Procedura di configurazione di AMP Update Server

Sommario

Introduzione Prerequisiti Fasi di installazione Tutte le piattaforme IIS di Windows Creazione directory Aggiorna creazione attività Configurazione Gestione IIS Apache/Nginx Configurazione criteri Verifica Informazioni correlate

Introduzione

In questo documento viene descritta in dettaglio la configurazione di Cisco Advanced Malware Protection (AMP) TETRA Update Server.

Prerequisiti

- Conoscenza degli host server, ad esempio Windows 2012R2 o CentOS 6.9 x86_64.
- Conoscenza di software di hosting come IIS (solo Windows), Apache, Nginx
- Host del server configurati con HTTPS abilitato e certificato attendibile valido installato.
- Opzione del server di aggiornamento locale HTTPS configurata.

Nota: Per informazioni dettagliate sull'abilitazione della configurazione e dei requisiti di Local Update Server, fare riferimento al capitolo 25 della Guida per l'utente di AMP for Endpoints, disponibile <u>qui</u>.

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

Nota: Gli host server (IIS, Apache, Nginx) sono prodotti di terze parti e non sono supportati da Cisco. Per domande che esulano dalle procedure fornite, fare riferimento ai team di supporto dei rispettivi prodotti.

Avviso: Se AMP è configurato con un server proxy, tutto il traffico di aggiornamento (incluso TETRA) continuerà a essere inviato tramite il server proxy al server locale. Accertarsi che il traffico possa passare al proxy senza modifiche mentre è in transito.

Fasi di installazione

Tutte le piattaforme

- 1. Confermare il sistema operativo del server di hosting.
- 2. Confermare il portale AMP for Endpoints Dashboard, scaricare il pacchetto software dell'Updater e il file di configurazione.

AMP for Endpoints Console:

STATI UNITI - 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

IIS di Windows

Nota: I passaggi seguenti si basano sul nuovo pool di applicazioni di IIS per ospitare le firme, non sul pool di applicazioni predefinito. Per utilizzare il pool predefinito, modificare la cartella —mirror nei passaggi forniti in modo che rifletta il percorso di hosting Web predefinito (C:\inetpub\wwwroot)

Creazione directory

- 1. Creare una nuova cartella sull'unità principale, denominandola TETRA.
- 2. Copiare il pacchetto del software di aggiornamento dell'AMP compresso e il file di configurazione nella cartella TETRA creata.
- 3. Decomprimere il pacchetto software in questa cartella.
- 4. Creare una nuova cartella denominata Signatures all'interno della cartella TETRA.

Aggiorna creazione attività

- 1. Aprire la riga di comando e passare alla cartella C:\TETRA.cd C:\TETRA
- 2. Eseguire il comando update-win-x86-64.exe fetch -config="C:\TETRA\config.xml" -once -mirror C:\TETRA\Signatures
- 3. Aprire l'Utilità di pianificazione e creare una nuova attività. (Azione > Crea task) per eseguire automaticamente il software di aggiornamento con le seguenti opzioni, se necessario:
- 4. Selezionare la scheda Generale. Immettere un nome per il task.Selezionare Esegui indipendentemente dal fatto che l'utente sia connesso o meno.Selezionare Esegui con i privilegi più elevati.Selezionare sistema operativo dall'elenco a discesa Configura.

Θ		Create Task			×			
General Trig	gers Actions Cond	itions Settings						
Name:	Name: TETRAUPDATES							
Location:	X.							
Author:	WIN-MFM1SN38U6	J\Administrator						
Description:								
- Security opt	ions							
When runni	ng the task, use the fo	ollowing user account:						
WIN-MFM1	SN3BU6U\Administra	tor		Change User	r or Group			
O Run only	O Run only when user is logged on							
Run whee	ther user is logged on	or not						
🗌 Do n	ot store password. Th	ne task will only have access to	o local computer re	esources.				
Run with highest privileges								
Hidden	Configure for:	Windows Server 2012 R2			~			
				ОК	Cancel			

5. Selezionare la scheda Trigger.

- Fare clic su New.
- Selezionare In base a una pianificazione dall'elenco a discesa Inizia il task.
- Selezionare **Daily** in Settings (Impostazioni).
- Selezionare Ripeti attività ogni, selezionare 1 ora dall'elenco a discesa e scegliere Indefinito dal menu "per una durata di:"
- Verificare che l'opzione Enabled sia selezionata.
- Fare clic su 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. Selezionare la scheda Azioni

- Fare clic su New.
- Selezionare Avvia un programma dal menu a discesa Azione.
- Immettere C:ITETRAlupdate-win-x86-64.exe nel campo Programma/script.
- Immettere fetch -config C:\TETRA\config.xml -once -mirror C:\TETRA\Signatures nel campo Aggiungi argomenti.
- Immettere C:\TETRA nel campo Inizia in
- Fare clic su OK.

	New Action	n ×				
You must specify what action this task will perform.						
Action:	Start a program	~				
Setting	5					
Progra	im/script:					
C:\TE	RA\update-win-x86-64.exe	Browse				
Add a	rguments (optional):	fetchconfig C:\TETRA'				
Start in	n (optional):	C:\TETRA				
		OK Cancel				

7. [Facoltativo] Selezionare la scheda Condizioni.

Selezionare l'opzione Riattiva il computer per eseguire questa attività.

O Creat	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	ermine 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 v
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
	moure.
Any connection	v
	OK Cancel

8 Selezionare la scheda Settings.

- Verificare che l'opzione Non avviare una nuova istanza sia selezionata in Se l'attività è già in esecuzione.
- Fare clic su OK.

O Create Task		x
General Triggers Actions Conditions Settings Specify additional settings that affect the behavior of the task.		٦
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 🗸 🗸	
If the task is already running, then the following rule applies:		
Do not start a new instance 🗸		
	OK Cancel	

9. Immettere le credenziali per l'account che eseguirà il task.

Nota: Andare al passaggio 5 quando è configurato il pool di applicazioni predefinito.

1. Passare a (IIS) Manager (In Server Manager > Strumenti)

2. Espandere la colonna destra fino a quando la **cartella Siti** è visibile, **Fare clic con il pulsante destro del mouse e selezionare Aggiungi sito Web**.

<i>\$</i>]		Int	ernet Information Services (IIS) Manager	= 0 X
🐨 💽 🔹 🖬 WN-MPM19408	IUSU + Stes +				₩ = 5 (0 ·
File View Help					
Connections Q. • Image: State Page	Sites	• 🐨 Go - 🖓 Show A	U Group by: No Grouping		Actions Add Website Set Website Defaults
- 2 Application Pools	Name *	ID Status	Binding	Path	e neg
Add Website	M.D.Hault Web Site	1 Stated (H	~:00 (Hrtp)	NSystemDrive Nunetpubliummoot	
Refresh					
Switch to Content Vie	ew				
4 10 3	features View 🕡	Content View			
Ready					41.

3. Scegliere un nome. Per Percorso fisico selezionare la cartella *C:\TETRA\Signatures* in cui sono state scaricate le firme.

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 II Unassigned Host name: tetraupdate.bgl-amp.lab Example: www.contoso.com or marketing.contoso.com
✓ Start Website immediately
OK Cancel

4. Non modificare le associazioni. **Configurare un nome host** e un nome server **separati**. I nomi scelti devono essere risolvibili dai client. URL che verrà configurato nel criterio.

5. Selezionare il sito, passare a Tipi MIME e aggiungere i seguenti tipi MIME:

- .gzip, flusso di applicazioni/ottetti
- .dat, flusso di applicazioni/ottetti
- .id, flusso-applicazione/ottetto
- .sig, Application/octet-stream

Image: State Image: State	Internet Information Services (IIS) Manager	_ O X
File: View Help Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints <thconstraints< th=""> Constraints<td>😧 🕜 🔮 a WINAMINTSKIBURU a Step a tetra a</td><td>6 = 0 0 ·</td></thconstraints<>	😧 🕜 🔮 a WINAMINTSKIBURU a Step a tetra a	6 = 0 0 ·
Consections	File View Help	
The second	Connection Image: Start Fage Image: Start Fage	Action Action Edit Ster Endings Ensic Settings Vew Applications Vew Visual Overctories Manage Website Stat Stat Stat Stat Stat Stat Stat Stat Stat Constant Advanced Settings Configure Limits Help
Feedy 91	Ready	•q.,

6. Passare al **file web.config** (che si trova nella cartella mirror), aggiungere le seguenti righe all'inizio del file.

S			Internet Information Services (IIS) Manager		_ 0 X
why MMSX20000 > Step > tetra >					₩ = 5 0 -
File View Help					
Connections	-				Actions
9-01019	MIME	Types			
A Stat Pase	-				
WIN-MEMISNIBUSU (WIN-M	Use this feature to	manage the list of file nam	ne extensions and associated content types that are served as static files by the Web server.		Lat.
- 2 Application Pools	Group by: No-G	rouping +			A femove
a 📓 Stes	Extension*	MME Type	Entry Type	A	Help
5 😜 Default Web Site	-101	application/x-quic	Inherited		
2 🥸 tetra	.ed	application/octet	Inherited		
	.0	audio/v.pn-realau	Inherited		
	.ram	audio/s-pn-realau	Inherited		
	100	application/octet	Inherited		
	.465	image/s-cmu-raster	inherited		
		image/vnd.m-real	Inherited		
	.sgb	image/s-rgb	Inherited		
	.m	application/vnd.m	Inherited		
	.mi	audio/mid	Inherited		
	.roff	application/s-buff	Inherited		
	.spm	audio/s-pn-realau	Inherited		
	11	application/iff	Inherited		
	AL.	ted/incheet	Inherited		
	acd	application/s-mss	Inherited	1	
	-543	ted/scriptlet	Inherited	-	
	-348	application/octet	Inherited		
	setpay	application/set-pa	Inherited		
	.sebeg	application/set-re	Inherited		
	sgmi	ted/spml	Inherited		
	sh	application/x-sh	inherited		
	shar	application/s-shar	Inherited		
	00	application/octet	Local		
		Annie Wenn's - that's	and the second s		
C 10 2	Features View	Content View			
Configuration: 'tetra' web.config					9 27

Al termine, il contenuto del file C:\TETRA\Signatures\web.config apparirà come tale quando visualizzato in un editor di testo. La sintassi e la spaziatura devono rimanere invariate rispetto all'esempio fornito.

Nota: AMP for Endpoints Connector richiede la presenza dell'intestazione HTTP del server nella risposta per il corretto funzionamento. Se l'intestazione HTTP del server è stata disattivata, è possibile che il server Web richieda una configurazione aggiuntiva specificata di seguito.

Ènecessario installare l'estensione per la riscrittura dell'URL. Aggiungere il seguente frammento XML alla configurazione del server in /[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>
</rewrite>
```

Nota: Eseguire questa modifica manualmente con un editor di testo o con Gestione IIS utilizzando il modulo URL Rewrite. Il modulo Rewrite può essere installato dal seguente URL (<u>https://www.iis.net/downloads/microsoft/url-rewrite</u>)

Al termine, il contenuto del file C:\TETRA\Signatures\web.config apparirà come tale quando visualizzato in un editor di testo. La sintassi e la spaziatura devono rimanere invariate rispetto all'esempio fornito.

Apache/Nginx

Nota: I passaggi forniti presuppongono che le firme vengano fornite dalla directory predefinita del software di hosting Web.

- 1. Creare una nuova cartella sull'unità radice denominata TETRA.
- 2. Decomprimere il pacchetto di script scaricato in questa cartella.
- 3. Eseguire il comando Chmod +x update-linux* per concedere agli script l'autorizzazione di esecuzione.
- 4. Eseguire il comando per recuperare i file di aggiornamento TETRA.

This command may vary depending on your directory structure.

5. Per automatizzare il processo di aggiornamento del server, aggiungere un processo cron al server:

0 ****/TETRA/update-linux-x86-64 fetch --config /TETRA/config.xml --once --mirror /var/www/html/
 6. Continuare a seguire la procedura descritta in Configurazione dei criteri per configurare i criteri in modo che utilizzino il server di aggiornamento.

Configurazione criteri

1. Passare al criterio per utilizzare il server di aggiornamento e in *Impostazioni avanzate > TETRA* selezionare: Casella di controllo per il server

di aggiornamento AMP localell nome host o l'indirizzo IP del server di aggiornamento nel formato <hostname.domain.root> o indirizzo IP.

Attenzione: Non includere alcun protocollo prima o dopo le sottodirectory; in caso contrario, si verificherà un errore durante il download.

[Facoltativo] Casella di controllo Usa HTTPS per gli aggiornamenti della definizione TETRA: se il server locale è configurato con un certificato corretto e per i connettori per usare HTTPS.

Verifica

Passare alla directory C:\inetpub\wwwroot\, C:\TETRA\Signature o /var/www/html e verificare che le firme aggiornate siano visibili. Le firme verranno scaricate dal server al client finale in attesa del successivo ciclo di sincronizzazione oppure in attesa dell'eliminazione manuale delle firme esistenti e del download. L'impostazione predefinita è un intervallo di 1 ora per la verifica della disponibilità di un aggiornamento.

Informazioni correlate

- Documentazione e supporto tecnico Cisco Systems
- Cisco AMP for Endpoints Note tecniche
- <u>Cisco AMP for Endpoints Guida per l'utente</u>