# AMP更新伺服器配置步驟

### 目錄

<u>簡介</u> <u>必備條件</u> <u>安裝步驟</u> <u>所有平台</u> <u>Windows IIS</u> <u>目錄建立</u> <u>更新任務建立</u> <u>IIS管理器配置</u> <u>Apache/Nginx</u> <u>策略配置</u> <u>驗證</u> 相關資訊

# 簡介

本檔案介紹思科進階惡意軟體防護(AMP)TETRA更新伺服器的詳細組態步驟。

# 必備條件

- 瞭解伺服器主機,例如Windows 2012R2或CentOS 6.9 x86\_64。
- 具備託管軟體(例如IIS(僅限Windows)、Apache、Nginx的相關知識
- 已配置的伺服器主機啟用了HTTPS,安裝了有效的受信任證書。
- 已配置HTTPS本地更新伺服器選項。

**附註**:有關啟用本地更新伺服器配置和要求的完整詳細資訊,請參閱此處提供的《面向終端的 AMP使用手冊》的第<u>25章</u>。 (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf)

**附註**:伺服器主機(IIS、Apache、Nginx)是第三方產品,思科不支援這些產品。請參閱相應產 品的支援團隊,瞭解所提供步驟之外的問題。

**警告:**如果AMP配置了代理伺服器,所有更新流量(包括TETRA)將繼續通過代理伺服器傳 送,並定向到您的本地伺服器。確保在傳輸期間允許流量通過Proxy,且未進行任何修改。

## 安裝步驟

### 所有平台

- 1. 確認您的託管伺服器作業系統(OS)。
- 2. 確認面向終端的AMP控制面板門戶,下載更新程式軟體包和配置檔案。

### AMP端點控制檯:

美國-<u>https://console.amp.cisco.com/tetra\_update</u>

歐盟- <u>https://console.eu.amp.cisco.com/tetra\_update</u>

亞太地區地區 — https://console.apjc.amp.cisco.com/tetra\_update

#### Windows IIS

**附註**:以下步驟基於託管簽名的新IIS應用程式池,而非**默**認應用程式池。要使用預設池,請 在提供的步驟中更改—mirror資料夾,以反映預設的Web宿主路徑(C:\inetpub\wwwroot)

#### 目錄建立

- 1. 在根驅動器上建立一個新資料夾,將其命名為TETRA。
- 2. 將壓縮的AMP更新程式軟體包和配置檔案複製到建立的TETRA資料夾中。
- 3. 解壓縮此資料夾中的軟體包。
- 4. 在TETRA資料夾內建立一個名為Signatures的新資料夾。

#### 更新任務建立

system。

- 1. 開啟命令列並導航到C:\TETRA資料夾.cd C:\TETRA
- 2. 運行命令update-win-x86-64.exe fetch —config="C:\TETRA\config.xml" —once —mirror C:\TETRA\Signatures
- 3. 開啟「任務計畫程式」並建立一個新任務。(操作>建立任務)根據需要使用以下選項自動運行更新程式軟體:
- 4. 選擇「常規」頁籤。 輸入任務的名稱。選擇Run (無論使用者是否登入)。選擇使用最高許可權運行。從Configure下拉選單中選擇operating

٥	Create Task X					
General Trig	gers Actions Conditions Settings					
Name:	Name: TETRAUPDATES					
Location: \						
Author:	Author: WIN-MFM1SN38U6U\Administrator					
Description:	Description:					
-Security opt	tions					
When runni	ing the task, use the following user account:					
WIN-MFM1	WIN-MFM1SN3BU6U\Administrator Change User or Group					
O Run only	O Run only when user is logged on					
Run whee	ether 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					
	OK Cancel					

5.選擇「觸發器」標籤。

- 按一下「新建」。
- 從Begin the task下拉選單中選擇On a schedule。
- 在「設定」下選擇**Daily**。
- 選中Repeat task every,然後從下拉選單中選擇1 hour,然後在「duration of:」中選擇Indefinitely
- 確認Enabled是否已選中。
- 按一下「**OK**」(確定)。

New Trigger ×					
Begin the task: On a schedule  Settings One time Start: 12/20/2018  8:40:56 PM Synchronize across time zones					
Veekly     Monthly					
Advanced settings					
Delay task for up to (random delay): 1 hour					
✓ Repeat task every: 1 hour ✓ for a duration of: Indefinitely ✓					
Stop all running tasks at end of repetition duration					
Stop task if it runs longer than: 3 days					
Expire: 12/20/2019 🗊 🔹 8:40:56 PM 😨 Synchronize across time zones					
Enabled					
OK Cancel					

### 6.選擇「活動」標籤

- 按一下「**New**」。
- 從Action下拉選單中選擇Start a program。
- 在Program/script欄位中輸入C:\TETRA\update-win-x86-64.exe。
- 在Add arguments欄位中輸入fetch —config C:\TETRA\config.xml —once —mirror C:\TETRA\Signatures。
- 在「Start」欄位中輸入*C:\TETRA*
- 按一下「**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):	fetcho	onfig C:\TETRA			
Start in	n (optional):	C:\TETR	C:\TETRA			
		OK	Cancel			

7. [*可選]* 選擇「條件」頁籤。

選中「喚醒電腦以運行此任務」選項。

• Create	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 v					
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	ilabler					
	nourc.					
Any connection	Y					
	OK Cancel					

8選擇「設定」頁籤。

- 確認在If the task is already running下選擇了Do not start a new instance。
- 按一下「**OK**」(確定)。

O 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	ł				
□ If the task fails, restart every:	1 minute v				
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 🗸 🗸				
If the task is already running, then the following rule applies:					
Do not start a new instance 🗸					
	OK Cancel				

### 9.輸入將運行**任務的帳戶的身份證明**。

附註: 配置預設應用程式池時跳至步驟5。

1.導航到(IIS)管理器(在「伺服器**管理器」>「工具」下**)

2.展開右側列,直到顯示「站點」文**件夾,然**後按一下右鍵,然後選擇「新增網站」。

<b>6</b> ]	Internet Information Services (II	i) Manager	= 0 X
WIN-MPMISVAUU + Stel +			<b>₩</b> = 5 <b>0</b> •
File View Help			
Connections         Sites           Q         Image: Site Sites           Visit Sites         Sites	• 🍸 Go - 🥁 Show All   Group by: No Grouping		Actions Add Website Set Website Defaults
Application Pools Name *	ID Status Binding	Path	e reg
Add Webske	1 James pr., 100 propr		
C B Fedures View	Content View		
Ready			۹.

3.選擇選擇的名稱。對於物理路徑,選擇C:\TETRA\Signatures資料夾,該資料夾用於下載簽名。

Add Website	? ×
Site name: Application pool: tetra tetra	Select
Content Directory Physical path: C:\TETRA\Signatures Pass-through authentication Connect as Test Settings	
Binding         Type:       IP address:         http       Image: All Unassigned         Host name:         tetraupdate.bgl-amp.lab         Example: www.contoso.com or marketing.contoso.com	Port: 80
Start Website immediately	
	OK Cancel

4.保持繫結獨立。配置**單獨的主機名和**伺服器名稱,選定的名稱必須由客戶端解析。這是您將在策 略中配置的URL。

5.選擇站點並導航到MIME型別,然後新增以下MIME型別:

- •.gzip,應用程式/八位元流
- •.dat,應用程式/二進位制八位數流
- .id , Application/octet-stream
- .sig , Application/octet-stream

With Add/MISSIBURU + Stei + tetu +     File:     View:   Help     Connection:   Q   Image: Connection:   Q   Image: Connection:   Q   Image: Connection:   Image: Conn
File       View       Help         Connections       Image: Connections       Image: Connections       Image: Connections         Image: Start Fage       Image: Connections       Image: Connections       Image: Connections         Image: Start Fage       Image: Connections       Image: Connections       Image: Connections       Image: Connections         Image: Start Fage       Image: Connections       Image: Connections       Image: Connections       Image: Connections         Image: Connections       Image: Connections       Image: Connections       Image: Connections       Image: Connections         Image: Connections       Image: Connections       Image: Connections       Image: Connections       Image: Connections         Image: Connections       Image: Connections       Image: Connections       Image: Connections       Image: Connections         Image: Connections       Image: Connections       Image: Connections       Image: Connections       Image: Connections         Image: Connections       Image: Connections       Image: Connections       Image: Connections       Image: Connections         Image: Connections       Image: Connections       Image: Connections       Image: Connections       Image: Connections         Image: Connections       Image: Connections       Image: Connections       Image: Connections
Connection       Connection       Action         Q
Management Configuration Later Later Management Later Later Management Later Later Management Later Lat
Feedy 91

# 6.導航到**web.config**檔案(位於映象資料夾中),將以下行新增到檔案頂部。

<b>9</b>			Internet Information Services (IIS) Manager		_ 0 X
WINAMMISOBURU + Sec + Mis +					10 = 5 10 ·
File View Help					
Connections	0				Actions
Q 🗟 🖄 👂.	MIME	types			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.			tet	
A WIN-MEMISABUSU (WIN-M	Analysis in Analysis and				× Remove
A Stat	Group by: Ner Gr	augurg -	Inter Trans	1.0	Help
5 Default Web Site	Literation	mante rype	totoy rype	-	
2 😜 tetra		approximation in that	Inherited .		
		approximation and a	labelled .		
	4400	audio/s-pn-reales	Inheited		
	110	application/orbit-	Inharitad		
	48	image/s-cmu-rather	Inherited		
		image/und.m-real	Inherited		
	190	image/s-rgb	Inherited		
	and the second s	application/vnd.m	Inherited		
	.mi	audio/mid	Inherited		
	April 1	application/s-boff	Inherited		
	.spm	audio/s-pn-realau	Inherited		
	11	application/itf	Inherited		
	AL.	ted/iichted	Inherited		
	.acd	application/s-mss	Inherited		
	-545	ted/scriptlet	Inherited	- 12	
	-348	application/octet	Inherited		
	setpey	application/set-pa	Inherited		
	.setreg	application/set-re	Inherited		
	.sgml	text/sgml	Inherited		
	.sh	application/x-sh	Inherited		
	shar	application/s-shar	Inherited		
	-00	application/octet	Local	-	
		Anote stick is shall a	Inherited		
C III 3	E Features View	Content View			
Configuration: 'tetra' web.config					•12

完成後,在文本編輯器中檢視*C*:\*TETRA\Signatures\web.config*檔案內容時,檔案內容會顯示為此類內容。(語法和間距應與提供的示例相同。)

### **附註**:面向終端的AMP聯結器要求在響應中存在伺服器HTTP報頭才能正常運行。如果已禁用 伺服器HTTP標頭,則Web伺服器可能需要下面指定的其他配置。

必須安裝url-rewrite擴展。將以下XML片段新增到伺服器配置中 :/[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>
</rules>
```

**附註**:使用文本編輯器或IIS管理器(使用URL重寫模組)手動執行此更改。可以通過以下 URL(<u>https://www.iis.net/downloads/microsoft/url-rewrite</u>)安裝重寫模組

完成後,在文本編輯器中檢視*C*:\TETRA\Signatures\web.config檔案內容時,檔案內容會顯示為此類內容。(語法和間距應與提供的示例相同。)

Apache/Nginx

附註:提供的步驟假定您提供來自Web託管軟體的預設目錄的簽名。

- 1. TETRA
- 2.
- 3. Chmod +x update-linux\*
- 4. 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.cron

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

6.

1. Advanced Settings > TETRA AMPIP<hostname.domain.root>IP

注意:請勿在下載之前或之後包含任何協定,否則下載時會導致錯誤。

[]TETRAHTTPSHTTPS

導航到C:\inetpub\wwwroot\、C:\TETRA\Signature或/var/www/html目錄,驗證更新的簽名是否可見 ,通過等待下一個同步週期或手動刪除現有簽名,然後等待下載簽名,將簽名從伺服器下載到終端 客戶端。預設值為1小時的時間間隔以檢查更新。

# 相關資訊

- 技術支援與文件 Cisco Systems
- 思科終端進階惡意軟體防護
- <u>面向終端的思科AMP 使用手册</u>