AMP TETRA -Prem em etapas da configuração do servidor

Índice

[Introdução](#)
[Pré-requisitos](#)
[AMP TETRA -Prem em etapas da configuração do servidor](#)
[Transferência da assinatura ao servidor local](#)
[Serviço das assinaturas aos conectores](#)
[Windows IIS](#)
[Apache](#)
[Nginx](#)
[Verificação](#)

Introdução

Este documento descreve as etapas de configuração em detalhe para Cisco avançou a proteção do malware (AMP) TETRA -premesis no server.

Pré-requisitos

- O usuário tem configurado já Windows 2012R2 ou o server de CentOS para hospedar a instalação.
- (Windows somente) a característica IIS já é instalada e os princípios são configurados. Este guia configurará um IIS novo do “pool aplicativo” mas as mesmas etapas poderiam ser aplicadas ao pool do aplicativo IIS do padrão.
- [AMP para a estratégia de distribuição dos valores-limite](#)
- [AMP para o Guia do Usuário dos valores-limite](#)

AMP TETRA -Prem em etapas da configuração do servidor

Transferência da assinatura ao servidor local

Setup a tarefa do esforço pelas etapas no AMP para o Guia do Usuário dos valores-limite, tomando a nota do lugar do diretório configurado do espelho. Opcionalmente, você pode aplicar o comando manual do esforço, tomando outra vez a nota do lugar do diretório configurado do espelho.

Serviço das assinaturas aos conectores

Windows IIS

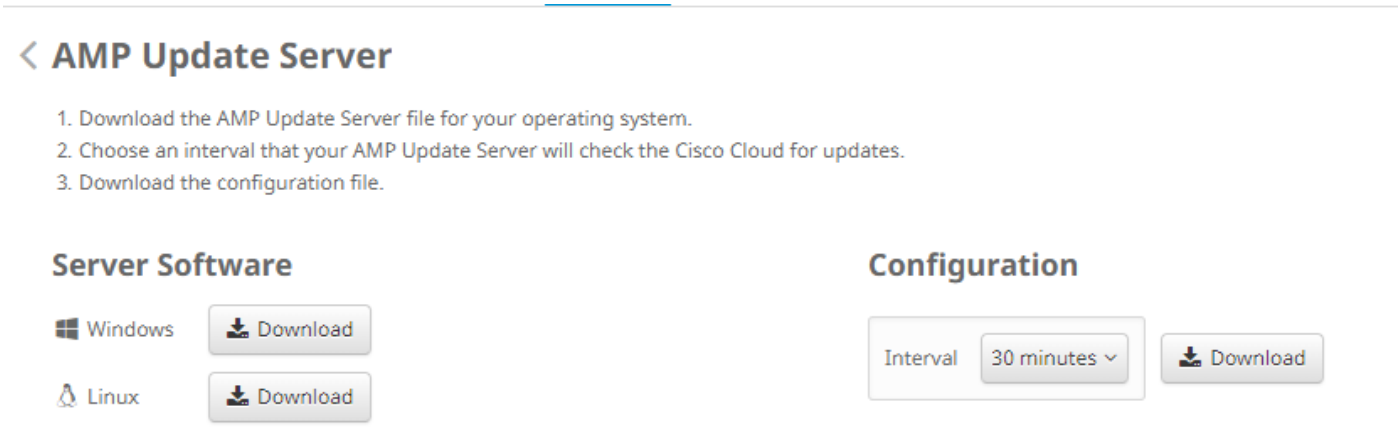
1. Navegue ao gerente (IIS) {sob o gerenciador do servidor | Ferramentas}
2. Expanda a coluna à direita até que o dobrador dos locais aparecer, clicam com o botão direito e seleto *adicionar o Web site.*
3. Nomeie o local como você deseja; Para o caminho físico selecione o dobrador do espelho onde as assinaturas foram transferidas.
4. Os emperramentos podem ser deixados sozinhos; Configurar um hostname separado então o nome do servidor e assegure-se de que os clientes possam resolver isto e você faça uma anotação. Esta é a URL que você configurará na política.
5. Uma vez que configurado; Selecione o local e navegue PARA MIMICAR tipos e para adicionar o seguinte MIMICAR tipos: .gzip, aplicativo/córrego.DAT, aplicativo/córrego.id, aplicativo/córregosig, aplicativo/córrego
6. Navegue ao arquivo web.config (situado no dobrador do espelho) e adicionar as seguintes linhas:

```
<rewrite>
<rules>
<rule name="Rewrite fetch URL">
<match url="^(.*)_[\d]*\/avx\/(.*)$" />
<action type="Redirect" url="{R:1}/avx/{R:2}" appendQueryString="false" />
</rule>
</rules>
</rewrite>
```

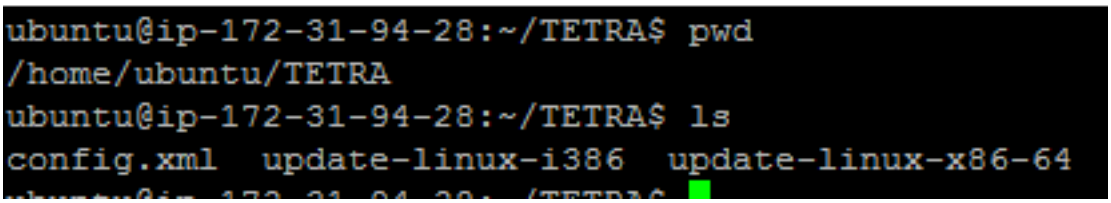
   (A amostra web.config A é anexada igualmente a este artigo.)
7. Configurar a política com a URL configurada em etapa 4. em cima do registro, conectores será utilização -Prem no server para atualizações de assinatura.

Apache

Transfira o software do server e a configuração da atualização AMP diretamente ao server de acolhimento, ou transfira-a localmente e transfira-a então sobre:



Coloque o software do server e o arquivo de configuração no mesmo diretório:



Os script de atualização-Linux precisam de ser executáveis antes que você possa os executar. Mude as permissões de arquivo executando o **update-linux* do chmod +x**. Você usará somente o

script que combina o tipo da arquitetura de server de acolhimento:

```
ubuntu@ip-172-31-94-28:~/TETRA$ chmod +x update-linux-*
ubuntu@ip-172-31-94-28:~/TETRA$ ls -al
total 18468
drwxrwxr-x 2 ubuntu ubuntu     4096 Mar 21 12:22 .
drwxr-xr-x 5 ubuntu ubuntu     4096 Mar 21 12:20 ..
-rw-r--r-- 1 ubuntu ubuntu     1029 Mar 21 12:21 config.xml
-rwxr-xr-x 1 ubuntu ubuntu  8755622 Jan  8 22:33 update-linux-i386
-rwxr-xr-x 1 ubuntu ubuntu 10141387 Jan  8 22:33 update-linux-x86-64
```

Instale Apache. Para o exemplo, Ubuntu 16.04 é usado, assim que o comando é o intsall **apache2 do** sudo apto-**GET - y**:

```
ubuntu@ip-172-31-94-28:~$ sudo apt-get install apache2 -y
```

Isto pode variar segundo sua versão de Linux.

Execute o comando buscar os arquivos TETRA da atualização, **esforço de ./update-linux-x86-64 do sudo --configuração config.xml --espelho /var/www/html/:**

```
ubuntu@ip-172-31-94-28:~/TETRA$ sudo ./update-linux-x86-64 fetch --config config.xml --mirror /var/www/html/
INFO: [update-linux-x86-64] 2018/03/21 12:26:44 Updating 927 entries for the av32bit AV database.
INFO: [update-linux-x86-64] 2018/03/21 12:26:44 Fetching updates.
```

Isto pode variar segundo sua estrutura do diretório.

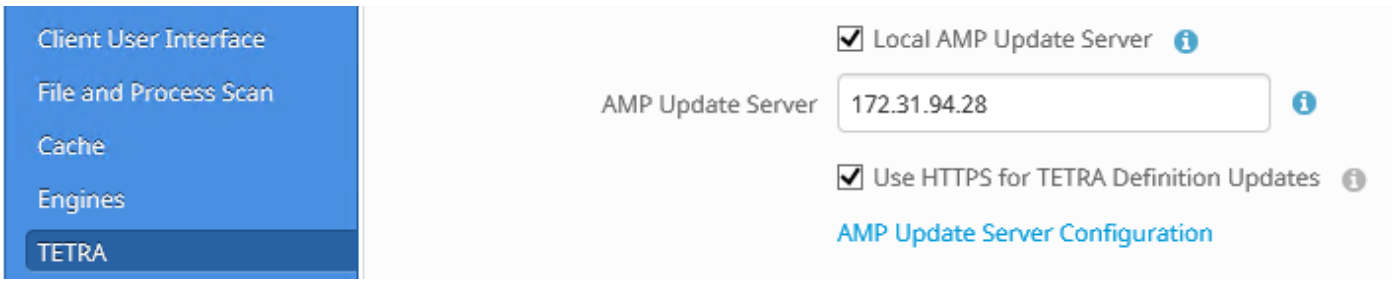
Quando o comando terminou transferir os arquivos e está pronto, segundo seu nível do log você pode ver que uma mensagem que indica o sistema ativando está sendo construída no Server do HTTP:

```
DEBUG: [update-linux-x86-64] 2018/03/21 12:28:05 tetra.go:527: Activating the built-in HTTP server
```

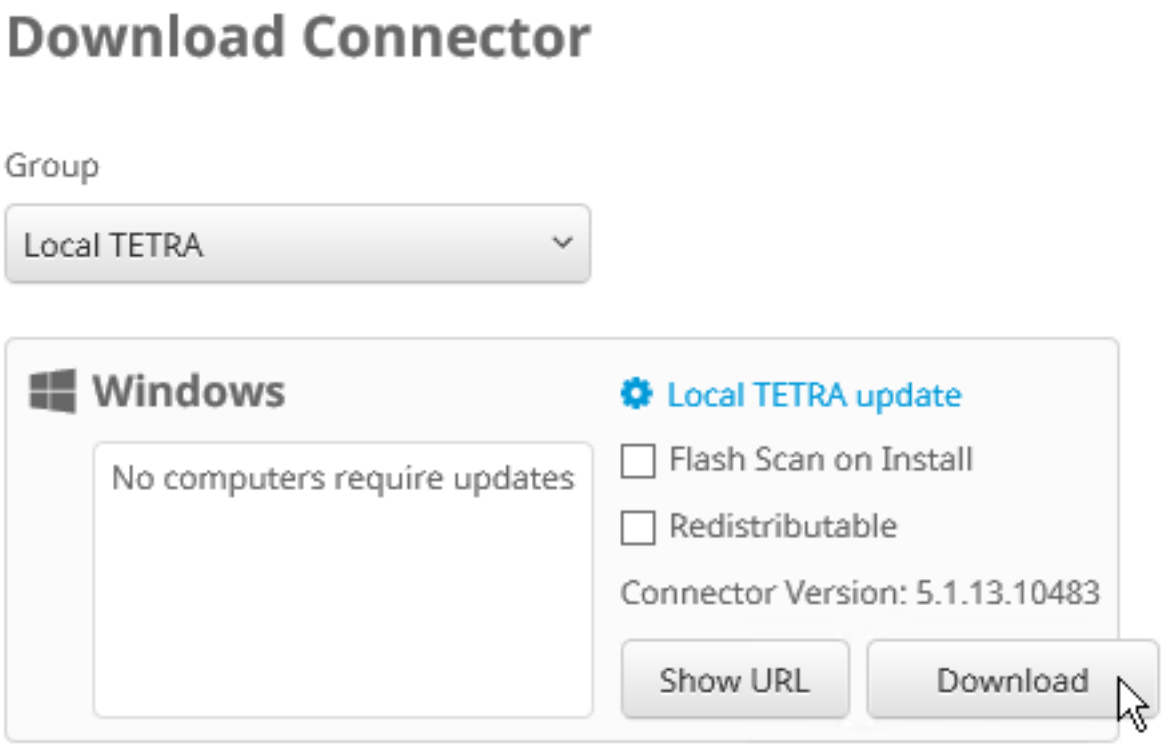
Para verificar o tamanho dos arquivos transferidos para TETRA, você pode executar o comando **du - /var/www/html/ sh**, ou seu caminho de diretório:

```
ubuntu@ip-172-31-94-28:~$ du -sh /var/www/html
756M    /var/www/html
```

Assegure-se de que sua política AMP tenha as opções Server locais da atualização AMP especificadas e se aponte ao server configurado acima. Aponte somente ao IP ou ao hostname, nenhuns sub-diretórios, ou o cliente não poderá conectar corretamente ao server da atualização:



Em seguida, ultrapasse a sua máquina cliente e transfira o conector associado com a política que inclui seu server local da atualização



AMP:

Execute o instalador.

Os arquivos de programa > Cisco > o AMP > tetra > diretório dos **encaixes** serão placa até que uma atualização TETRA da definição esteja puxada do servidor local. Você pode monitorar o server executando o **tail -f /var/log/apache2/access.log** para ver quando é alcançado pelo cliente:

```
ubuntu@ip-172-31-94-28:~$ tail -f /var/log/apache2/access.log
172.31.92.41 - - [21/Mar/2018:13:14:55 +0000] "GET /v2/repository/1/6/F/E/yishield.xmd.16fe55b5f9369afcec02fc0b5db7de86.gzip HTTP/1.1" 200 2220 "-" "WSLib 1.4 [3, 0, 0, 129]"
172.31.92.41 - - [21/Mar/2018:13:14:55 +0000] "GET /v2/repository/5/A/3/9/z.xmd.5a39c18bf0d8f65c4124909f2ba424c9.gzip HTTP/1.1" 200 2143 "-" "WSLib 1.4 [3, 0, 0, 129]"
172.31.92.41 - - [21/Mar/2018:13:14:55 +0000] "GET /v2/repository/5/6/3/3/zip.xmd.5633f8e1149f115fbcb43fc4408a9d8b.gzip HTTP/1.1" 200 65242 "-" "WSLib 1.4 [3, 0, 0, 129]"
172.31.92.41 - - [21/Mar/2018:13:14:55 +0000] "GET /v2/repository/A/0/F/5/zoo.xmd.a0f5c371ecf1c7e0c5d353f29472c706.gzip HTTP/1.1" 200 691 "-" "WSLib 1.4 [3, 0, 0, 129]"
172.31.92.41 - - [21/Mar/2018:13:14:55 +0000] "GET /v2/repository/D/E/C/3/ocra.xmd.dec3926b91784c08bf5701a43a7492c1.gzip HTTP/1.1" 200 9394 "-" "WSLib 1.4 [3, 0, 0, 129]"
172.31.92.41 - - [21/Mar/2018:13:14:55 +0000] "GET /v2/repository/D/C/C/5/pyinstaller.xmd.dcc578a12db0ff08b5e3b71917326c91.gzip HTTP/1.1" 200 8161 "-" "WSLib 1.4 [3, 0, 0, 129]"
172.31.92.41 - - [21/Mar/2018:13:14:55 +0000] "GET /v2/repository/D/8/4/7/vbtok.cvd.d8471c9cc7a11ecbdaa0cd8c3fc03b1d.gzip HTTP/1.1" 200 43077 "-" "WSLib 1.4 [3, 0, 0, 129]"
172.31.92.41 - - [21/Mar/2018:13:14:55 +0000] "GET /v2/repository/F/9/8/7/sysarch.xmd.f987c3a9d4550c1103d234de720575d4.gzip HTTP/1.1" 200 1697 "-" "WSLib 1.4 [3, 0, 0, 129]"
172.31.92.41 - - [21/Mar/2018:13:14:55 +0000] "GET /v2/repository/A/D/2/B/syscan.xmd.ad2b11023df38ecdd94a86c978c4cf6f.gzip HTTP/1.1" 200 4077 "-" "WSLib 1.4 [3, 0, 0, 129]"
172.31.92.41 - - [21/Mar/2018:13:14:55 +0000] "GET /v2/repository/C/4/8/C/bdcore.dll.c48c78076fe757b39e8671bafaaeea96.gzip HTTP/1.1" 200 35246 "-" "WSLib 1.4 [3, 0, 0, 129]"
```

Você pode igualmente verificar os ajustes no cliente nos arquivos de programa > em Cisco > no arquivo AMP > policy.xml:

```
<updater>
  <server>172.31.94.28</server>
  <interval>3600</interval>
  <enable>1</enable>
  <https>1</https>
</updater>
```

Se você selecionou a opção HTTPS para o server local da atualização, assegure-se de que você tenha um válido, certificado confiável em seu server e o tráfego esteja forçado ao HTTPS.

Para automatizar o processo de atualização do server, você pode adicionar um cron job ao server:

```
0 * * * * [Full path to binary]/update-linux-[i386 or x86-64] fetch --once --config [Full path to config]/config.xml - -mirror MIRRORDIR
```

De meu exemplo seria:

```
0 * * * * /home/ubuntu/TETRA/update-linux-x86-64 fetch --once --config /home/ubuntu/TETRA/config.xml --mirror /var/www/html/
```

Se a conexão não estabelece, para verificar **arquivos de programa > Cisco > AMP > 5.1.13 > sfc.exe.log** para ver se há o seguinte mensagem:

```
ERROR: TetraUpdateInterface::update Update failed with error -2100
```

Se você vê este erro, indica que o servidor local é incapaz de ser alcançado. Certifique-se que os arquivos estão hospedados no diretório raiz para apache e não um sub-diretório.

Nginx

As etapas são as mesmas que as etapas da atualização de Apache exceto executar Ngnix, instalado executando o **sudo apto-GET instalam o nginx da** linha de comando. Os arquivos hospedados estão ainda no diretório “/var/www/html/”.

Verificação

Você pode verificar as assinaturas transferidas do server qualquer um esperando até o ciclo seguinte da sincronização ou manualmente suprimindo das assinaturas existentes e então esperando as assinaturas para transferir. O padrão é um intervalo de 1-hora a verificar para ver se há uma atualização.