AMP更新伺服器配置步驟

目錄

簡介

本檔案介紹思科進階惡意軟體防護(AMP)TETRA更新伺服器的詳細組態步驟。

必備條件

- 瞭解伺服器主機，例如Windows 2012R2或CentOS 6.9 x86_64。
- 具備託管軟體(例如IIS（僅限Windows）、Apache、Nginx的相關知識
- 已配置的伺服器主機啟用了HTTPS，安裝了有效的受信任證書。
- 已配置HTTPS本地更新伺服器選項。

附註：有關啟用本地更新伺服器配置和要求的完整詳細資訊，請參閱此處提供的《面向終端的AMP使用手冊》的第25章。
(https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf)

附註：伺服器主機(IIS、Apache、Nginx)是第三方產品，思科不支援這些產品。請參閱相應產品的支援團隊，瞭解所提供步驟之外的問題。

警告：如果AMP配置了代理伺服器，所有更新流量（包括TETRA）將繼續通過代理伺服器傳送，並定向到您的本地伺服器。確保在傳輸期間允許流量通過Proxy，且未進行任何修改。

安裝步驟

所有平台

1. 確認您的託管伺服器作業系統(OS)。
2. 確認面向終端的AMP控制面板門戶，下載更新程式軟體包和配置檔案。

AMP端點控制檯：

美國- https://console.amp.cisco.com/tetra_update

歐盟- https://console.eu.amp.cisco.com/tetra_update

亞太地區地區 — https://console.apjc.amp.cisco.com/tetra_update

Windows IIS

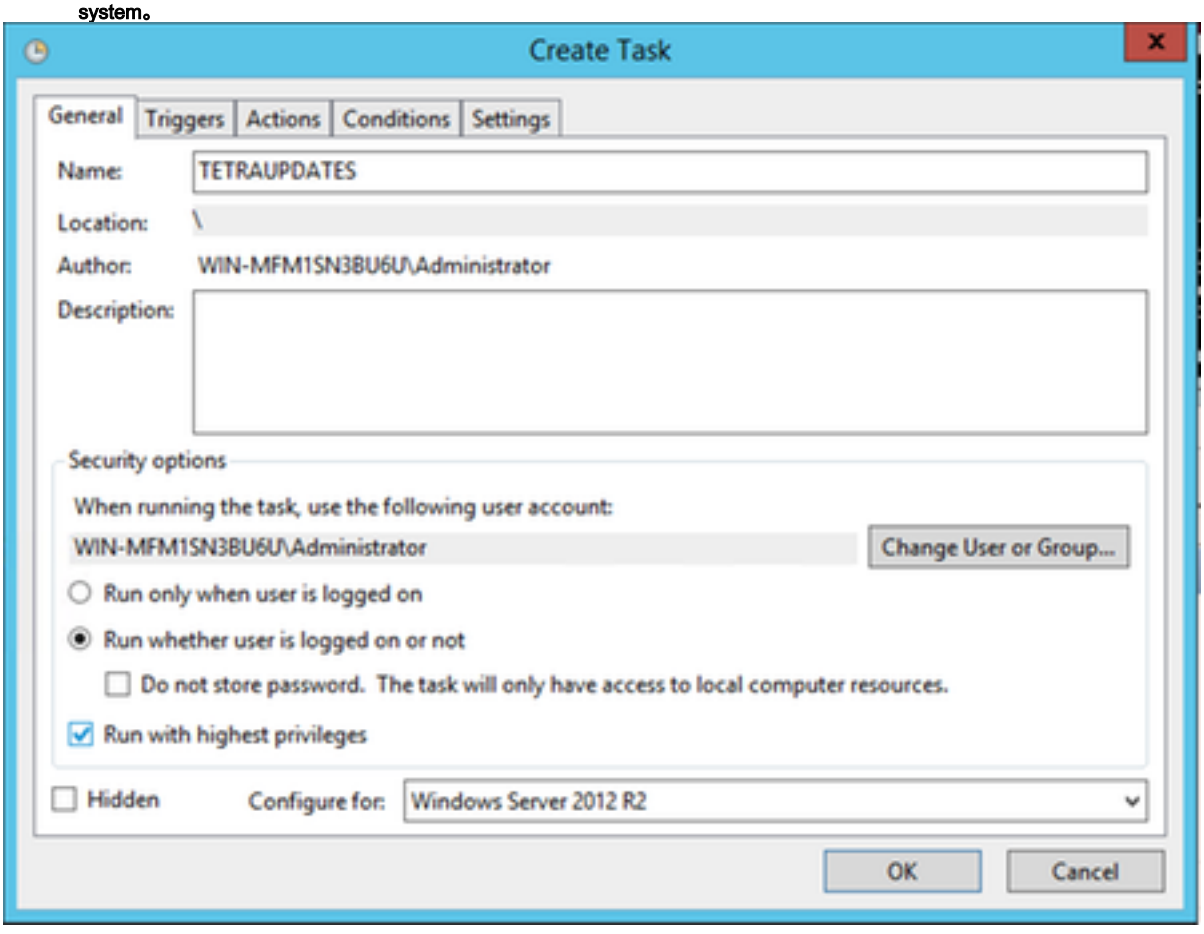
> **附註**：以下步驟基於託管簽名的新IIS應用程式池，而非**默**認應用程式池。要使用預設池，請在提供的步驟中更改—**mirror**資料夾，以反映預設的Web宿主路徑(**C:\inetpub\wwwroot**)

目錄建立

1. 在根驅動器上建立一個新資料夾，將其命名為**TETRA**。
2. 將壓縮的AMP更新程式軟體包和配置檔案複製到建立的**TETRA**資料夾中。
3. 解壓縮此資料夾中的軟體包。
4. 在TETRA資料夾內建立一個名為**Signatures**的新資料夾。

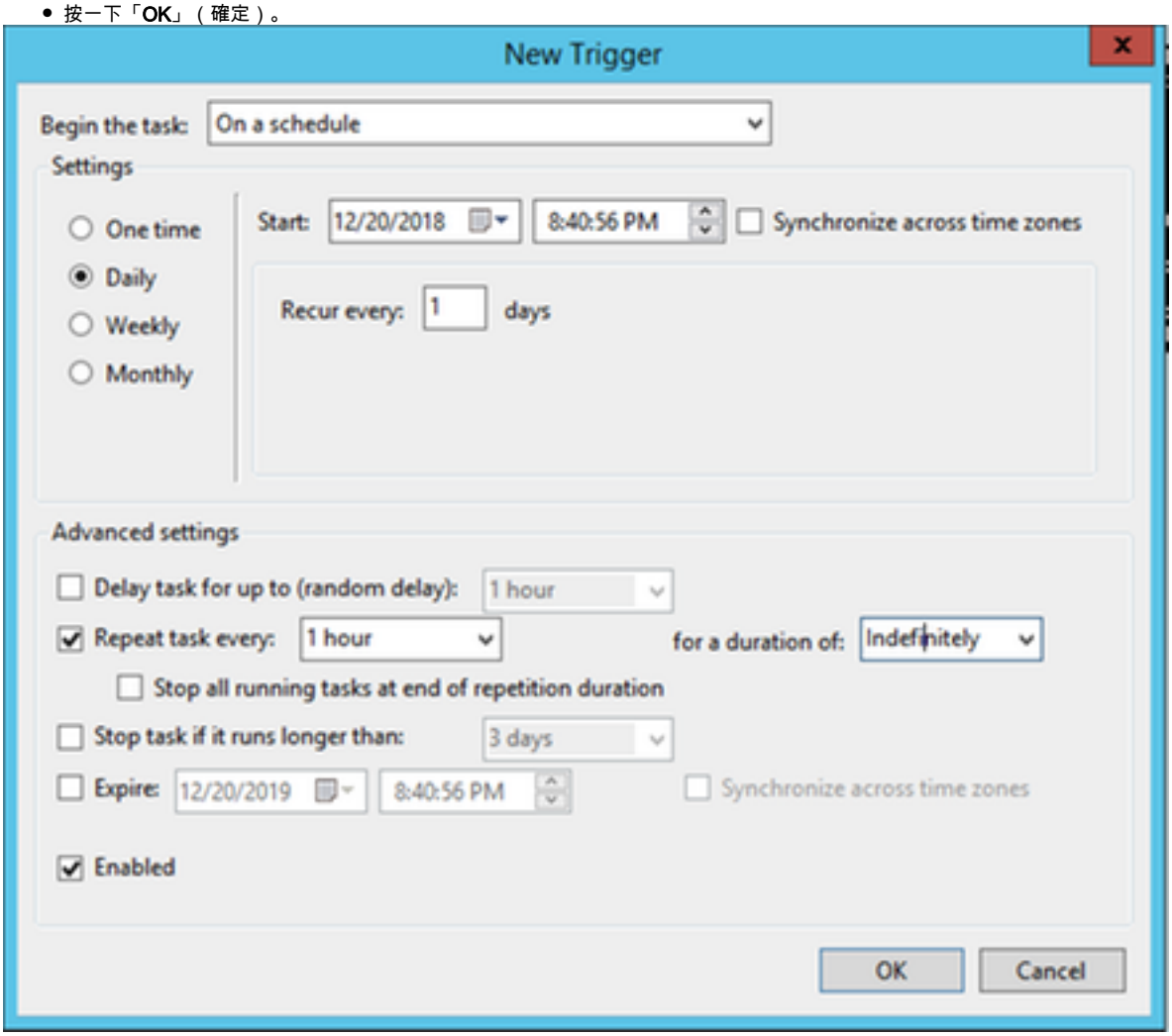
更新任務建立

1. 開啟命令列並導航到*C:\TETRA*資料夾.***cd C:\TETRA***
2. 運行命令***update-win-x86-64.exe fetch —config="C:\TETRA\config.xml" —once —mirror C:\TETRA\Signatures***
3. 開啟「任務計畫程式」並建立一個新任務。（操作>建立任務）根據需要使用以下選項自動運行更新程式軟體：
4. 選擇「常規」頁籤。 輸入任務的名稱。選擇**Run（無論使用者是否登入）**。選擇**使用最高許可權運行。**從**Configure**下拉選單中選擇**operating system。**



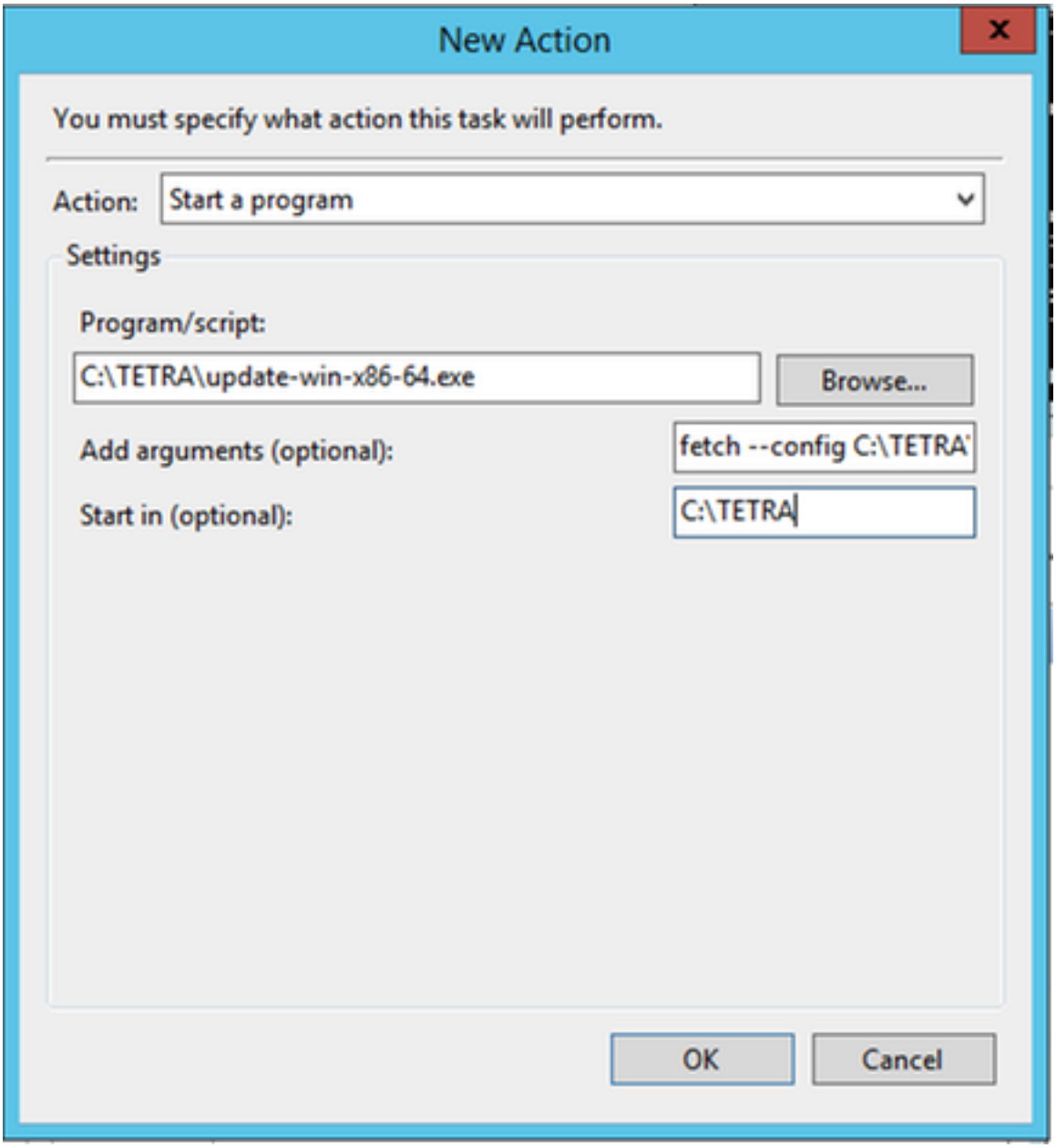
5.選擇「觸發器」標籤。

- 按一下「新建」。
- 從**Begin the task**下拉選單中選擇**On a schedule**。
- 在「設定」下選擇**Daily**。
- 選中**Repeat task every**，然後從下拉選單中選擇**1 hour**，然後在「**duration of：」中選擇Indefinitely**
- 確認**Enabled**是否已選中。
- 按一下「**OK**」（確定）。



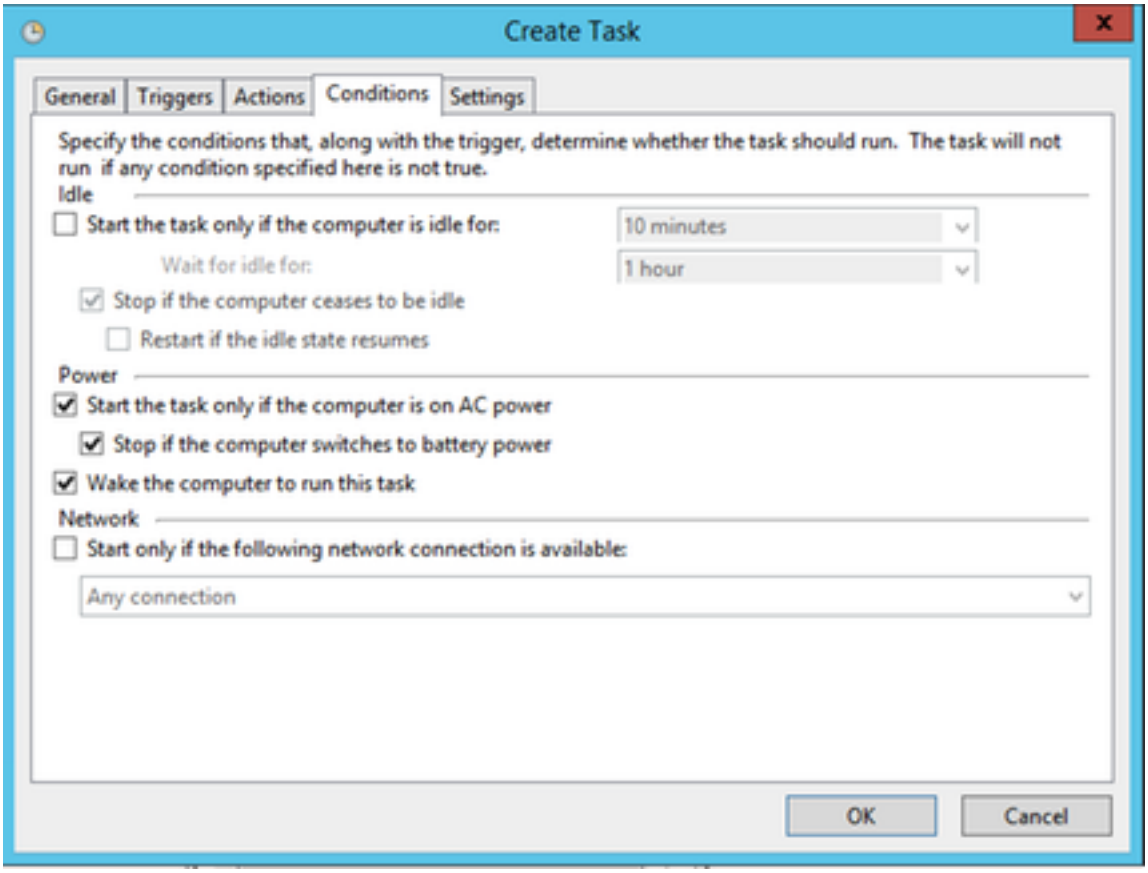
6.選擇「活動」標籤

- 按一下「**New**」。
- 從**Action**下拉選單中選擇**Start a program**。
- 在**Program/script**欄位中輸入*C:\TETRA\update-win-x86-64.exe*。
- 在**Add arguments**欄位中輸入*fetch —config C:\TETRA\config.xml —once —mirror C:\TETRA\Signatures*。
- 在「**Start**」欄位中輸入*C:\TETRA*
- 按一下「**OK**」



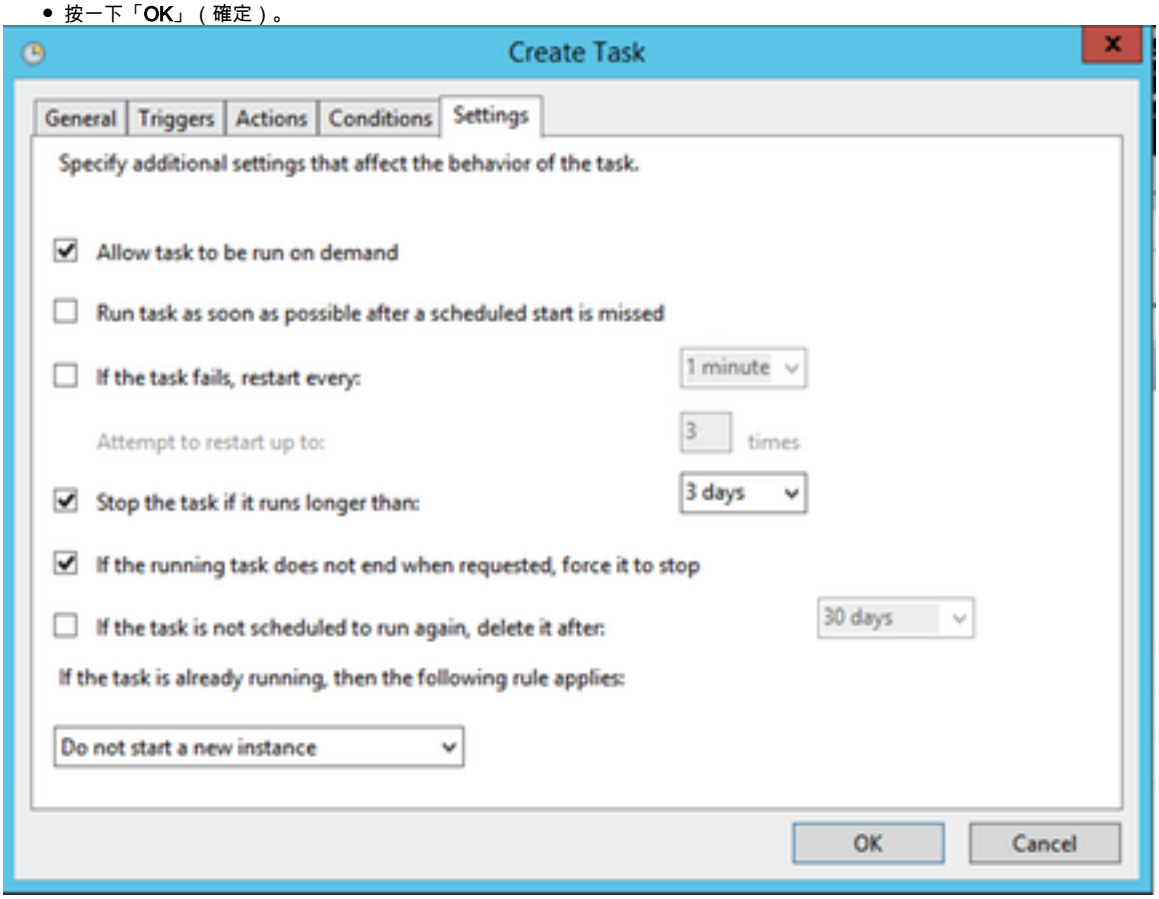
7. [*可選*] 選擇「條件」頁籤。

   選中「喚醒電腦以運行此任務」選項。



8選擇「設定」頁籤。

- 確認在*If the task is already running*下選擇了**Do not start a new instance**。
- 按一下「**OK**」（確定）。



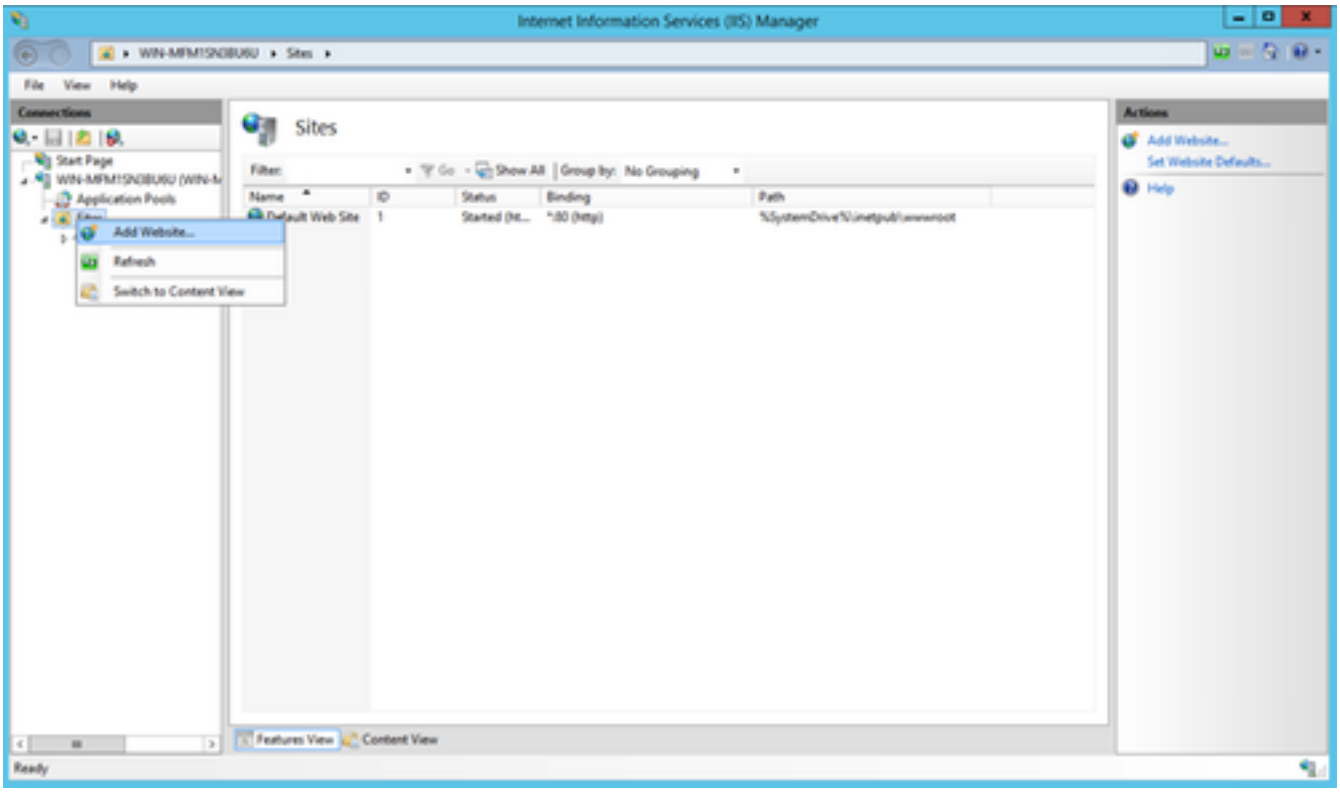
9.輸入將運行**任務的帳戶的身份證明**。

IIS管理器配置

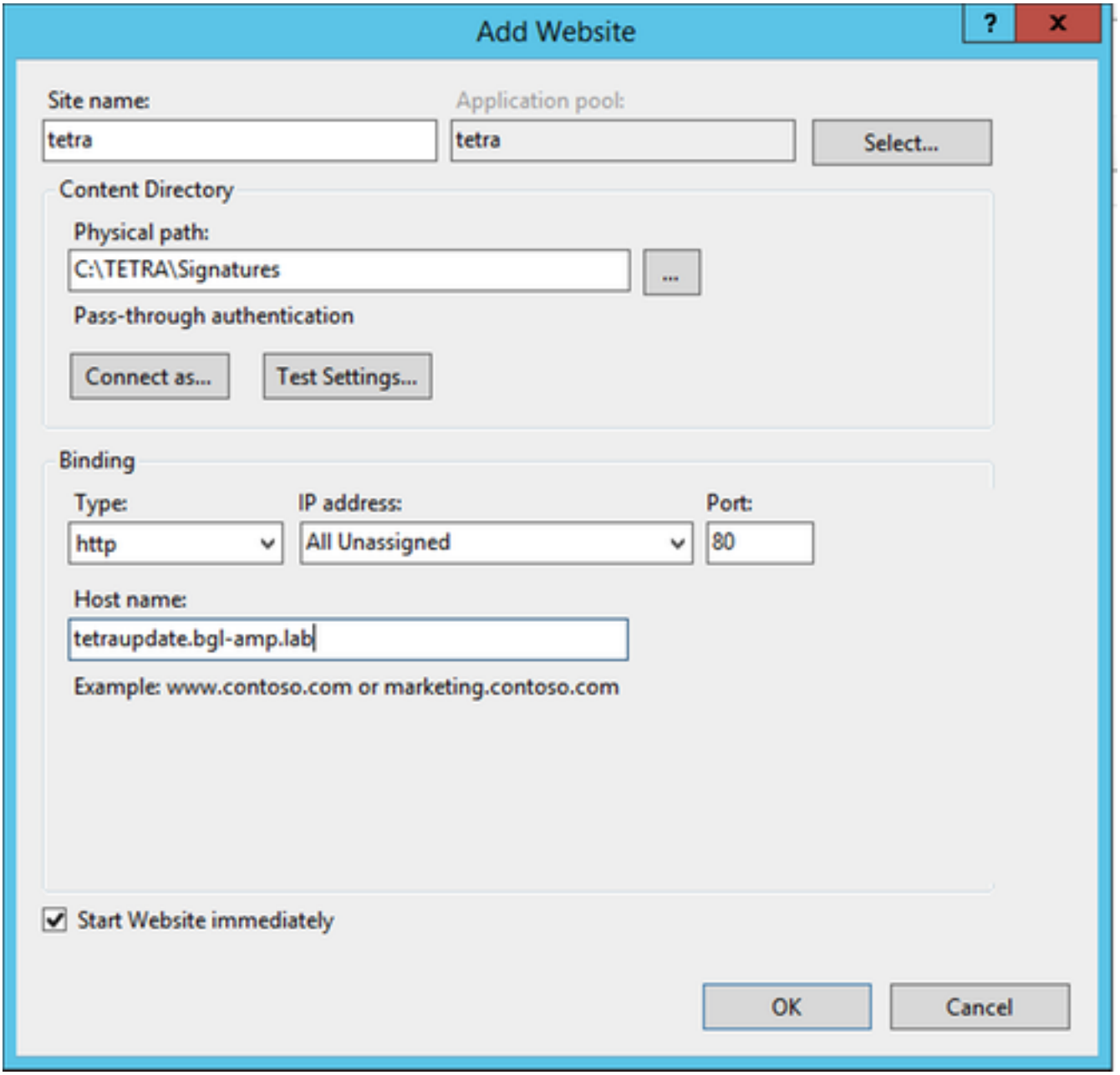
附註：配置預設應用程式池時跳至步驟5。

1.導航到(IIS)管理器(在「伺服器**管理器」>「工具」**下)

2.展開右側列，直到顯示「站點」文**件夾，然**後按一下右鍵，**然後選擇「新增網站」**。



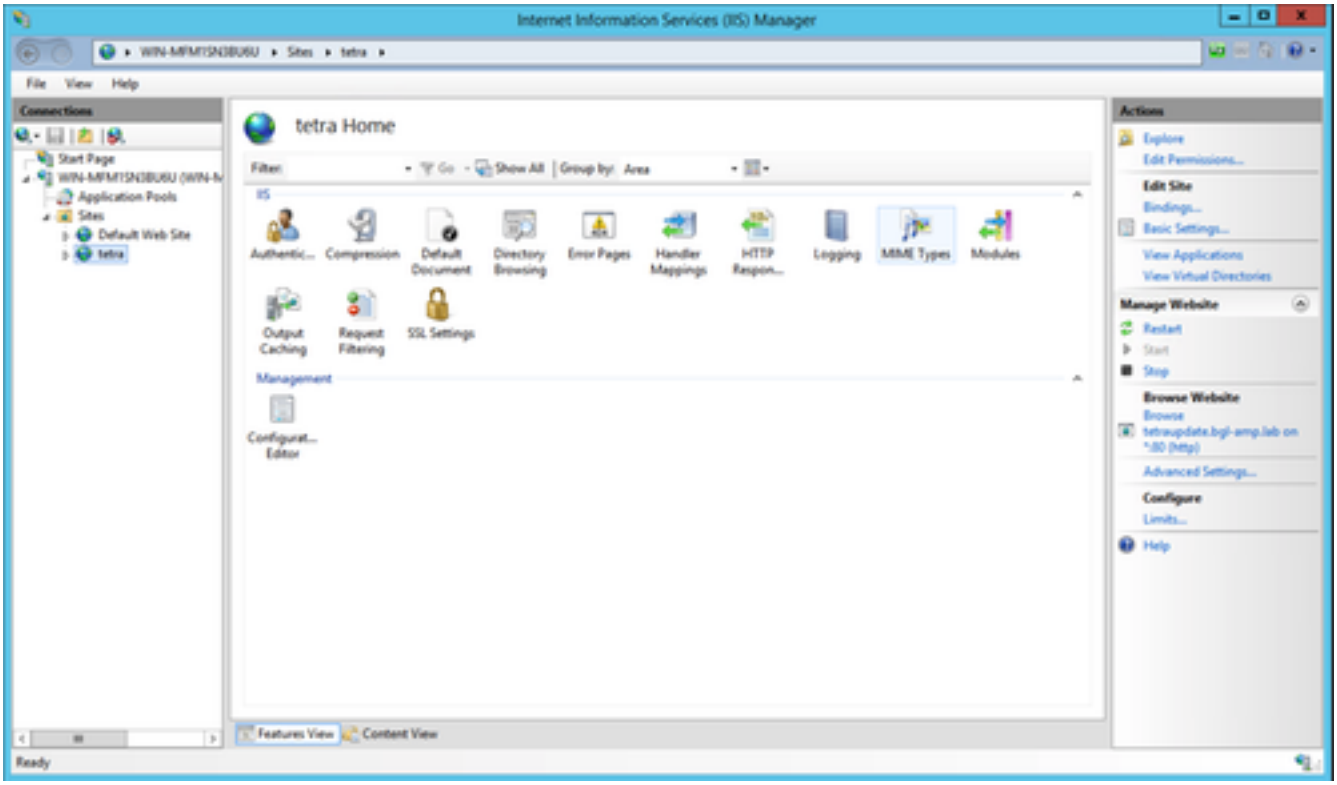
3.選擇選擇的名稱。對於物理路徑，選擇*C:\TETRA\Signatures*資料夾，該資料夾用於下載簽名。



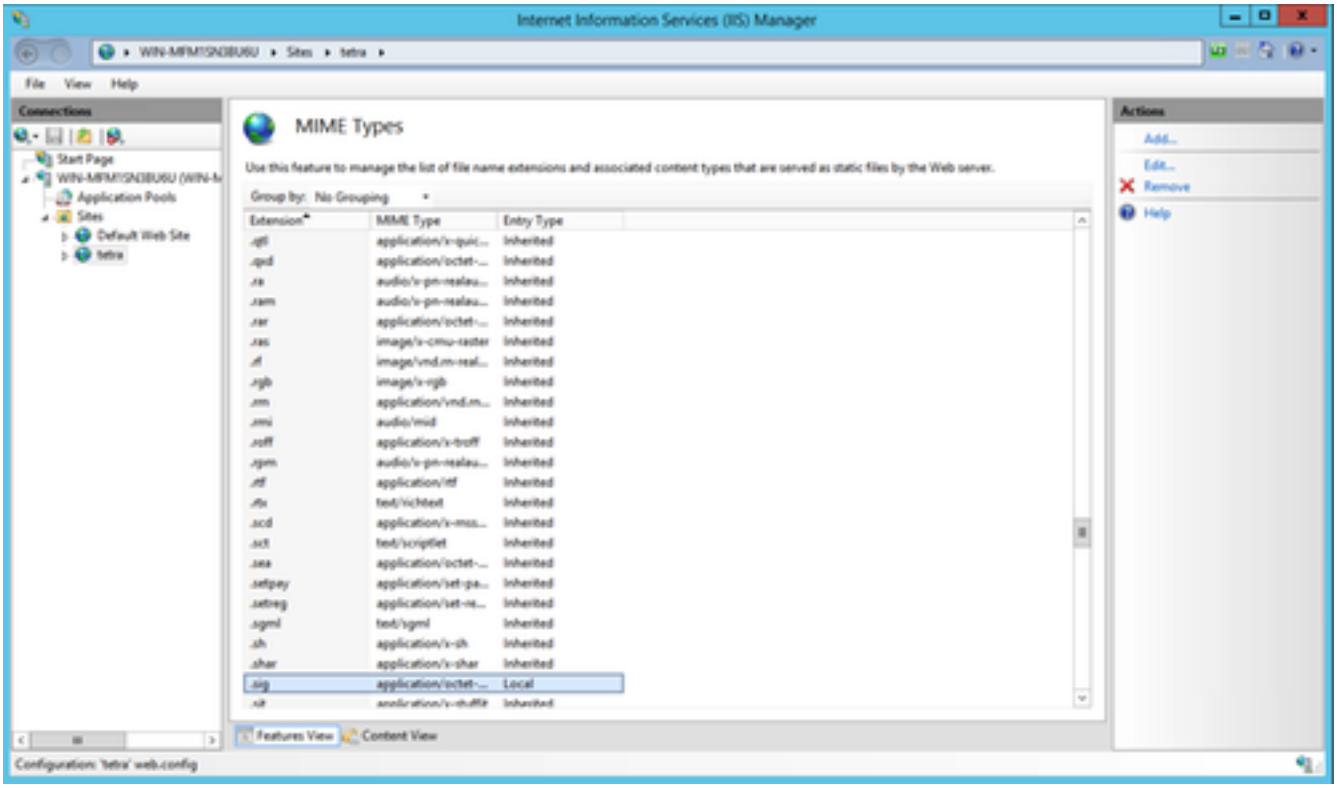
4.保持繫結獨立。配置**單獨的主機名和**伺服器名稱，選定的名稱必須由客戶端解析。這是您將在策略中配置的URL。

5.選擇站點並導航到**MIME型別**，然**後新增以下MIME型別**:

- .gzip，應用程式/八位元流
- .dat，應用程式/二進位制八位數流
- .id， Application/octet-stream
- .sig， Application/octet-stream



6.導航到**web.config**檔案（位於映象資料夾中），將以下行新增到檔案頂部。



完成後，在文本編輯器中檢視*C:\TETRA\Signatures\web.config*檔案內容時，檔案內容會顯示為此類內容。（語法和間距應與提供的示例相同。）

附註：面向終端的AMP聯結器要求在響應中存在伺服器HTTP報頭才能正常運行。如果已禁用伺服器HTTP標頭，則Web伺服器可能需要下面指定的其他配置。

必須安裝url-rewrite擴展。將以下XML片段新增到伺服器配置中
：/[MIRROR_DIRECTORY]/web.config:

```
<rewrite>
  <rules>
   <rule name="Rewrite fetch URL">
    <match url="^(.*)_[\d]*\/avx\/(.*)$" />
    <action type="Redirect" url="{R:1}/avx/{R:2}" appendQueryString="false" />
   </rule>
  </rules>
</rewrite>
```

附註：使用文本編輯器或IIS管理器（使用URL重寫模組）手動執行此更改。可以通過以下URL(https://www.iis.net/downloads/microsoft/url-rewrite)安裝重寫模組

完成後，在文本編輯器中檢視*C:\TETRA\Signatures\web.config*檔案內容時，檔案內容會顯示為此類內容。（語法和間距應與提供的示例相同。）

Apache/Nginx

附註：提供的步驟假定您提供來自Web託管軟體的預設目錄的簽名。

1. *TETRA*
2.
3. ***Chmod +x update-linux****
4. TETRA

sudo ./update-linux-x86-64 fetch --config config.xml --once --mirror /var/www/html/:

This command may vary depending on your directory structure.

5.cron

0 * * * * /TETRA/update-linux-x86-64 fetch --config /TETRA/config.xml --once --mirror /var/www/html/

6.

1. ***Advanced Settings > TETRA*** AMPIP<hostname.domain.root>IP

注意：請勿在下載之前或之後包含任何協定，否則下載時會導致錯誤。

[]TETRAHTTPSHTTPS

導航到C:\inetpub\wwwroot\、C:\TETRA\Signature或/var/www/html目錄，驗證更新的簽名是否可見，通過等待下一個同步週期或手動刪除現有簽名，然後等待下載簽名，將簽名從伺服器下載到終端客戶端。預設值為1小時的時間間隔以檢查更新。

相關資訊

- 技術支援與文件 - Cisco Systems
- 思科終端進階惡意軟體防護
- 面向終端的思科AMP — 使用手冊

.