Pasos de configuración del servidor de actualización de AMP

Contenido

Introducción Requisitos previos Pasos de instalación Todas las plataformas IIS de Windows Creación de directorios Actualizar creación de tarea Configuración del Administrador IIS Apache / Nginx Configuración de políticas Verificación Información Relacionada

Introducción

Este documento describe los pasos de configuración detallados para el servidor de actualización TETRA de protección frente a malware avanzado (AMP) de Cisco.

Requisitos previos

- Conocimiento de hosts de servidor como Windows 2012R2 o CentOS 6.9 x86_64.
- Conocimiento de software de alojamiento como IIS (sólo Windows), Apache, Nginx
- Hosts de servidor configurados con HTTPS activado, certificado de confianza válido instalado.
- Opción HTTPS Local Update Server configurada.

Nota: Para obtener más información sobre cómo habilitar la configuración y los requisitos de Local Update Server, consulte el capítulo 25 de la Guía del usuario de AMP para terminales, disponible <u>aquí</u>.

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

Nota: Los hosts de servidor (IIS, Apache, Nginx) son productos de terceros y no son compatibles con Cisco. Consulte los equipos de soporte de los productos correspondientes para obtener información sobre las preguntas que no se indican en los pasos proporcionados.

Advertencia: Si AMP se configura con un servidor proxy, todo el tráfico de actualización (incluido TETRA) se seguirá enviando a través del servidor proxy, dirigido al servidor local. Asegúrese de que el tráfico se permita pasar el proxy sin ninguna modificación durante el

tránsito.

Pasos de instalación

Todas las plataformas

- 1. Confirme el sistema operativo del servidor de alojamiento (SO).
- 2. Confirme el portal del panel de AMP para terminales, descargue el paquete de software de actualización y el archivo de configuración.

Consola de AMP para terminales:

- EE. UU. 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 de Windows

Nota: Los pasos siguientes se basan en el nuevo grupo de aplicaciones IIS para alojar las firmas, **no** en el grupo de aplicaciones predeterminado. Para utilizar el conjunto predeterminado, cambie la carpeta—**reflejar** en los pasos proporcionados para reflejar la ruta predeterminada de alojamiento web (**C:\inetpub\wwwroot**)

Creación de directorios

- 1. Cree una nueva carpeta en la unidad raíz, denle el nombre TETRA.
- 2. Copie el paquete de software y el archivo de configuración del actualizador de AMP comprimido en la carpeta TETRA creada.
- 3. Descomprima el paquete de software en esta carpeta.
- 4. Cree una nueva carpeta llamada Firmas dentro de la carpeta TETRA.

Actualizar creación de tarea

- 1. Abra la línea de comandos y navegue hasta la carpeta C:\TETRA.cd C:\TETRA
- 2. Ejecute el comando update-win-x86-64.exe fetch —config="C:\TETRA\config.xml" —once —Mirror C:\TETRA\Signatures
- 3. Abra el Programador de tareas y cree una nueva tarea. (Acción > Crear tarea) para ejecutar automáticamente el software actualizador con las siguientes opciones cuando sea necesario:
- 4. Seleccione la ficha General. Introduzca un nombre para la tarea.Seleccione Ejecutar si el usuario ha iniciado sesión o no.Seleccione Ejecutar con los privilegios más altos.Seleccione sistema operativo en el menú desplegable Configurar.

•		Create Task			×			
General Trig	gers Actions Cond	itions Settings						
Name:	Name: TETRAUPDATES							
Location:	Location:							
Author:	WIN-MFM1SN38U6	/\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 or	or not						
🗌 Do n	ot store password. Th	e task will only have access to loo	cal computer re	esources.				
Run with	highest privileges							
Hidden	Configure for:	Windows Server 2012 R2			~			
				ОК	Cancel			

5. Seleccione la ficha Desencadenadores.

- Haga clic en New.
- Seleccione En una programación en el menú desplegable Comenzar la tarea.
- Seleccione **Daily** en Settings.
- Marque Repetir tarea cada y seleccione 1 hora en la lista desplegable y seleccione Indefinidamente de la opción "por una duración de:"
- Verifique que Enabled esté marcado.
- Click 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. Seleccione la ficha Acciones

- Haga clic en New.
- Seleccione Iniciar un programa en el menú desplegable Acción.
- Ingrese C:\TETRA\update-win-x86-64.exe en el campo Programa/script.
- Ingrese fetch -config C:\TETRA\config.xml -once -Mirror C:\TETRA\Signatures en el campo Agregar argumentos.
- Escriba C:\TETRA en el campo Start en
- Haga clic en OK (Aceptar).

	New Action	on
You mus	t specify what action this task will p	erform.
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. [Opcional] Seleccione la ficha Condiciones.

Marque la opción Despertar el ordenador para ejecutar esta tarea.

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 r	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 as:	vilable	
Any connection		~
	0	K Cancel
	0	conce

8 Seleccione la ficha Settings (Parámetros).

• Verifique que No iniciar una nueva instancia esté seleccionada en Si la tarea ya se está ejecutando.

•				Cre	ate Task			
General Specify	Triggers additional	Actions settings t	Conditions hat affect the	Settings behavior	of the task.			
I Allo	ow task to b	e run on	demand					
Rur	n task as soo	on as pos	sible after a s	cheduled s	tart is missed			
🗌 lft	ne task fails,	restart ev	very:			1 minute v		
Att	empt to rest	tart up to	:			3: times		
Sto	p the task if	it runs lo	nger than:			3 days 🗸 🗸		
🖌 if th	ne running t	task does	not end whe	n requeste	d, force it to s	top		
🗆 if ti	ne task is no	t schedul	led to run aga	sin, delete	it after:		30 days	\sim
If the ta	sk is already	y running	, then the fol	lowing rul	e applies:			
Do not	start a new	instance		~				
							OK	Cancel

9. Introduzca las credenciales para la cuenta que ejecutará la tarea.

Nota: Vaya al paso 5 cuando se configura el grupo de aplicaciones predeterminado.

1. Vaya a Administrador (IIS) (En Administrador del servidor > Herramientas)

2. Expanda la columna de la derecha hasta que la **carpeta Sitios** esté visible, **haga clic con el botón derecho y seleccione Agregar sitio web**.

\$]		Int	ernet Information Services	(IS) Manager	= 0 X
🐨 💽 🔹 🖬 WN-MPM19408	USU + Stei +				□ = 2 ⊕ •
File View Help					
Connections Q, 2 Q, Start Page	Sites	• 7 60 - 🔂 Show A	8 Group by: No Grouping		Actions Add Website Set Website Defaults
- Application Pools	Name *	ID Status	Binding	Path	e Help
Add Website	Contault Web Site	1 Started (H	":00 (Hmp)	%SystemDriveWinetpubliamment	
E Refresh					
Switch to Content Vie	-				
4 10 3	features View 😺	Content View			
Ready					9.

3. Elija el nombre que desee. Para la ruta física, seleccione la carpeta *C:\TETRA\Signatures* donde se descargaron las firmas.

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

4. Deje a Bindings en paz. **Configure un nombre de host separado** y un nombre de servidor, los nombres elegidos deben ser resueltos por los clientes. Esta es la URL que configurará en la política.

5. Seleccione el sitio y navegue hasta Tipos MIME y agregue los siguientes tipos MIME:

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

Image: Configuration	Internet Information Services (IIS) Manager	= 0 X
File View Help Section Section </td <td>WINAMMERCAUUU + Stel + Mta +</td> <td>6 - G 10 -</td>	WINAMMERCAUUU + Stel + Mta +	6 - G 10 -
Semention Image: Construction Image: Seminal Section For For Section For Section For For Section For	File View Help	
(II) Content year	Constant Constant Configuration C	Actions Copiese Edit Permissions Edit Site Bindings Bindings Vew Applications Vew Applications Vew Virtual Overtonies Manage Website Browse Return Stag Browse Website Browse Browse Website Browse Browse Settings Configure Limits Help
range and a second s	Ready	•1.

6. Navegue hasta el **archivo web.config** (ubicado en la carpeta reflejada), agregue las líneas siguientes a la parte superior del archivo.

9			Internet Information Services (IIS) Manager		_ 0 X
www.www.soa www.soa ww.soa www.soa www.soa ww.soa www.soa www.soa	USU + Stei + t	eta +			0 - 2 0
File View Help				_	
Connections	-				Actions
0 🗔 👔 😥	MIME	Types			A44
No Start Page					10
WIN-MEMISNOBUSU (WIN-M	Use this heature to	manage the sist of the nam	e entensions and associated content types that are served as static free by the web server.		¥ Inne
- 2 Application Pools	Group by: No-Gr	A nemone			
a 😹 Stes	Extension*	MME Type	Entry Type	~	ey Help
5 😔 Default Web Site	-45	application/x-quic	Inherited		
> 🐶 tetra	.pd	application/octet	Inherited		
	-10	audio/s-pn-realau	Inherited		
	.ram	audio/s-pn-realau	Inherited		
	187	application/ochet	Inherited		
	.785	image/s-cmu-raster	Inherited		
	A	image/vnd.m-real	Inherited		
	-190	image/s-rgb	Inherited		
	.m	application/vnd.m	Inherited		
	.mi	audio/mid	Inherited		
	.neff	application/s-broff	Inherited		
	.spm	audio/s-pn-realau	Inherited		
	м	application/itf	Inherited		
		ted/inched	Inherited		
	act	application/s-mea	Inherited		
	-543	ted/scriptlet	Inherited	-	
	-368	application/octet	Inherited		
	setpey	application/set-pa	Inherited		
	.setreg	application/set-re	Inherited		
	.sgml	ted/sgml	Inherited		
	.sh	application/x-sh	Inherited		
	shar	application/s-shar	Inherited		
	-10	application/octel	Local	-	
		and/stion/s-millit	Inharited		
c	E Features View	Content View			
Configuration: 'betra' web.config					9.7

Cuando haya terminado, el contenido del archivo C:ITETRA\Signatures\web.config aparecerá como tal cuando se visualice en un editor de texto. (La sintaxis y el espaciado deben ser los mismos que el ejemplo proporcionado.)

Nota: AMP para el conector de terminales requiere la presencia del encabezado HTTP del servidor en la respuesta para un funcionamiento adecuado. Si se ha desactivado el encabezado HTTP del servidor, es posible que el servidor Web necesite una configuración adicional especificada a continuación.

Se debe instalar la extensión url-rewrite. Agregue el siguiente fragmento XML a la configuración del servidor en /[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>
</rules>
```

Nota: Realice este cambio manualmente con un editor de texto o con el administrador IIS mediante el módulo Reescritura de URL. El módulo Rewrite se puede instalar desde la siguiente URL (<u>https://www.iis.net/downloads/microsoft/url-rewrite</u>)

Cuando haya terminado, el contenido del archivo C:ITETRA\Signatures\web.config aparecerá como tal cuando se visualice en un editor de texto. (La sintaxis y el espaciado deben ser los mismos que el ejemplo proporcionado.)

Apache / Nginx

Nota: En los pasos proporcionados se asume que está atendiendo las firmas del directorio predeterminado del software de alojamiento web.

- 1. Cree una nueva carpeta en su unidad raíz llamada TETRA.
- 2. Descomprima el paquete de scripts descargados en esta carpeta.
- 3. Ejecute el comando Chmod +x update-linux* para dar a los scripts el permiso ejecutable.
- 4. Ejecute el comando para buscar los archivos de actualización de TETRA.

This command may vary depending on your directory structure.

5. Para automatizar el proceso de actualización del servidor, agregue un trabajo cron al servidor:

0 ****/TETRA/update-linux-x86-64 fetch --config /TETRA/config.xml --once --mirror /var/www/html/ 6. Siga los pasos en Configuración de políticas para configurar su política para utilizar el servidor de actualización.

Configuración de políticas

1. Navegue hasta la política para utilizar Update Server y en *Advanced Settings > TETRA* seleccione: Casilla de verificación para servidor de actualización de AMP localEl nombre de host o IP para el servidor de actualización con el formato <hostname.domain.root> o dirección IP.

Precaución: No incluya ningún protocolo antes o ningún subdirectorio después de lo contrario, esto dará lugar a un error mientras se descarga.

[Optional] Checkbox Use HTTPS para las actualizaciones de definición de TETRA: si el servidor local está configurado con un certificado adecuado y para que los conectores utilicen HTTPS.

Verificación

Navegue hasta el directorio C:\inetpub\wwwroot\, C:\TETRA\Signature o /var/www/html y verifique que las firmas actualizadas sean visibles, las firmas se descargan del servidor al cliente final esperando hasta el siguiente ciclo de sincronización o eliminando manualmente las firmas existentes y luego esperando a que las firmas se descarguen. El valor predeterminado es un intervalo de 1 hora para buscar una actualización.

Información Relacionada

- Soporte Técnico y Documentación Cisco Systems
- Cisco AMP para terminales: notas técnicas
- Cisco AMP para terminales: guía del usuario