# Étapes de configuration du serveur de mise à jour AMP

# Contenu

Introduction Prérequis Étapes d'installation Toutes les plates-formes Windows IIS Création de répertoire Mettre à jour la création de la tâche Configuration du Gestionnaire IIS Apache / Nginx Configuration de la stratégie Vérification Informations connexes

# 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 <u>ici</u>.

(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:ITETRA. cd C:ITETRA
- 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.

•		Create Task			×
General Trig	gers Actions Cond	itions Settings			
Name: TETRAUPDATES					
Location:	X.				
Author:	WIN-MFM1SN3BU60	/\Administrator			
Description:					
- Security opt	ions				
When runni	ng the task, use the fo	ollowing user account:			
WIN-MFM1	SN3BU6U\Administra	tor		Change Use	r or Group
O Run only when user is logged on					
Run whe	ther user is logged on	or not			
Do not store password. The task will only have access to local computer resources.					
Run with	highest privileges				
🗌 Hidden	Configure for:	Windows Server 2012 R2			~
				ОК	Cancel

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.

New Trigger	x
Begin the task: On a schedule   Settings   One time   Daily   Weekly   Monthly     Recur every:     1     days	
Advanced settings  Delay task for up to (random delay): 1 hour  Repeat task every: 1 hour  for a duration of: Indefinitely  for a duration of: Stop all running tasks at end of repetition duration Stop task if it runs longer than: 3 days  Expire: 12/20/2019  Ket Adv:56 PM  Synchronize across time zones  Enabled	
OK Cancel	

## 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:ITETRA dans le champ Démarrer.
- Click OK

	New Action	×			
You must specify what action this task will perform.					
Action:	Start a program	~			
Settings	;				
Progra	m/script:				
C:\TET	RA\update-win-x86-64.exe	Browse			
Add ar	guments (optional):	fetchconfig C:\TETRA			
Start in	n (optional):	C:\TETRA			
		OK Cancel			

7. [Facultatif] Sélectionnez l'onglet Conditions.

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

O Creat	e Task	×			
General Triggers Actions Conditions Settings					
Specify the conditions that, along with the trigger, determine whether the task should run. The task will not run if any condition specified here is not true.					
Start the task only if the computer is idle for:	10 minutes	~			
Wait for idle for:	1 hour	~			
Stop if the computer ceases to be idle					
Restart if the idle state resumes					
Power					
Start the task only if the computer is on AC power					
Stop if the computer switches to battery power					
Wake the computer to run this task					
Network     Start only if the following network connection is ava	ilable:				
Any connection		~			
	OK	Cancel			
		concer			

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.

🕒 Create Task	×
General Triggers Actions Conditions Settings	
Specify additional settings that affect the behavior of the task.	
Allow task to be run on demand	
Run task as soon as possible after a scheduled start is missed	4
If the task fails, restart every:	1 minute 🗸
Attempt to restart up to:	3: times
Stop the task if it runs longer than:	3 days 🗸
If the running task does not end when requested, force it to	stop
If the task is not scheduled to run again, delete it after:	30 days v
If the task is already running, then the following rule applies:	
Do not start a new instance 🗸	
	OK Cancel

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

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**.

<b>S</b> J		In	ternet Information Services (	IS) Manager	= 0 X
🐨 🛛 🔹 🗰 WA-MIMISKO	IUSU + Stei +				<u>a</u> = 5 € .
File View Help					
Connections Q I P. S. Start Page View Mith-MFM15PCBU0U (WH-M- Application Peels Application Peels Connections Application Peels Connection	Sites Fite: Name Autoraut Web Ste	• 🗑 Go - 🕁 Show / ID Status 1 Status (H	W Group by: No Grouping Binding *80 (http)	• Path NSystemDriveNUnetpublisewaroot	Actions Add Website Set Website Defaults Holp
	Febrer Ver	-network View			
Ready					<b>4</b> 1.
- and					

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

Add Website		? X
Site name: Application pool: tetra	Select	
Content Directory Physical path: C:\TETRA\Signatures Pass-through authentication Connect as Test Settings		
Binding Type: IP address: http v All Unassigned Host name: tetraupdate.bgl-amp.lab	Port:	
Example: www.contoso.com or marketing.contoso.com		
Start Website immediately	ОК	ancel

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

<b>8</b> ]	Internet Information Services (IIS) Manager	= 0 X
WIN-MIMISING	URJ + Stei + teta +	6 6 6 <del>6</del> -
File View Help		
Connections Q- Start Page With-AMMTSDUDUU (WNH-h- Application Pools Star P Dofwalt Web Ster P Dofwalt Web Ster P Dofwalt Web Ster	Vertra Home         Fitter       If Go - Show All Group by: Area       If Co         Authontic:       Compression       Default       Directory         Codput       Frequent       Directory       Every Every         Codput       Frequent       SS. Settings         Configurat       Editor	Actions  Act
Ready		•Q.

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

Internet Information Services (IIS) Manager	= 0 X
WIN-MEMISKOUGU + Sea + tels +	0 = Q Q -
Fire View Hole	
The set of	1.000
MIME Types	Actions
	A44
Start Page Use this feature to manage the list of file name extensions and associated content types that are served as static files by the Web server.	tex.
WHEN MEMORY AND ADD TO A THE ADD ADD ADD ADD ADD ADD ADD ADD ADD AD	X Remove
age registration more services and the service services and the services and	e Hele
b Orland Web Ste	
2 Sta	
approximation and a second sec	
and added on states. Indexing	
are antipipy order. Intering	
Jac impacts conversitier inherited	
A image/ind.m.seal_ inherited	
agb image's rigb inherited	
am application/vnd.m_ inherited	
.mi audio/mid Inheited	
soff application/s-truff inherited	
.pm audio'u-pn-realau Inherited	
.rd application/ird inherited	
As technichted inheited	
.acd application's-mail. Inherited	
act ted/sciptet inherited	
.sea application/octet inherited	
setpay application/set-pa. Inherited	
.setreg application/set-re Inherited	
agent tody'sgent inherited	
.sh application in International	
shar application's shar inherited	
age application when a cost	
c as 3 Testures View 💦 Content View	
Configuration: 'betra' web.config	41

Lorsque vous avez terminé, le contenu du fichier C:ITETRAISignatures lweb.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>
</rule>
</rule>
</rule>
```

**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 (<u>https://www.iis.net/downloads/microsoft/url-rewrite</u>)

Lorsque vous avez terminé, le contenu du fichier C:ITETRAlSignatures 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
- <u>Cisco AMP for Endpoints TechNotes</u>
- <u>Cisco AMP for Endpoints Guide de l'utilisateur</u>