Étapes de configuration du serveur de mise à jour d'AMP

Contenu

Introduction

Ce document décrit des étapes de configuration détaillée pour Cisco a avancé serveur de mise à jour de protection de malware le TÉTRA (AMP).

Prerequistes

- La connaissance des hôtes de serveur comme, du Windows 2012R2 ou du CentOS 6.9 x86_64.
- La connaissance d'accueillir le logiciel comme, IIS (Windows seulement), Apache, Nginx
- Hôtes de serveur configurés avec HTTPS activé, certificat de confiance valide installé.
- Option de serveur locale configurée de mise à jour HTTPS.

Note: Pour les détails complets dans activer la configuration du serveur locale et les conditions requises de mise à jour, référez-vous s'il vous plaît au chapitre 25 du guide d'utilisateur final d'AMP, disponible ici. (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf)

Note: Les hôtes de serveur (IIS, Apache, Nginx) sont des produits tiers et ne sont pas pris en charge par Cisco, se rapportent s'il vous plaît aux équipes d'assistance pour les Produits respectifs pour des questions en dehors des étapes fournies.

Avertissement : Si l'AMP est configuré avec un serveur proxy, tout le trafic de mise à jour (TÉTRA y compris) continuera à être envoyé par le serveur proxy, dirigé vers votre serveur local. Assurez que là le trafic est permis à passage le proxy sans n'importe quelle modification en transit.

Installez les étapes

Toutes les plates-formes

1. Confirmez votre système d'exploitation serveur de accueil (SYSTÈME D'EXPLOITATION).
2. Confirmez votre AMP pour le portail de tableau de bord de points finaux, téléchargez le progiciel et le fichier de configuration d'Updater.

AMP pour le portail de tableau de bord de points finaux :

Les USA - https://console.amp.cisco.com/tetra_update

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

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

Windows IIS

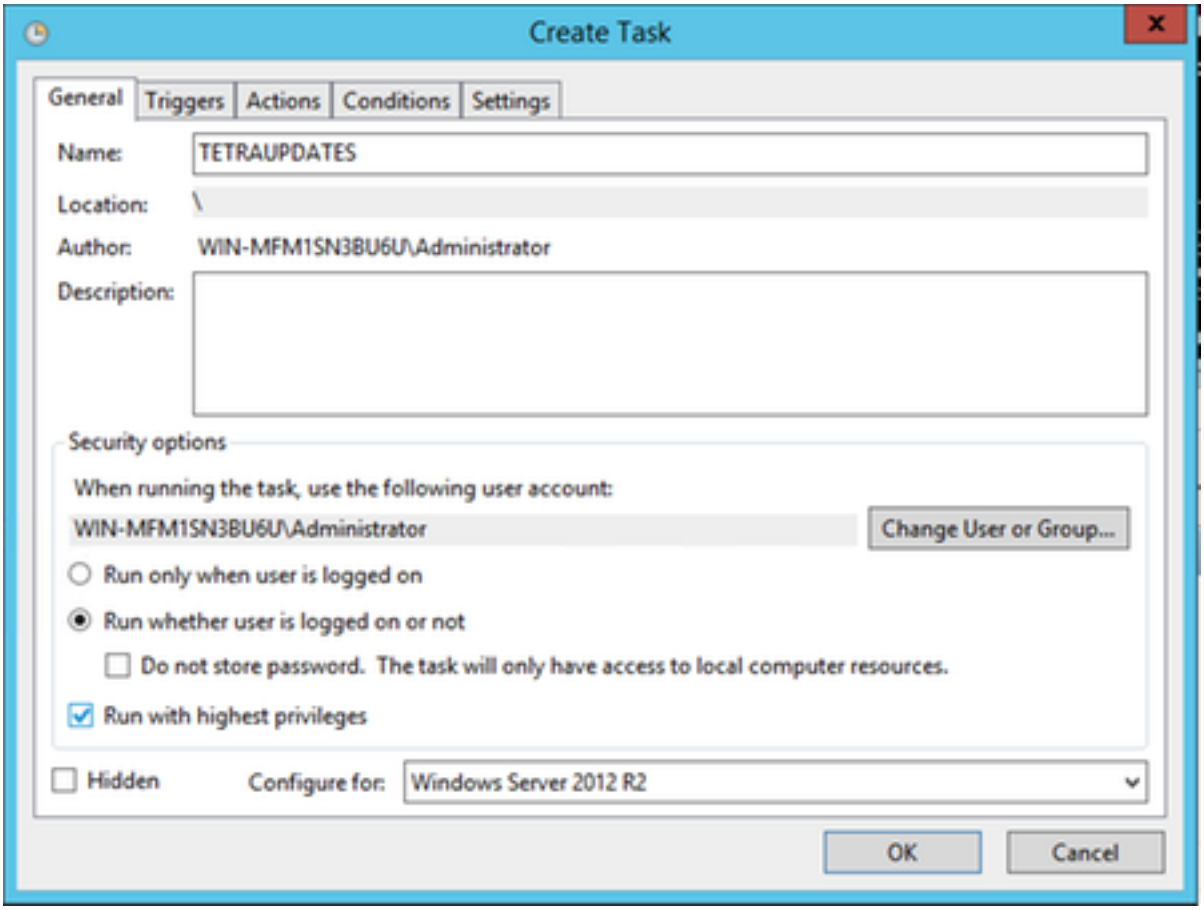
> **Note**: Les étapes ci-dessous ne sont basées sur le nouveau groupe d'application IIS pour héberger les signatures, **pas le** groupe par défaut d'application. Pour utiliser le groupe par défaut, changez **--reflétez le** répertoire dans les étapes fournies pour refléter le chemin d'accueil de web par défaut (**C:\inetpub\wwwroot**)

Création de répertoire

1. Créez un nouveau répertoire sur le lecteur de racine, nommez-le **TÉTRA**.
2. Copiez le progiciel et le fichier de configuration fermés la fermeture éclair d'updater d'AMP sur le **TÉTRA** répertoire créé.
3. Défaites la fermeture éclair du progiciel dans ce répertoire.
4. Créez un nouveau répertoire appelé **Signatures** à l'intérieur du TÉTRA répertoire.

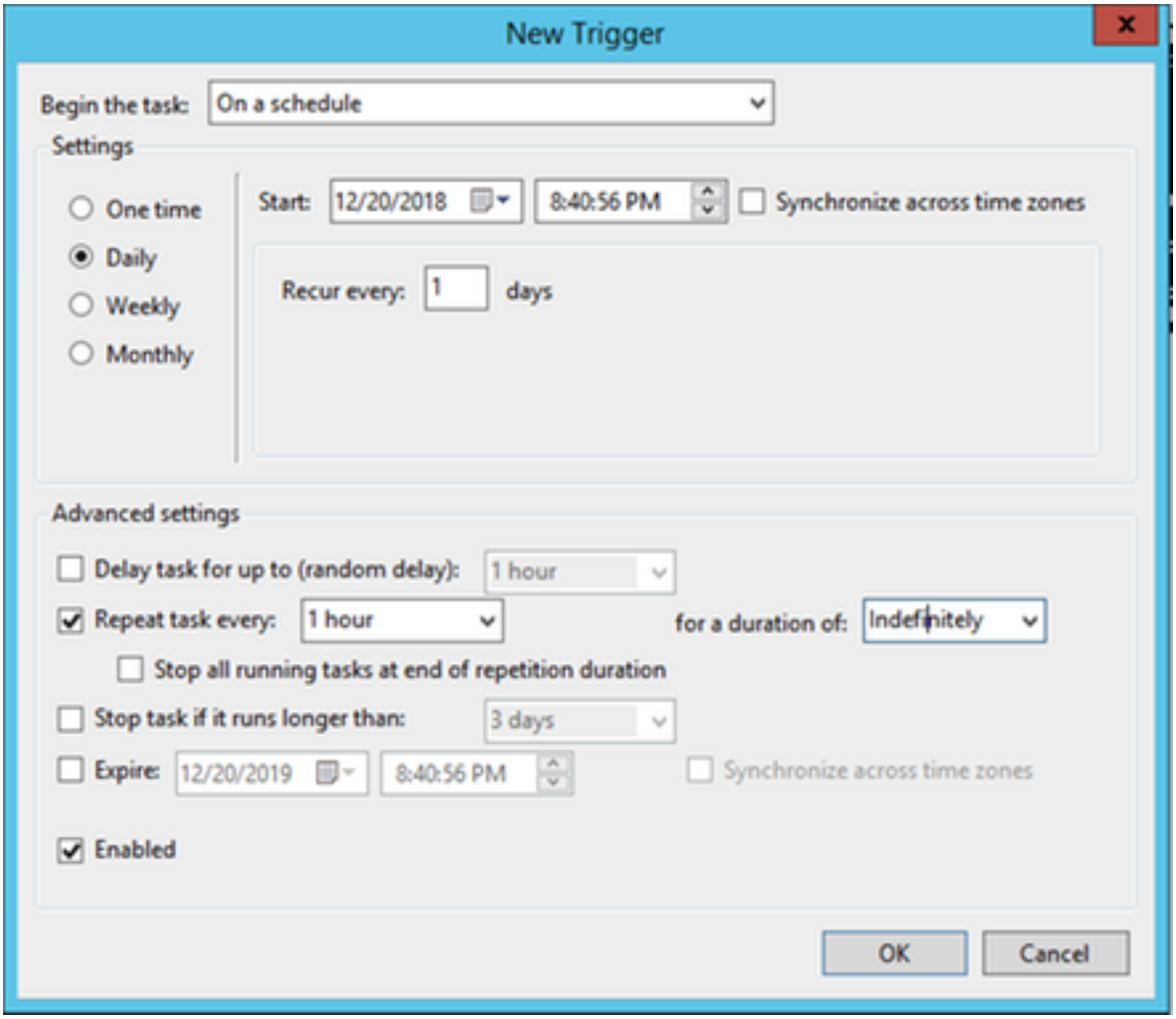
Création de tâche de mise à jour

1. Ouvrez la ligne de commande et naviguez vers *C:\TETRA* folder.cd ***C:\TETRA***
2. Exécutez l'***effort de la*** commande ***update-win-x86-64.exe --config= " C:\TETRA\config.xml » --une fois que --miroir C:\TETRA\Signatures***
3. Ouvrez le gestionnaire de tâches et créez une nouvelle tâche. (L'action > créent la tâche) pour exécuter le logiciel d'updater automatiquement avec les options suivantes où nécessaire :
4. Sélectionnez l'onglet Général. Écrivez un nom pour la tâche.Sélectionnez le **passage, que l'utilisateur soit ouvert une session ou pas**.**Passage choisi avec les privilèges les plus élevés.Le système d'exploitation choisi du configurer chutent vers le bas.**



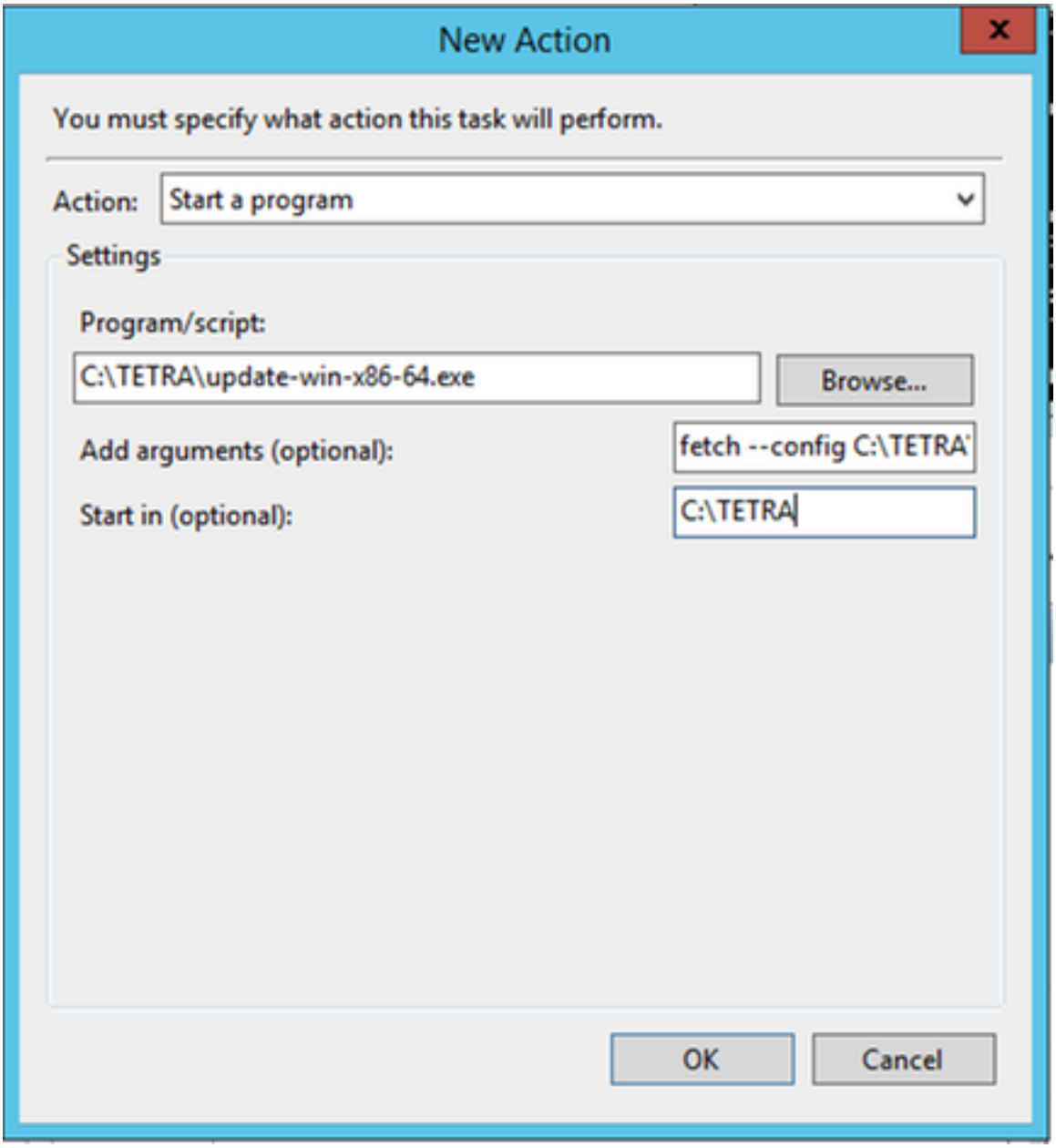
5. Sélectionnez l'onglet de déclencheurs.

- Cliquez sur **New**.
- Sélectionnez **sur un programme du commencer que la tâche** relâchent vers le bas.
- Sélectionnez le **journal** sous des configurations.
- **La tâche de répétition de contrôle chaque et sélectionnent 1 heure de la baisse vers le bas et la sélectionnent indéfiniment du « pour une durée de : "**
- Vérifiez qui **a activé est vérifié**.
- Cliquez sur **OK**.



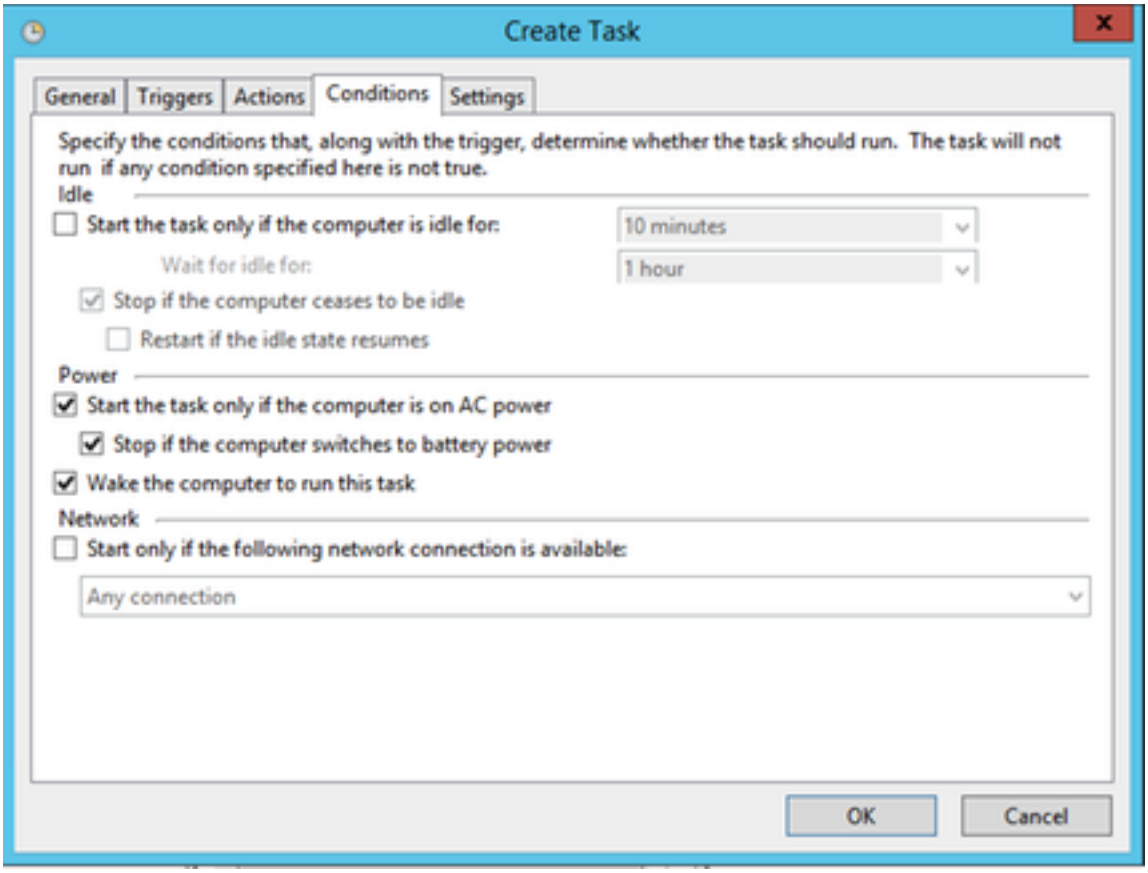
6. Sélectionnez l'onglet d'actions

- Cliquez sur **New**.
- Sélectionnez le **début un programme de l'action** pour relâcher vers le bas.
- Écrivez ***C:\TETRA\update-win-x86-64.exe*** dans le domaine de **programme/script**.
- Écrivez l'***effort --config C:\TETRA\config.xml --une fois que --miroir C:\TETRA\Signatures*** dans le domaine d'**arguments d'ajouter**.
- Entrez dans ***C:\TETRA*** dans le **début** dans le domaine
- Cliquez sur OK



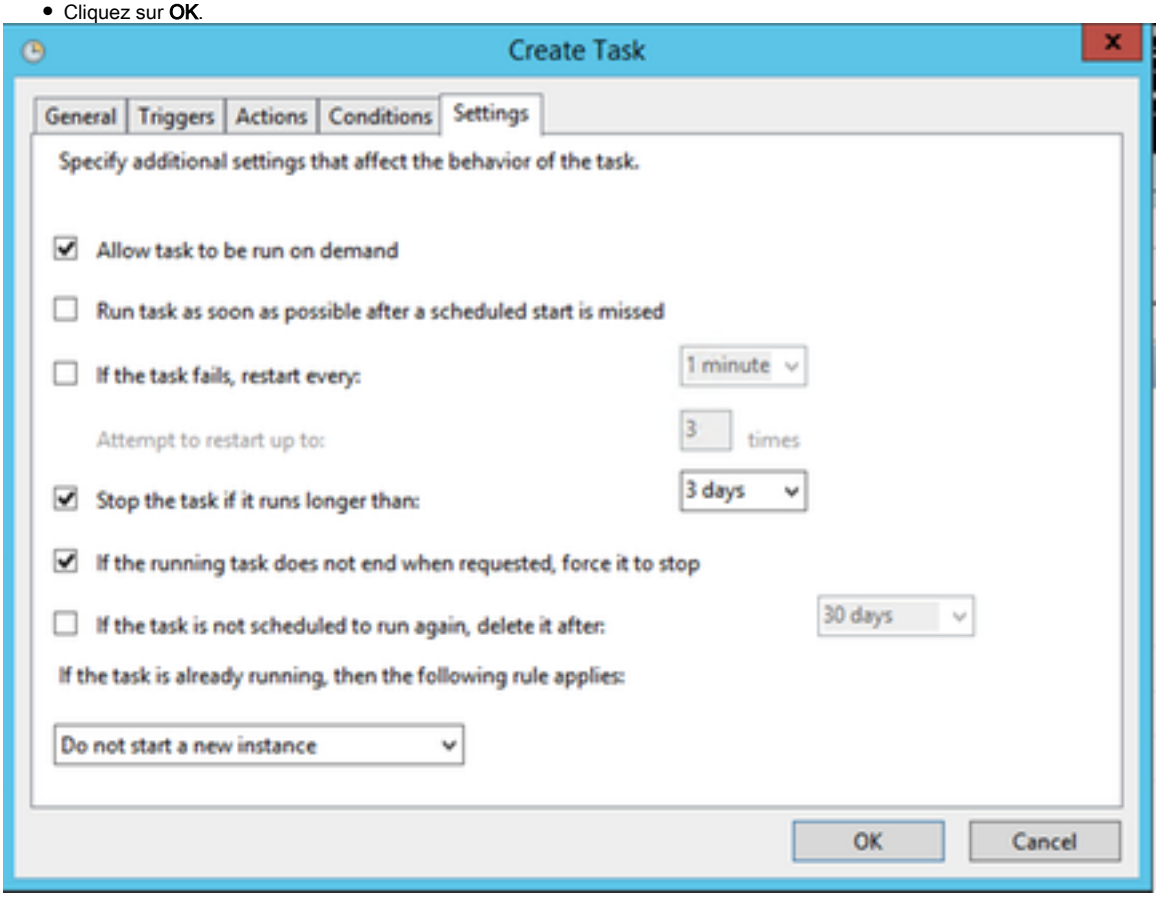
7. *[facultatif]* sélectionnez l'onglet de conditions.

   Vérifiez le sillage l'ordinateur pour exécuter cette option de tâche.



8 sélectionnez l'onglet Settings.

- Vérifiez qui **ne commencent pas un nouvel exemple** est sélectionné *dessous* **si la tâche s'exécute déjà.**
- Cliquez sur **OK**.

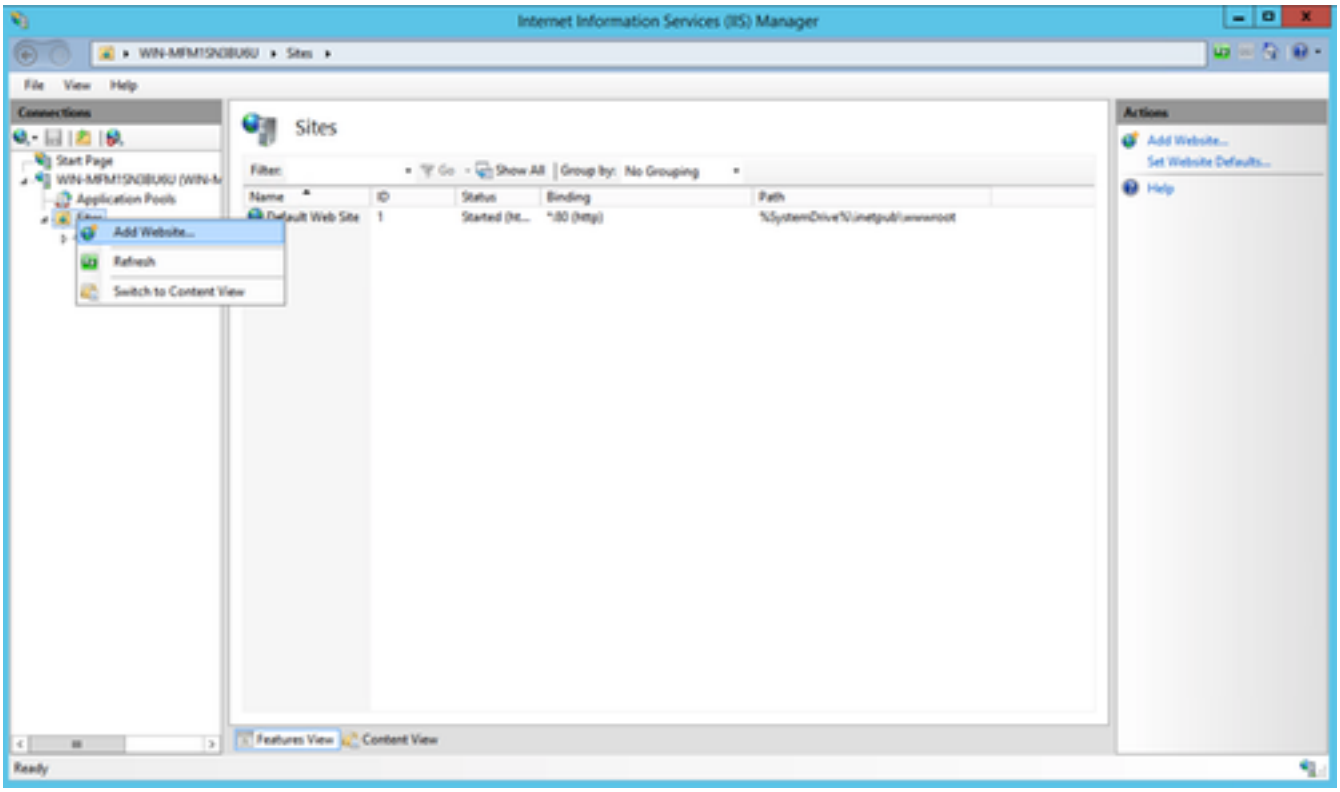


9. Entrez dans les qualifications pour le **compte qui exécutera la tâche**.

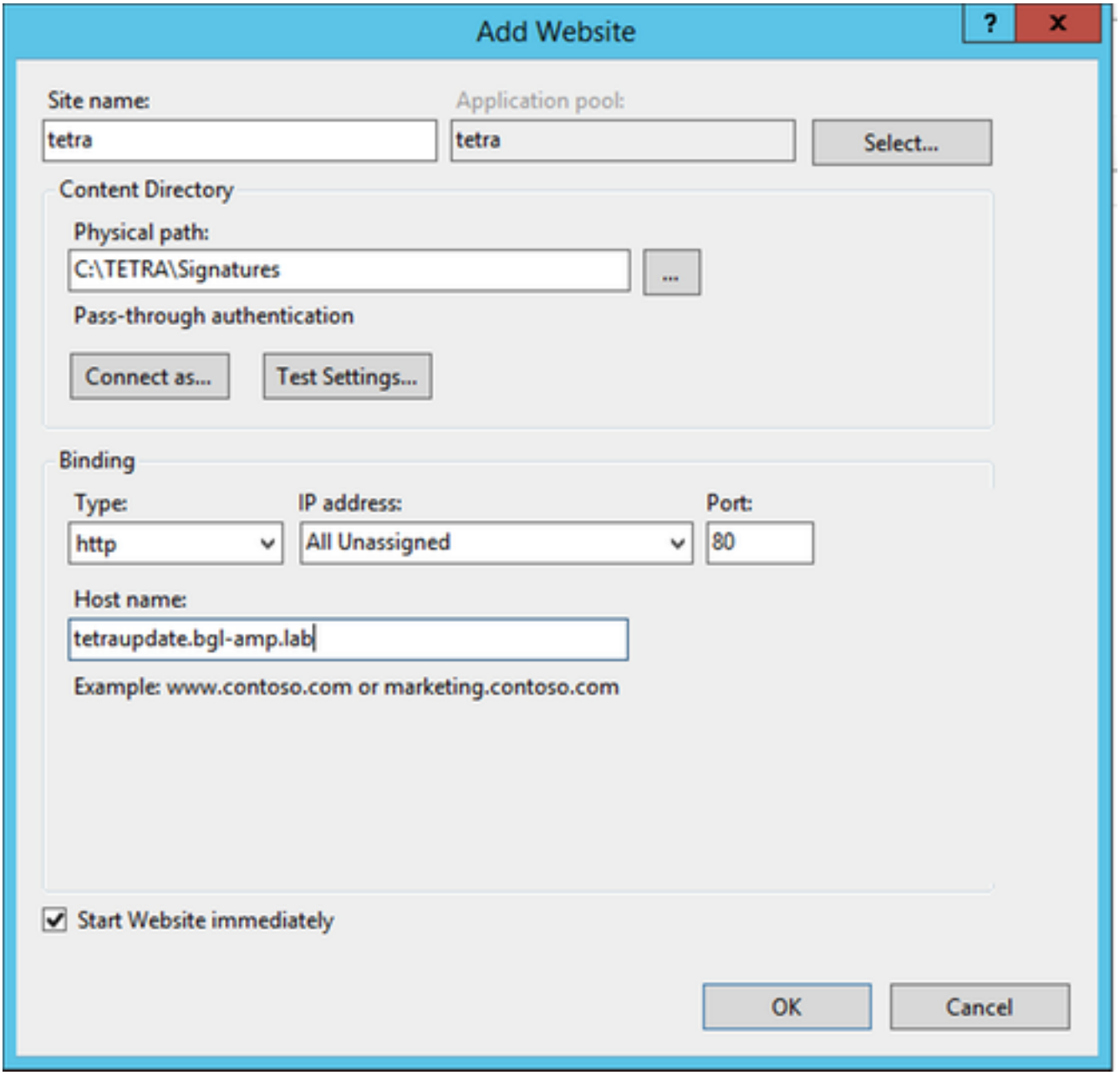
Note: Ignorez à l'étape 5 quand le groupe par défaut d'application est configuré.

1. Naviguez vers le gestionnaire (IIS) (**sous le gestionnaire du serveur > les outils**)

2. Développez la colonne de droite jusqu'à ce que le **répertoire de sites** soit visible, **clic droit et choisi ajoutez le site Web**.



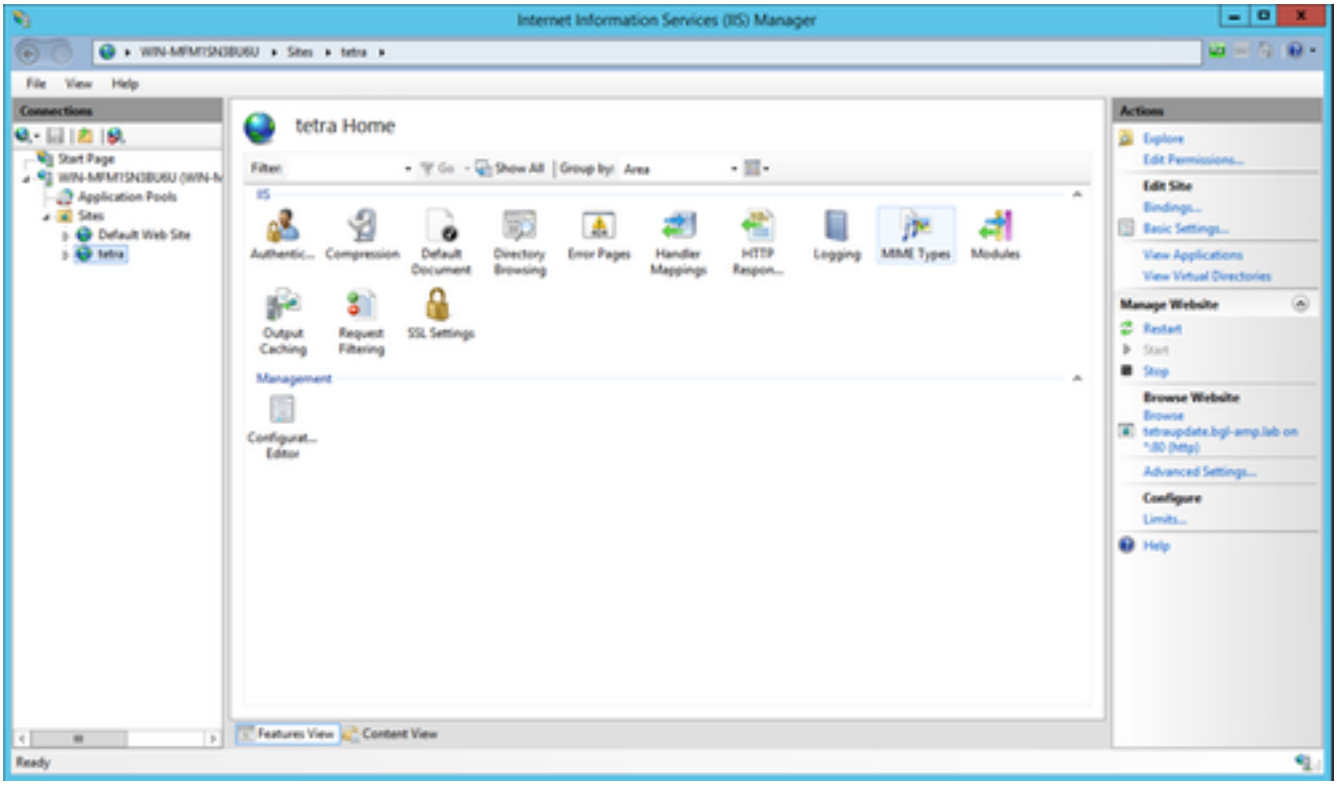
3. Choisissez un nom de choix. Pour le chemin physique sélectionnez le répertoire de *C:\TETRA\Signatures* où les signatures ont été téléchargées.



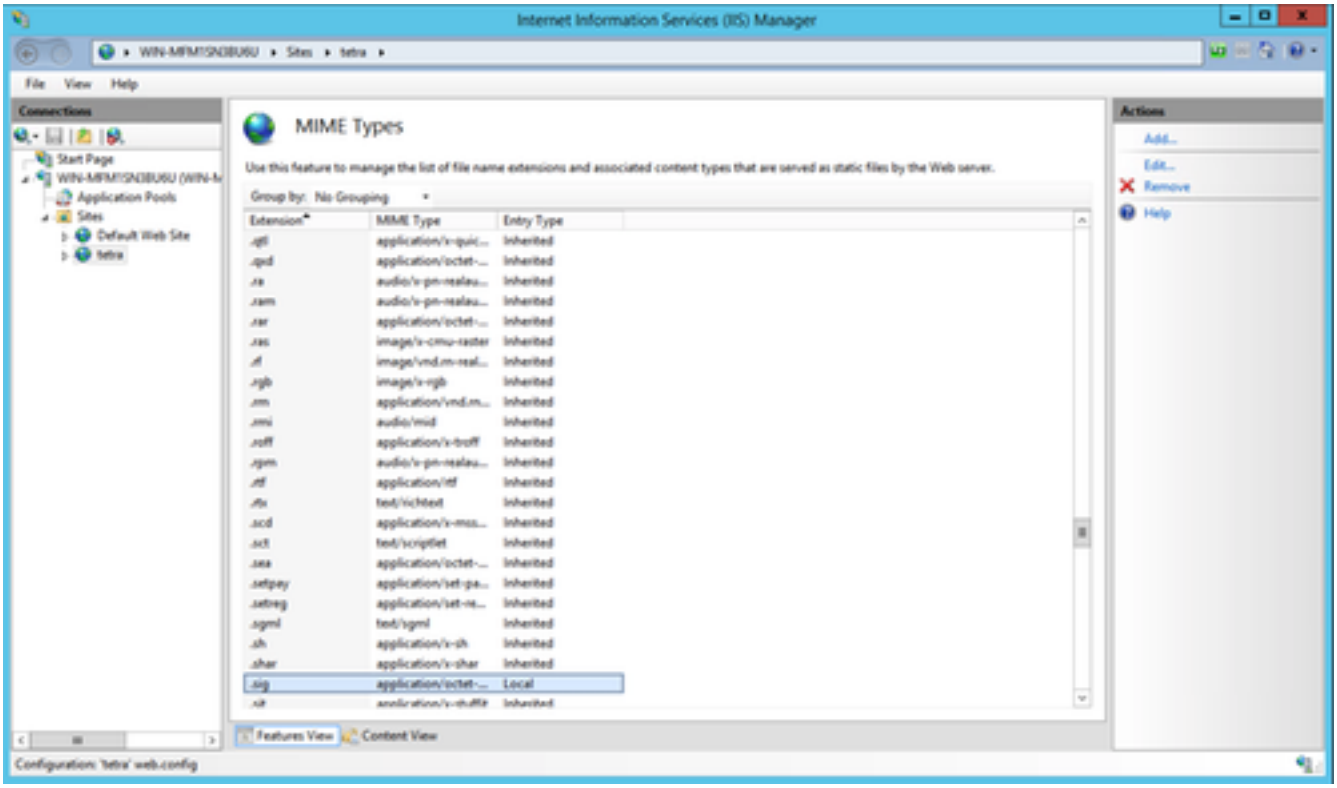
4. Laissez les attaches seules. **Configurez une adresse Internet distincte** et le nom du serveur, des noms choisis doit être résoluble par des clients. C'est l'URL que vous configurerez dans la stratégie.

5. Sélectionnez le site et naviguez vers des **types MIME** et **ajoutez les types MIME suivants** :

- .gzip, application/octet-flot
- .dat, application/octet-flot
- .id, application/octet-flot
- .sig, application/octet-flot



6. Naviguez vers le **fichier web.config (localisé** dans le répertoire de miroir), ajoutez les lignes suivantes au dessus du fichier.



Suivez les étapes sous la **configuration de politique** afin de configurer votre stratégie pour utiliser le serveur de mise à jour.

> **Note**: Cette modification manuellement avec un éditeur de texte ou avec le gestionnaire IIS à l'aide du module d'url rewrite. Le module de réécriture peut être installé de l'URL suivant ([https://www.iis.net/downloads/microsoft/url-rewrite)](https://www.iis.net/downloads/microsoft/url-rewrite)

Quand terminé les contenus du fichier de *C:\TETRA\Signatures\web.config* apparaîtront en tant que tels quand visualisé dans un éditeur de texte. (Le besoin de syntaxe et d'interligne de rester les mêmes que l'exemple fourni.)

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
    <system.webServer>
<directoryBrowse enabled="true" showFlags="Extension" />
<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>
        <staticContent>
            <mimeMap fileExtension="." mimeType="applicaton/octet-stream" />
            <mimeMap fileExtension=".gzip" mimeType="applicaton/octet-stream" />
            <mimeMap fileExtension=".dat" mimeType="application/octet-stream" />
            <mimeMap fileExtension=".id" mimeType="application/octet-stream" />
            <mimeMap fileExtension=".sig" mimeType="application/octet-stream" />
        </staticContent>
    </system.webServer>
</configuration>
```

Apache/Nginx

> Note: Les étapes fournies suppose que vous servez les signatures à partir du répertoire par défaut du logiciel d'accueil de Web.

1. **Créez un nouveau répertoire** sur votre lecteur de *racine* nommé **TETRA.**
2. **Défaites la fermeture éclair du** module téléchargé de scripts dans ce répertoire.
3. Exécutez l'***update-linux* du Chmod +x de*** commande pour donner aux scripts l'autorisation exécutable.
4. Exécutez la commande de chercher les TÉTRA fichiers de mise à jour.

sudo ./update-linux-x86-64 fetch --config config.xml --once --mirror /var/www/html/:
This command may vary depending on your directory structure.

5. Pour automatiser le processus de la mise à jour du serveur, ajoutez un travail de cron au serveur :

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

6. Continuez à suivre les étapes sous la **configuration de politique** afin de configurer votre stratégie pour utiliser le serveur de mise à jour.

Configuration de politique

1. Naviguez vers la stratégie pour utiliser le serveur de mise à jour et sous des ***paramètres avancés > TÉTRA*** sélectionnez : Case à cocher pour le serveur local de mise à jour d'AMPL'adresse Internet ou l'IP pour le serveur de mise à jour dans le format de <hostname.domain.root> ou d'adresse IP.

> Attention : N'incluez aucun protocole avant ou tous les sous-répertoires après autrement, ceci aura comme conséquence une erreur tout en téléchargeant.

Utilisation *[facultative]* **HTTPS de** case à cocher **pour de TÉTRA mises à jour de Definitin :** si le serveur local est configuré avec un certificat approprié et pour que les connecteurs utilisent HTTPS.

Vérification

Naviguez vers **C:\inetpub\wwwroot\, C:\TETRA\Signature,** ou le **répertoire de /var/www/html** et vérifiez les signatures mises à jour sont visibles, les signatures sont téléchargées du serveur au client d'extrémité par l'un ou l'autre attendant jusqu'au prochain cycle de sync ou supprimant manuellement les signatures existantes et attendant alors les signatures pour télécharger. Le par défaut est un intervalle d'une heure pour vérifier une mise à jour.

Informations connexes

- Support et documentation techniques - Cisco Systems
- AMP de Cisco pour des points finaux - TechNotes
- AMP de Cisco pour des points finaux - Guide utilisateur

.