AMP更新服务器配置步骤

目录

简介

本文档介绍思科高级恶意软件防护(AMP)TETRA更新服务器的详细配置步骤。

预请求

- 了解Windows 2012R2或CentOS 6.9 x86_64等服务器主机。
- 对托管软件(如IIS（仅限Windows）、Apache、Nginx)的知识
- 已配置服务器主机，已启用HTTPS，且已安装有效的受信任证书。
- 已配置HTTPS本地更新服务器选项。

注意：有关启用本地更新服务器配置和要求的完整详细信息，请参阅此处提供的《面向终端的AMP用户指南》第25[章](#)。
(https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf)

注意：服务器主机(IIS、Apache、Nginx)是第三方产品，思科不支持这些产品，请向支持团队咨询各自产品，以了解所提供步骤之外的问题。

警告：如果AMP配置了代理服务器，所有更新流量（包括TETRA）将继续通过代理服务器发送，并定向到本地服务器。确保允许流量在传输过程中通过代理而不进行任何修改。

安装步骤

所有平台

1. 确认托管服务器操作系统(OS)。
2. 确认面向终端的AMP控制面板门户，下载更新程序软件包和配置文件。

面向终端的AMP控制台：

美国- https://console.amp.cisco.com/tetra_update

欧盟- https://console.eu.amp.cisco.com/tetra_update

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

Windows IIS

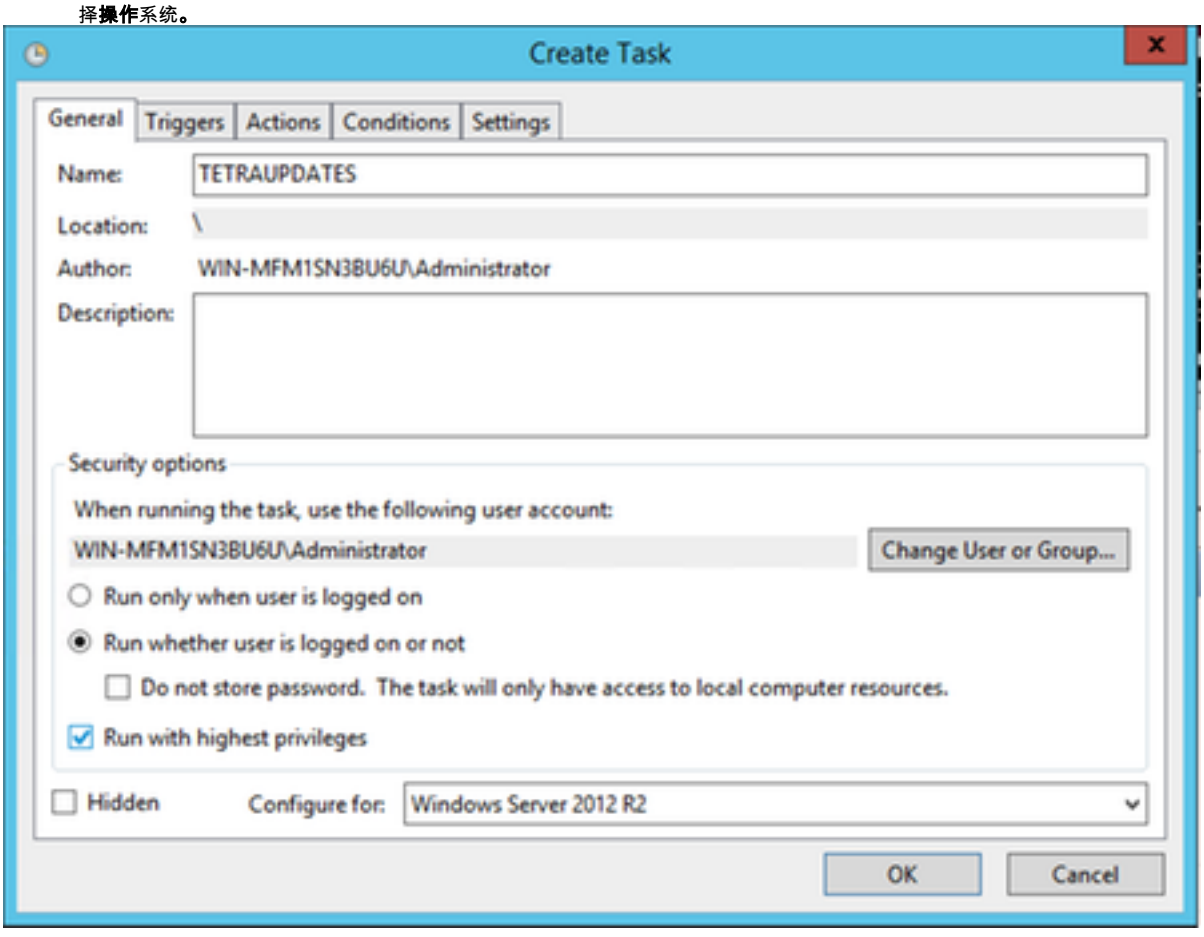
> **注意**：以下步骤基于新的IIS应用程序池来托管签名，而不是**默认**的应用程序池。要使用默认池，请在提供的步**骤中更**改 — mirror文件夹，以反映默认Web托管路径(**C:\inetpub\wwwroot**)

目录创建

1. 在根驱动器上创建新文件夹，将其命**名为TETRA**。
2. 将压缩的AMP更新程序软件包和配置文件复制到所**创建的**TETRA文件夹。
3. 解压缩此文件夹中的软件包。
4. 在TETRA文件夹内创建名**为Signatures**的新文件夹。

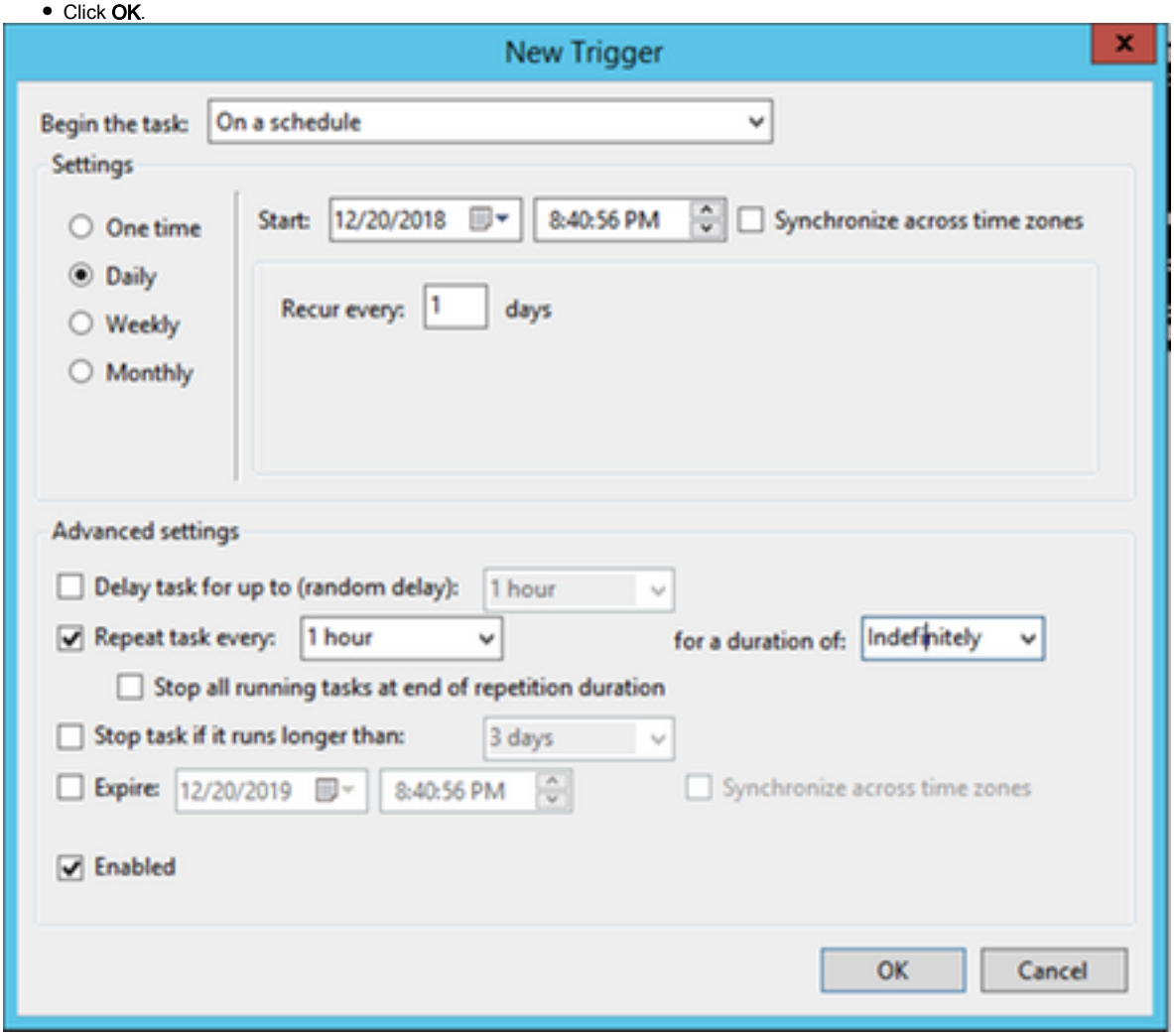
更新任务创建

1. 打开命令行并导航至C:\TETRA文*件夹.**cd C:\TETRA***
2. 运行命**令*update-win-x86-64.exe fetch —config="C:\TETRA\config.xml" —once —mirror C:\TETRA\Signatures***
3. 打开任务计划程序并创建新任务。（操作>创建任务），以在需要时使用以下选项自动运行更新程序软件：
4. 选择General选项卡。 输入任务的名称。选择**Run when user is logged or not.(运行用户是否登录。**)选择"**使用最高权限运行"。**从"配**置"下**拉菜单中选择**操作**系统**。**



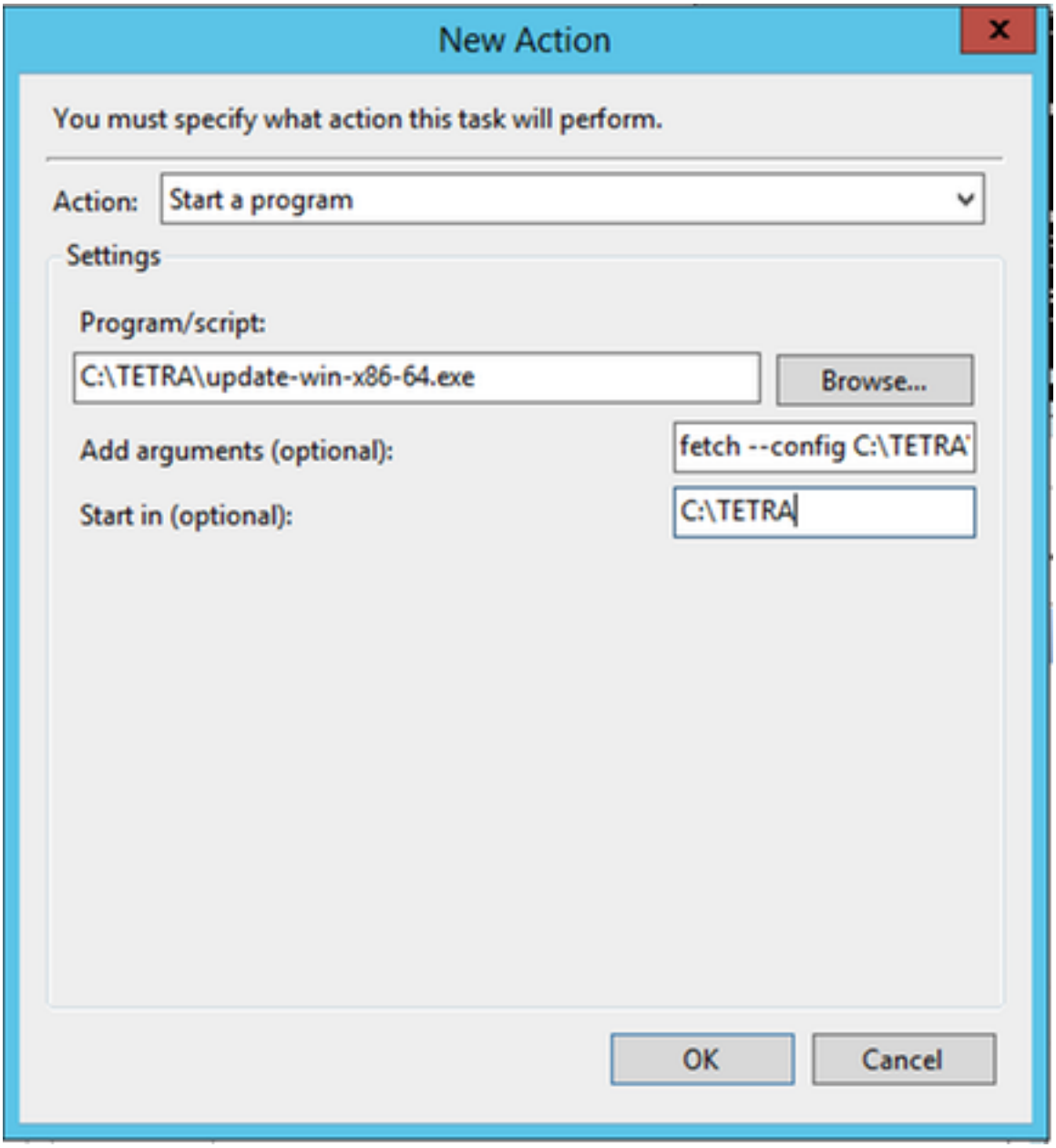
5.选择“触发器”选项卡。

- 单击 New。
- 从“**开始任务**”下**拉菜单中选择**计划。
- 在“设置**”下**选择“每日”。
- 选**中Repeat task every ,然后从下拉**菜单中选择**1 hour ，然后从“Indentible** ”中选择**Indentively** :
- 验证是否**选中**了“**Enabled”**。
- Click **OK**.



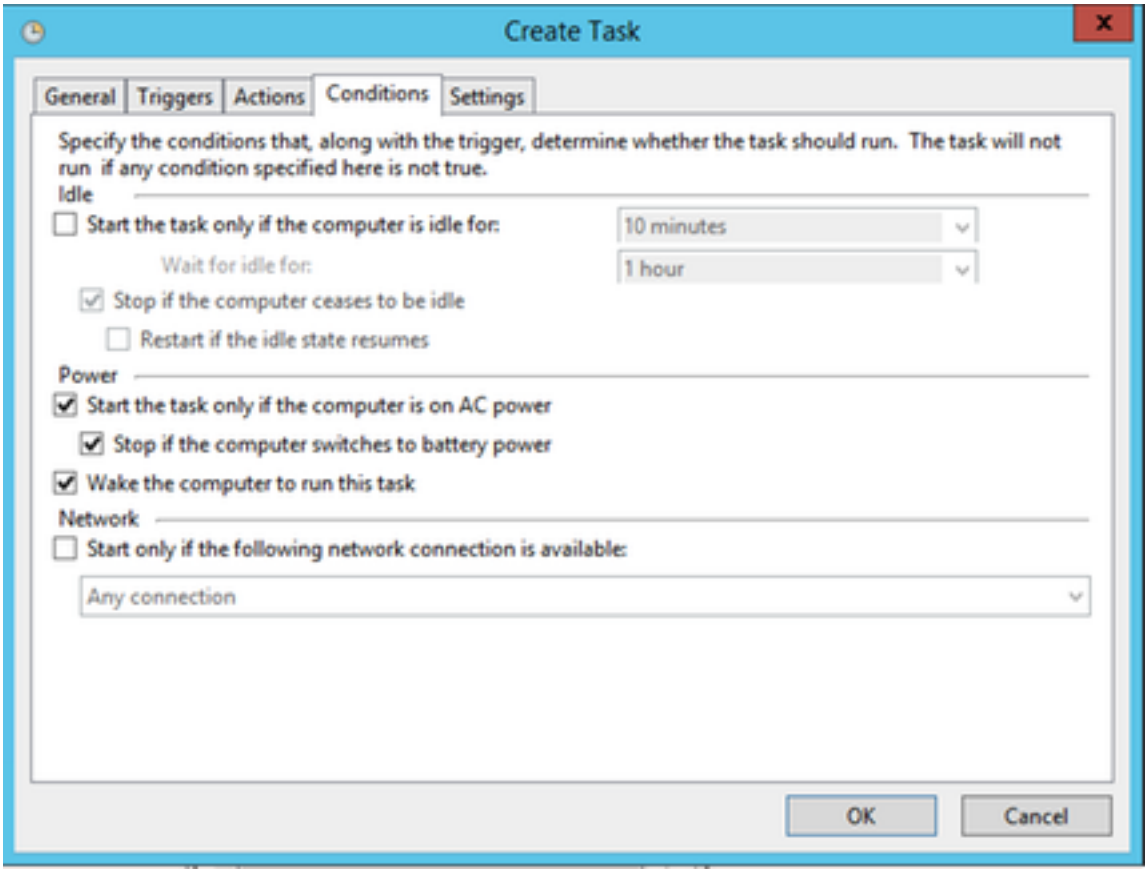
6.选择“操作”选项卡

- 单击 **New**。
- 从“**操作”下**拉菜单中选择**“启**动程序”。
- 在“***Program/***script”字**段中输入**C:\TETRA\update-win-x86-64.exe。
- 在“添***加参数”(Add arguments)字段中输***入fetch —config C:\TETRA\config.xml **—once —mirror** C:\TETRA\Signatures。
- 在“开***始位***置”字**段中**输入C:\TETRA
- 单击 **OK**



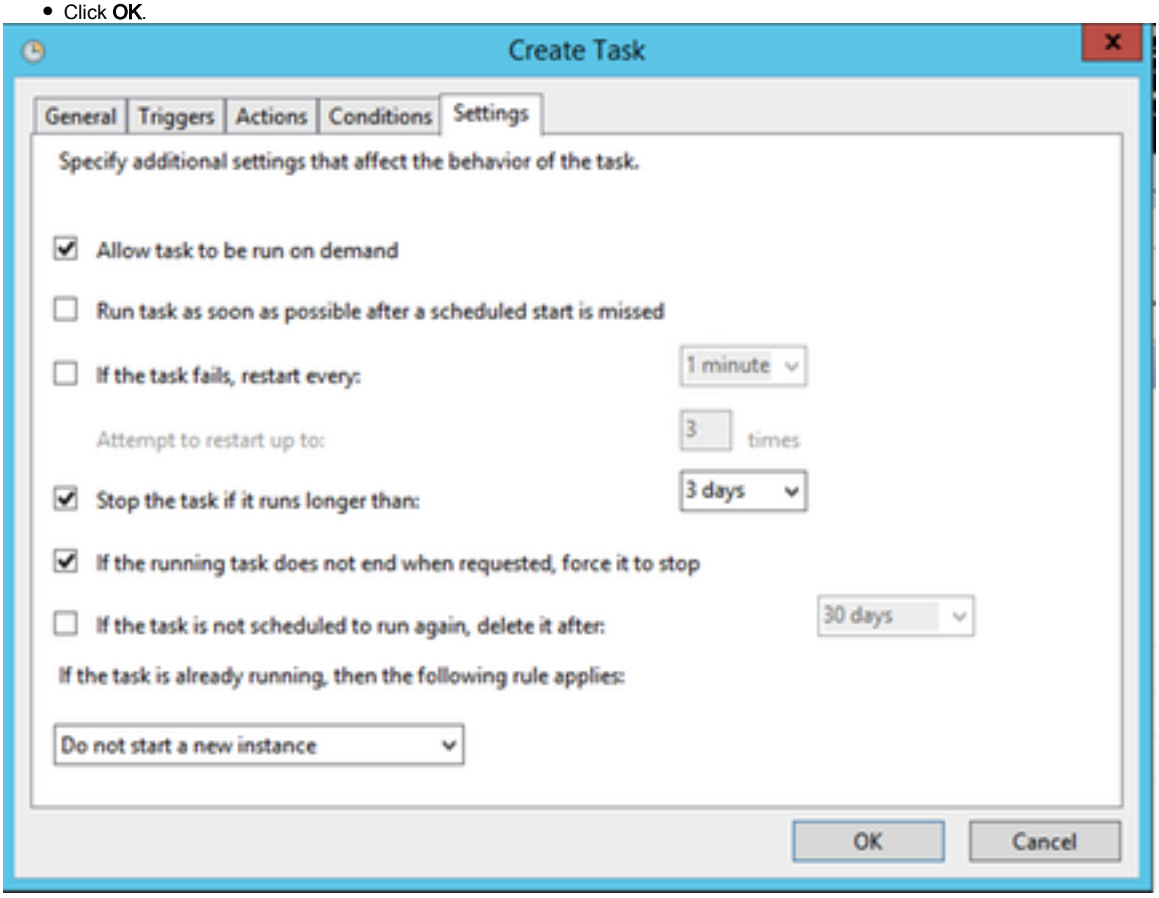
7. [*可选*]*选*择“条件”选项卡。

选中唤醒计算机以运行此任务选项。



8选择“设置”选项卡。

- 验证是否**在“如果任务已**在运行，*则*不启动新实例”下选中。
- Click **OK**.



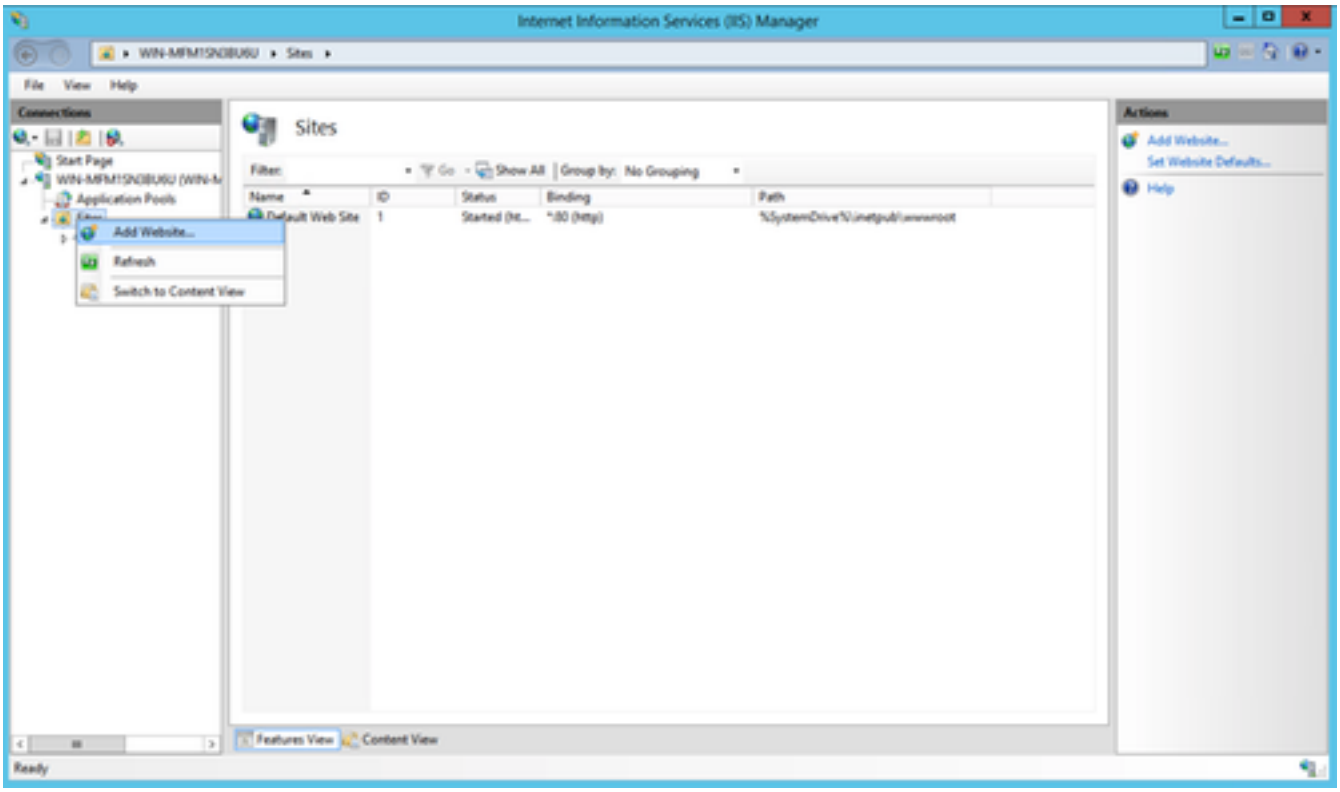
9.输入将运行任**务的帐户的凭据。**

IIS管理器配置

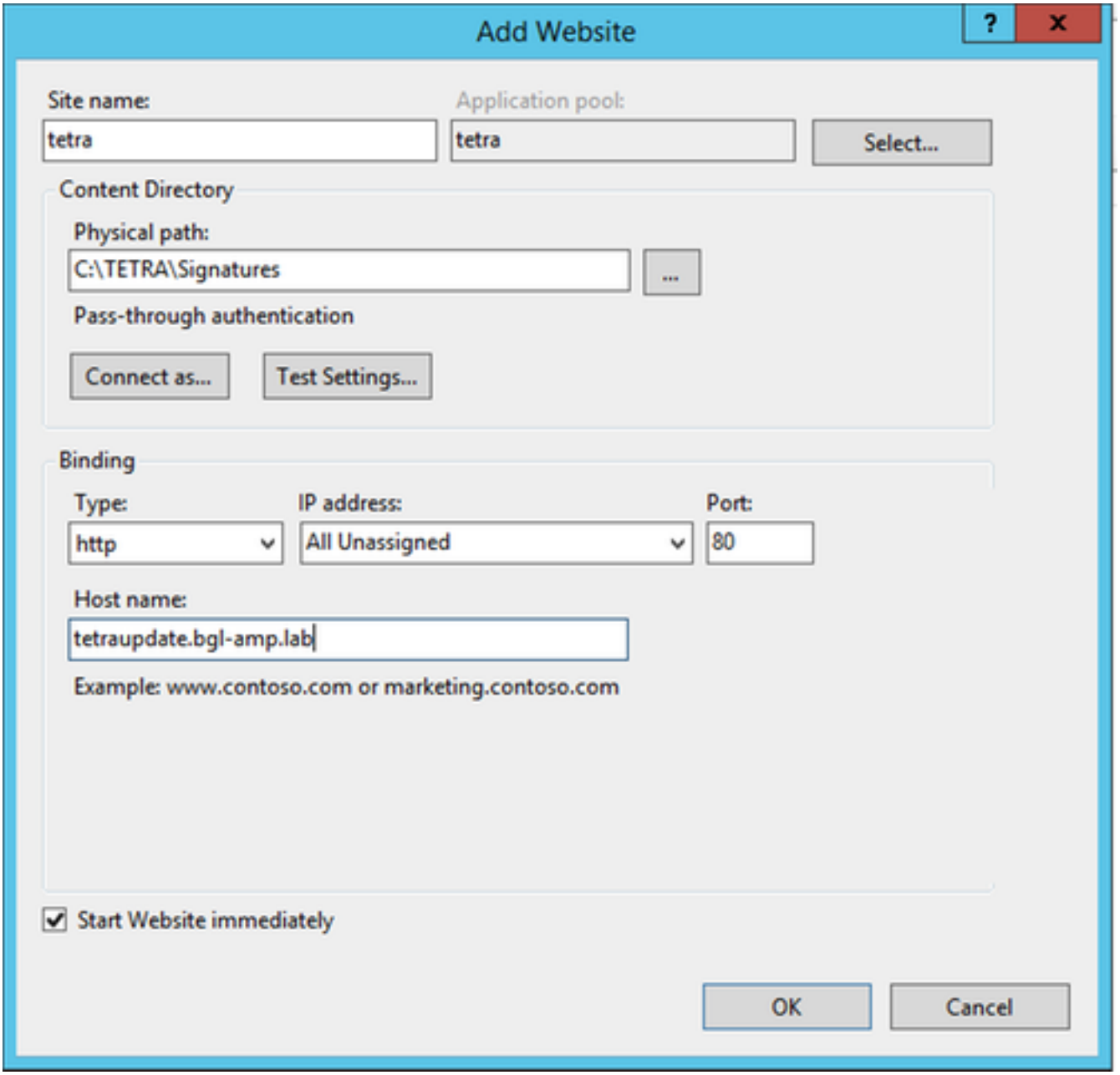
注意：配置默认应用池时，跳至步骤5。

1.导航至(IIS)管理器(在“服务器管**理器”>“工具”下**)

2.展开右侧列，直到显示“站点”**文件夹**，然后**右键单击并选择“添加网站”**。



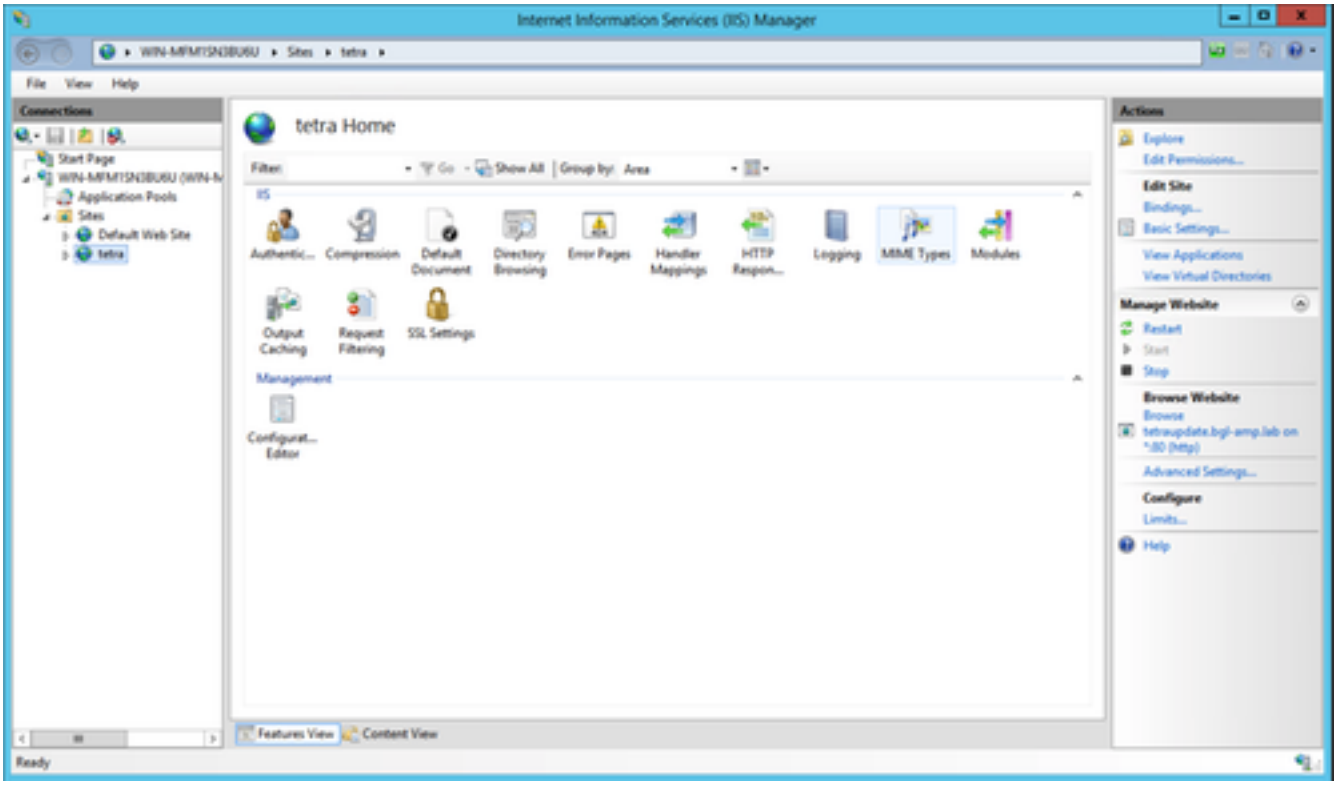
3.选择选择的名称。对于物理路径，选择***下载签名***的C:\TETRA\Signatures文件夹。



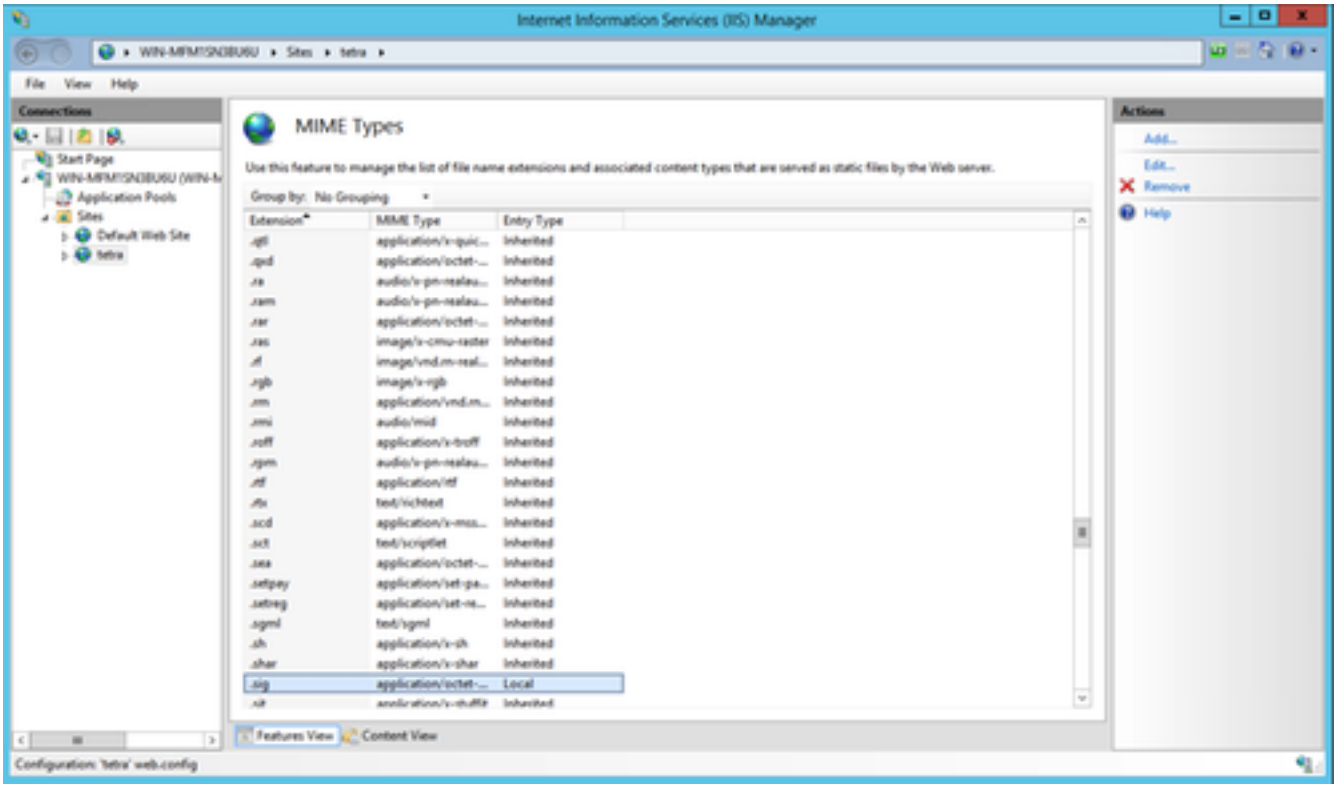
4.单独保留绑定。配**置单独的主机名**和服务器名称，所选名称必须可由客户端解析。这是您将在策略中配置的URL。

5.选择站点并导航到MIME**类型**并添**加以下MIME类型**:

- .gzip，应用/二进制八位数流
- .dat，应用/二进制八位数流
- .id，应用/二进制八位数流
- .sig，应用/二进制八位数流



6.导航至**web.config文**件（位于镜像文件夹中），将以下行添加到文件顶部。



完成后，在文*本编辑器*中查看时，C:\TETRA\Signatures\web.config文件内容将显示为这样。（语法和间距需要与提供的示例保持相同。）

注意：面向终端的AMP连接器要求服务器HTTP报头在响应中存在，以便正确操作。如果服务器HTTP报头已禁用，则Web服务器可能需要在下面指定的其他配置。

必须安装url-rewrite扩展。在/[MIRROR_DIRECTORY]/web.config的服务器配置中添加以下XML代码段：

```
<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>
```

注意：使用文本编辑器或IIS管理器使用URL重写模块手动执行此更改。可以从以下URL(https://www.iis.net/downloads/microsoft/url-rewrite)安装重写模块。

完成后，在文本*编辑器*中查看时，C:\TETRA\Signatures\web.config文件内容将显示为这样。（语法和间距需要与提供的示例保持相同。）

阿帕奇/恩吉克斯

注意：提供的步骤假定您正在从Web托管软件的默认目录中提供签名。

1. *TETRA*
2.
3. ***Chmod +x update-linux****
4. 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.cron

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

6.

1. “”(Advanced Settings)>“TETRA”(TETRA)“”(Update Server): AMPIP<hostname.domain.root>IP

警告：请勿在之前或之后包含任何协议子目录，否则，在下载时将导致错误。

[]**HTTPSTETRA**HTTPS

导航至C:\inetpub\wwwroot\、C:\TETRA\Signature或/var/www/html目录，并验证更新的签名是否可见，通过等待到下一个同步周期或手动删除现有签名，然后等待签名下载，签名从服务器下载到最终客户端。默认为1小时间隔，用于检查更新。

相关信息

- 技术支持和文档 - Cisco Systems
- 面向终端的思科AMP — 技术说明
- 面向终端的思科AMP — 用户指南

。