Étapes de configuration du serveur de mise à jour AMP

Contenu

Introduction

Ce document décrit les étapes de configuration détaillées du serveur de mise à jour TETRA de Cisco Advanced Malware Protection (AMP).

Prérequis

- Connaissance des hôtes du serveur tels que Windows 2012R2 ou CentOS 6.9 x86_64.
- Connaissance des logiciels d'hébergement tels que, IIS (Windows uniquement), Apache, Nginx
- Hôtes du serveur configurés avec HTTPS activé, certificat approuvé valide installé.
- Option de serveur de mise à jour local HTTPS configurée.

Note: Pour plus d'informations sur l'activation de la configuration et des exigences du serveur de mise à jour local, reportez-vous au Chapitre 25 du Guide de l'utilisateur d'AMP for Endpoints, 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. Veuillez vous référer aux équipes d'assistance pour les produits respectifs pour toute question en dehors des étapes fournies.

Avertissement : Si AMP est configuré avec un serveur proxy, tout le trafic de mise à jour (y compris TETRA) continuera à être envoyé via le serveur proxy, dirigé vers votre serveur local. Assurez-vous que le trafic est autorisé à passer le proxy sans aucune modification pendant le transit.

Étapes d'installation

Toutes les plates-formes

1. Confirmez le système d'exploitation (OS) de votre serveur d'hébergement.
2. Confirmez votre portail de tableau de bord AMP for Endpoints, téléchargez le package logiciel Updater et le fichier de configuration.

Console AMP for Endpoints :

États-Unis - 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

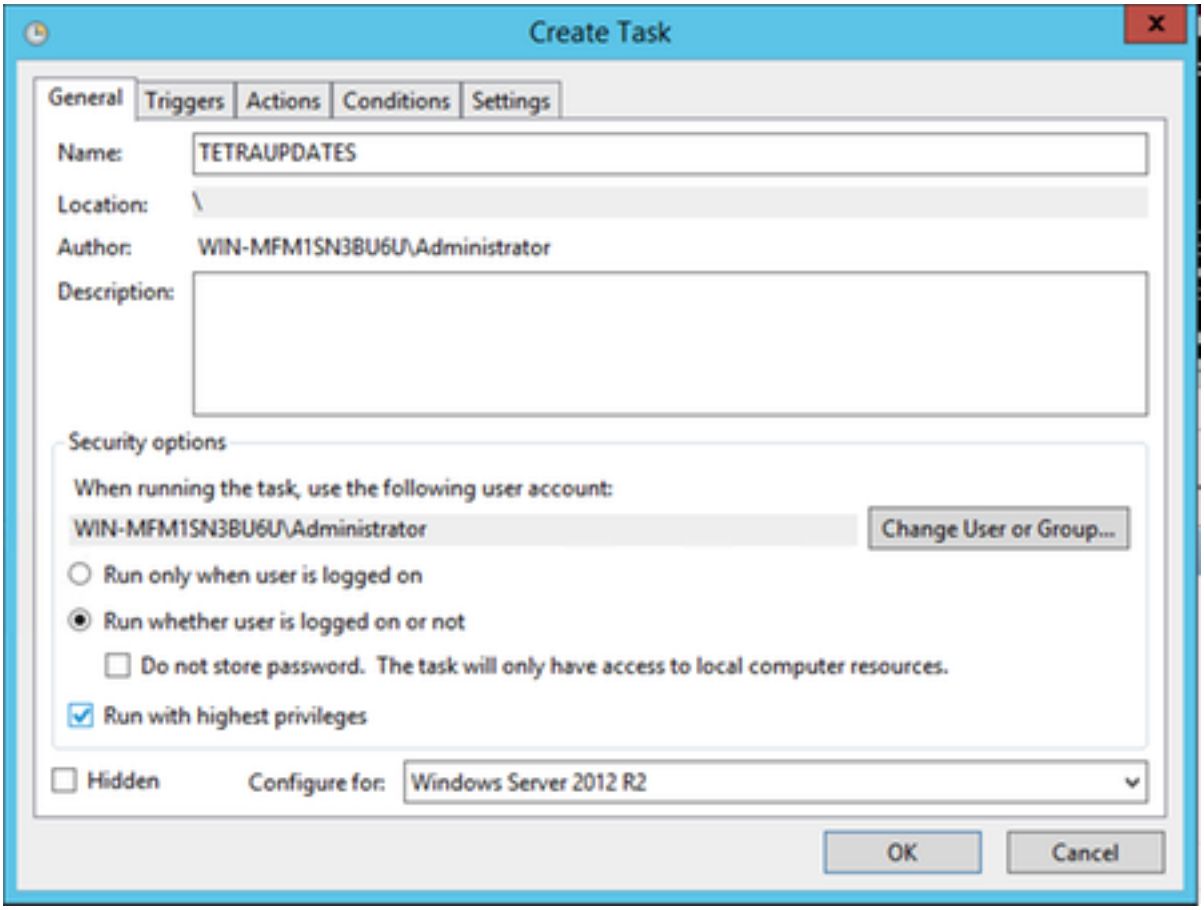
> **Note**: Les étapes ci-dessous sont basées sur le nouveau pool d'applications IIS pour héberger les signatures, **pas** le pool d'applications par défaut. Pour utiliser le pool par défaut, modifiez le dossier **—miroir** dans les étapes fournies pour refléter le chemin d'hébergement Web par défaut (**C:\inetpub\wwwroot**)

Création de répertoire

1. Créez un nouveau dossier sur le lecteur racine, nommez-le **TETRA**.
2. Copiez le package logiciel de mise à jour AMP compressé et le fichier de configuration dans le dossier **TETRA** créé.
3. Décompressez le package logiciel dans ce dossier.
4. Créez un nouveau dossier appelé **Signatures** dans le dossier TETRA.

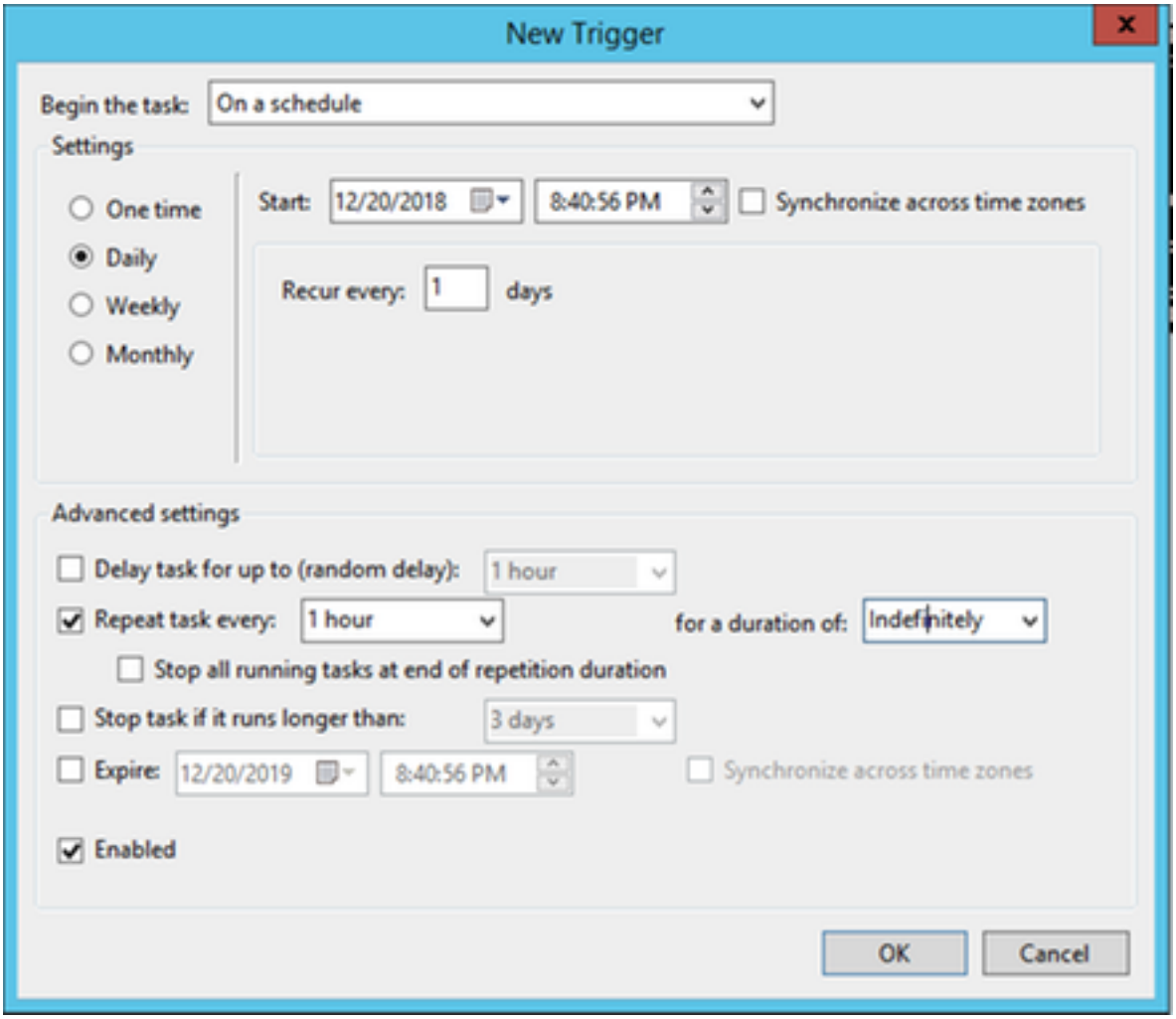
Mettre à jour la création de la tâche

1. Ouvrez la ligne de commande et accédez au dossier *C:\TETRA.**cd C:\TETRA***
2. Exécutez la commande ***update-win-x86-64.exe fetch —config="C:\TETRA\config.xml" —once —miroir C:\TETRA\Signatures***
3. Ouvrez le Planificateur de tâches et créez une nouvelle tâche. (Action > Créer une tâche) pour exécuter automatiquement le logiciel de mise à jour avec les options suivantes si nécessaire :
4. Sélectionnez l'onglet Général. Entrez un nom pour la tâche.Sélectionnez **Exécuter si l'utilisateur est connecté ou non**.Sélectionnez **Exécuter avec les privilèges les plus élevés.**Sélectionnez **le système d'exploitation** dans la liste déroulante **Configurer.**



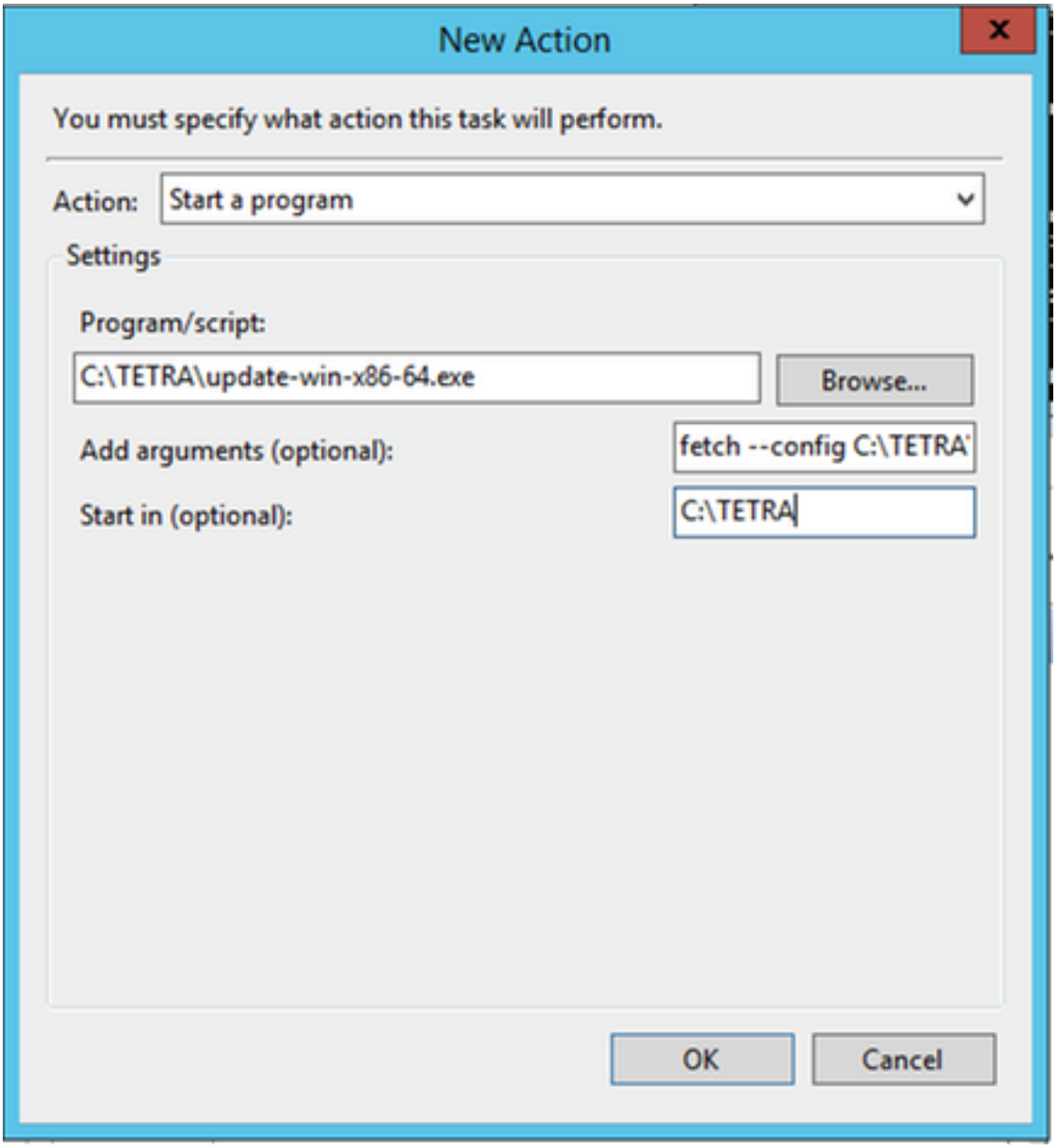
5. Sélectionnez l'onglet Déclencheurs.

- Cliquez sur New.
- Sélectionnez **Sur un planning** dans la liste déroulante **Commencer la tâche**.
- Sélectionnez **Quotidien** sous Paramètres.
- Cochez **Répéter la tâche toutes les** et **sélectionnez 1 heure** dans la liste déroulante et sélectionnez **Indéfiniment** dans la zone "**pour une durée de : »**
- Vérifiez que **Enabled** est **coché**.
- Cliquez sur **OK**.



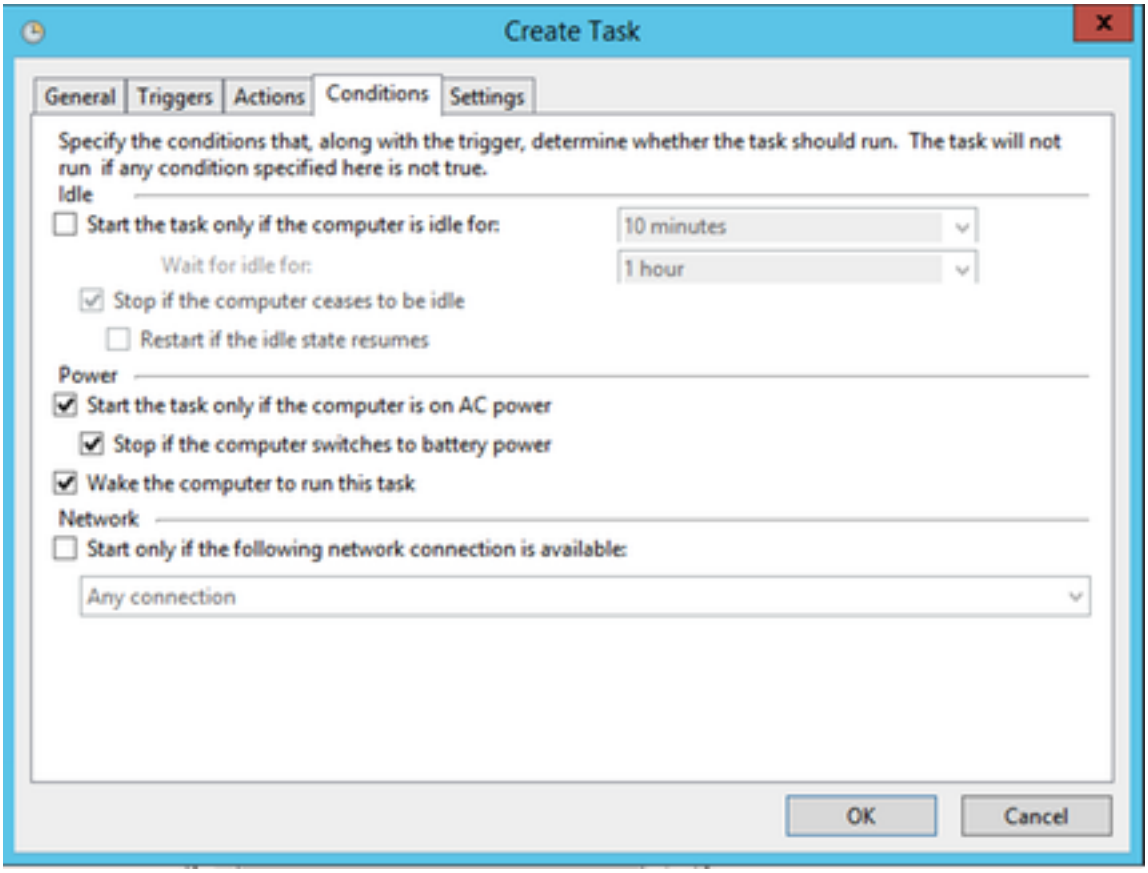
6. Sélectionnez l'onglet Actions

- Cliquez sur **New**.
- Sélectionnez **Démarrer un programme** dans la liste déroulante **Action**.
- Entrez ***C:\TETRA\update-win-x86-64.exe*** dans le champ **Programme/script**.
- Entrez ***fetch —config C:\TETRA\config.xml —once —miroir C:\TETRA\Signatures*** dans le champ **Ajouter des arguments**.
- Entrez ***C:\TETRA*** dans le champ **Démarrer**.
- Click OK



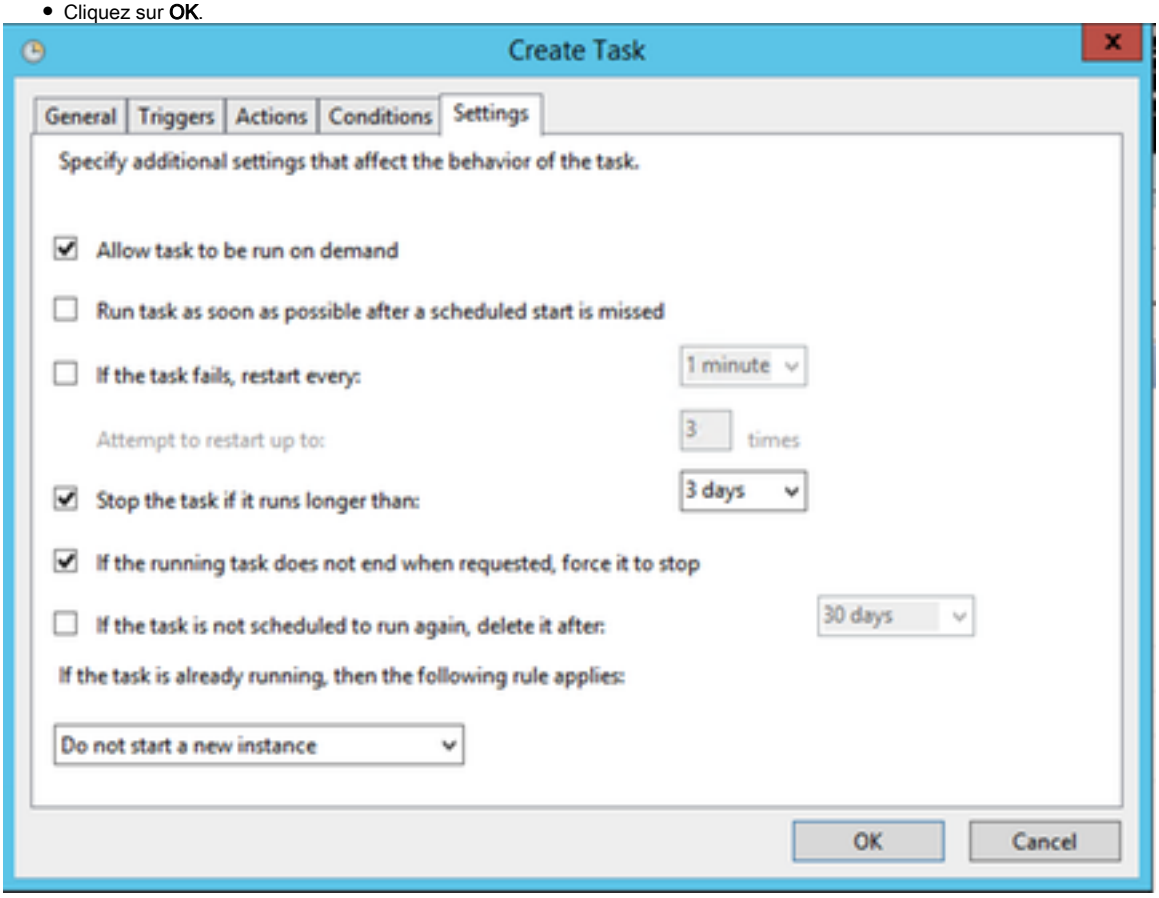
7. *[Facultatif]* Sélectionnez l'onglet Conditions.

   Cochez la case Réveiller l'ordinateur pour exécuter cette option de tâche.



8 Sélectionnez l'onglet Paramètres.

- Vérifiez que **Ne pas démarrer une nouvelle instance** est sélectionné *sous* **Si la tâche est déjà en cours d'exécution.**
- Cliquez sur **OK**.



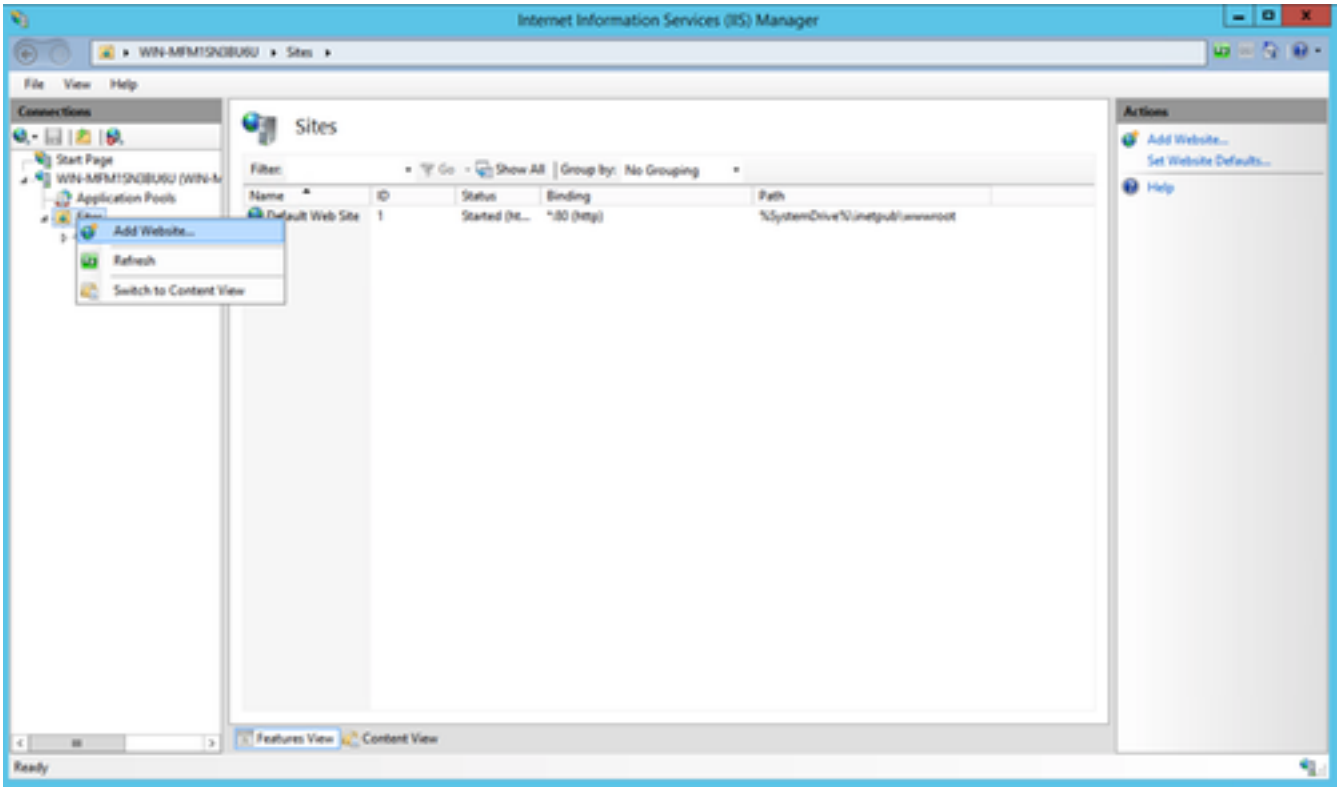
9. Entrez les informations d'identification **du compte qui exécutera la tâche**.

Configuration du Gestionnaire IIS

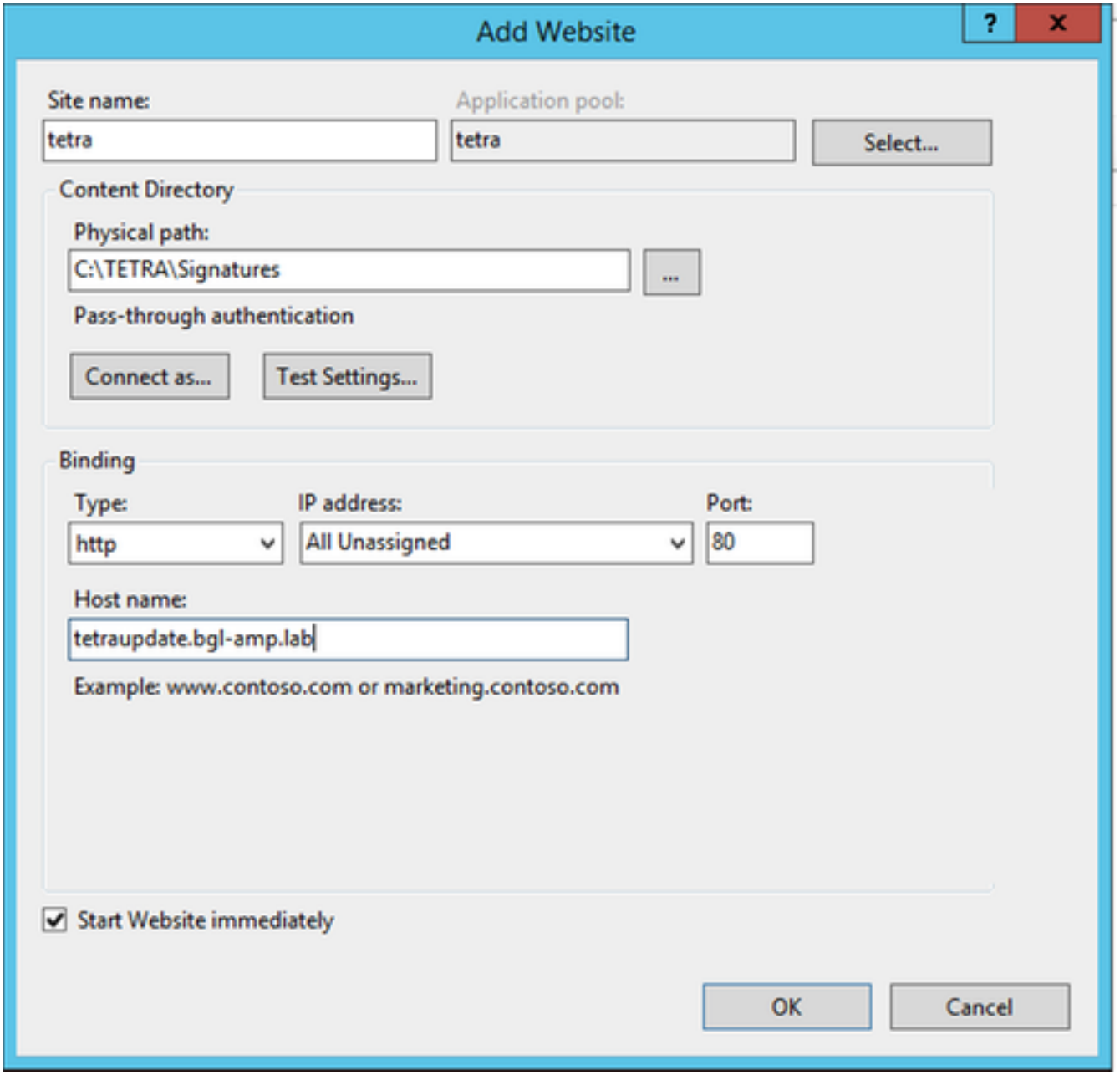
Note: Passez à l'étape 5 lorsque le pool d'applications par défaut est configuré.

1. Naviguez jusqu'au Gestionnaire (IIS) (**sous Gestionnaire de serveur > Outils**)

2. Développez la colonne de droite jusqu'à ce que le **dossier Sites** soit visible, **Cliquez avec le bouton droit et sélectionnez Ajouter un site Web**.



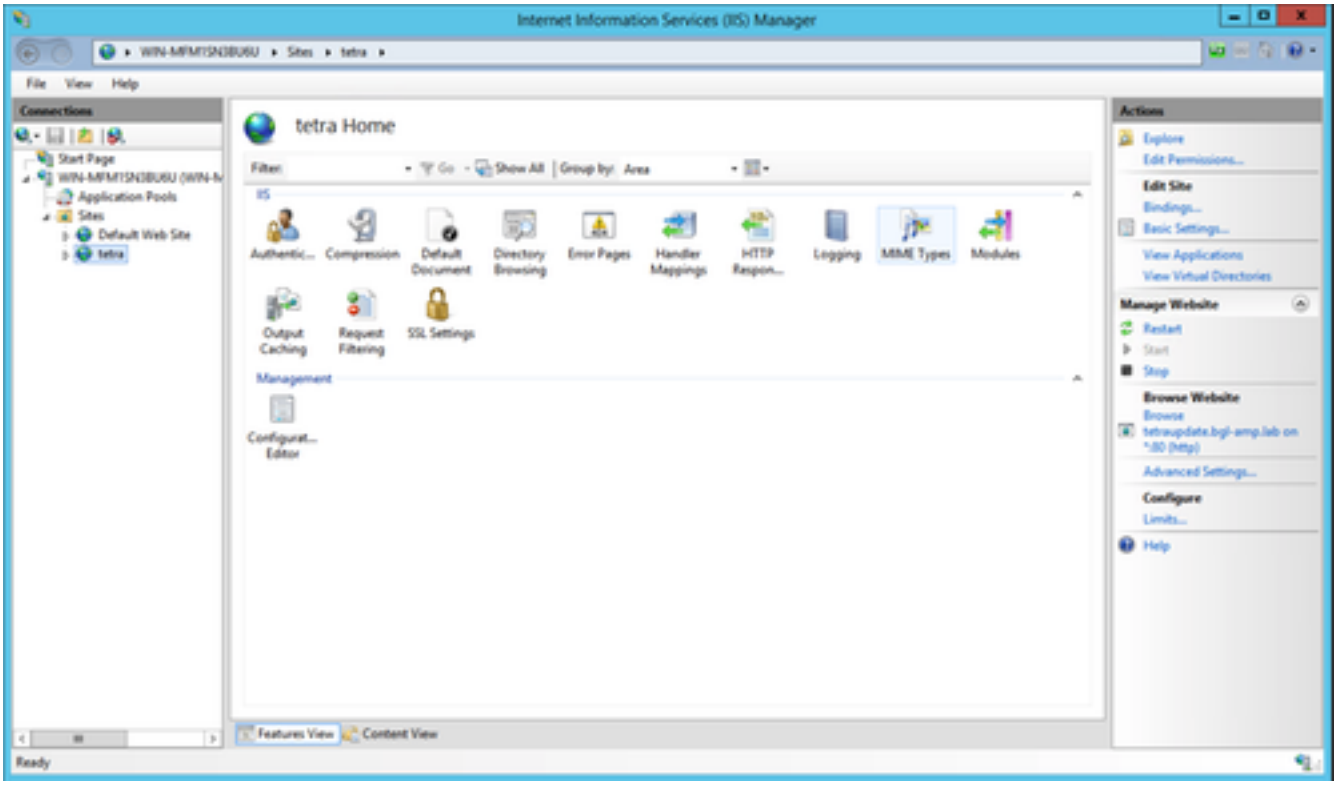
3. Choisissez un nom de choix. Pour le chemin physique, sélectionnez le dossier *C:\TETRA\Signatures* dans lequel les signatures ont été téléchargées.



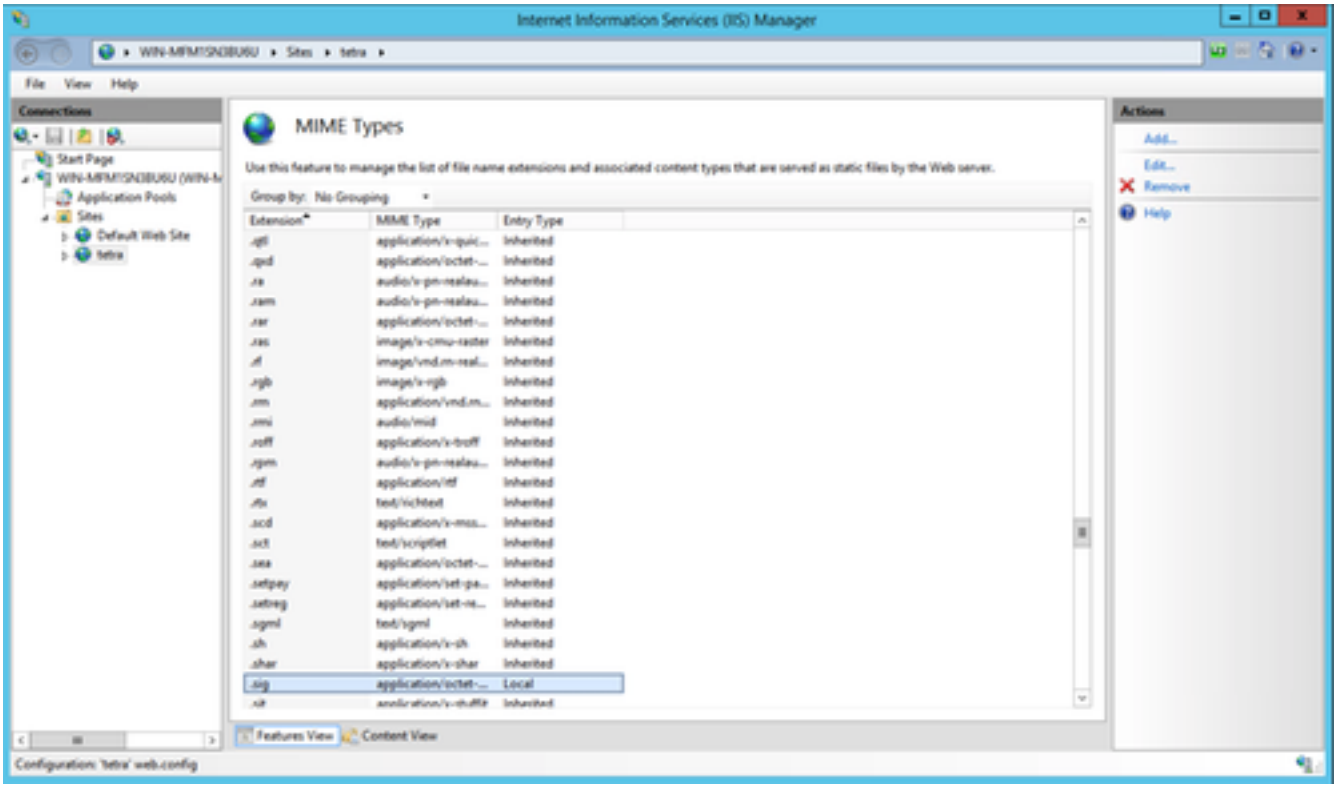
4. Laissez les liaisons tranquilles. **Configurez un nom d'hôte** et un nom de serveur distincts, les noms choisis doivent pouvoir être résolus par les clients. Il s'agit de l'URL que vous allez configurer dans la stratégie.

5. Sélectionnez le site et accédez aux **types MIME** et **ajoutez les types MIME suivants** :

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



6. Accédez au **fichier web.config** (situé dans le dossier miroir), ajoutez les lignes suivantes en haut du fichier.



Lorsque vous avez terminé, le contenu du fichier *C:\TETRA\Signatures\web.config* apparaît comme tel lorsqu'il est affiché dans un éditeur de texte. (La syntaxe et l'espacement doivent rester les mêmes que dans l'exemple fourni.)

> **Note**: Le connecteur AMP for Endpoints nécessite la présence de l'en-tête HTTP du serveur dans la réponse pour un bon fonctionnement. Si l'en-tête HTTP du serveur a été désactivé, le serveur Web peut avoir besoin d'une configuration supplémentaire spécifiée ci-dessous.

L'extension url-rewrite doit être installée. Ajoutez l'extrait XML suivant à la configuration du serveur sur /[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>
```

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

Lorsque vous avez terminé, le contenu du fichier *C:\TETRA\Signatures\web.config* apparaît comme tel lorsqu'il est affiché dans un éditeur de texte. (La syntaxe et l'espacement doivent rester les mêmes que dans l'exemple fourni.)

Apache / Nginx

> **Note**: Les étapes fournies supposent que vous servez les signatures du répertoire par défaut du logiciel d'hébergement Web.

1. **Créez un nouveau dossier** sur votre lecteur *racine* nommé **TETRA.**
2. **Décompressez** le package de scripts téléchargés dans ce dossier.
3. Exécutez la commande ***Chmod +x update-linux**** pour donner l'autorisation exécutable aux scripts.
4. Exécutez la commande pour récupérer les fichiers de mise à jour 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. Pour automatiser le processus de mise à jour du serveur, ajoutez une tâche 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 **Configuration de stratégie** afin de configurer votre stratégie pour utiliser le serveur de mise à jour.

Configuration de la stratégie

1. Accédez à la stratégie pour utiliser le serveur de mise à jour et sous ***Paramètres avancés > TETRA*** sélectionnez : Case à cocher pour le serveur de mise à jour AMP localNom d'hôte ou adresse IP du serveur de mise à jour au format <hostname.domain.root> ou adresse IP.

Attention : N'incluez aucun protocole avant ou aucun sous-répertoire après le reste, cela entraînera une erreur lors du téléchargement.

[Facultatif] Case à cocher **Utiliser HTTPS pour les mises à jour de définition TETRA :** si le serveur local est configuré avec un certificat approprié et que les connecteurs utilisent HTTPS.

Vérification

Accédez au **répertoire C:\inetpub\wwwroot\, C:\TETRA\Signature** ou **/var/www/html** et vérifiez que les signatures mises à jour sont visibles. Les signatures sont téléchargées du serveur vers le client final en attendant le cycle de synchronisation suivant ou en supprimant manuellement les signatures existantes, puis en attendant le téléchargement des signatures. La valeur par défaut est un intervalle d'une heure pour vérifier la présence d'une mise à jour.

Informations connexes

- Support et documentation techniques - Cisco Systems
- Cisco AMP for Endpoints - TechNotes
- Cisco AMP for Endpoints - Guide de l'utilisateur

.