AMP TÉTRA sur-Prem des étapes de configuration du serveur

Contenu

Introduction

Ce document décrit les étapes de configuration en détail pour Cisco a avancé la protection de malware (AMP) TÉTRA sur-premesis le serveur.

Conditions préalables

- L'utilisateur a déjà configuré Windows 2012R2 ou le serveur de CentOS pour héberger l'installation.
- (Windows seulement) la caractéristique IIS est déjà installée et des fondements est configurés. Ce guide configurera un nouvel IIS « groupe d'application » mais les mêmes étapes pourraient être appliquées au groupe d'application du par défaut IIS.
- [AMP pour la stratégie de déploiement de points finaux](#)
- [AMP pour le guide utilisateur de points finaux](#)

AMP TÉTRA sur-Prem des étapes de configuration du serveur

Téléchargement de signature au serveur local

Installez la tâche d'effort par étapes dans l'AMP pour le guide utilisateur de points finaux, notant l'emplacement du répertoire configuré de miroir. Sur option, vous pouvez appliquer la commande manuelle d'effort, notant de nouveau l'emplacement du répertoire configuré de miroir.

Service des signatures aux connecteurs

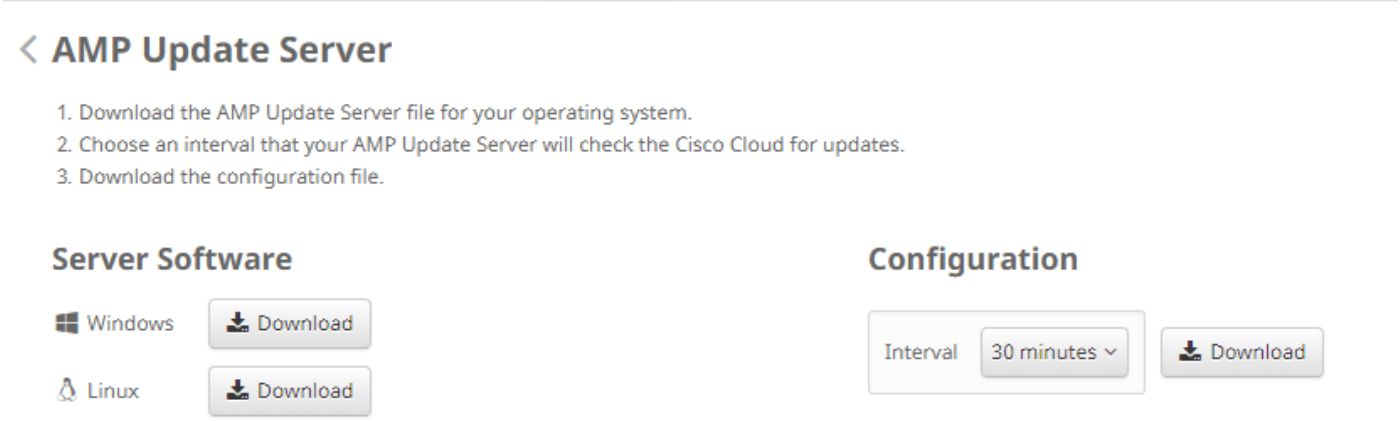
Windows IIS

1. Naviguez vers le gestionnaire (IIS) {sous le gestionnaire du serveur | Outils}

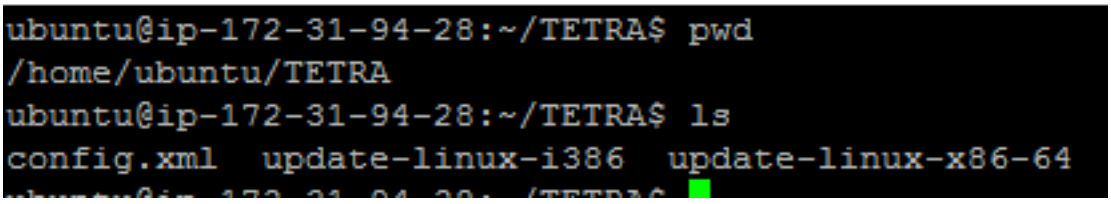
2. Développez la colonne de droite jusqu'à ce que le répertoire de sites apparaisse, cliquent avec le bouton droit et choisi *ajoutez le site Web.*
3. Nommez le site comme vous souhaitez ; Pour le chemin physique sélectionnez le répertoire de miroir où les signatures ont été téléchargées.
4. Des attaches peuvent être conservées ; Configurez une adresse Internet distincte puis le nom du serveur et assurez-vous que les clients peuvent résoudre ceci et vous faites une note. C'est l'URL que vous configurerez dans la stratégie.
5. Une fois que configuré ; 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-flotsig, application/octet-flot
6. Naviguez vers le fichier web.config (localisé dans le répertoire de miroir) et ajoutez les lignes suivantes :
```
<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>
```
(L'échantillon web.config A est également relié à cet article.)
7. Configurez la stratégie avec l'URL configuré dans l'étape 4. lors de l'enregistrement, des connecteurs sera utilisation sur-Prem le serveur pour des mises à jour de signature.

Apache

Téléchargez le logiciel de serveur et la configuration de mise à jour d'AMP directement au serveur principal, ou téléchargez-la localement et transférez-alors la plus de :



Placez le logiciel de serveur et le fichier de configuration dans le même répertoire :



La nécessité de scripts de mise à jour-Linux d'être exécutable avant que vous puissiez les exécuter. Changez les permissions du fichier par l'**update-linux* du chmod +x d'**exécution. Vous utiliserez seulement le script le type de l'architecture du serveur principal étant assorti :

```
ubuntu@ip-172-31-94-28:~/TETRA$ chmod +x update-linux-*
ubuntu@ip-172-31-94-28:~/TETRA$ ls -al
total 18468
drwxrwxr-x 2 ubuntu ubuntu     4096 Mar 21 12:22 .
drwxr-xr-x 5 ubuntu ubuntu     4096 Mar 21 12:20 ..
-rw-r--r-- 1 ubuntu ubuntu     1029 Mar 21 12:21 config.xml
-rwxr-xr-x 1 ubuntu ubuntu  8755622 Jan  8 22:33 update-linux-i386
-rwxr-xr-x 1 ubuntu ubuntu 10141387 Jan  8 22:33 update-linux-x86-64
```

Installez Apache. Pour l'exemple, Ubuntu 16.04 est utilisé, ainsi la commande est sudo convenable-**obtiennent l'**intsall **apache2 - y** :

```
ubuntu@ip-172-31-94-28:~$ sudo apt-get install apache2 -y
```

Ceci peut varier selon votre version de Linux.

Exécutez la commande de chercher les TÉTRA fichiers de mise à jour, **effort de ./update-linux-x86-64 de sudo --config config.xml** --**miroir /var/www/html/ :**

```
ubuntu@ip-172-31-94-28:~/TETRA$ sudo ./update-linux-x86-64 fetch --config config.xml --mirror /var/www/html/
INFO: [update-linux-x86-64] 2018/03/21 12:26:44 Updating 927 entries for the av32bit AV database.
INFO: [update-linux-x86-64] 2018/03/21 12:26:44 Fetching updates.
```

Ceci peut varier selon votre structure de répertoire.

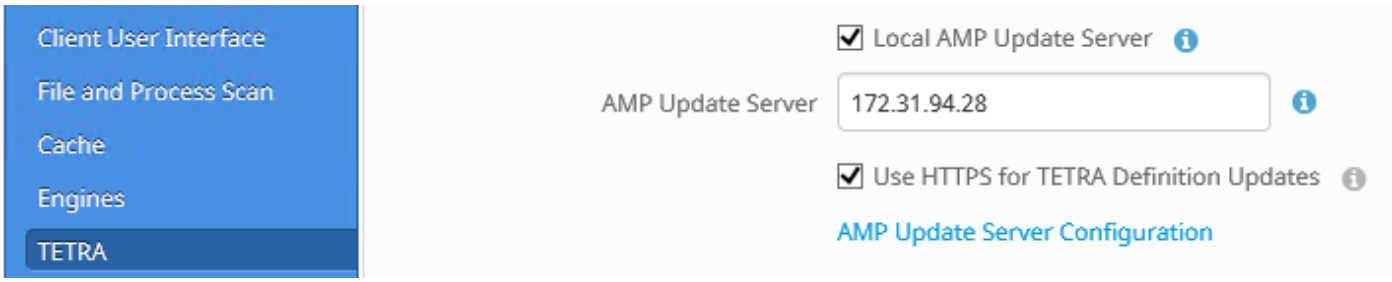
Quand la commande a fini de télécharger les fichiers et est prête, selon votre log nivelez-vous peut voir qu'un message indiquant le système lançant est établi dans le serveur HTTP :

```
DEBUG: [update-linux-x86-64] 2018/03/21 12:28:05 tetra.go:527: Activating the built-in HTTP server
```

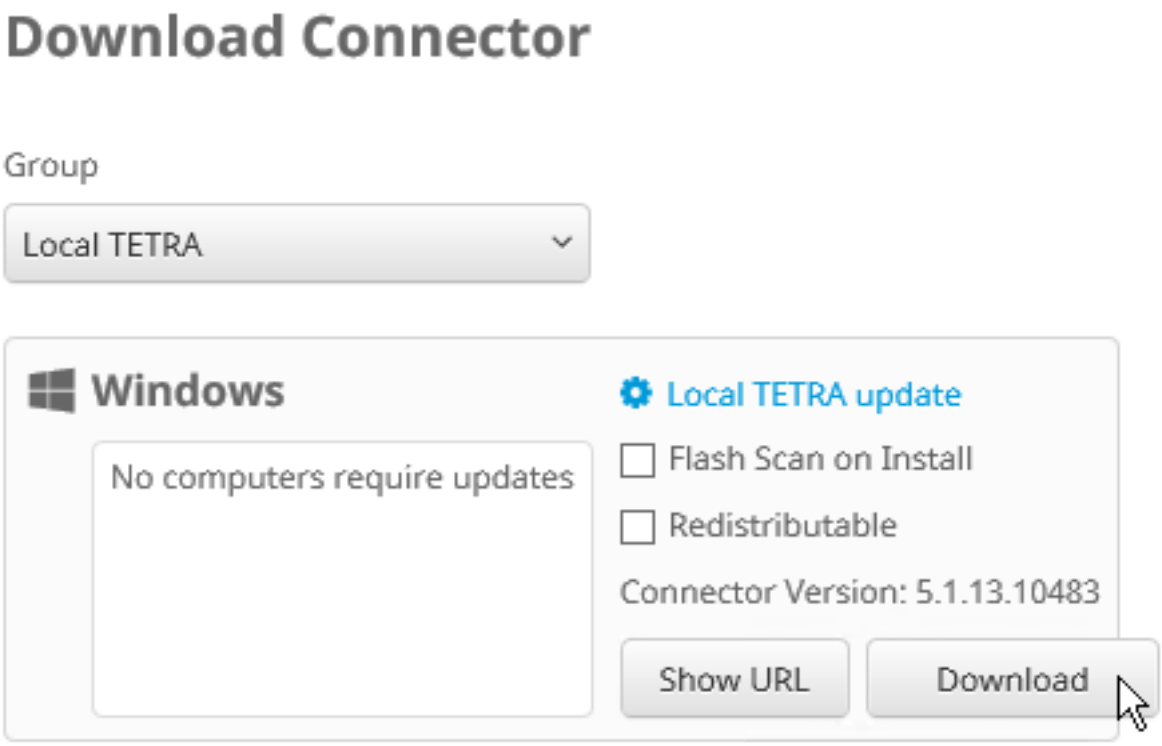
Pour vérifier la taille des fichiers téléchargés pour TÉTRA, vous pouvez exécuter la commande **du - /var/www/html/ SH**, ou votre chemin du répertoire :

```
ubuntu@ip-172-31-94-28:~$ du -sh /var/www/html
756M    /var/www/html
```

Assurez que votre stratégie d'AMP a les options de serveur locales de mise à jour d'AMP spécifiées et indiquez le serveur configuré ci-dessus. Seulement le point à l'IP ou l'adresse Internet, aucun sous-répertoires, ou le client ne pourra pas se connecter correctement au serveur de mise à jour :



Ensuite, faites un saut à votre machine cliente et téléchargez le connecteur associé avec la stratégie comprenant votre serveur local de mise à jour d'AMP



:

Exécutez l'installateur.

Les fichiers > Cisco > l'AMP de programme > tétra > répertoire de **modules d'extension** seront blanc jusqu'à ce qu'une TÉTRA mise à jour de définition soit tirée du serveur local. Vous pouvez surveiller le serveur par la **queue d'**exécution **- f /var/log/apache2/access.log** pour voir quand il est accédé à par le client :

```
ubuntu@ip-172-31-94-28:~$ tail -f /var/log/apache2/access.log
172.31.92.41 - - [21/Mar/2018:13:14:55 +0000] "GET /v2/repository/1/6/F/E/yishield.xmd.16fe55b5f9369afcec02fc0b5db7de86.gzip HTTP/1.1" 200 2220 "-" "WSLib 1.4 [3, 0, 0, 129]"
172.31.92.41 - - [21/Mar/2018:13:14:55 +0000] "GET /v2/repository/5/A/3/9/z.xmd.5a39c18bf0d8f65c4124909f2ba424c9.gzip HTTP/1.1" 200 2143 "-" "WSLib 1.4 [3, 0, 0, 129]"
172.31.92.41 - - [21/Mar/2018:13:14:55 +0000] "GET /v2/repository/5/6/3/3/zip.xmd.5633f8e1149f115fbcb43fc4408a9d8b.gzip HTTP/1.1" 200 65242 "-" "WSLib 1.4 [3, 0, 0, 129]"
172.31.92.41 - - [21/Mar/2018:13:14:55 +0000] "GET /v2/repository/A/0/F/5/zoo.xmd.a0f5c371ecf1c7e0c5d353f29472c706.gzip HTTP/1.1" 200 691 "-" "WSLib 1.4 [3, 0, 0, 129]"
172.31.92.41 - - [21/Mar/2018:13:14:55 +0000] "GET /v2/repository/D/E/C/3/ocra.xmd.dec3926b91784c08bf5701a43a7492c1.gzip HTTP/1.1" 200 9394 "-" "WSLib 1.4 [3, 0, 0, 129]"
172.31.92.41 - - [21/Mar/2018:13:14:55 +0000] "GET /v2/repository/D/C/C/5/pyinstaller.xmd.dcc578a12db0ff08b5e3b71917326c91.gzip HTTP/1.1" 200 8161 "-" "WSLib 1.4 [3, 0, 0, 129]"
172.31.92.41 - - [21/Mar/2018:13:14:55 +0000] "GET /v2/repository/D/8/4/7/vbtok.cvd.d8471c9cc7a11ecbdaa0cd8c3fc03b1d.gzip HTTP/1.1" 200 43077 "-" "WSLib 1.4 [3, 0, 0, 129]"
172.31.92.41 - - [21/Mar/2018:13:14:55 +0000] "GET /v2/repository/F/9/8/7/sysarch.xmd.f987c3a9d4550c1103d234de720575d4.gzip HTTP/1.1" 200 1697 "-" "WSLib 1.4 [3, 0, 0, 129]"
172.31.92.41 - - [21/Mar/2018:13:14:55 +0000] "GET /v2/repository/A/D/2/B/syscan.xmd.ad2b11023df38ecdd94a86c978c4cf6f.gzip HTTP/1.1" 200 4077 "-" "WSLib 1.4 [3, 0, 0, 129]"
172.31.92.41 - - [21/Mar/2018:13:14:55 +0000] "GET /v2/repository/C/4/8/C/bdcore.dll.c48c78076fe757b39e8671bafaaeea96.gzip HTTP/1.1" 200 35246 "-" "WSLib 1.4 [3, 0, 0, 129]"
```

Vous pouvez également vérifier les configurations sur le client dans les fichiers de programme > Cisco > l'AMP > le fichier policy.xml :

```
<updater>
  <server>172.31.94.28</server>
  <interval>3600</interval>
  <enable>1</enable>
  <https>1</https>
</updater>
```

Si vous sélectionniez l'option HTTPS pour le serveur local de mise à jour, assurez que vous avez un certificat valide et de confiance sur votre serveur et le trafic est forcé à HTTPS.

Pour automatiser le processus de la mise à jour du serveur, vous pouvez ajouter un travail de cron au serveur :

```
0 * * * * [Full path to binary]/update-linux-[i386 or x86-64] fetch --once --config [Full path
```

```
to config]/config.xml - -mirror MIRRORDIR
```

De mon exemple il serait :

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

Si la connexion n'établit pas, le **programme de** contrôle **classe > Cisco > AMP > 5.1.13 > sfc.exe.log** pour le message suivant :

```
ERROR: TetraUpdateInterface::update Update failed with error -2100
```

Si vous voyez cette erreur, elle indique que le serveur local ne peut pas être atteint. Assurez-vous que les fichiers ne sont hébergés dans le répertoire racine pour Apaches et pas un sous-répertoire.

Nginx

Les étapes sont identiques que les étapes de mise à jour d'Apache excepté exécuter Ngnix, installé par **sudo d'**exécution convenable-**obtiennent installent le nginx de la** ligne de commande. Les fichiers hébergés sont toujours dans le répertoire « /var/www/html/ ».

Vérification

Vous pouvez vérifier les signatures téléchargées du serveur l'un ou l'autre en attendant jusqu'au prochain cycle de sync ou en supprimant manuellement les signatures existantes et en attendant alors les signatures pour télécharger. Le par défaut est un intervalle d'une heure pour vérifier une mise à jour.