[External] - AMP更新服务器配置步骤

Contents

Introduction

本文描述Cisco的详细配置步骤提前Malware保护(AMP)四更新服务器。

Prerequistes

- 服务器主机例如， Windows 2012R2或CentOS知识6.9 x86_64。
- 做主机软件知识例如， IIS (仅Windows)， Apache， Nginx
- 有HTTPS功能的被配置的服务器主机，安装的有效信任证书。
- 被配置的HTTPS本地更新服务器选项。

Note:关于全面的详细信息到启用本地更新服务器配置和需求里，请参见AMP终端用户指南的第25章，可用这里。
(https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf)

Note:Nginx)是第三方产品和Cisco不支持服务器主机(IIS， Apache，请参见各自的产品的支持小组问题的提供的步骤的外部。

警告：如果AMP配置有代理服务器，所有更新数据流(包括四)将继续通过代理服务器被发送，处理对您的当地服务器。保证数据流提供通过代理，不用任何修改在运送中。

安装步骤

所有平台

1. 确认您的主服务器操作系统(OS)。
2. 确认您的终端显示板门户的AMP，下载更新软件包和配置文件。

终端显示板门户的AMP ：

美国- 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

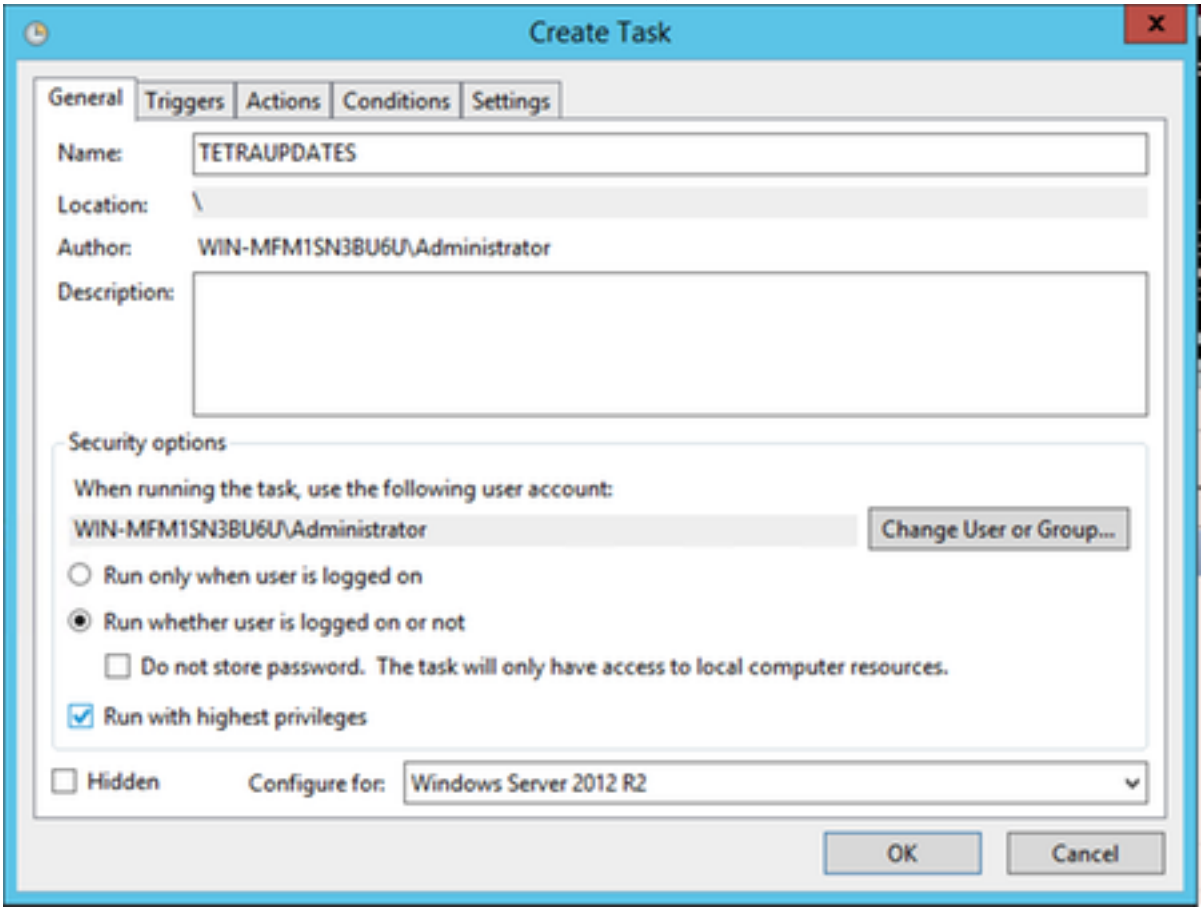
> **Note**:下面的步骤没有根据新的IIS应用程序池主机签名，**没有**默认应用池。要使用默认池，请更改 **--反映**在提供的步骤的文件夹反射默认Web托管路径(**C:\inetpub\wwwroot**)

目录创建

1. 创建在根驱动的一新文件夹，命名它**四**。
2. 复制压缩的AMP更新软件包和配置文件到被创建的**四**文件夹。
3. 解在此文件夹的软件包压缩。
4. 创建称为**Signatures的**一新文件夹在四文件夹里面。

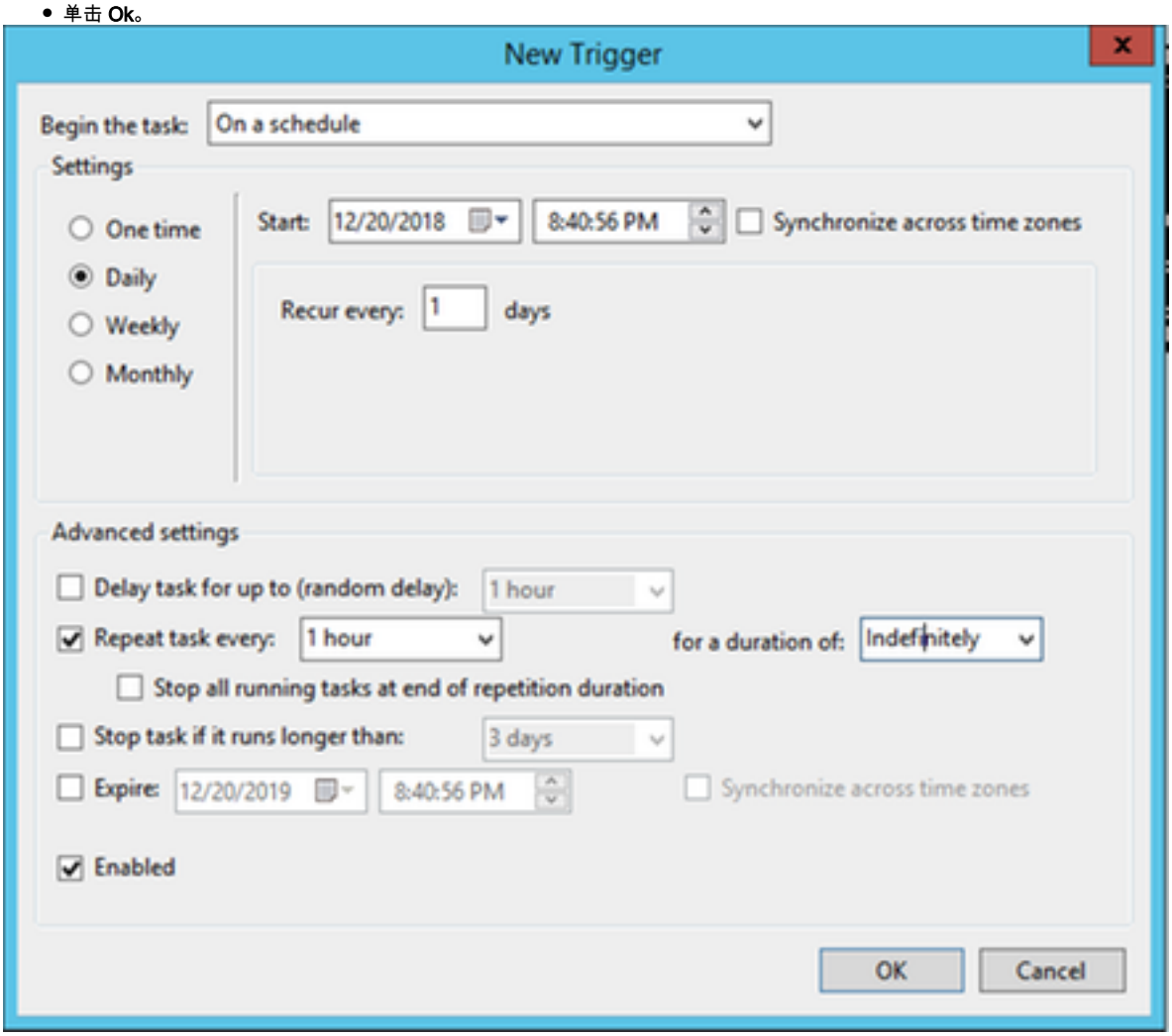
更新任务创建

1. 打开line命令并且连接对*C:\TETRA* folder.cd ***C:\TETRA***
2. 运行命令***update-win-x86-64.exe取指令--config= " C:\TETRA\config.xml"--一旦--镜像C:\TETRA\Signatures***
3. 打开任务管理器并且创建新任务。(动作>创建任务)自动地运行更新软件以以下选项哪里需要：
4. 选择一般选项。 输入一个名字对于任务。选择**运行是否用户被注册**。选择**运行有最高的权限。**选择**操作系统**从**配置**丢弃下来。



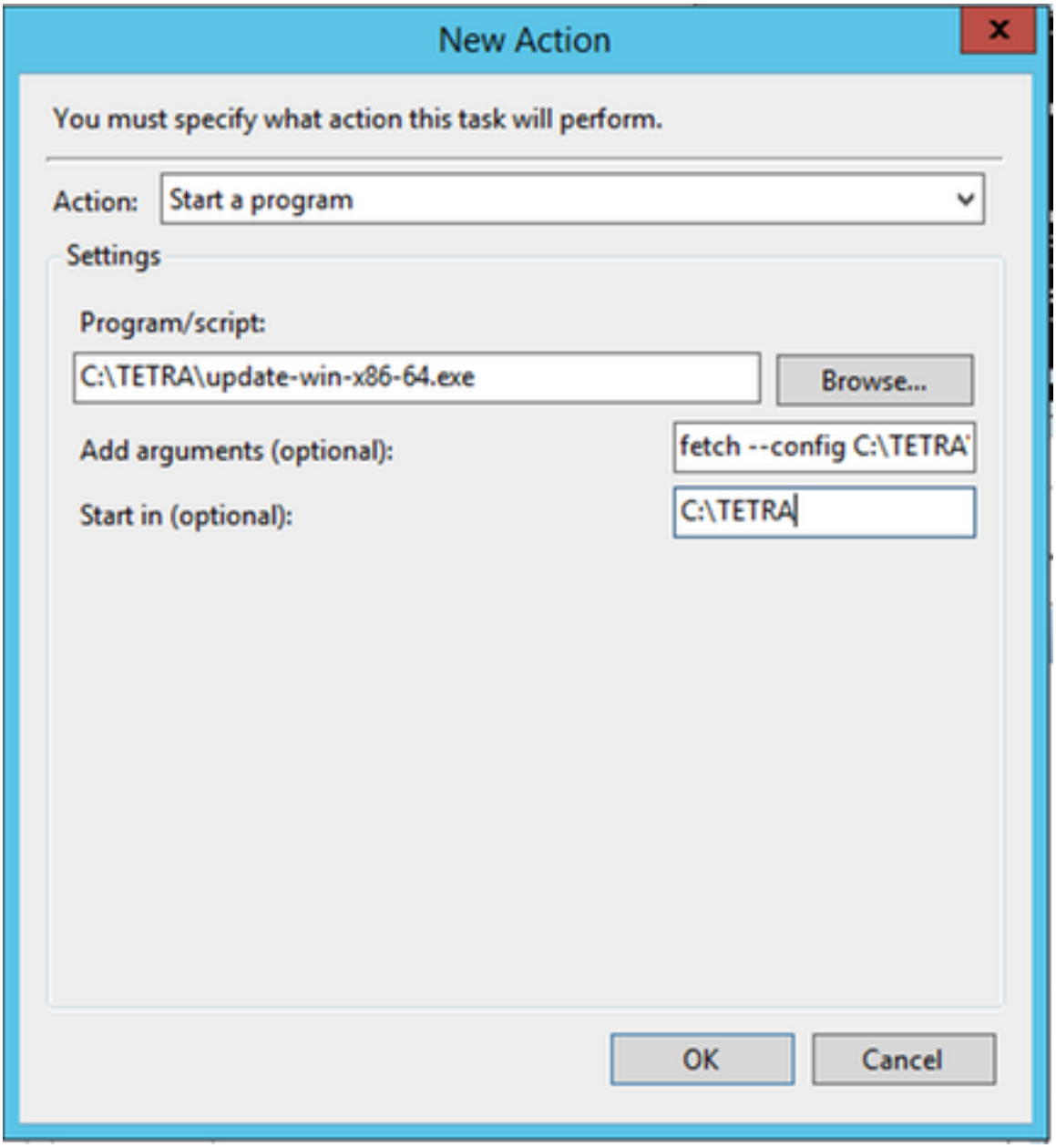
5. 选择触发器选项。

- 点击 **New（新建）**。
- 选择**在日程表**从**任务**下降下来的**开始**。
- **每日选择在设置下。**
- 检查**每重复的任务**并且**选择1小时**从丢弃下来并且**无限地**选择从“**期限的：**”
- 验证**启用了被检查**。
- 单击 **Ok**。



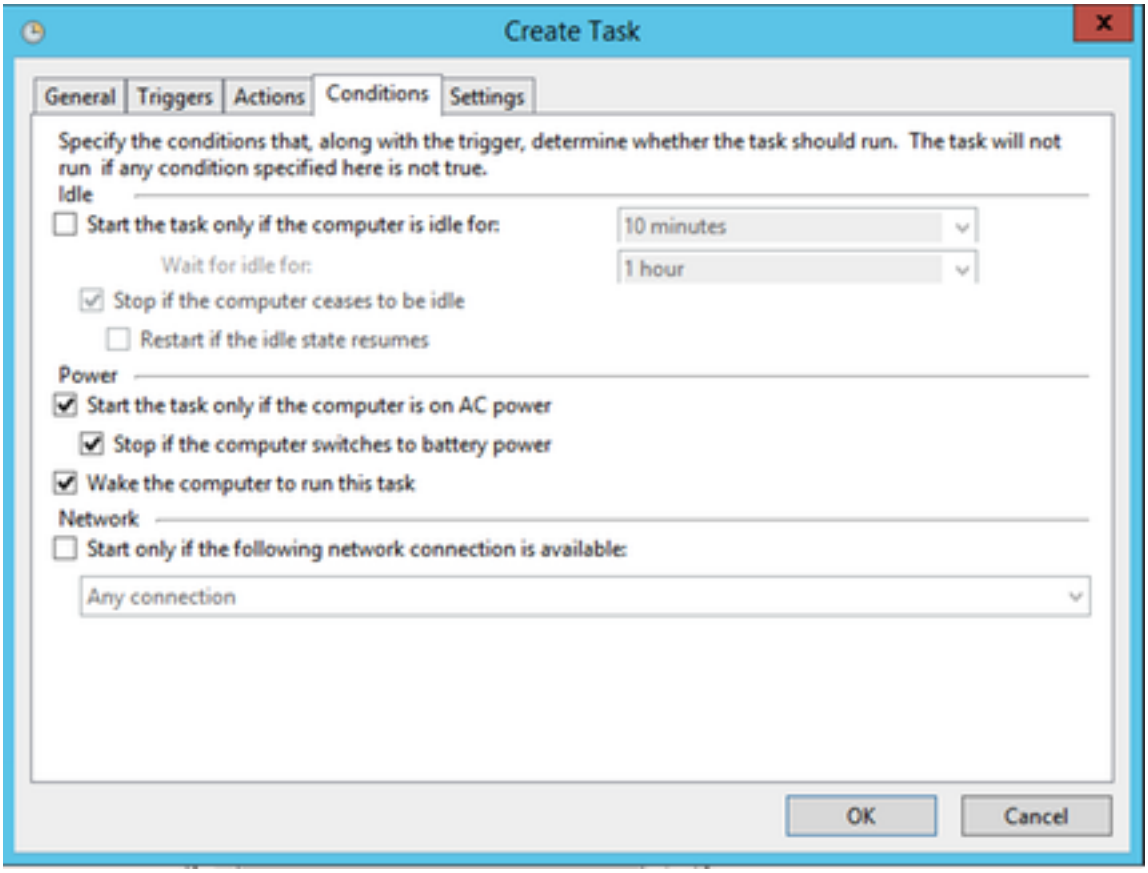
6. 选择动作选项

- 点击 **New（新建）**。
- 选择**开始程序**从**动作**丢弃下来。
- 输入*C:\TETRA\update-win-x86-64.exe*在**程序/脚本**字段。
- 输入***取指令--设置****C:\TETRA\config.xml--一旦--*在**添加参数**字段的**镜像***C:\TETRA\Signatures*。
- 送进*C:\TETRA*在字段的**开始**
- 单击 **OK**



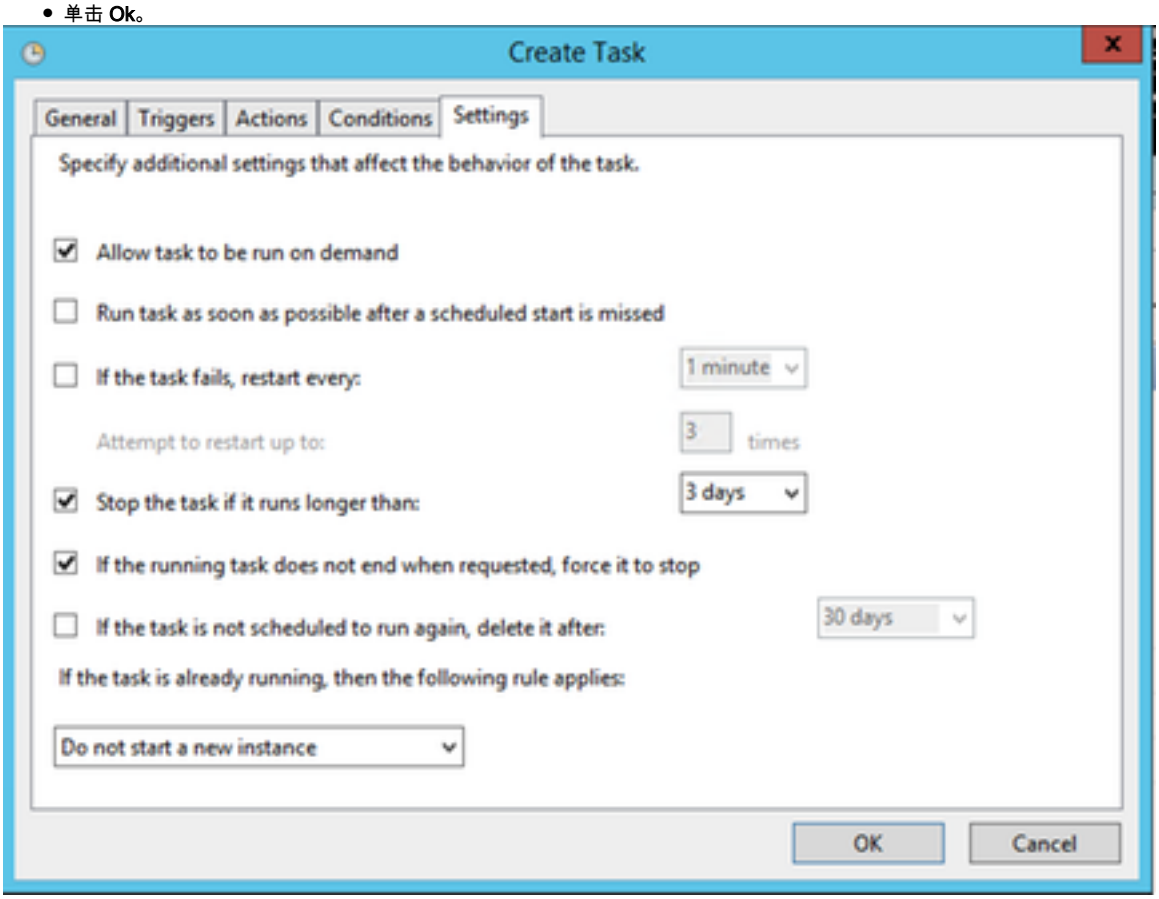
7. *[Optional]*选择情况选项。

检查苏醒计算机运行此任务选项。



8请选择Settings选项。

- 验证不**开始一个新的实例**选择得下，**如果任务已经运行。**
- 单击 **Ok**。



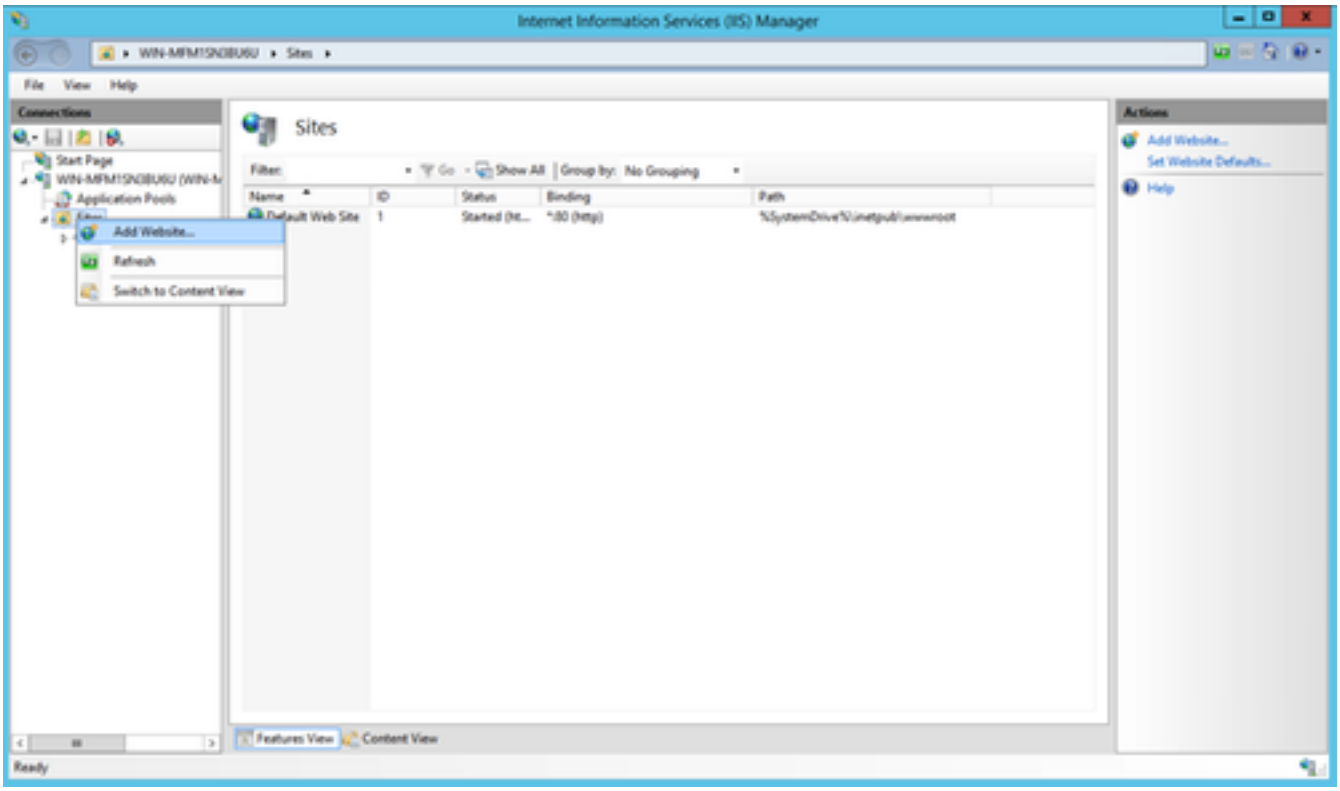
9. 进入**将运行任务的帐户的**证件。

IIS管理器配置

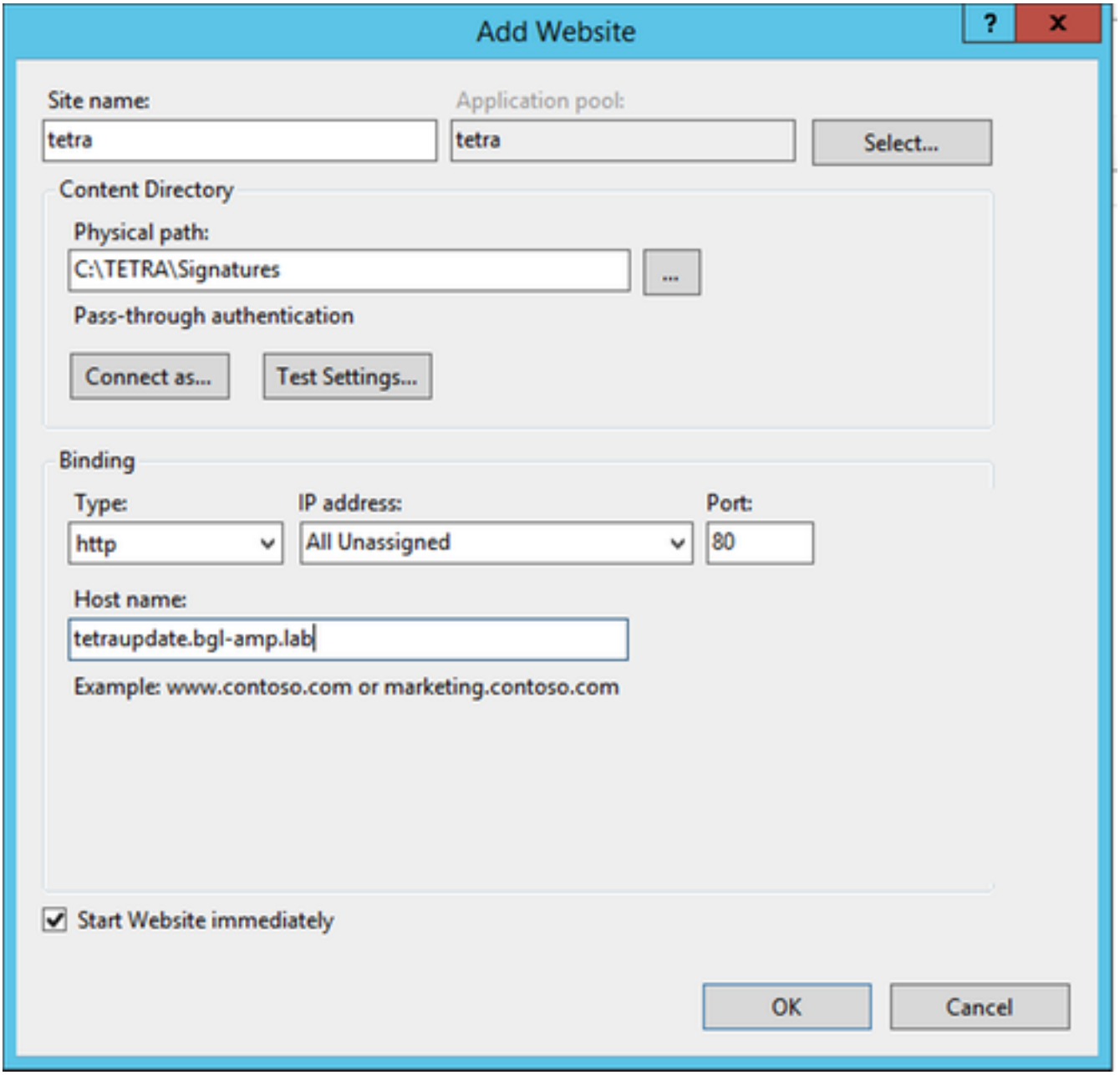
Note:当配置时，请跳到第5步默认应用池。

1. 连接给(IIS)管理器(**在服务器管理器>工具下**)

2. 请扩展右侧列，直到**站点文件夹**是可视的，**用鼠标右键单击并且选择添加网站。**



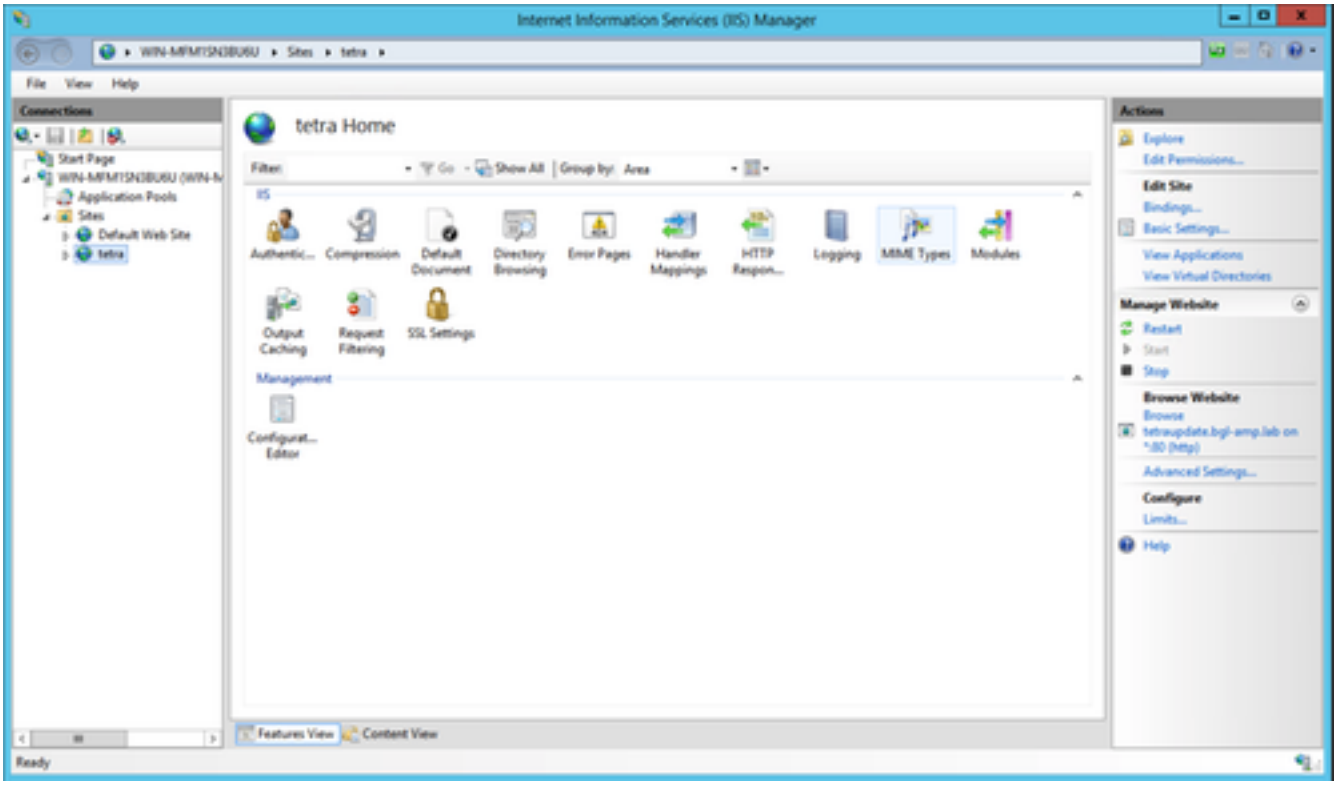
3. 选择选择的名字。对于物理路径请选择下载签名的*C:\TETRA\Signatures*文件夹。



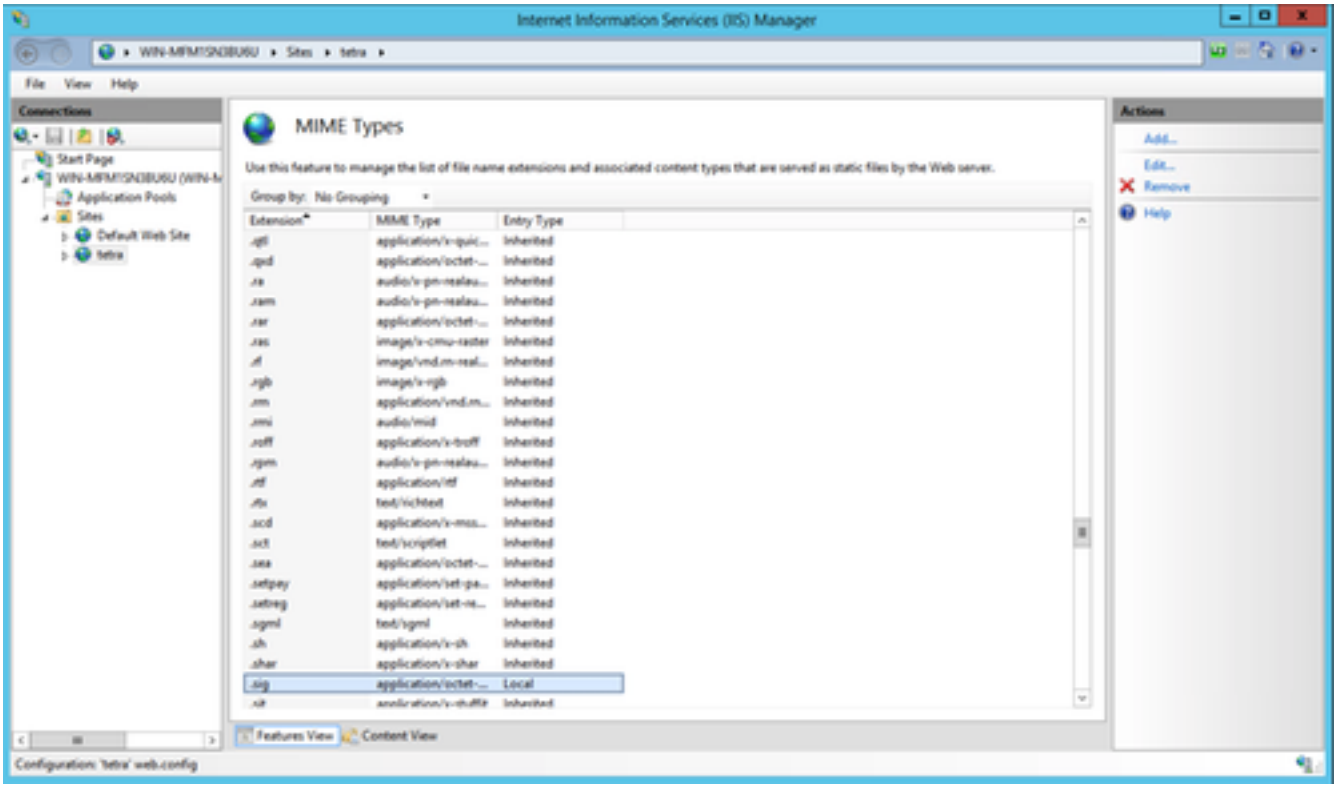
4. 不理会捆绑。 **配置一个分开的主机名-，**并且服务器名，选择的名字一定是可溶解的由客户端。这是您在策略将配置的URL。

5. 选择站点并且连接对**MIME类型**并且**添加以下MIME类型**：

- .gzip，应用程序/八位位组流
- .dat，应用程序/八位位组流
- .id，应用程序/八位位组流
- .sig，应用程序/八位位组流



6. 连接对**web.config文件**(位于镜像文件夹)，在文件的顶层添加以下线路。



遵从步骤在**策略配置下**为了配置您的策略使用更新服务器。

> **Note**: 手工此更改与文本编辑或与通过使用URL重写模块的IIS管理器。重写模块可以从以下URL (https://www.iis.net/downloads/microsoft/url-rewrite)安装

当完成时*C:\TETRA\Signatures\web.config*文件目录在文本编辑将出现象这样，当查看。(语法和间距需要保持同提供的示例一样。)

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
    <system.webServer>
<directoryBrowse enabled="true" showFlags="Extension" />
<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>
        <staticContent>
            <mimeMap fileExtension="." mimeType="applicaton/octet-stream" />
            <mimeMap fileExtension=".gzip" mimeType="applicaton/octet-stream" />
            <mimeMap fileExtension=".dat" mimeType="application/octet-stream" />
            <mimeMap fileExtension=".id" mimeType="application/octet-stream" />
            <mimeMap fileExtension=".sig" mimeType="application/octet-stream" />
        </staticContent>
    </system.webServer>
</configuration>
```

Apache/Nginx

Note:提供的步骤假设您服务签名从Web托管软件的默认目录。

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

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. **>** AMP-IP<hostname.domain.root>IP

警告：请勿包括任何协议前面否则在否则以后的所有子目录，这将导致错误，当下载时。

*[Optional]***DefinitinHTTPS** HTTPS

连接对C:\inetpub\wwwroot\、C:\TETRA\Signature或者/var/www/html目录并且验证更新的签名是可视的，签名从服务器下载到末端客户端由等待直到下个同步循环或手工删除现有的签名然后等待签名的二者之一下载。默认值是检查的1小时间隔更新。

Related Information

- Technical Support & Documentation - Cisco Systems
- 终端的Cisco AMP - TechNotes
- 终端的Cisco AMP -用户指南

.o