# Etapas de configuração do servidor de atualização do AMP

## Contents

Introduction Pré-requisitos Etapas de instalação Todas as plataformas Windows IIS Criação de Diretório Atualizar Criação de Tarefas Configuração do gerenciador do IIS Apache / Nginx Configuração de política Verificação Informações Relacionadas

# Introduction

Este documento descreve as etapas detalhadas de configuração do Cisco Advanced Malware Protection (AMP) TETRA Update Server.

# Pré-requisitos

- Conhecimento de hosts do servidor, como Windows 2012R2 ou CentOS 6.9 x86\_64.
- Conhecimento de software de hospedagem, como IIS (somente Windows), Apache, Nginx
- Hosts do servidor configurados com HTTPS ativado, certificado confiável válido instalado.
- Opção de servidor de atualização local HTTPS configurada.

**Note**: Para obter detalhes completos sobre como ativar a configuração e os requisitos do Local Update Server, consulte o Capítulo 25 do Guia do usuário da AMP para endpoints, disponível <u>aqui</u>.

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

**Note**: Os hosts de servidor (IIS, Apache, Nginx) são produtos de terceiros e não são suportados pela Cisco. Consulte as equipes de suporte para os respectivos produtos para esclarecer dúvidas fora das etapas fornecidas.

**aviso:** Se o AMP estiver configurado com um servidor Proxy, todo o tráfego de atualização (incluindo TETRA) continuará a ser enviado através do servidor proxy, direcionado para o servidor local. Certifique-se de que o tráfego tenha permissão para passar pelo proxy sem nenhuma modificação enquanto estiver em trânsito.

## Etapas de instalação

#### Todas as plataformas

- 1. Confirme o sistema operacional (SO) do servidor de hospedagem.
- 2. Confirme o portal do painel do AMP para endpoints, faça o download do Pacote de software do atualizador e do arquivo de configuração.

#### Console do AMP para endpoints:

EUA - 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

#### Windows IIS

Note: As etapas abaixo baseiam-se no novo IIS Application Pool para hospedar as assinaturas, **não** no Application Pool padrão. Para usar o pool padrão, altere a pasta **—espelho** nas etapas fornecidas para refletir o caminho de hospedagem da Web padrão (C:\inetpub\wwwroot)

#### Criação de Diretório

- 1. Crie uma nova pasta na unidade raiz, nomeie-a TETRA
- 2. Copie o pacote de software do atualizador AMP zipado e o arquivo de configuração para a pasta TETRA criada.
- **3.** Descompacte o pacote de software nesta pasta.
- 4. Crie uma nova pasta chamada Assinaturas dentro da pasta TETRA.

#### Atualizar Criação de Tarefas

- 1. Abra a linha de comando e navegue até a pasta C:ITETRA. cd C:ITETRA
- 2. Execute o comando update-win-x86-64.exe fetch config="C:\TETRA\config.xml" once mirror C:\TETRA\Signatures
- 3. Abra o Agendador de Tarefas e crie uma nova Tarefa. (Ação > Criar tarefa) para executar o software do atualizador automaticamente com as seguintes opções quando necessário:
- 4. Selecione a guia Geral. Insira um nome para a tarefa.Selecione Executar se o usuário está conectado ou não.Selecione Executar com os privilégios mais altos.Selecione o sistema operacional na lista suspensa Configurar.

Θ		Create Task			×			
General Trig	gers Actions Cond	itions Settings						
Name:	Name: TETRAUPDATES							
Location:	X.							
Author:	WIN-MFM1SN3BU6	J\Administrator						
Description:								
- Security opt	ions							
When runni	ing 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 local computer re	esources.				
Run with	highest privileges							
Hidden	Configure for:	Windows Server 2012 R2			~			
				ОК	Cancel			

5. Selecione a guia Disparadores.

- Clique em New.
- Selecione Em um agendamento no menu suspenso Iniciar tarefa.
- Selecione **Daily** em Settings (Configurações).
- Marque Repetir tarefa a cada e selecione 1 hora na lista suspensa e selecione Indefinidamente na opção "por uma duração de:"
- Verifique se Enabled (Habilitado) está 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  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. Selecione a guia Ações

- Clique em New.
- Selecione Iniciar um programa no menu suspenso Ação.
- Digite C:\TETRA\update-win-x86-64.exe no campo Programa/script.
- Digite fetch config C:\TETRA\config.xml once mirror C:\TETRA\Signatures no campo Add Arguments.
- Digite C:\TETRA no campo Iniciar
- Clique em OK.

	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] Selecione a guia Condições.

Marque a opção Ativar o computador para executar essa tarefa.

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 avi	vilable	
Any connection		~
	0	K Cancel
	0	conce

8 Selecione a guia Settings (Configurações).

• Verifique se Não iniciar uma nova instância está selecionado em Se a tarefa já estiver em execução.

				Cre	ate Task			
General	Triggers	Actions	Conditions	Settings	6-1 - 1			
Specify	/ additional	settings t	hat affect the	behavior o	of the task.			
	ow task to b	e run on	demand					
Ru	n task as so	on as pos	sible after a s	cheduled s	tart is missed			
🗆 lift	he task fails,	, restart e	very:			1 minute v		
Att	empt to res	tart up to	c			3: times		
Sto	p the task if	f it runs k	onger than:			3 days ∨		
🗹 lft	he running	task does	not end whe	n requeste	d, force it to s	top		
🗆 ift	he task is no	xt schedu	led to run ag	ain, delete i	t after:		30 days	$\vee$
If the t	ask is alread	y running	g, then the fo	llowing rule	applies:			
Do not	start a new	instance		~				
						Γ	OK	Cancel

9. Digite as credenciais para a conta que executará a tarefa.

Note: Vá para a etapa 5 quando o Pool de aplicativos padrão estiver configurado.

1. Navegue até (IIS) Manager (**em Server Manager > Tools**)

2. Expanda a coluna à direita até que a **pasta Sites** esteja visível, **clique com o botão direito do mouse e selecione Adicionar site**.

<b>S</b>		Int	emet Information Services (I	5) Manager	= 0 X
🐨 👔 🖬 WIN-MEMISKA	U6U + Stei +				<b>₩</b> = 5 ( <b>0</b> •
File View Help					
Connections Q,- 🔐 🙇 😥	Sites				Actions
Start Page	Filter	• 7 60 - Show A	I Group by: No Grouping		Set Website Defaults
- Application Peels	Name *	ID Status	Binding	Path	e Help
Add Website	Codault Web Site	1 Started (H	1.00 (Hrty)	%SystemDriveWinetpublismmmoot	
20 Reheah					
Switch to Content Vie					
(	Features View	Content View			
Ready					41
- and					

3. Escolha um nome de sua escolha. Para o Caminho físico, selecione a pasta *C:\TETRA\Signatures* onde as assinaturas foram baixadas.

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

4. Deixe o Bindings em paz. **Configure um nome de host** e um nome de servidor **separados**, os nomes escolhidos devem ser resolvidos pelos clientes. Este é o URL que você configurará na diretiva.

5. Selecione o site e navegue até MIME Types e adicione os seguintes MIME Types:

- .gzip, Application/octeto-stream
- .dat, aplicativo/octeto-stream
- .id, Application/octeto-stream
- .sig, Application/octeto-stream

Image: With Addition (1)     For     For     Image: With Addition (1)     Image	Internet Information Services (IIS) Manager	= 0 X
The View Help         Constraine         Image: Search and State St	WINAMMERNBURU + Stel + Mts +	$\omega = 0.00$
Consections       Image: State Fage: S	File View Help	
e m 5 Extension Content View	Consection Consec	Actions Captors Edit Premissions Edit She Bindings Edit She Bindings Vew Vehicular Detections Vew Vehicular Detections Captors Provest Website Biosos Exerces Settings Configure Limits Provest Website Detections
Ready 🔨	Ready	<b>9</b> 1

6. Navegue até o **arquivo web.config** (localizado na pasta espelho), adicione as seguintes linhas à parte superior do arquivo.

<i>8</i> ]			Internet Information Services (IIS) Manager		= 0 X
WN-MM1940	IUSU + Sites + tet				10 × 5 10 -
File View Help				_	
Connections					Actions
0.00	MIME 1	Types			
Stat Pass	-				A05.
WIN-MEMISNEUSU (WIN-M	Use this feature to n	ranage the list of file nan	ne extensions and associated content types that are served as static files by the Web server.		ldt.
Application Pools	Group by: No-Gro	uping +			× Remove
a 📓 Sites	Extension*	MME Type	Entry Type		😧 Help
5- Q Default Web Site	-45	application/s-quic	Inherited		
2 🥹 tetra	.ed	application/octet	Inherited		
	.0	audio/s-pn-realau	Inherited		
	Jam	audio/s-pn-realau	inherited		
	100	application/octet	Inherited		
	.485	image/s-cmu-raster	inherited		
		image/vnd.m-real	Inherited		
	.agb	image/s-rgb	Inheited		
	.em	application/vnd.m	Inherited		
	.mi	audio/mid	Inherited		
	.roff	application/s-buff	Inherited		
	spen	audio/s-pn-realau	Inherited		
	м	application/iff	Inherited		
	AL.	ted/inchted	Inherited		
	-aod	application/x-mss	inherited		
	-set	ted/scriptlet	Inherited		
	-368	application/octet	Inheited		
	setpey	application/set-pa	Inherited		
	Jatreg	application/set-re	inherited		
	Agent	ted spril	inhered .		
	sh	approation/s-sh	Interior I		
		approximity similar	Incel .		
		approximation (which it	Inherited	~	
	-				
C III 2	Features View	Content View			
Configuration: 'tetra' web.config					<b>9</b> 22

Ao terminar, o conteúdo do arquivo C:\TETRA\Signatures\web.config aparecerá como tal quando exibido em um editor de texto. (A sintaxe e o espaçamento precisam permanecer iguais aos do exemplo fornecido.)

**Note**: O conector AMP para endpoints requer a presença do cabeçalho HTTP do servidor na resposta para uma operação adequada. Se o Cabeçalho HTTP do Servidor foi desabilitado, o servidor Web pode precisar de configuração adicional especificada abaixo.

A extensão url-rewrite deve ser instalada. Adicione o seguinte trecho XML à configuração do servidor em /[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>
</rule>
</rule>
```

**Note**: Execute essa alteração manualmente com um editor de texto ou com o gerenciador do IIS usando o módulo de regravação de URL. O módulo de regravação pode ser instalado a partir do seguinte URL (<u>https://www.iis.net/downloads/microsoft/url-rewrite</u>)

Ao terminar, o conteúdo do arquivo C:ITETRAISignatures\web.config aparecerá como tal quando exibido em um editor de texto. (A sintaxe e o espaçamento precisam permanecer iguais aos do exemplo fornecido.)

#### Apache / Nginx

**Note**: As etapas fornecidas pressupõem que você esteja servindo as assinaturas do diretório padrão do software de hospedagem na Web.

- 1. Crie uma nova pasta na sua unidade raiz chamada TETRA.
- 2. Descompacte o pacote de scripts baixados nesta pasta.
- 3. Execute o comando Chmod +x update-linux\* para dar permissão aos scripts executáveis.
- 4. Execute o comando para buscar os arquivos de atualização do TETRA.

sudo ./update-linux-x86-64 fetch --config config.xml --once --mirror /var/www/html/: This command may vary depending on your directory structure. 5. Para automatizar o processo de atualização do servidor, adicione um trabalho cron ao servidor:

0 \* \* \* \* /TETRA/update-linux-x86-64 fetch --config /TETRA/config.xml --once --mirror /var/www/html/ 6. Continue a seguir as etapas em Configuração de política para configurar sua política para usar o servidor de atualização.

#### Configuração de política

1. Navegue até a diretiva para usar o Servidor de atualização e, em Configurações avançadas > TETRA, selecione: Caixa de seleção do

servidor de atualização do AMP localO nome de host ou IP do servidor de atualização no formato de <hostname.domain.root> ou endereço IP.

**Caution**: Não inclua nenhum protocolo antes ou qualquer subdiretório depois do contrário, isso resultará em um erro durante o download.

[Opcional] Caixa de seleção Usar HTTPS para atualizações de definição TETRA: se o servidor local estiver configurado com um certificado apropriado e se os conectores usarem HTTPS.

#### Verificação

Navegue até o **diretório C:\inetpub\wwwroot\, C:\TETRA\Signature** ou **/var/www/html** e verifique se as assinaturas atualizadas estão visíveis; as assinaturas são baixadas do servidor para o cliente final aguardando até o próximo ciclo de sincronização ou excluindo manualmente as assinaturas existentes e aguardando o download das assinaturas. O padrão é um intervalo de 1 hora para verificar se há uma atualização.

## Informações Relacionadas

- Suporte Técnico e Documentação Cisco Systems
- <u>Cisco AMP para endpoints Notas técnicas</u>
- <u>Cisco AMP para endpoints Guia do usuário</u>