AMPアップデートサーバの設定手順

内容

<u>概要</u> <u>前提条件</u> <u>インストール手順</u> <u>すべてのプラットフォーム</u> <u>Windows IIS</u> <u>ディレクトリの作成</u> <u>更新タスクの作成</u> <u>IISマネージャの設定</u> <u>Apache/Nginx</u> <u>ポリシー設定</u> <u>確認</u> <u>関連情報</u>

概要

このドキュメントでは、Cisco Advanced Malware Protection(AMP)TETRAアップデートサーバの 詳細な設定手順について説明します。

前提条件

- Windows 2012R2やCentOS 6.9 x86_64などのサーバホストに関する知識。
- IIS (Windowsのみ)、Apache、Nginxなどのホスティングソフトウェアに関する知識
- •HTTPSが有効で、有効な信頼できる証明書がインストールされた設定済みのサーバホスト。
- HTTPS Local Update Serverオプションを設定しました。

注: Local Update Serverの設定と要件の有効化の詳細については、『AMP for Endpoints User Guide』の第25章を参照してく<u>ださ</u>い。 (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf)

注:サーバホスト(IIS、Apache、Nginx)はサードパーティ製品であり、シスコではサポート されていません。提供されている手順の範囲外の質問については、各製品のサポートチーム を参照してください。

警告:AMPがプロキシサーバで設定されている場合、すべての更新トラフィック (TETRAを含む)は、引き続きプロキシサーバを経由してローカルサーバに送信されます 。転送中にトラフィックが変更されずにプロキシを通過できることを確認します。

インストール手順

すべてのプラットフォーム

- 1. ホスティングサーバーオペレーティングシステム(OS)を確認します。
- 2. AMP for Endpointsダッシュボードポータルを確認し、Updater Software Packageと設定フ ァイルをダウンロードします。

AMP for Endpointsコンソール:

米国- <u>https://console.amp.cisco.com/tetra_update</u>

EU:https://console.eu.amp.cisco.com/tetra_update

APJC:https://console.apjc.amp.cisco.com/tetra_update

Windows IIS

注:次の手順は、シグニチャをホストする新しいIISアプリケーションプールに基づいており、デフォルトのアプリケーションプールに基づいていません。デフォルトのプールを使用 するには、次の手順で---mirrorフォルダを変更し、デフォルトのWebホスティングパス (C:\inetpub\wwwroot)を反映します

ディレクトリの作成

- 1. ルートドライブに新しいフォルダを作成し、TETRAという名前を付けます。
- 2. zip圧縮されたAMPアップデータソフトウェアパッケージと構成ファイルを、作成されたTETRAフォ**ルダにコ**ピーします。
- 3. このフォルダのソフトウェアパッケージを解凍します。
- 4. TETRAフォルダ内にSignaturesという新しいフォルダを作成します。

更新タスクの作成

- 1. コマンドラインを開き、C:\TETRAフォルダ.cd C:\TETRAに移動します
- 2. update-win-x86-64.exe fetch —config="C:\TETRA\config.xml" —once —mirror C:\TETRA\Signaturesコマンドを実行します
- タスクスケジューラを開き、新しいタスクを作成します。([アクション(Action)] > [タスクの作成(Create Task)])を選択して、必要に応じて次のオプションを使用してアップデータソフトウェアを自動的に実行します。
- 4. [General]タブを選択します。 タスクの名前を入力します。[ユーザーがログオンしているかどうかを実行]を選択します。「最高の権限で実行」を 選択します。[構成]ドロップダウンダウンからオペレーティングシステムを選択します。

Θ	Create Task	x					
General Trigg	ers Actions Conditions Settings	_					
Name: TETRAUPDATES							
Location:	\						
Author:	WIN-MFM1SN38U6U\Administrator						
Description:							
- Security opti	ons						
When runni	ng the task, use the following user account:						
WIN-MFM1	5N3BU6U\Administrator Change User or Group						
O Run only	when user is logged on						
Run whe	ther user is logged on or not						
Don	at 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. 「トリガー」タブを選択します。
 - [New] をクリックします。
 - [タスク**の開始]ドロップダ**ウンから[ス**ケジュール]を**選択します。
 - [設定]の**[日**次]を選択します。
 - [Repeat task every]をオンにして、ドロップダウンから[1 hour]を選択し、[duration of:]から[Indefinitely]を選択します。
 - [有効]にチェックマーク**が付いて**いることを**確認します**。
 - [OK] をクリックします。

New Trigger	×
Begin the task: On a schedule Settings One time Start: 12/20/2018 St	s
Daily Weekly Monthly	
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: Indefinitely 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 Repeat task every: 8:40:56 PM Synchronize across time zones Enabled	
OK Cance	8

6.「処理」タブの選択

- [New] をクリックします。
- [アクション]ドロップダウンから[プログラムの開始]を選択します。
- [プログ*ラム/スク*リプト]フィールドにC:\TETRA\update-win-x86-64.exeと入力します。
- [Add arguments] フィールドにfetch config C:\TETRA\config.xml once mirror C:\TETRA\Signaturesと入力します。
- [Start **in]フィ**ールドにC:\TETRA**と入力**します。
- [OK] をクリックします。

	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. [オプション] [条件]タブを選択します。

[Wake the computer to run this task]オプションをオンにします。

O Create	e Task
General Triggers Actions Conditions Settings	
Specify the conditions that, along with the trigger, deter 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	
Start only if the following network connection is avai	lable
	in the second
Any connection	Ŷ
	OK Cancel

8 [Settings]タブを選択します。

- [タスクが既に実行中の場合]で[新しいインスタンスを開始しない]が選択されていることを確認します。
- [OK] をクリックします。

٥	Create Tas	k X
General Specify	Triggers Actions Conditions Settings additional settings that affect the behavior of the task	
☑ AII	ow task to be run on demand	
🗆 Ru	n task as soon as possible after a scheduled start is miss	red
🗆 ift	he task fails, restart every:	1 minute 🗸
Att	empt to restart up to:	3 times
🗹 Sto	p the task if it runs longer than:	3 days 🗸
🗹 lft	he running task does not end when requested, force it	to stop
	he task is not scheduled to run again, delete it after:	30 days 🗸
If the t	ask is already running, then the following rule applies:	
Do not	start a new instance 🗸 🗸	
		OK Cancel

9.タスクを実行するアカ**ウントの資格証明を入力します**。

注:デフォルトアプリケーションプールが設定されている場合は、ステップ5に進みます。

1. (IIS) Managerに移動します([サー**バーマネージャ] > [ツール]で**)

2.「サイト」フォルダが表示されるまで右側の列を展開し、「右クリック」を選択して、「 Webサイトの追加」を選択します。

<i>Ø</i>		Int	ernet Information Services	(IS) Manager	= 0 X
🐨 🔹 🖬 WN-MPM1908	U6U + Stei +				<u>u</u> = 5 € .
File View Help					
Connections Q, • 🔡 💋 19,	Sites				Actions
Stat Page	Filter	- 77 Go - 🖓 Show J	I Group by: No Grouping		Set Website Defaults
- D Application Peels	Name *	ID Status	Binding	Path	• • • • • •
Add Website	Default Web Site	1 Started (H	*100 (Hmp)	%SystemDriveWinetpublismmmoot	
E Refresh					
Switch to Content Vie					
(Teatures View	Content View			
Ready					9 .

3.任意の名前を選択します。[Physical Path]で、署名がダウンロードさ**れた** *C:\TETRA\Signaturesフ*ォルダを選択します。

Add Website	е ?	x
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 IIP address: All Unassigned Host name: tetraupdate.bgl-amp.lab Example: www.contoso.com or marketing.contoso.com	Port:	
✓ Start Website immediately	OK Cancel	

4.バインディングは単独で行います。**ホスト名とサーバー名を別**々に構成してください。選択した名前はクライアントで解決できる必要があります。これは、ポリシーで設定するURLです。

5.サイトを選択し、「MIMEタイプ」にナビゲート**し、次の**MIMEタ**イプを追加します**。

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

Internet Information Services (IIS) Manager				
WN-MMISNER	200 + Ster + tetra +	₩ = 5 0 -		
File View Help				
Connections Q - La 2 D. Start Page WINA-MYMTSHOUGU (WYN-hr Application Pools Star D Default Web Ste D Default Web Ste D Default Web Ste	Etra Home Fare Image: Show All Group by: Area S Authentic Compression Default Decomment Decomment Browsing Fore Pages Hindler HTTP Logging MMLType Modules Processed Stationary Conjugat Request Stationary Stationary Conjugat Request Stationary Stationary Conjugat Request Stationary	Actions Actions Captors Edit Permissions Idit She Endings Two-Applications Vew Votual Electories Manage Website Proves Revars Revars Proves Website Revars Proves Revars Revars		
Ready	A CONTRACTOR OF	•1		

6.ミラーフォルダにあるweb.configファイルに移動し、ファイルの先頭に次の行を追加します。

9			Internet Information Services (IIS) Manager		_ 0 X
WN-MPM1948	USU + Stei + ti	eta +			₩ = Q 0 •
File View Help					
Connections		-			Actions
Q [i] 2 (Q.	MIME	Types			A44_
Start Page	Use this feature to	manage the lat of file page	a extension and approxided context time that are parent to static film in the Web caner.		10.
A WIN-MEMISNOBUSU (WIN-M	Use this heature to manage the tot of the name extensions and associated content types that are served as static files by the view server.			X famous	
- 2 Application Pools	Group by: No Gr	ouping .			O link
4 8 5065	Extension*	MME Type	Entry Type	~	A Link
5 Cefault men ste	-45	application/x-quic	Inherited		
2 9 2012	-qui	application/octet	Inherited		
	-10	audio/s-pn-realau	Inherited		
	Jam	audio/v-pn-realau	inherited		
	.187	application/octet	Inherited		
	.785	image/s-cmu-raster	Inherited		
		image/vnd.m-real	Inherited		
	.agb	image/s-rgb	Inherited		
	.m	application/vnd.m	Inherited		
	.mi	audio/mid	Inherited		
	.roff	application/s-boff	Inherited		
	.spm	audio/s-pn-realau	Inherited		
	18	application/iff	Inherited		
	AL.	ted/inchited	Inherited		
	-acd	application/s-mss	Inheited		
	-845	ted/scriptlet	Inherited		
	-348	application/octet	inheited		
	.setpay	application/set-pa	Inherited		
	.setreg	application/set-re	inherited		
	aged	ted/sgml	Inherited		
	.sh	application/x-sh	inherited		
	shar	application/s-shar	Inherited		
	.sig	application/octet	Local		
		anniestion/s-malik	Inharited	v	
< m >	Teatures View	Content View			
Configuration: 'betra' web.config					9 .

終了すると、*C:\TETRA\Signatures\web.configファイル*の内容は、テキストエディタで表示すると、そのように表示されます。(構文と間隔は、指定した例 と同じままにする必要があります)。 **注**:エンドポイント用AMPコネクタが正常に動作するには、応答にサーバHTTPヘッダーが存在する必要があります。サーバのHTTPヘッダーが無効になっている場合、Webサーバでは次に示す追加の設定が必要になる場合があります。

url-rewrite拡張をインストールする必要があります。次のXMLスニペットを /[MIRROR_DIRECTORY]/web.configのサーバ設定に追加します。

<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>

注:テキストエディタまたはIISマネージャを使用して、URLリライトモジュールを使用して、この変更を手動で実行します。Rewriteモジュールは、次の URL(<u>https://www.iis.net/downloads/microsoft/url-rewrite</u>)からインストールできます

終了すると、*C:\TETRA\Signatures\web.configファイル*の内容は、テキストエディタで表示すると、そのように表示されます。(構文と間隔は、指定した例 と同じままにする必要があります)。

Apache/Nginx

注:この手順では、Webホスティングソフトウェアのデフォルトディレクトリからシグニチャを提供していることを前提としています。

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.

0 ****/TETRA/update-linux-x86-64 fetch --config /TETRA/config.xml --once --mirror /var/www/html/ 6. [Policy configuration]

1. > AMP<hostname.domain.root>IPIP

注意:それ以外の場合は、前のプロトコルやサブディレクトリを含めないと、ダウンロード 中にエラーが発生します。

[]TETRAHTTPS

C:\inetpub\wwwroot\、C:\TETRA\Signature、または/var/www/htmlディレクトリに移動して、更新 されたシグニチャが表示されていることを確認します。次の同期サイクルまで待つか、既存のシ グニチャを手動で削除し、シグニチャのダウンロードを待機して、サーバからエンドクライアン トにシグニチャををダウンロードします。デフォルトでは、更新を確認するための1時間インター バルです。

関連情報

- <u>テクニカル サポートとドキュメント Cisco Systems</u>
- ・エンドポイント向けCisco AMP テクニカルノート
- ・ <u>エンドポイント向けCisco AMP ユーザガイド</u>