Configuratiestappen voor AMP-server

Inhoud

Inleiding Voorwaarden Installatiestappen Alle platforms Windows IS Map maken Taakmaken bijwerken Configuratie IS Manager Apache / Nginx Beleidsconfiguratie Verificatie Gerelateerde informatie

Inleiding

Dit document beschrijft gedetailleerde configuratiestappen voor Cisco Advanced Malware Protection (AMP), TETRA Update Server.

Voorwaarden

- Kennis van serverhosts zoals Windows 2012R2 of CentOS 6.9 x86_64.
- Kennis van het organiseren van software zoals, IS (alleen Windows), Apache, Nginx
- Geconfigureren serverhosts met HTTPS ingeschakeld, geldig vertrouwd certificaat geïnstalleerd.
- Optie HTTPS lokale update Server configureren.

Opmerking: Raadpleeg voor volledige informatie over het inschakelen van de configuratie en vereisten van de lokale update serveren het raadplegen van hoofdstuk 25 van de AMP for Endpoints <u>hier</u> beschikbaar<u>gebruikersgids</u>.

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

Opmerking: Server Hosts (IS, Apache, NGINX) zijn producten van derden en worden niet ondersteund door Cisco. Raadpleeg de ondersteuningsteams voor respectievelijke producten voor vragen buiten de meegeleverde stappen.

Waarschuwing: Als AMP met een Proxyserver is ingesteld, wordt al het update verkeer (inclusief TETRA) verzonden via de proxy-server, naar uw lokale server. Zorg ervoor dat het verkeer is toegestaan zonder wijziging de volmacht passeert tijdens het vervoer.

Installatiestappen

Alle platforms

- 1. Bevestig het besturingssysteem van de Hosted Server.
- 2. Bevestig uw Advanced Malware Protection voor Endpoints Dashboard portal, download het Updater Software Package en het configuratiebestand.

Advanced Malware Protection voor endpoints:

- VS 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 IS

Opmerking: De onderstaande stappen zijn gebaseerd op het nieuwe IIS-toepassingspool om de handtekeningen te ontvangen, **en niet** op de standaardapplicatie. Als u de standaard pool wilt gebruiken, wijzigt u de map —spiegel in de meegeleverde stappen om het standaard web host pad weer te geven (**C:\inetpub\wwwroot**)

Map maken

- 1. Geef een nieuwe map op het basisstation op en noem deze TETRA.
- 2. Kopieer het zipped AMP-softwarepakket en het configuratiebestand naar de TETRA-map die is gemaakt.
- 3. Koppel het softwarepakket in deze map los.
- 4. Maak een nieuwe map die handtekeningen heet in de TETRA-map.

Taakmaken bijwerken

- 1. Open de opdrachtregel en navigeer naar de C:ITETRA map.cd C:ITETRA
- 2. Start de opdracht update-win-x86-64.exe fetch -fig="C:\TETRA\config.xml" -once -mirror C:\TETRA\Signatures
- 3. Open de taakplanner en maak een nieuwe taak. (Actie > Task) om de software van het update automatisch met de volgende opties uit te voeren waar nodig:
- 4. Selecteer het tabblad Algemeen. Voer een naam in voor de taak.Selecteer Start of de gebruiker is aangemeld of niet.Selecteer Run met de hoogste privileges.Selecteer het besturingssysteem uit de vervolgkeuzelijst Configureren.

•		Create Task			×		
General Trig	gers Actions Cond	itions Settings					
Name: TETRAUPDATES							
Location:	X.						
Author:	WIN-MFM1SN38U6	/\Administrator					
Description:							
- Security opt	ons						
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 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. Selecteer het tabblad triggers.

- Klik op Nieuw.
- Selecteer In een programma uit de vervolgkeuzelijst Beginnen met de taak.
- Selecteer **Dagelijks** programma onder Instellingen.
- Controleer de taak elke keer herhalen en selecteer 1 uur uit de vervolgkeuzelijst en selecteer Voor onbeperkt in de modus voor een duur van:
- Controleer dat deze optie is ingeschakeld.
- Klik op 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 Stop all running tasks at end of repetition duration Stop task if it runs longer than: 3 days Kepire: 12/20/2019 Keyire: 12/20/2019 Keyire: 12/20/2019 Keyire: 12/20/2019 Keyire: 12/20/2019 Keyire: 12/20/2019 Keyire: 12/	
OK Cancel	

6. Selecteer het tabblad Handelingen

- Klik op Nieuw.
- Selecteer Start een programma vanuit de vervolgkeuzelijst Action.
- Voer C:\TETRA\update-win-x86-64.exe in het veld Programma/script in.
- Voer een fetch in ----configuratie C:\TETRA\config.xml -- eens -- spiegelend C:\TETRA\Signatures in het veld Add argumenten.
- Voer C:ITETRA in het veld Start in
- Klik op OK

New A	ction	X					
You must specify what action this task will 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. [Optioneel] Selecteer het tabblad Voorwaarden.

Controleer de computer om deze taak uit te voeren.

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	~
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 ava	ailable:	
Any connection		¥
	0	K Cancel

8 Selecteer het tabblad Settings.

• Controleer dat U geen nieuw exemplaar start, maar onder Als de taak al actief is.

٠	Klik	ор	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 ∨
If the task is already running, then the following rule applies:	
Do not start a new instance 🗸	
	OK Cancel

9. Voer de aanmeldingsgegevens in voor de account die de taak gaat uitvoeren.

Opmerking: Naar stap 5 overslaan wanneer Default Application Pool is ingesteld.

1. Navigeren naar (IS) Manager (onder Server Manager > Tools)

2. Vouw de rechterkolom uit totdat de **map Sites** zichtbaar is, **rechtsklik en selecteer website toevoegen**.

9			ternet Information Service	es (IIS) Manager	= 0 X
🐨 🔹 + WN-MPMISKO	BUBU + Shei +				w=5.0+
File View Help					
Connections Q In Page Start Page Application Paols Application P	Filter Filter Name Distant Web Site	+ 1 Go - Dens D Setus 1 Started (H.	All Group by: No Grouping Binding - 130 (kmp)	* Path NSystemDriveWinetpublianwaroot	Artions Image: Constraint of the second s
Ready	the second second				4 2.
- and					

3. Kies een naam naar keuze. Selecteer voor het fysieke pad de *C:\TETRA\Signatures* map waarin de handtekeningen zijn gedownload.

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 Image:	
Start Website immediately	
ОК	Cancel

4. Laat Bindings alleen. **Configureer een afzonderlijke hostname** en servernaam, de gekozen namen moeten door de klanten kunnen worden opgelost. Dit is de URL die u in het beleid zult configureren.

5. Selecteer de locatie en navigeer naar MIME-typen en voeg de volgende MIME-typen toe:

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

Internet Information Services (IIS) Manager	- 0 X
WINAMM/SOBULU + Step + tetra +	$\Theta=\Theta_{1}\Theta_{2}$
File View Help	
Consection Q	insiens
Ready	9 .

6. Navigeer naar het **web.fig-bestand** (in de spiegelmap bevindt), voeg de volgende lijnen aan de bovenkant van het bestand toe.

6			Internet Information Services (IIS) Manager		_ 0 X
WN-MMISA	IUIU + Shei + 1	eta +			0 = 5 € .
File View Help					
Connections	-				Actions
9-01018	MIME	Types			
A Start Page	-				
WIN-MEMISIOEUSU (WIN-M)	Use this feature to manage the list of file name extensions and associated content types that are served as static files by the Web server. Group by: Na Grouping •			Lat.	
- D Application Pools				A Remove	
a Stes	Extension*	MME Type	Entry Type	~	e Hulp
5 😳 Default Web Site	-10	application/x-quic	Inherited		
2 40 Mitu	.ed	application/octet	Inherited		
	-0	audio/s-pn-realau	Inherited		
	.cam	audio/u-pn-realau	Inherited		
	-107	application/octet	Inherited		
	.485	image/s-cmu-raster	Inherited		
		image/vnd.m-real	Inherited		
	.spb	image/s-rgb	Inherited		
		application/vnd.m	Inherited		
	Jami	audio/mid	Inherited		
	Joff .	application/s-boff	Inherited		
	.spm	audio/s-pn-realau	Inherited		
	18	application/itf	Inherited		
		ted/ichted	Inherited		
	acd	application/x-mes	Inherited		
	-543	ted/scriptlet	Inherited		
	-348	application/octet	Inherited		
	-setpay	application/set-pa	Inherited		
	.sebeg	application/set-re	Inherited		
	.sgml	ted/sgml	Inherited		
	-sh	application/x-sh	Inherited		
	shar	application/s-shar	Inherited		
	.sig	application/ochet	Local	-	
		analysiss/s-milli	Inherited	(v)	
C III 2	E Features View	Content View			
Configuration: 'betra' web.config					•1.

Wanneer de inhoud van het C:\TETRA\Signatures\web.config-bestand klaar is, verschijnt deze als zodanig wanneer u het in een teksteditor bekijkt. (Syntax and spacing moeten hetzelfde blijven als het voorgelegde voorbeeld.)

Opmerking: De Advanced Malware Protection voor Endpoints Connector vereist de aanwezigheid van de server HTTP-header in de reactie op een correct gebruik. Als de Server HTTP Header is uitgeschakeld, heeft de webserver mogelijk nog een configuratie nodig die hieronder is gespecificeerd.

De verlenging moet worden geïnstalleerd. Voeg het volgende XML fragment toe aan de serverconfiguratie op /[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>
```

Opmerking: Voer deze verandering handmatig uit met een teksteditor of met de ISbeheerder door de URL-herschrijfmodule te gebruiken. De herschrijfmodule kan vanaf de volgende URL (<u>https://www.iis.net/downloads/microsoft/url-rewrite</u>) worden geïnstalleerd

Wanneer de inhoud van het C:\TETRA\Signatures\web.config-bestand klaar is, verschijnt deze als zodanig wanneer u het in een teksteditor bekijkt. (Syntax and spacing moeten hetzelfde blijven als het voorgelegde voorbeeld.)

Apache / Nginx

Opmerking: De geboden stappen veronderstellen dat u de handtekeningen van de standaard folder van de web host software serveert.

- 1. Maak een nieuwe map op uw *basisstation* met de naam TETRA.
- 2. Unzip het gedownload scripts pakket in deze map.
- 3. Start de opdracht Chmod +x update-linux* om de scripts uitvoerbare toestemming te geven.
- 4. Start de opdracht om de TETRA update files te halen.

This command may vary depending on your directory structure.

5. Als u het uploadproces van de server wilt automatiseren, voegt u een snijtaak toe aan de server:

0 ****/TETRA/update-linux-x86-64 fetch --config /TETRA/config.xml --once --mirror /var/www/html/ 6. Ga verder met de stappen onder **Beleidsconfiguratie** om uw beleid te configureren voor het gebruik van de Update server.

Beleidsconfiguratie

1. Navigeer naar het beleid om de Update Server te gebruiken en onder Geavanceerde Instellingen > TETRA selecteer: Selectieknop voor

lokale AMP-update serverDe hostname of IP voor de update server in het formaat van <hostname.domein.root> of IP-adres.

Voorzichtig: Voeg geen protocollen vóór of subdirectories toe nadat het tegendeel is gebeurd, dit leidt tot een fout bij het downloaden.

[Optioneel] Selectieknop Gebruik HTTPS voor TETRA Standaard updates: als de lokale server is geconfigureerd met een correct certificaat en voor de connectors om HTTPS te gebruiken.

Verificatie

Navigeer naar de directory C:\inetpub\wwwroot\, C:\TETRA\Signature of /var/www/html en controleer of de bijgewerkte handtekeningen zichtbaar zijn, de handtekeningen worden gedownload van de server naar de eindclient door te wachten tot de volgende synchronisatiecyclus of handmatig de bestaande handtekeningen te verwijderen en dan te wachten tot de handtekeningen worden gedownload. De standaardinstelling is een interval van 1 uur om voor een update te controleren.

Gerelateerde informatie

- <u>Technische ondersteuning en documentatie Cisco Systems</u>
- <u>Cisco Advanced Malware Protection voor endpoints TechNotes</u>
- <u>Cisco Advanced Malware Protection voor endpoints gebruikershandleiding</u>