# AMP更新服务器配置步骤

### 目录

<u>简介</u> <u>预请求</u> <u>安装步骤</u> <u>所有平台</u> <u>Windows IIS</u> <u>目录创建</u> <u>更新任务创建</u> <u>IIS管理器配置</u> <u>阿帕奇/恩吉克斯</u> <u>策略配置</u> <u>确认</u> 相关信息

## 简介

本文档介绍思科高级恶意软件防护(AMP)TETRA更新服务器的详细配置步骤。

## 预请求

- 了解Windows 2012R2或CentOS 6.9 x86\_64等服务器主机。
- 对托管软件(如IIS(仅限Windows)、Apache、Nginx)的知识
- 已配置服务器主机,已启用HTTPS,且已安装有效的受信任证书。
- •已配置HTTPS本地更新服务器选项。

**注意:**有关启用本地更新服务器配置和要求的完整详细信息,请参阅此处提供的《面向终端的 AMP用户指南》第25<u>章</u>。

(https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf)

**注意:**服务器主机(IIS、Apache、Nginx)是第三方产品,思科不支持这些产品,请向支持团队 咨询各自产品,以了解所提供步骤之外的问题。

**警告:**如果AMP配置了代理服务器,所有更新流量(包括TETRA)将继续通过代理服务器发 送,并定向到本地服务器。确保允许流量在传输过程中通过代理而不进行任何修改。

### 安装步骤

#### 所有平台

- 1. 确认托管服务器操作系统(OS)。
- 2. 确认面向终端的AMP控制面板门户,下载更新程序软件包和配置文件。

### 面向终端的AMP控制台:

- 美国- <u>https://console.amp.cisco.com/tetra\_update</u>
- 欧盟-<u>https://console.eu.amp.cisco.com/tetra\_update</u>
- APJC https://console.apjc.amp.cisco.com/tetra\_update

#### Windows IIS

**注意:**以下步骤基于新的IIS应用程序池来托管签名,而不是**默认**的应用程序池。要使用默认 池,请在提供的步**骤中更**改—mirror文件夹,以反映默认Web托管路径(**C:\inetpub\wwwroot**)

#### 目录创建

- 1. 在根驱动器上创建新文件夹,将其命名为TETRA。
- 2. 将压缩的AMP更新程序软件包和配置文件复制到所创建的TETRA文件夹。
- 3. 解压缩此文件夹中的软件包。
- 4. 在TETRA文件夹内创建名为Signatures的新文件夹。

#### 更新任务创建

- 1. 打开命令行并导航至C:\TETRA文件夹.cd C:\TETRA
- 2. 运行命令update-win-x86-64.exe fetch —config="C:\TETRA\config.xml" —once —mirror C:\TETRA\Signatures
- 3. 打开任务计划程序并创建新任务。(操作>创建任务),以在需要时使用以下选项自动运行更新程序软件:
- 4. 选择General选项卡。 输入任务的名称。选择Run when user is logged or not.(运行用户是否登录。)选择"使用最高权限运行"。从"配置"下拉菜单中选

择 <b>操作</b> 系统。	

3		Create Task		-	×
General Trig	gers Actions Cond	itions Settings			
Name:	TETRAUPDATES				
Location:	X.				
Author:	WIN-MFM1SN3BU60	D.Administrator			
Description:					
-Security op	tions				
When runn	ing the task, use the fo	ollowing user account:			
WIN-MFM	1SN3BU6U\Administra	tor		Change User or Group	
O Run onl	y when user is logged	on			
Run who	ether user is logged on	or not			
Dor	not store password. Th	e task will only have access t	o local computer re	esources.	
🗹 Run wit	h highest privileges				
🗌 Hidden	Configure for:	Windows Server 2012 R2		~	
				OK Cancel	j

5.选择"触发器"选项卡。

- 单击 New。
- 从"**开始任务**"下**拉菜单中选择**计划。
- 在"设置**"下**选择"每日"。
- 选中Repeat task every, 然后从下拉菜单中选择1 hour, 然后从"Indentible "中选择Indentively:
- 验证是否**选中**了"Enabled"。
- Click OK.

	New Trigger	x
Begin the task: O Settings One time Daily Weekly Monthly	n a schedule v Start: 12/20/2018 v 8:40:56 PM  Synchronize across time zones Recur every: 1 days	
Advanced setting: Delay task for Repeat task en Stop all	s up to (random delay): 1 hour v very: 1 hour v for a duration of: Indefinitely v running tasks at end of repetition duration	
Stop task if it Expire: 12/20	runs longer than: 3 days v 1/2019 v 8:40:56 PM Synchronize across time zones	
	OK Cancel	

6.选择"操作"选项卡

- 单击 **New**。
- 从"**操作"下**拉菜单中选择**"启**动程序"。
- 在"Program/script"字段中输入C:\TETRA\update-win-x86-64.exe。
- 在"添**加参数"(Add arguments)字段中输**入fetch —config C:\TETRA\config.xml —once —mirror C:\TETRA\Signatures。
- 在"开**始位**置"字段中输入C:\TETRA
- 单击 OK

New A	ction	X
pecify what action this task wi	ll perform.	
tart a program		~
/script:		
\update-win-x86-64.exe		Browse
iments (optional):	fetcho	config C:\TETRA
optional):	C:\TETR	A
	ОК	Cancel
	New Average of the second seco	New Action         pecify what action this task will perform.         tart a program         /script:         \update-win-x86-64.exe         ments (optional):         ptional):         C:\TETR

7. [*可选]选*择"条件"选项卡。

选中唤醒计算机以运行此任务选项。

O Create	e Task 🛛 🗶
General Triggers Actions Conditions Settings	
Specify the conditions that, along with the trigger, dete run if any condition specified here is not true. Idle	rmine whether the task should run. The task will not
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     Start only if the following network connection is wa	ilabler
Any connection	
	OK Cancel

8选择"设置"选项卡。

● 验证是否**在"如果任务已**在运行,则**不启动新实例"下选中。** 

٠	Click	OK.

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	1
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 v
If the task is already running, then the following rule applies:	
Do not start a new instance 🗸 🗸	
	OK Cancel

9.输入将运行任**务的帐户的凭据**。

### **注意:**配置默认应用池时,跳至步骤5。

1.导航至(IIS)管理器(在"服务器管**理器">"工具"下**)

2.展开右侧列,直到显示"站点"**文件夹**,然后**右键单击并选择"添加网站"**。

Internet Information Services (IIS) Manager	= 0 X
WH-MMISORUU + Stel +	u = 2 ⊕ -
File Vew Help	
Connections         Attem           Q Inter         Sites           State Page         Filter:           WN-MM/IS/2000 (WN-M)         Filter:           Name         ID           Sates         Filter:	di Website Al Website Defaults Ap
Add Webste.	
Ready	<b>4</b> 14

3.选择选择的名称。对于物理路径,选择*下载签名*的C:\TETRA\Signatures文件夹。

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: Content in the image is a content of the
✓ Start Website immediately           OK         Cancel

4.单独保留绑定。配**置单独的主机名**和服务器名称,所选名称必须可由客户端解析。这是您将在策略中配置的URL。

5.选择站点并导航到MIME类型并添加以下MIME类型:

- •.gzip,应用/二进制八位数流
- •.dat,应用/二进制八位数流
- •.id,应用/二进制八位数流
- •.sig,应用/二进制八位数流

Internet Information Services (IIS) Manager	_ 0 X
WINAMATCADDUU + Stel + teta +	$\omega = 0 \cdot \Theta +$
File View Help	
Connection         Image: Start Fage         Image: Mart Start Mark Start Mark         Image: Mart Start Mark Start Mark         Image: Mark Start Mark Start Mark         Image: Mark Start Mark Start Mark         Image: Mark Start Mark Start Mark Start Mark         Image: Mark Start Mark Start Mark Start Mark         Image: Mark Start Mark St	Actions Control Contro
Ready	<b>9</b> 1/

6.导航至**web.config文**件(位于镜像文件夹中),将以下行添加到文件顶部。

<b>9</b>		Internet Information Services (IIS) Manager		_ 0 X
WN-MIMISV8U8U + Stel + N	da x			<b>₩</b> = 5 <b>€</b> •
File View Help				
Connections	-			Actions
🔍 - 🗟 🖄 😥 MIME	Types			A44_
Start Page Una this feature to	manage the list of file part	as astamines and associated contact turus that are security a static film by the Web secur		10.
WIN-MEMISIOBUEU (WIN-M		a construction of the cons		× Remove
Application Pools Group by: No Gr	ouping *		-	Inter
Litersion*	MME Type	Entry Type	~	
All and a	application/x-quic	Inherited		
. ad	application/octet	inherited		
	audio/s-pn-realau	Inherited		
. Ann	audio/v-pn-realau	Inherited		
14	application/octet	Inherited		
.46	image/s-cmu-raster	Inherited		
A	image/vnd.m-real	Inherited		
-190	image/s-rgb	Inherited		
-	application/vnd.m	Inherited		
	audio/mid	Inherited		
Box	application/s-buff	Inherited		
.gm	audio/s-pn-realau	Inherited		
A	application/iff	Inherited		
~	ted/inchted	Inherited		
bac	application/x-mss	Inherited	100	
ba.	ted/scriptlet	Inherited		
.368	application/octet	Inherited		
setpey	application/set-pa	Inherited		
Jatreg	application/set-re	inherited		
.spml	ted/spml	Inherited		
A	application/x-sh	inherited		
shar	application/s-shar	Inherited		
.sig	application/octet	Local		
.0	and/stion/s-milit	Inharitad	v	
c III > Features View	Content View			
Configuration: 'betra' web.config				· · · · · · · · · · · · · · · · · · ·

完成后,在文*本编辑器*中查看时,C:\TETRA\Signatures\web.config文件内容将显示为这样。(语法和间距需要与提供的示例保持相同。)

**注意:**面向终端的AMP连接器要求服务器HTTP报头在响应中存在,以便正确操作。如果服务器HTTP报头已禁用,则Web服务器可能需要在下面指定的其他配置。

必须安装url-rewrite扩展。在/[MIRROR\_DIRECTORY]/web.config的服务器配置中添加以下XML代码段:

```
<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>
```

### **注意:**使用文本编辑器或IIS管理器使用URL重写模块手动执行此更改。可以从以下 URL(https://www.iis.net/downloads/microsoft/url-rewrite)安装重写<u>模块</u>。

完成后,在文*本编辑器*中查看时,C:\TETRA\Signatures\web.config文件内容将显示为这样。(语法和间距需要与提供的示例保持相同。)

#### 阿帕奇/恩吉克斯

注意:提供的步骤假定您正在从Web托管软件的默认目录中提供签名。

- 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"(TETRA) "(Update Server): AMPIP<hostname.domain.root>IP

警告:请勿在之前或之后包含任何协议子目录,否则,在下载时将导致错误。

[]HTTPSTETRAHTTPS

导航至**C:\inetpub\wwwroot\、C:\TETRA\Signature或/var/www/html**目录,并验证更新的签名是否可 见,通过等待到下一个同步周期或手动删除现有签名,然后等待签名下载,签名从服务器下载到最 终客户端。默认为1小时间隔,用于检查更新。

## 相关信息

- <u>技术支持和文档 Cisco Systems</u>
- <u>面向终端的思科AMP 技术说明</u>
- 面向终端的思科AMP 用户指南
- 0