Configuratiestappen voor AMP-server

Inhoud

Inleiding

Dit document beschrijft gedetailleerde configuratiestappen voor Cisco Advanced Malware Protection (AMP), TETRA Update Server.

Voorwaarden

- Kennis van serverhosts zoals Windows 2012R2 of CentOS 6.9 x86_64.
- Kennis van het organiseren van software zoals, IS (alleen Windows), Apache, Nginx
- Geconfigureren serverhosts met HTTPS ingeschakeld, geldig vertrouwd certificaat geïnstalleerd.
- Optie HTTPS lokale update Server configureren.

Opmerking: Raadpleeg voor volledige informatie over het inschakelen van de configuratie en vereisten van de lokale update serveren het raadplegen van hoofdstuk 25 van de AMP for Endpoints hier beschikbaar gebruikersgids. (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf)

Opmerking: Server Hosts (IS, Apache, NGINX) zijn producten van derden en worden niet ondersteund door Cisco. Raadpleeg de ondersteuningsteams voor respectievelijke producten voor vragen buiten de meegeleverde stappen.

Waarschuwing: Als AMP met een Proxyserver is ingesteld, wordt al het update verkeer (inclusief TETRA) verzonden via de proxy-server, naar uw lokale server. Zorg ervoor dat het verkeer is toegestaan zonder wijziging de volmacht passeert tijdens het vervoer.

Installatiestappen

Alle platforms

1. Bevestig het besturingssysteem van de Hosted Server.
2. Bevestig uw Advanced Malware Protection voor Endpoints Dashboard portal, download het Updater Software Package en het configuratiebestand.

Advanced Malware Protection voor endpoints:

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

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

APJC - https://console.apjc.amp.cisco.com/tetra_update

Windows IS

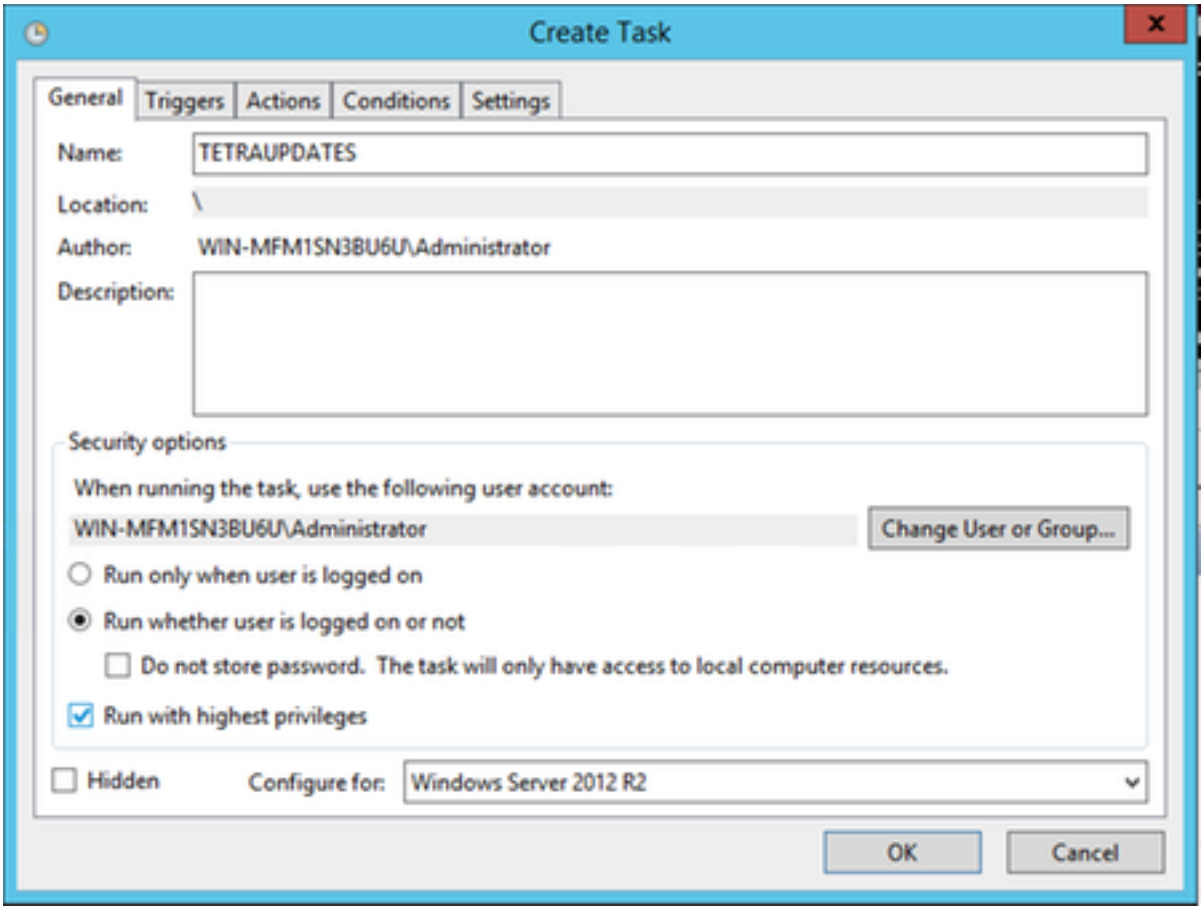
> Opmerking: De onderstaande stappen zijn gebaseerd op het nieuwe IIS-toepassingspool om de handtekeningen te ontvangen, **en niet** op de standaardapplicatie. Als u de standaard pool wilt gebruiken, wijzigt u de map —spiegel in de meegeleverde stappen om het standaard web host pad weer te geven (**C:\inetpub\wwwroot**)

Map maken

1. Geef een nieuwe map op het basisstation op en noem deze **TETRA**.
2. Kopieer het zipped AMP-softwarepakket en het configuratiebestand naar de **TETRA-**map die is gemaakt.
3. Koppel het softwarepakket in deze map los.
4. Maak een nieuwe map die **handtekeningen** heet in de TETRA-map.

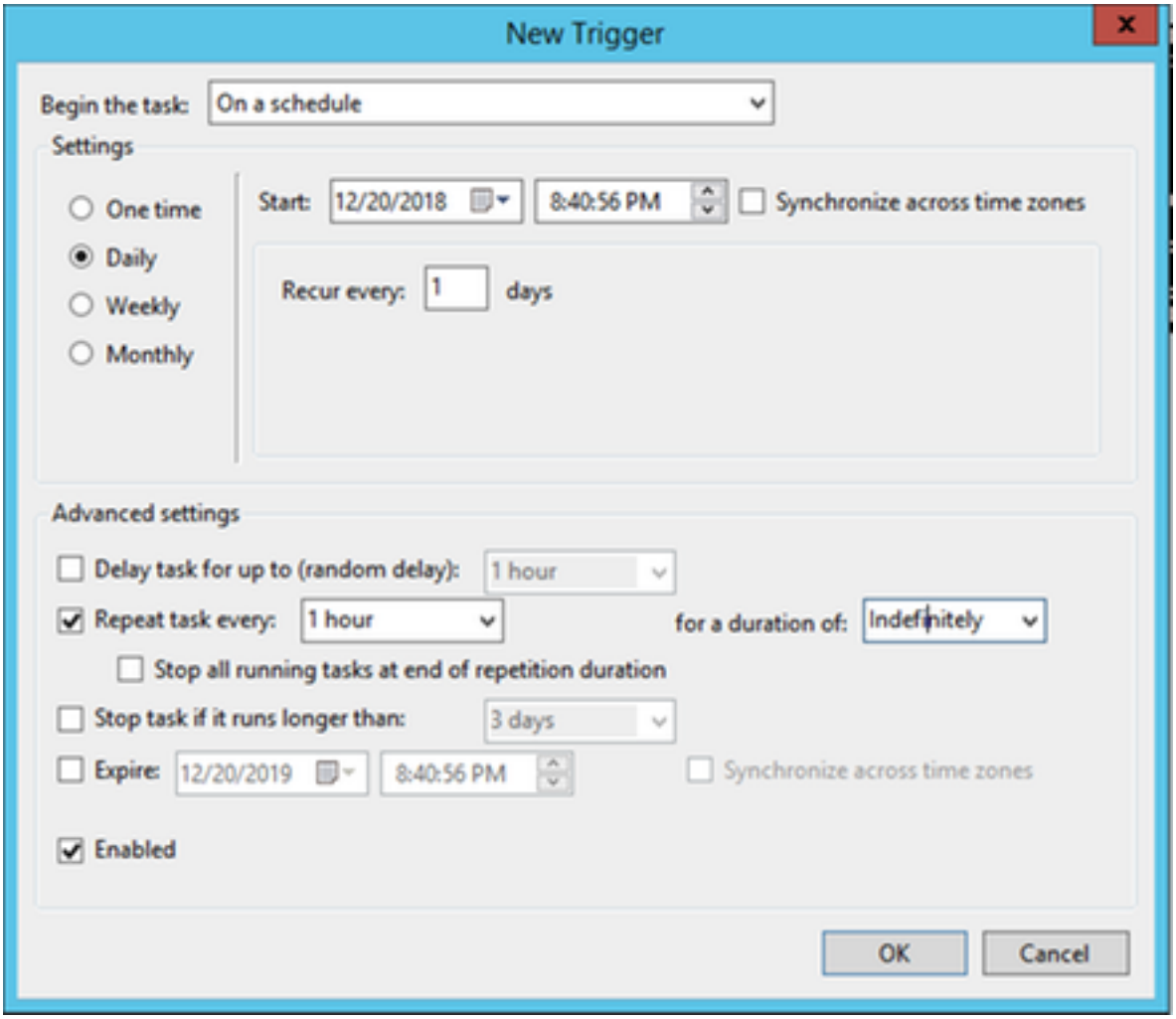
Taakmaken bijwerken

1. Open de opdrachtregel en navigeer naar de *C:\TETRA* map.***cd C:\TETRA***
2. Start de opdracht ***update-win-x86-64.exe fetch —fig="C:\TETRA\config.xml" —once —mirror C:\TETRA\Signatures***
3. Open de taakplanner en maak een nieuwe taak. (Actie > Task) om de software van het update automatisch met de volgende opties uit te voeren waar nodig:
4. Selecteer het tabblad Algemeen. Voer een naam in voor de taak.Selecteer **Start of de gebruiker is aangemeld of niet**.Selecteer **Run met de hoogste privileges.**Selecteer **het besturingssysteem** uit de vervolgkeuzelijst **Configureren.**



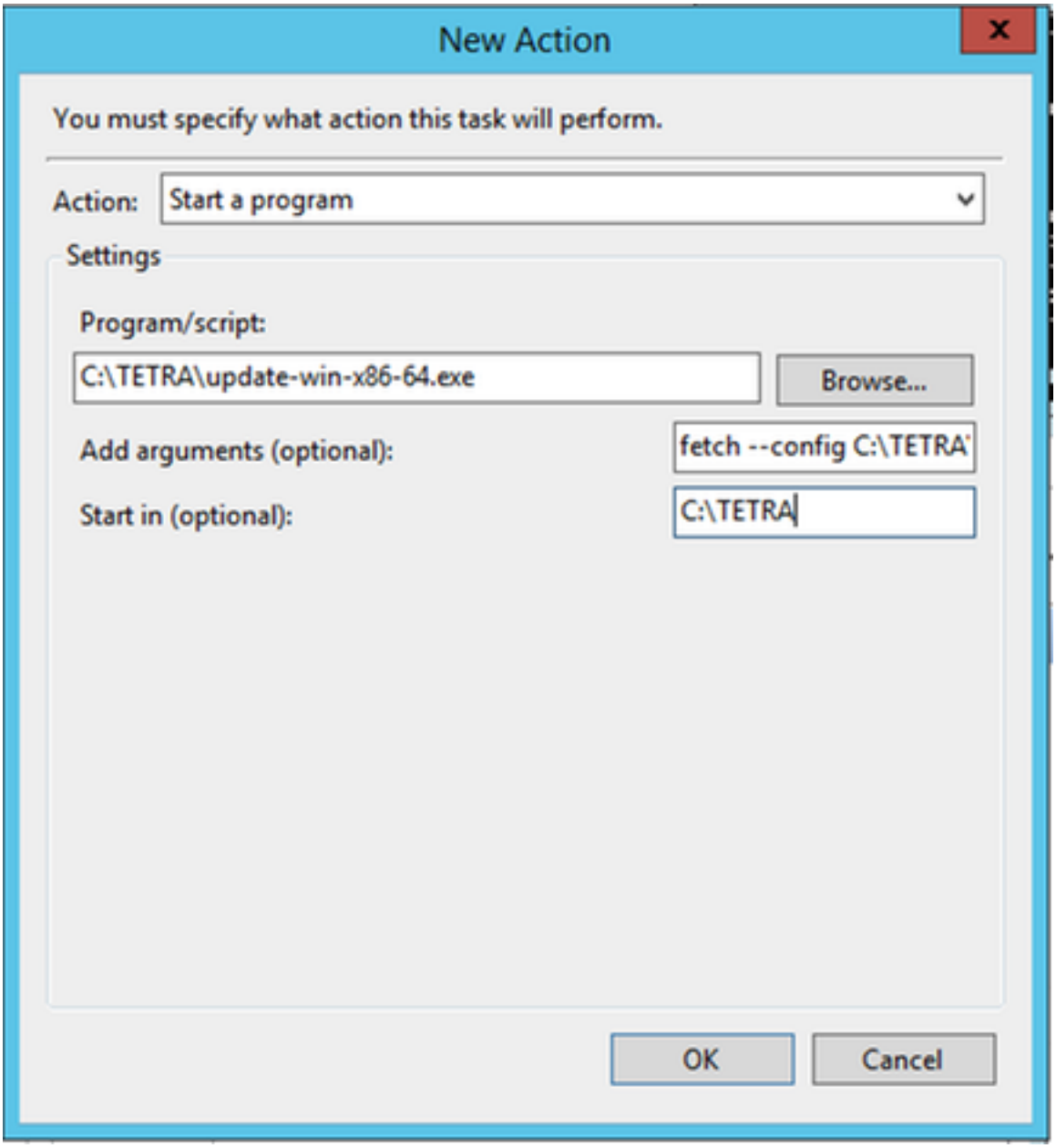
5. Selecteer het tabblad triggers.

- Klik op Nieuw.
- Selecteer **In een programma** uit de vervolgkeuzelijst **Beginnen met de taak**.
- Selecteer **Dagelijks** programma onder Instellingen.
- Controleer **de taak elke** keer herhalen en **selecteer 1 uur** uit de vervolgkeuzelijst en selecteer **Voor onbeperkt** in de **modus voor een duur van:**
- Controleer dat **deze optie** is **ingeschakeld**.
- Klik op **OK**.



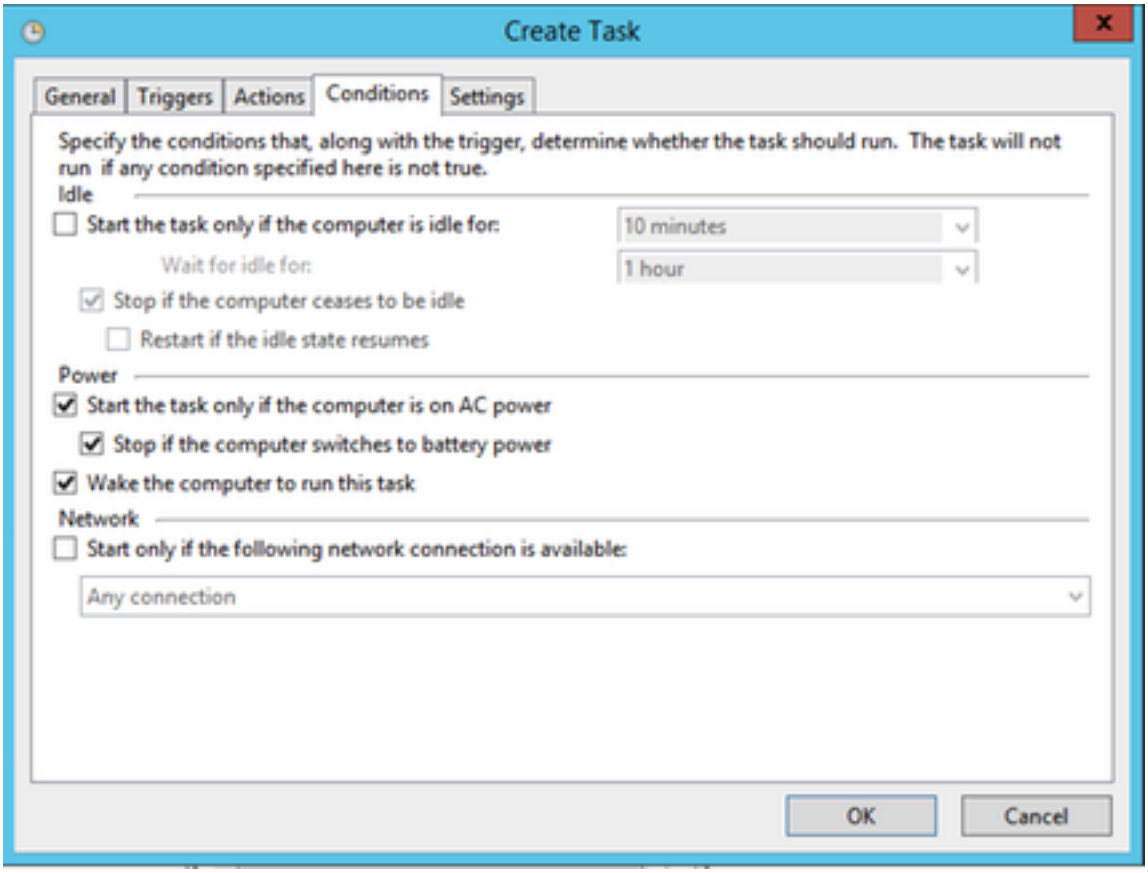
6. Selecteer het tabblad Handelingen

- Klik op **Nieuw**.
- Selecteer **Start een programma** vanuit de vervolgkeuzelijst **Action**.
- Voer ***C:\TETRA\update-win-x86-64.exe*** in het veld **Programma/script in**.
- Voer ***een fetch in — — —configuratie C:\TETRA\config.xml — eens — spiegelend C:\TETRA\Signatures*** in het veld **Add argumenten**.
- Voer ***C:\TETRA*** in het veld **Start** in
- Klik op **OK**



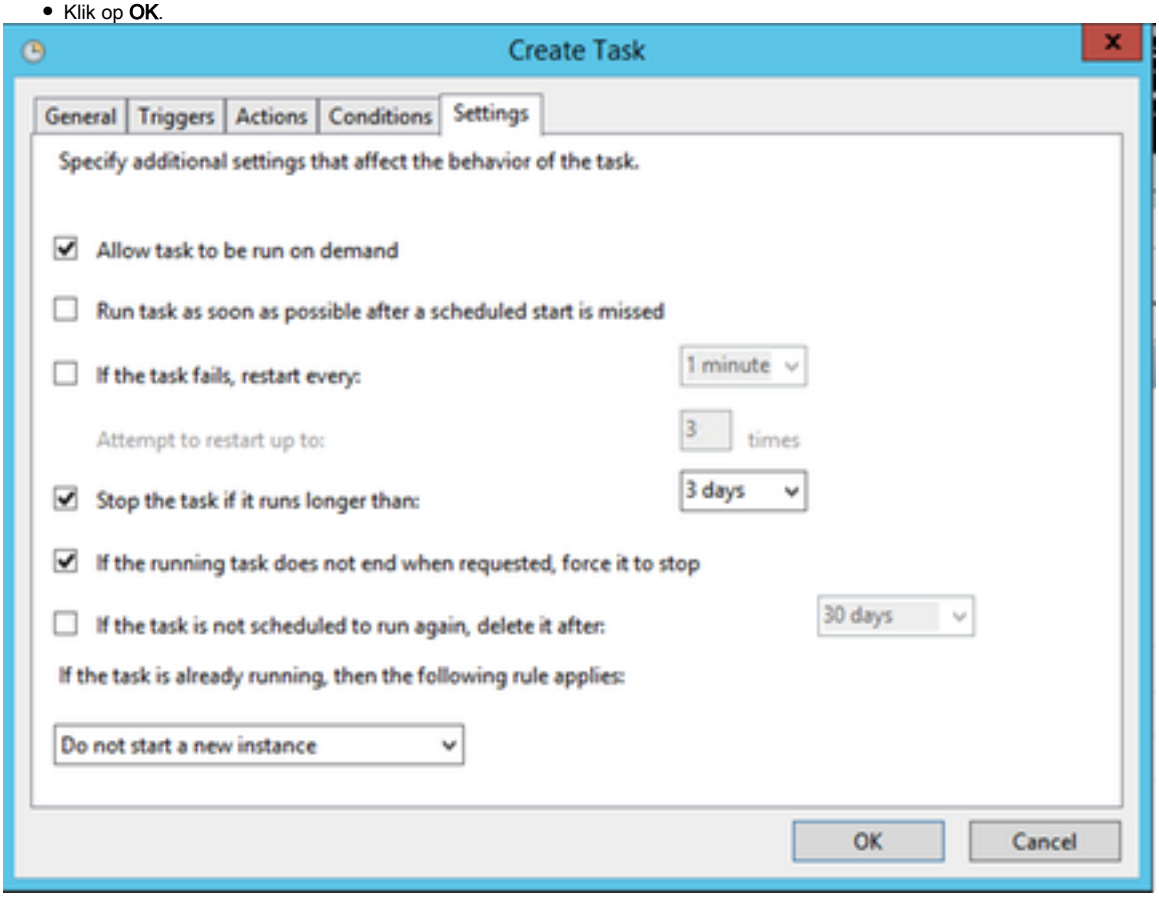
7. *[Optioneel]* Selecteer het tabblad Voorwaarden.

   Controleer de computer om deze taak uit te voeren.



8 Selecteer het tabblad Settings.

- Controleer dat **U geen nieuw exemplaar start**, maar *onder* **Als de taak al actief is.**
- Klik op **OK**.



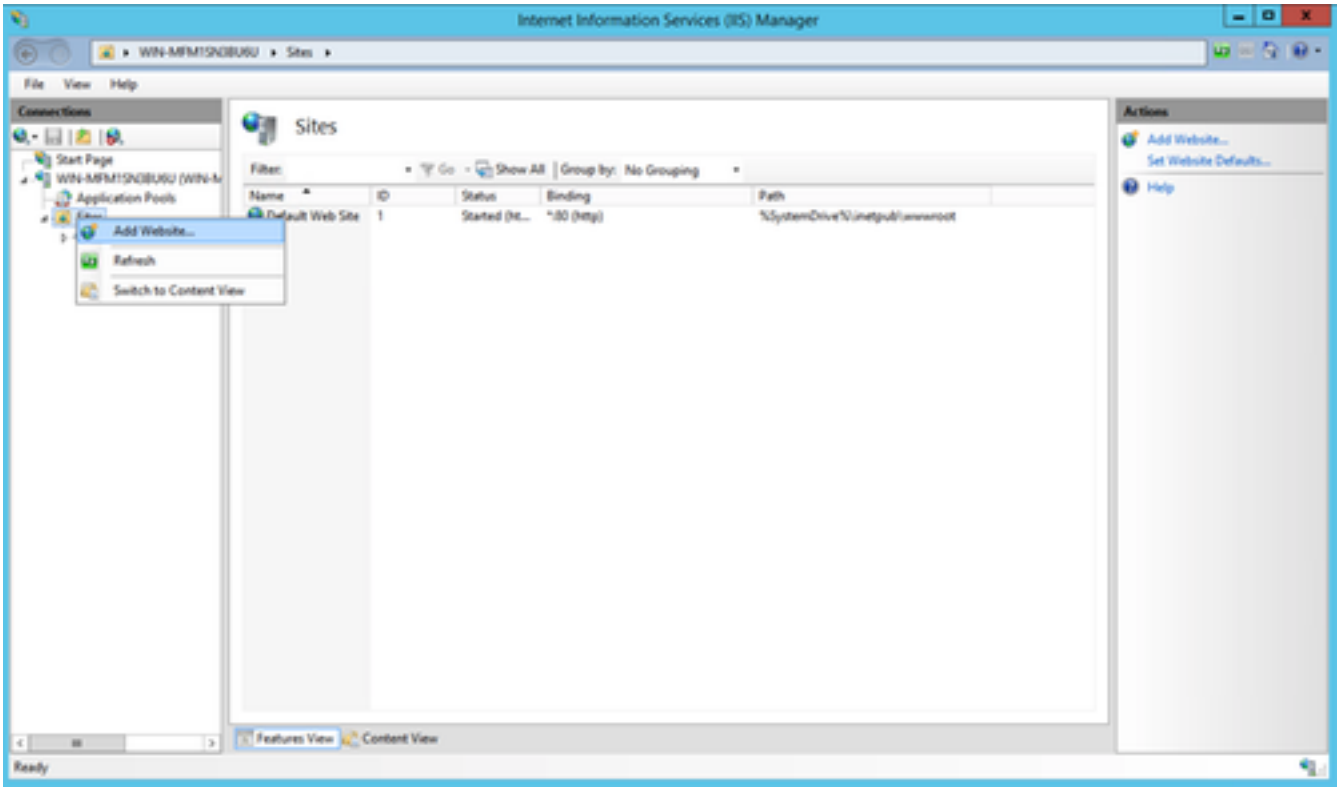
9. Voer de aanmeldingsgegevens in voor **de account die de taak gaat uitvoeren**.

Configuratie IS Manager

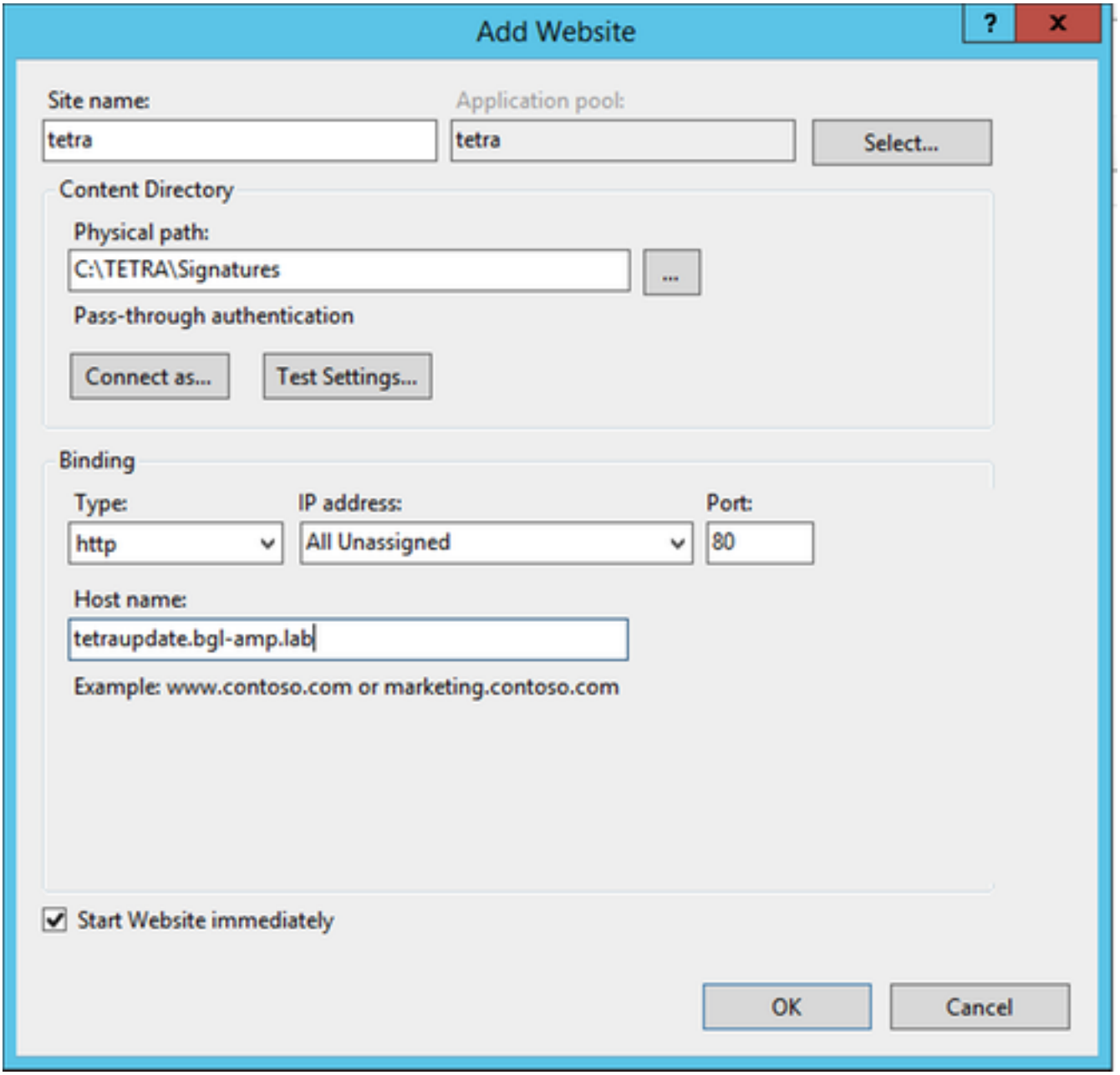
Opmerking: Naar stap 5 overslaan wanneer Default Application Pool is ingesteld.

1. Navigeren naar (IS) Manager (**onder Server Manager > Tools**)

2. Vouw de rechterkolom uit totdat de **map Sites** zichtbaar is, **rechtsklik en selecteer website toevoegen**.



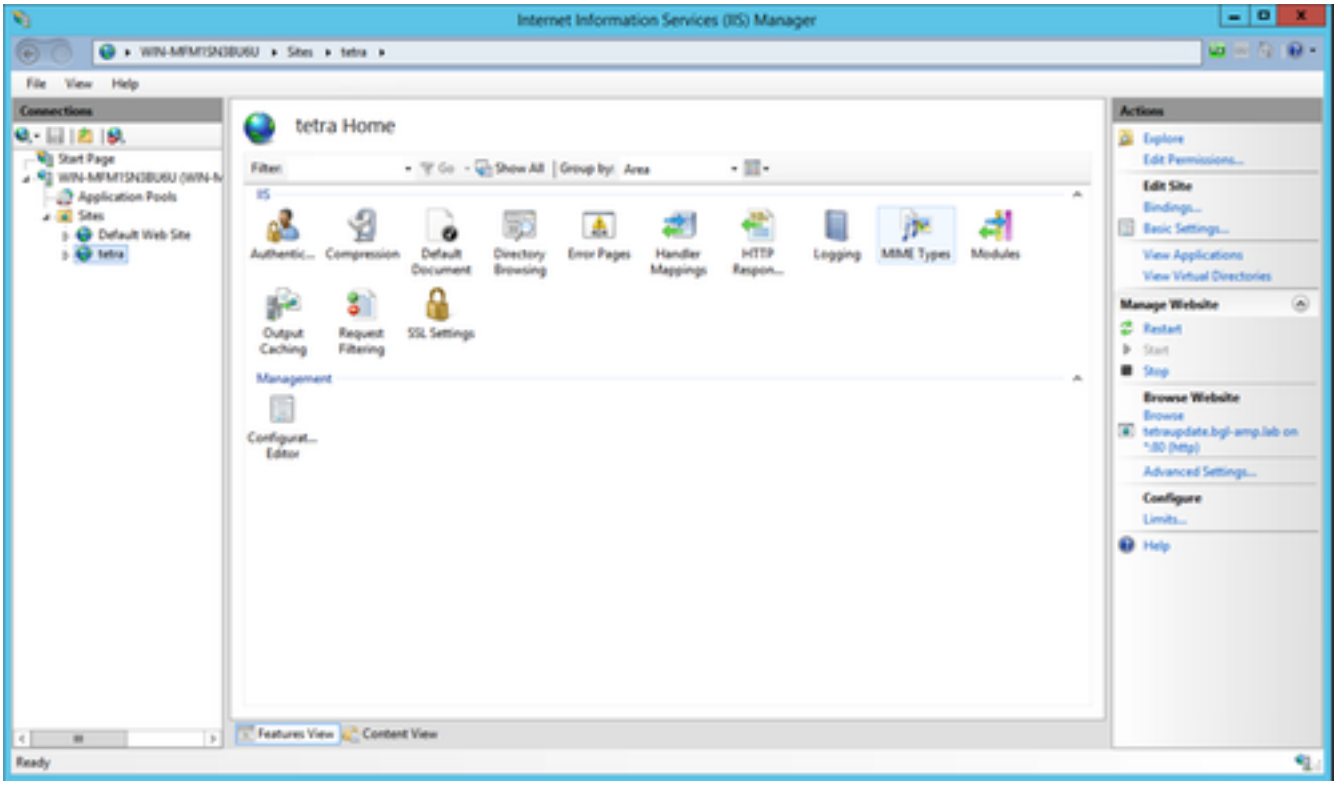
3. Kies een naam naar keuze. Selecteer voor het fysieke pad de *C:\TETRA\Signatures* map waarin de handtekeningen zijn gedownload.



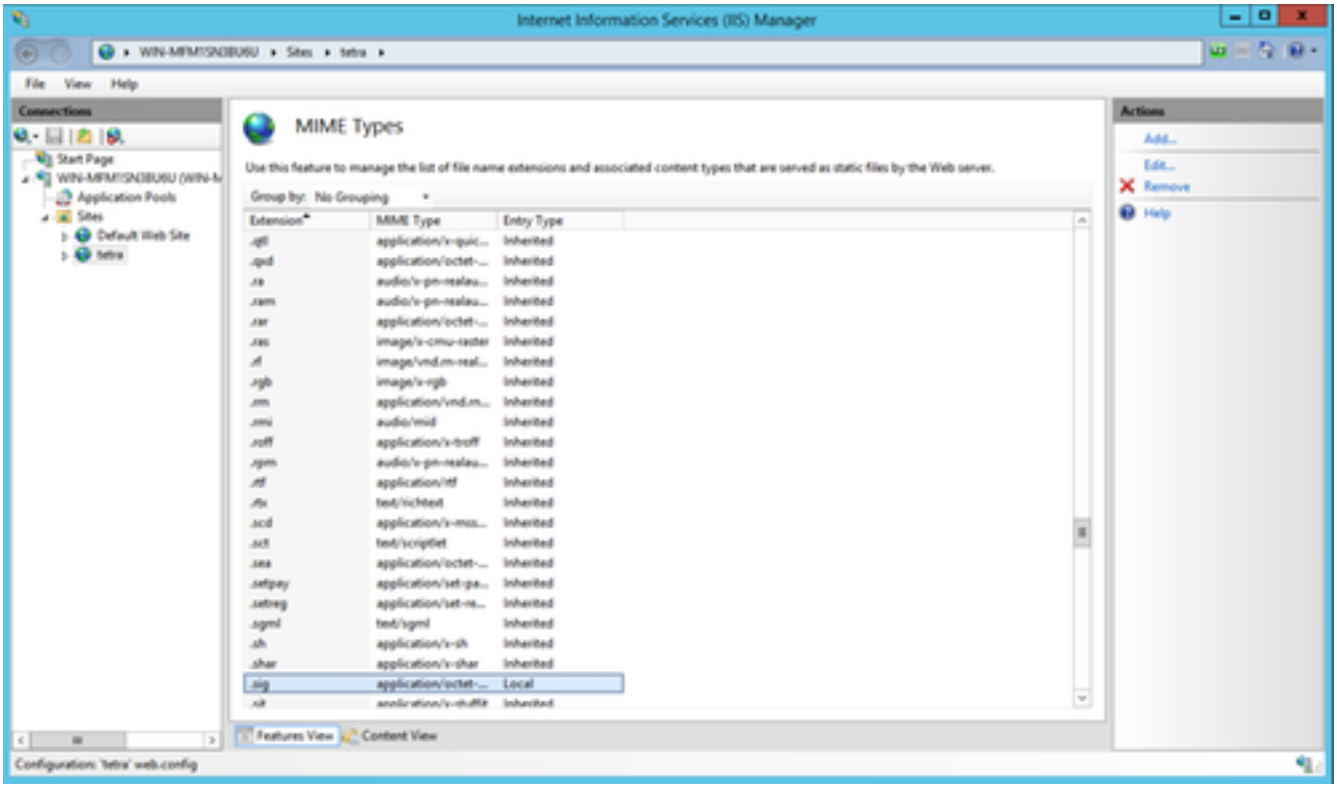
4. Laat Bindings alleen. **Configureer een afzonderlijke hostname** en servernaam, de gekozen namen moeten door de klanten kunnen worden opgelost. Dit is de URL die u in het beleid zult configureren.

5. Selecteer de locatie en navigeer naar **MIME-typen** en **voeg de volgende MIME-typen toe**:

- .gzip, toepassing/octet-stream
- .dat, Application/octet stream
- .id, toepassing/octet-stream
- .sig, toepassing/octet-stream



6. Navigeer naar het **web.fig-bestand** (in de spiegelmap bevindt), voeg de volgende lijnen aan de bovenkant van het bestand toe.



Wanneer de inhoud van het *C:\TETRA\Signatures\web.config*-bestand klaar is, verschijnt deze als zodanig wanneer u het in een teksteditor bekijkt. (Syntax and spacing moeten hetzelfde blijven als het voorgelegde voorbeeld.)

> Opmerking: De Advanced Malware Protection voor Endpoints Connector vereist de aanwezigheid van de server HTTP-header in de reactie op een correct gebruik. Als de Server HTTP Header is uitgeschakeld, heeft de webserver mogelijk nog een configuratie nodig die hieronder is gespecificeerd.

De verlenging moet worden geïnstalleerd. Voeg het volgende XML fragment toe aan de serverconfiguratie op /[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>
```

> Opmerking: Voer deze verandering handmatig uit met een teksteditor of met de IS-beheerder door de URL-herschrijfmodule te gebruiken. De herschrijfmodule kan vanaf de volgende URL (https://www.iis.net/downloads/microsoft/url-rewrite) worden geïnstalleerd

Wanneer de inhoud van het *C:\TETRA\Signatures\web.config*-bestand klaar is, verschijnt deze als zodanig wanneer u het in een teksteditor bekijkt. (Syntax and spacing moeten hetzelfde blijven als het voorgelegde voorbeeld.)

Apache / Nginx

> Opmerking: De geboden stappen veronderstellen dat u de handtekeningen van de standaard folder van de web host software serveert.

1. **Maak een nieuwe map** op uw *basisstation* met de naam **TETRA.**
2. **Unzip** het gedownload scripts pakket in deze map.
3. Start de opdracht ***Chmod +x update-linux**** om de scripts uitvoerbare toestemming te geven.
4. Start de opdracht om de TETRA update files te halen.

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

This command may vary depending on your directory structure.

5. Als u het uploadproces van de server wilt automatiseren, voegt u een snijtaak toe aan de server:

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

6. Ga verder met de stappen onder **Beleidsconfiguratie** om uw beleid te configureren voor het gebruik van de Update server.

Beleidsconfiguratie

1. Navigeer naar het beleid om de Update Server te gebruiken en onder ***Geavanceerde Instellingen > TETRA*** selecteer: Selectieknop voor lokale AMP-update serverDe hostname of IP voor de update server in het formaat van <hostname.domein.root> of IP-adres.

Voorzichtig: Voeg geen protocollen vóór of subdirectories toe nadat het tegendeel is gebeurd, dit leidt tot een fout bij het downloaden.

[Optioneel] Selectieknop **Gebruik HTTPS voor TETRA Standaard updates:** als de lokale server is geconfigureerd met een correct certificaat en voor de connectors om HTTPS te gebruiken.

Verificatie

Navigeer naar de **directory C:\inetpub\wwwroot\, C:\TETRA\Signature** of **/var/www/html** en controleer of de bijgewerkte handtekeningen zichtbaar zijn, de handtekeningen worden gedownload van de server naar de eindclient door te wachten tot de volgende synchronisatiecyclus of handmatig de bestaande handtekeningen te verwijderen en dan te wachten tot de handtekeningen worden gedownload. De standaardinstelling is een interval van 1 uur om voor een update te controleren.

Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems
- Cisco Advanced Malware Protection voor endpoints - TechNotes
- Cisco Advanced Malware Protection voor endpoints - gebruikershandleiding

.