilization` — 顯示用於處理電子郵件連結的可供使用及使用中的分析環境數目。

`> wf-vm-doc-utilization` — 顯示用於處理可攜式執行檔檔案的可供使用及使用中的分析環境數目。

範例輸出

以下為此命令的輸出。

```
admin@WF-500> show wildfire status Connection info:Wildfire
 cloud: s1.wildfire.paloaltonetworks.com Status:Idle Submit
 sample: disabled Submit report: disabled Selected VM: vm-5 VM
 internet connection: disabled VM network using Tor: disabled Best
 server:                    s1.wildfire.paloaltonetworks.com Device
 registered: yes Service route IP address:10.3.4.99 Signature
```

```
 verification: enable Server selection: enable Through a proxy: no
 admin@WF-500> show wildfire vm-images Supported VM images: vm-1
 Windows XP, Adobe Reader 9.3.3, Flash 9, Office 2003.Support PE,
 PDF, Office 2003 and earlier vm-2 Windows XP, Adobe Reader 9.4.0,
 Flash 10n, Office 2007.Support PE, PDF, Office 2007 and earlier
 vm-3 Windows XP, Adobe Reader 11, Flash 11, Office 2010.Support PE,
 PDF, Office 2010 and earlier vm-4 Windows 7 32bit, Adobe Reader 11,
 Flash 11, Office 2010.Support PE, PDF, Office 2010 and earlier vm-5
 Windows 7 64bit, Adobe Reader 11, Flash 11, Office 2010.Support
 PE, PDF, Office 2010 and earlier vm-6 Windows XP, Internet Explorer
 8, Flash 11.Support E-MAIL Links admin@WF-500> show wildfire wf-
sample-queue-status DW-ARCHIVE:4, DW-DOC:2, DW-ELINK:0, DW-PE:21, DW-
URL_UPLOAD_FILE:2, admin@WF-500> show wildfire wf-vm-pe-utilization
 { available:2, in_use:1, }
```

需要權限層級

superuser, superreader

show wildfire global

說明

顯示關於全球裝置的各種資訊和樣本狀態，例如可用的 API 金鑰、註冊資訊、樣本裁定變更、活動、樣本裝置原始來源及設備最近分析過的樣本。

階層位置

```
show wildfire global
```

語法

```
api-keys { all { details; } key <value>; } devices-reporting-data;
 last-device-registration { all; } local-verdict-change { all; sha256
 <value>; } } sample-analysis { number; type; } } sample-device-
lookup { sha256 { equal <value>; } sample-status { sha256 { equal
 <value>; } } signature-status { sha256 { equal <value>; } }
```

選項

`> api-keys` — 顯示在 WildFire 設備上產生的 API 金鑰詳細資料。您可以檢視上次使用金鑰的時間、金鑰名稱、狀態（啟用或停用），以及產生金鑰的日期/時間。

`> devices-reporting-data` — 顯示最新的註冊活動。

`> last-device-registration` — 顯示最新的註冊活動。

`> local-verdict-change` — 顯示裁定已變更的樣本。

`> sample-analysis` — 顯示 Wildfire 對最多 1,000 樣本的分析結果。

> `sample-status` — 顯示 wildfire 樣本狀態。輸入檔案的 SHA256 值來檢視目前的分析狀態。

> `sample-device-lookup` — 顯示傳送所指定 SHA256 樣本的防火牆。

> `signature-status` — 顯示 Wildfire 特徵碼狀態。輸入檔案的 SHA256 值來檢視目前的分析狀態。

範例輸出

以下為此命令的輸出。

```
admin@WF-500> show wildfire global api-keys all +------------
+-----------+---------+---------------------+---------------------
+ | Apikey | Name | Status | Create Time | Last Used Time |
 +------------+-----------+---------+---------------------
+---------------------+ | <API KEY> | happykey1 | Enabled |
 2017-03-01 23:21:02 | 2017-03-01 23:21:02 | +------------
+-----------+---------+---------------------+---------------------
+ admin@WF-500> show wildfire global devices-reporting-data
 +--------------+---------------------+-------------+------------
+----------+--------+ | _Device ID | Last Registered | Device IP | SW
 Version | HW Model | Status | +--------------+---------------------
+-------------+------------+----------+--------+ | 000000000000
 | 2017-03-01 22:28:25 | 10.1.1.1 | 8.1.4 | PA-220 | OK |
 +--------------+---------------------+-------------+------------
+----------+--------+ admin@WF-500> show wildfire global last-
device-registration all +--------------+---------------------
+-------------+------------+----------+--------+ | Device
 ID | Last Registered | Device IP | SW Version | HW Model |
 Status | +--------------+---------------------+-------------
+------------+----------+--------+ | 000000000000 | 2017-07-31
 12:35:53 | 10.1.1.1 | 8.1.4 | PA-220 | OK | +--------------
+---------------------+-------------+------------+----------
+--------+ admin@WF-500> show wildfire global local-verdict-change
 +-------------------------------------------------------------------
+---------+--------+ | SHA256 | Verdict | Source |
 +-------------------------------------------------------------------
+---------+--------+ |
 c883b5d2e16d22b09b176ca0786128f8064d47edf26186b95845aa3678868496| 2
 -> 1 | Yes |
 +-------------------------------------------------------------------
+---------+--------+ admin@WF-500> show wildfire global sample-
analysis Last Created 100 Malicious Samples +--------------
+---------------------+---------------------+-----------+ |
 SHA256 | Finish Date | Create Date | Malicious | +--------------
+---------------------+---------------------+-----------+ |
 <HASH VALUE> | 2017-03-01 23:27:57 | 2017-03-01 23:27:57 | Yes
 | +--------------+---------------------+--------------------
+-----------+ +---------------------+----------------
+---------------+----------------+ | Storage Nodes | Analysis Nodes
 | Status | File Type | +---------------------+----------------
+---------------+----------------+ | 00926ld1_2,0094:d1_2 |
 qa16 | Notify Finish | Elink File | +---------------------
+----------------+---------------+----------------+ Last Created
 100 Non-malicious Samples +--------------+--------------------
```

```
+----------------------+-----------+ | SHA256 | Finish Date |
 Create Date | Malicious | +--------------+--------------------
+----------------------+-----------+ | <HASH VALUE> | 2017-03-01
 23:31:15 | 2017-03-01 23:24:29 | No | +--------------
+----------------------+----------------------+-----------+
 +----------------------+----------------+--------------
+--------------------+ | Storage Nodes | Analysis Nodes |
 Status | File Type | +----------------------+----------------
+---------------+--------------------+ | 0712:smp_27,94:smp_7 |
 qa16 | Notify Finish | MS Office document | +----------------------
+----------------+--------------+--------------------+
 admin@WF-500> show wildfire global sample-device-lookup sha256 equal
 d75f2f71829153775fa33cf2fa95fd377f153551aadf0a642704595100efd460
 Sample
 1024609813c57fe174722c53b3167dc3cf5583d5c7abaf4a95f561c686a2116e
 last seen on following devices:
 +-------------------------------------------------------------------
+-----------+-----------+--------------------+ |
 SHA256 | Device ID | Device IP | Submitted Time |
 +-------------------------------------------------------------------
+-----------+-----------+--------------------+ |
 1024609813c57fe174722c53b3167dc3cf5583d5c7abaf4a95f561c686a2116e
 | Manual | Manual | 2019-08-05 19:24:39 |
 +-------------------------------------------------------------------
+-----------+-----------+--------------------+
 admin@WF-500> show wildfire global sample-status sha256 equal
 dc9f3a2a053c825e7619581f3b31d53296fe41658b924381b60aee3eeea4c088
 +----------------------+----------------------+-----------
+---------------------------+ | Finish Date | Create
 Date | Malicious | Storage Nodes | +--------------------
+----------------------+-----------+---------------------------
+ | 2017-03-01 22:34:17 | 2017-03-01 22:28:23 | No |
 009026:smp_27,097010smp_27 | +--------------------
+----------------------+-----------+---------------------------+
 +----------------+--------------+------------------+ | Analysis
 Nodes | Status | File Type | +----------------+--------------
+------------------+ | qa15 | Notify Finish | Adobe Flash
 File | +----------------+--------------+------------------
+ admin@WF-500> show wildfire global signature-status sha256
 equalc883b5d2e16d22b09b176ca0786128f8064d47edf26186b95845aa3678868496
 Signature Name:Virus/Win32.WPCGeneric.cr Current Status: released
 Release History: +--------------+---------------------+---------
+-------------+----------+ | Build Version | Timestamp | UTID |
 Internal ID | Status | +---------------+---------------------
+---------+-------------+----------+ | 155392 | 2017-02-03 10:11:06 |
 5000259 | 10411 | released | +---------------+---------------------
+---------+-------------+----------+
```

需要權限層級

superuser, superreader

show wildfire local

說明

顯示關於本機裝置和樣本的各種資訊，例如活動、設備最近分析過的樣本及基本 WildFire 統計資料。

階層位置

```
show wildfire local
```

語法

```
latest { analysis { filter malicious|benign; sort-by SHA256|Submit
 Time|Start Time|Finish Time|Malicious|Status; sort-direction asc|
desc; limit 1-20000; days 1-7; } OR... samples { filter malicious|
benign; sort-by SHA256|Create Time|File Name|File Type|File Size|
Malicious|Status; sort-direction asc|desc; limit 1-20000; days
 1-7; } sample-processed { count 1-1000; time {last-1-hr|last-12-
hrs|last-15-minutes|last-24-hrs|last-30-days|last-7-days|last-
calender-day|last-calender-month; } sample-status { sha256 { equal
 <value>; } } statistics days <1-31> | hours <0-24> | minutes
 <0-60>; }
```

選項

`> latest` — 顯示最新的 30 個活動，包括最新的 30 個分析活動、最近分析的 30 個檔案、已分析檔案和已上載至公共雲端伺服器檔案的網路工作階段資訊。

`> sample-processed` — 顯示在指定時間範圍內本機處理的樣本數目或最大樣本數目。

`> sample-status` — 顯示 wildfire 樣本狀態。輸入檔案的 SHA256 值來檢視目前的分析狀態。

`> statistics` — 顯示基本 wildfire 統計資料。

範例輸出

以下為此命令的輸出。

```
admin@WF-500> show wildfire latest analysis Latest
 analysis information: +-------------+---------------------
+----------------------+----------------------+ | SHA256 | Submit Time
 | Start Time | Finish Time | +-------------+--------------------
+----------------------+----------------------+ | <HASH VALUE>|
 2017-03-01 14:28:26 | 2017-03-01 14:28:26 | 2017-03-01 14:34:24 | |
 <HASH VALUE>| 2017-03-01 14:28:25 | 2017-03-01 14:28:25 | 2017-03-01
 14:28:41 | | <HASH VALUE>| 2017-03-01 14:28:25 | 2017-03-01 14:28:25
 | 2017-03-01 14:28:26 | +-------------+--------------------
+----------------------+----------------------+ +------------
+-------------------------------------------------------------
+-----------+ | Malicious | VM Image | Status | +------------
```

```
+-----------------------------------------------------------
+-----------+ | Yes | Windows 7 x64 SP1, Adobe Reader
 11, Flash 11, Office 2010 | completed | | No | Java/
Jar Static Analyzer | completed | | Suspicious |
 Java/Jar Static Analyzer | completed | +-----------
+-----------------------------------------------------------
+-----------+ admin@WF-500> show wildfire local latest samples
 Latest samples information: +--------------+--------------------
+----------------+---------------+ | SHA256 | Create Time |
 File Name | File Type | +--------------+--------------------
+----------------+---------------+ | <HASH VALUE> | 2017-03-01
 14:28:25 | | JAVA Class | | <HASH VALUE> | 2017-03-01
 14:28:25 | | JAVA Class | | <HASH VALUE> | 2017-03-01
 14:28:25 | | PE | +--------------+--------------------
+----------------+---------------+ +--------------+----------
+------------------+ | File Size | Malicious | Status |
 +--------------+----------+------------------+ | 20,407 |
 No | analysis complete | | 1,584 | Yes | analysis complete | |
 259,024 | No | analysis complete | +--------------+----------
+-------------------+ admin@WF-500> show wildfire local sample-
processed count 2 Time Window: last-15-minutes Display Count:2:
 +-----------------------------------------------------------------------
+---------------------+----------+------------+----------
+------------+------------------+ | SHA256 | Create Time
 | File Name | File Type | File Size | Malicious | Status |
 +-----------------------------------------------------------------------
+---------------------+----------+------------
+----------+------------+------------------+ |
 ce752b7b76ac2012bdff2b76b6c6af18e132ae8113172028b9e02c6647ee19bb |
 2018-12-09 16:55:53 | | Email Link | 31,522 | | download complete |
 | 349e57e51e7407abcd6eccda81c8015298ff5d5ba4cedf09c7353c133ceaa74b |
 2018-12-09 16:53:40 | | Email Link | 39,679 | | download complete |
 +-----------------------------------------------------------------------
+---------------------+----------+------------
+----------+------------+------------------+
 admin@WF-500> show wildfire local sample-status sha256 equal
 0f2114010d00d7fa453177de93abca9643f4660457536114898c56149f819a9b
 Sample information: +--------------------+----------
+----------------------------------+ | Create Time | File
 Name | File Type | +--------------------+----------
+----------------------------------+ | 2017-03-01 22:28:24 |
 rmr.doc | Microsoft Word 97 - 2003 Document | +--------------------
+----------+----------------------------------+ +----------
+----------+------------------+ | File Size | Malicious
 | Status | +----------+----------+------------------+ |
 133120 | Yes | analysis complete | +----------+----------
+------------------+ Analysis information: +--------------------
+--------------------+--------------------+------------+ | Submit
 Time | Start Time | Finish Time | Malicious | +--------------------
+--------------------+--------------------+------------+
 | 2017-03-01 22:28:24 | 2017-03-01 22:28:24 | 2017-03-01
 22:28:24 | Suspicious | | 2017-03-01 22:28:24 | 2017-03-01
 22:28:24 | 2017-03-01 22:34:07 | Yes | +--------------------
+--------------------+--------------------+------------+
 +-----------------------------------------------------------
+-----------+ | VM Image | Status |
```

```
 +-------------------------------------------------------------
+-----------+ | DOC/CDF Static Analyzer | completed | | Windows
 7 x64 SP1, Adobe Reader 11, Flash 11, Office 2010 | completed
 | +-------------------------------------------------------------
+-----------+ admin@WF-500> show wildfire local
 statistics Current Time:2017-03-01 17:44:31 Received
 After:2017-02-28 17:44:31 Received Before:2017-03-01 17:44:31
 ------------------------------------------------------------------------------
 | Wildfire Stats |
 +----------------------------------------------------------------------------
+ |
+-----------------------------------------------------------------------------
+| || Executable || |
+-----------------------------------------------------------------------------
+| || FileType | Submitted | Analyzed | Pending
 | Malware | Grayware | Benign | Error || |
+-----------------------------------------------------------------------------
+| || exe | 2 | 2 | 0 | 0 | 0 | 2 | 0 || |
+-----------------------------------------------------------------------------
+| || dll | 0 | 0 | 0 | 0 | 0 | 0 | 0 || |
+-----------------------------------------------------------------------------
+| Environment Analysis Summary for Executable:VM Utilization :0/10
 Files Analyzed :2
 +----------------------------------------------------------------------------
+ || Non-Executable || |
+-----------------------------------------------------------------------------
+| || FileType | Submitted | Analyzed | Pending
 | Malware | Grayware | Benign | Error || |
+-----------------------------------------------------------------------------
+| || pdf | 0 | 0 | 0 | 0 | 0 | 0 | 0 || |
+-----------------------------------------------------------------------------
+| || jar | 0 | 0 | 0 | 0 | 0 | 0 | 0 || |
+-----------------------------------------------------------------------------
+| || doc | 1 | 1 | 0 | 1 | 0 | 0 | 0 || |
+-----------------------------------------------------------------------------
+| || ppt | 0 | 0 | 0 | 0 | 0 | 0 | 0 || |
+-----------------------------------------------------------------------------
+| || xls | 0 | 0 | 0 | 0 | 0 | 0 | 0 || |
+-----------------------------------------------------------------------------
+| || docx | 0 | 0 | 0 | 0 | 0 | 0 | 0 || |
+-----------------------------------------------------------------------------
+| || pptx | 0 | 0 | 0 | 0 | 0 | 0 | 0 || |
+-----------------------------------------------------------------------------
+| || xlsx | 0 | 0 | 0 | 0 | 0 | 0 | 0 || |
+-----------------------------------------------------------------------------
+| || rtf | 0 | 0 | 0 | 0 | 0 | 0 | 0 || |
+-----------------------------------------------------------------------------
+| || class | 2 | 2 | 0 | 1 | 0 | 1 | 0 || |
+-----------------------------------------------------------------------------
+| || swf | 1 | 1 | 0 | 0 | 0 | 1 | 0 || |
+-----------------------------------------------------------------------------
+| Environment Analysis Summary for Non-
Executable:VM Utilization :0/16 Files Analyzed :4
 +----------------------------------------------------------------------------
+ || Links || |
+-----------------------------------------------------------------------------
```

```
+| || FileType | Submitted | Analyzed | Pending
 | Malware | Grayware | Benign | Error || |
+-------------------------------------------------------------------------------
+| || elink | 1 | 1 | 0 | 1 | 0 | 0 | 0 || |
+-------------------------------------------------------------------------------
+| Environment Analysis Summary for Links:Files Analyzed :1
 ------------------------------------------------------- | General
 Stats | +-------------------------------------------------------
+ Total Disk Usage:67/1283(GB) (5%) ||+--------------------------
+-----------+-+-----------+|| ||| Sample Queue ||| ||
+-----------------+-------------------+-------------+|| |||
 SUBMITTED | ANALYZED | PENDING ||| ||+--------------------------
+-----------+-+-----------+|| ||| 7 | 7 | 0 ||| ||
+---------------------------+-----------+-+----------+||| |
+---------------------------+---------------------------+| |||
 Verdicts ||| ||+---------------------------+-------------------------
+|| ||| Malware | Grayware | Benign | Error ||| ||
+------------------------------+----------------------+|| ||| 3 | 0
 | 4 | 0 ||| ||+---------------------------+-----------+-+----------
+||| |+---------------------------+---------------------------+|
 ||| Session and Upload Count ||| ||+--------------------------
+--------------------------+|| ||| Sessions | Uploads ||| ||
+--------------------------+-------------------------+|| ||| 7 | 5
 ||| ||+--------------------------+-------------------------+||
```

需要權限層級

superuser, superreader

測試 wildfire 登錄

說明

執行測試以確認 WildFire 設備或 Palo Alto Networks 防火牆向 WildFire 伺服器的登錄狀態。如果測試成功，將顯示 WildFire 伺服器的 IP 位址或伺服器名稱。WildFire 裝置或防火牆需要成功登錄才可轉送檔案至 WildFire 伺服器。

語法

```
test { wildfire { registration; } }
```

選項

無額外的選項。

範例輸出

以下顯示在能夠與 WildFire 設備通訊的防火牆上的成功輸出。如果這是指向 Palo Alto Networks WildFire Cloud 的 WildFire 設備，則會在 `select the best server:` 欄位中顯示其中一個雲端伺服器的名稱。

```
Testing wildfire Public Cloud wildfire registration: successful
 download server list: successful select the best server: ca-
s1.wildfire.paloaltonetworks.com
```

需要權限層級

superuser, superreader