Konfigurationsschritte für den AMP-Aktualisierungsserver

Inhalt

Einführung Voraussetzungen Installationsschritte Alle Plattformen Windows IIS Verzeichniserstellung Task-Erstellung aktualisieren IIS-Manager-Konfiguration Apache/Nginx Richtlinienkonfiguration Überprüfung Zugehörige Informationen

Einführung

Dieses Dokument beschreibt detaillierte Konfigurationsschritte für den TETRA Update Server (AMP) von Cisco Advanced Malware Protection.

Voraussetzungen

- Kenntnis von Server-Hosts wie Windows 2012R2 oder CentOS 6.9 x86_64.
- Kenntnisse über Hostingsoftware wie IIS (nur Windows), Apache, Nginx
- Konfigurierte Server-Hosts mit aktiviertem HTTPS, gültiges vertrauenswürdiges Zertifikat installiert.
- Option für lokalen HTTPS-Aktualisierungsserver konfiguriert.

Hinweis: Ausführliche Informationen zur Aktivierung der Konfiguration und der Anforderungen des lokalen Update-Servers finden Sie in Kapitel 25 des Benutzerhandbuchs zu AMP für Endgeräte, das <u>hier</u> verfügbar ist. (<u>https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf</u>)

Hinweis: Server-Hosts (IIS, Apache, Nginx) sind Drittanbieterprodukte und werden von Cisco nicht unterstützt. Bei Fragen, die über die angegebenen Schritte hinausgehen, wenden Sie sich bitte an die Support-Teams für die jeweiligen Produkte.

Warnung: Wenn AMP mit einem Proxy-Server konfiguriert ist, wird der gesamte Aktualisierungsdatenverkehr (einschließlich TETRA) weiterhin über den Proxyserver an den lokalen Server gesendet. Stellen Sie sicher, dass der Datenverkehr während der Übertragung den Proxy ohne Änderungen passieren darf.

Installationsschritte

Alle Plattformen

- 1. Bestätigen Sie das Betriebssystem des Hostservers.
- 2. Bestätigen Sie Ihr AMP für Endpoints-Dashboard-Portal, laden Sie das Updater-Softwarepaket und die Konfigurationsdatei herunter.

AMP für Endgeräte-Konsole:

- USA https://console.amp.cisco.com/tetra_update
- EU https://console.eu.amp.cisco.com/tetra_update
- APJC https://console.apjc.amp.cisco.com/tetra_update

Windows IIS

Hinweis: Die folgenden Schritte basieren auf dem neuen IIS-Anwendungspool zum Hosten der Signaturen, **nicht** auf dem Standardanwendungspool. Um den Standardpool zu verwenden, ändern Sie den Ordner —**spiegeln** in den angegebenen Schritten, um den Standardpfad für das Webhosting wiederzugeben (**C:\inetpub\wwwroot**).

Verzeichniserstellung

- 1. Erstellen Sie einen neuen Ordner auf dem Root-Laufwerk, nennen Sie ihn TETRA.
- 2. Kopieren Sie das gezippte AMP-Aktualisierungspaket und die Konfigurationsdatei in den erstellten TETRA-Ordner.
- 3. Entpacken Sie das Softwarepaket in diesem Ordner.
- 4. Erstellen Sie einen neuen Ordner mit dem Namen Signaturen im TETRA-Ordner.

Task-Erstellung aktualisieren

- 1. Öffnen Sie die Befehlszeile, und navigieren Sie zum C: ITETRA Ordner. cd C: ITETRA.
- 2. Führen Sie den Befehl update-win-x86-64.exe fetch -config="C:\TETRA\config.xml" -once -spiegelt C:\TETRA\Signatures aus.
- 3. Öffnen Sie den Taskplaner, und erstellen Sie eine neue Aufgabe. (Aktion > Aufgabe erstellen), um die Aktualisierungssoftware bei Bedarf automatisch mit den folgenden Optionen auszuführen:
- 4. Wählen Sie die Registerkarte Allgemein. Geben Sie einen Namen f
 ür die Aufgabe ein.Wählen Sie Ausf
 ühren aus, ob ein Benutzer angemeldet ist oder nicht.W
 ählen Sie Mit den h
 öchsten Berechtigungen ausf
 ühren aus.W
 ählen Sie das Betriebssystem aus dem Dropdown-Men
 ü Konfigurieren aus.

•		Create Task			×		
General Trig	gers Actions Cond	itions Settings					
Name: TETRAUPDATES							
Location:							
Author:	WIN-MFM1SN3BU60	/\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 whee	ther 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					
				ОК	Cancel		

5. Wählen Sie die Registerkarte Trigger aus.

- Klicken Sie auf Neu.
- Wählen Sie In einem Zeitplan aus dem Dropdown-Menü Aufgabe starten aus.
- Wählen Sie Täglich unter Einstellungen aus.
- Aktivieren Sie Task alle wiederholen, wählen Sie aus dem Dropdown-Menü eine Stunde aus, und wählen Sie Unbegrenzt aus der Option "für eine Dauer von:" aus.
- Stellen Sie sicher, dass Enabled (Aktiviert) aktiviert ist.
- Klicken Sie auf 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 v Repeat task every: 1 hour v for a duration of: Indefinitely v Stop all running tasks at end of repetition duration Stop task if it runs longer than: 3 days v Expire: 12/20/2019 * &40:56 PM * Synchronize across time zones Expire: 12/20/2019 * &40:56 PM *	
OK Cancel	

6. Registerkarte Aktionen auswählen

- Klicken Sie auf Neu.
- Wählen Sie im Dropdown-Menü Aktion die Option Programm starten aus.
- Geben Sie C:ITETRA\update-win-x86-64.exe in das Feld Programm/Skript ein.
- Geben Sie fetch -config C:\TETRA\config.xml -once -spiegeln C:\TETRA\Signatures im Feld Argumente hinzufügen ein.
- Geben Sie C:ITETRA in das Feld Start ein.
- Klicken Sie auf OK

New Action ×						
You must specify what action this task will perform.						
~						
•						
C:\TETRA						
_						

7. [Optional] Registerkarte Bedingungen auswählen.

Aktivieren Sie die Option Computer zum Ausführen dieser Aufgabe aktivieren.

O Creat	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							
Stop if the computer switches to battery power							
Wake the computer to run this task							
Start only if the following network connection is ava	ailable:						
Any connection		~					
	01	Cancel					

8 Wählen Sie die Registerkarte Einstellungen.

• Vergewissern Sie sich, dass Sie keine neue Instanz starten aktiviert ist unter Wenn die Aufgabe bereits ausgeführt wird.

• Klicken Sie auf OK.

Create Tas	k 🛛 🗶							
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								
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. Geben Sie die Anmeldeinformationen für das Konto ein, das die Aufgabe ausführen soll.

Hinweis: Fahren Sie mit Schritt 5 fort, wenn der Standard-Anwendungspool konfiguriert wurde.

1. Navigieren Sie zum (IIS)-Manager (**Unter Server Manager > Tools**).

2. Erweitern Sie die rechte Spalte, bis der **Ordner Sites** angezeigt wird, **klicken Sie mit der rechten Maustaste, und wählen Sie Website hinzufügen aus**.

\$]		inte	emet Information Services (85) Manager	_ 0 X
. WN-MPMI908	USU + Stei +				₩ = 5 0 •
File View Help					
Connections	Cites				Actions
Q,- 🗟 🖄 👂	Siles				🧳 Add Website
Start Page	Filter	• 7 Go - 🔂 Show A	A Group by: No Grouping .		Set Website Defaults
- D Application Pools	Name *	ID Status	Binding	Path	e Help
Add Website	Default Web Site	1 Started (HL	*:00 (Hmp)	%SystemDriveWinetpublismmont	
E Refuelt					
Suitch to Contact Vie	-				
	Testure Very	content View			
Realy	and the second				÷.
					10

3. Wählen Sie einen gewünschten Namen aus. Wählen Sie für Physical Path den Ordner *C:\TETRA\Signatures* aus, in dem die Signaturen heruntergeladen wurden.

Add Website		? X
Site name: Application pool: tetra tetra	Select]
Physical path: C:\TETRA\Signatures Pass-through authentication		
Connect as Test Settings Binding		
Type: IP address: http v All Unassigned Host name:	Port:	
tetraupdate.bgl-amp.lab		
Start Website immediately	OK Cano	cel

4. Lassen Sie Bindungen allein. Konfigurieren Sie einen separaten Hostnamen und einen separaten Servernamen. Ausgewählte Namen müssen von Clients auflösbar sein. Dies ist die URL, die Sie in der Richtlinie konfigurieren werden.

5. Wählen Sie die Site aus, navigieren Sie zu **MIME Types**, und **fügen Sie die folgenden MIME-Typen hinzu**:

- .gzip, Anwendung/Oktett-Stream
- .dat, Anwendung/Oktett-Stream
- .id, Application/Oktett-Stream
- .sig, Application/Oktett-Stream

Image: Second
File View Help Connections Actions Q (a) 20 [9]. Extra Home Start Page Files - (a) Good phy. Area - (a) - (a) Show AB (Group by. Area Files - (a) Good phy. Area - (a) - (a) Show AB (Group by. Area - (a) -
Connections Actions Q. • [] 2 [Q. • [] 2 <t< td=""></t<>
Authentic Compression Pagin → Default tick Sce → Default tic
Feady

6. Navigieren Sie zur **Datei web.config** (im Ordner spiegeln), und fügen Sie die folgenden Zeilen am Anfang der Datei hinzu.

8]			Internet Information Services (IIS) Manager		= 0 X	
WN-MFM1940	IUSU + Stei + 5	eta +			10 × 5 10 +	
File View Help						
Connections	_				Artists	
0.000	MIME	Types				
M. 101 (11 10)	-				A86	
 Start Page Starts Page 	All Start Page Use this feature to manage the list of file name extensions and associated context types that are served as static files by the Web server.					
Apple ation Pools	Growther, No Growing .			× Remove		
A Shes	Edension [®]	MAR Tune	fairs have		Help	
5 Gefault Web Site	at	and states to make	loke/ted			
> 😜 tetra	ad	application/octat-	Inheited			
	4	audio/s-pn-realau	Inherited			
	Jam	audio/s-pn-realau_	Inherited			
	100	application/ochet	Inherited			
	.485	image/s-cmu-satter	inherited			
		image/vnd.m-real	Inherited			
	190	image/s-rgb	Inherited			
	.m	application/vnd.m	Inherited			
	.mi	audio/mid	Inherited			
	Joff .	application/s-boff	Inherited			
	.spm	audio/s-pn-realau	Inherited			
	18	application/itf	Inherited			
		ted/ichted	Inherited			
	acd	application/s-mes	Inherited			
	-543	ted/scriptlet	Inherited	-		
	-348	application/octet	inheited			
	setpey	application/set-pa	Inherited			
	setting	application/set-re	Inherited			
	agent	ted/sgml	Inherited			
	.sh	appncation/x-sh	Inherited Links (
	and a	application/s-shar	inherited			
		application with dia	Liberthand	*		
		And Brown I - States				
C III D	Features View	Content View				
Configuration: 'tetra' web.config					9 27	

Nach Beendigung wird der C:\TETRA\Signatures\web.config-Dateiinhalt als solcher angezeigt, wenn er in einem Texteditor angezeigt wird. (Syntax und Abstand müssen mit dem angegebenen Beispiel übereinstimmen.)

Hinweis: Der AMP für Endpoints-Connector benötigt für den ordnungsgemäßen Betrieb das Vorhandensein des Server-HTTP-Headers in der Antwort. Wenn der Server-HTTP-Header deaktiviert wurde, benötigt der Webserver möglicherweise eine zusätzliche Konfiguration, die unten angegeben ist.

Die Erweiterung url-rewrite muss installiert werden. Fügen Sie der Serverkonfiguration unter /[MIRROR_DIRECTORY]/web.config den folgenden XML-Ausschnitt hinzu:

```
<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>
```

Hinweis: Führen Sie diese Änderung manuell mit einem Text-Editor oder mit dem IIS-Manager durch, indem Sie das Modul URL Rewrite verwenden. Das Rewrite-Modul kann über die folgende URL installiert werden (<u>https://www.iis.net/downloads/microsoft/url-</u> <u>rewrite</u>):

Nach Beendigung wird der C: ITETRAlSignatures web. config-Dateiinhalt als solcher angezeigt, wenn er in einem Texteditor angezeigt wird. (Syntax und Abstand müssen mit dem angegebenen Beispiel übereinstimmen.)

Apache/Nginx

Hinweis: Bei den angegebenen Schritten wird davon ausgegangen, dass Sie die Signaturen aus dem Standardverzeichnis der Webhosting-Software bereitstellen.

- 1. Erstellen Sie einen neuen Ordner auf Ihrem Stammlaufwerk mit dem Namen TETRA.
- 2. Entpacken Sie das heruntergeladene Skriptpaket in diesem Ordner.
- 3. Führen Sie den Befehl Chmod +x update-linux* aus, um die ausführbare Berechtigung der Skripte zu erhalten.
- 4. Führen Sie den Befehl aus, um die TETRA-Aktualisierungsdateien abzurufen.

sudo ./update-linux-x86-64 fetch --config config.xml --once --mirror /var/www/html/:
 <u>This command may vary depending on your directory structure.</u>
 Um den Aktualisierungsprozess des Servers zu automatisieren, fügen Sie dem Server einen Cron-Auftrag hinzu:

0 * * * * /*TETRA/update-linux-x86-64 fetch --config /TETRA/config.xml --once --mirror /var/www/html/* 6. Fahren Sie mit den Schritten unter **Richtlinienkonfiguration fort**, um Ihre Richtlinie für die Verwendung des Aktualisierungsservers zu konfigurieren.

Richtlinienkonfiguration

 Navigieren Sie zur Richtlinie, um den Aktualisierungsserver zu verwenden, und wählen Sie unter Erweiterte Einstellungen > TETRA folgende Option aus: Kontrollkästchen für lokalen AMP-AktualisierungsserverDer Hostname oder die IP-Adresse für den Aktualisierungsserver im Format <hostname.domain.root> oder IP-Adresse.

Vorsicht: Schließen Sie keine Protokolle vor oder Unterverzeichnisse nach anderen, das führt zu einem Fehler beim Herunterladen.

[Optional] Kontrollkästchen HTTPS für Aktualisierungen der TETRA-Definition verwenden: wenn der lokale Server mit einem entsprechenden Zertifikat konfiguriert ist und die Verbindungen HTTPS verwenden.

Überprüfung

Navigieren Sie zum Verzeichnis C:\inetpub\wwwroot\, C:\TETRA\Signature oder /var/www/html, und überprüfen Sie, ob die aktualisierten Signaturen sichtbar sind. Die Signaturen werden vom Server auf den Endclient heruntergeladen, indem Sie entweder auf den nächsten Synchronisierungszyklus warten oder die vorhandenen Signaturen manuell löschen und dann auf den Download der Signaturen warten. Der Standardwert ist ein 1-Stunden-Intervall, in dem nach einer Aktualisierung gesucht wird.

Zugehörige Informationen

- <u>Technischer Support und Dokumentation Cisco Systems</u>
- <u>Cisco AMP für Endgeräte Technische Hinweise</u>
- <u>Cisco AMP für Endgeräte Benutzerhandbuch</u>