AMPアップデートサーバの設定手順

内容

概要

このドキュメントでは、Cisco Advanced Malware Protection(AMP)TETRAアップデートサーバの詳細な設定手順について説明します。

前提条件

- Windows 2012R2やCentOS 6.9 x86_64などのサーバホストに関する知識。
- IIS（Windowsのみ）、Apache、Nginxなどのホスティングソフトウェアに関する知識
- HTTPSが有効で、有効な信頼できる証明書がインストールされた設定済みのサーバホスト。
- HTTPS Local Update Serverオプションを設定しました。

注：Local Update Serverの設定と要件の有効化の詳細については、『AMP for Endpoints User Guide』の第25章を参照してくださ[い](#)。(https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf)

注：サーバホスト(IIS、Apache、Nginx)はサードパーティ製品であり、シスコではサポートされていません。提供されている手順の範囲外の質問については、各製品のサポートチームを参照してください。

警告：AMPがプロキシサーバで設定されている場合、すべての更新トラフィック（TETRAを含む）は、引き続きプロキシサーバを経由してローカルサーバに送信されます。転送中にトラフィックが変更されずにプロキシを通過できることを確認します。

インストール手順

すべてのプラットフォーム

1. ホスティングサーバーオペレーティングシステム(OS)を確認します。
2. AMP for Endpointsダッシュボードポータルを確認し、Updater Software Packageと設定ファイルをダウンロードします。

AMP for Endpointsコンソール：

米国- 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

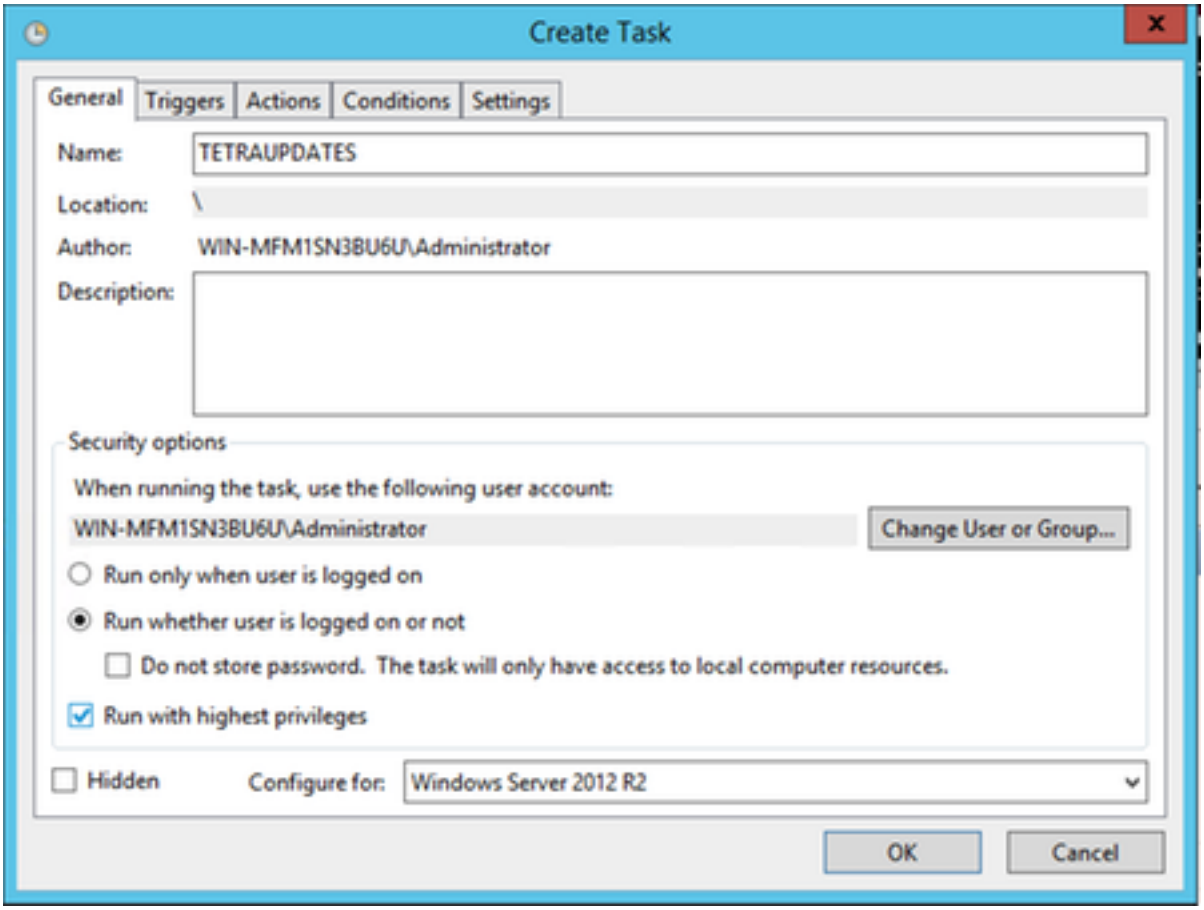
> **注：**次の手順は、シグニチャをホストする新しいIISアプリケーションプールに基づいており、デフォルトのアプリケーション**プール**に基づいていません。デフォルトのプールを使用するには、次の手順で**—mirrorフォルダ**を変更し、デフォルトのWebホスティングパス(**C:\inetpub\wwwroot**)を反映します

ディレクトリの作成

1. ルートドライブに新しいフォルダを作成し、TETRAという名前**を付けます**。
2. zip圧縮されたAMPアップデータソフトウェアパッケージと構成ファイルを、作成されたTETRAフォ**ルダにコ**ピーします。
3. このフォルダのソフトウェアパッケージを解凍します。
4. TETRAフォルダ内にSignaturesという新**しいフォ**ルダを作成します。

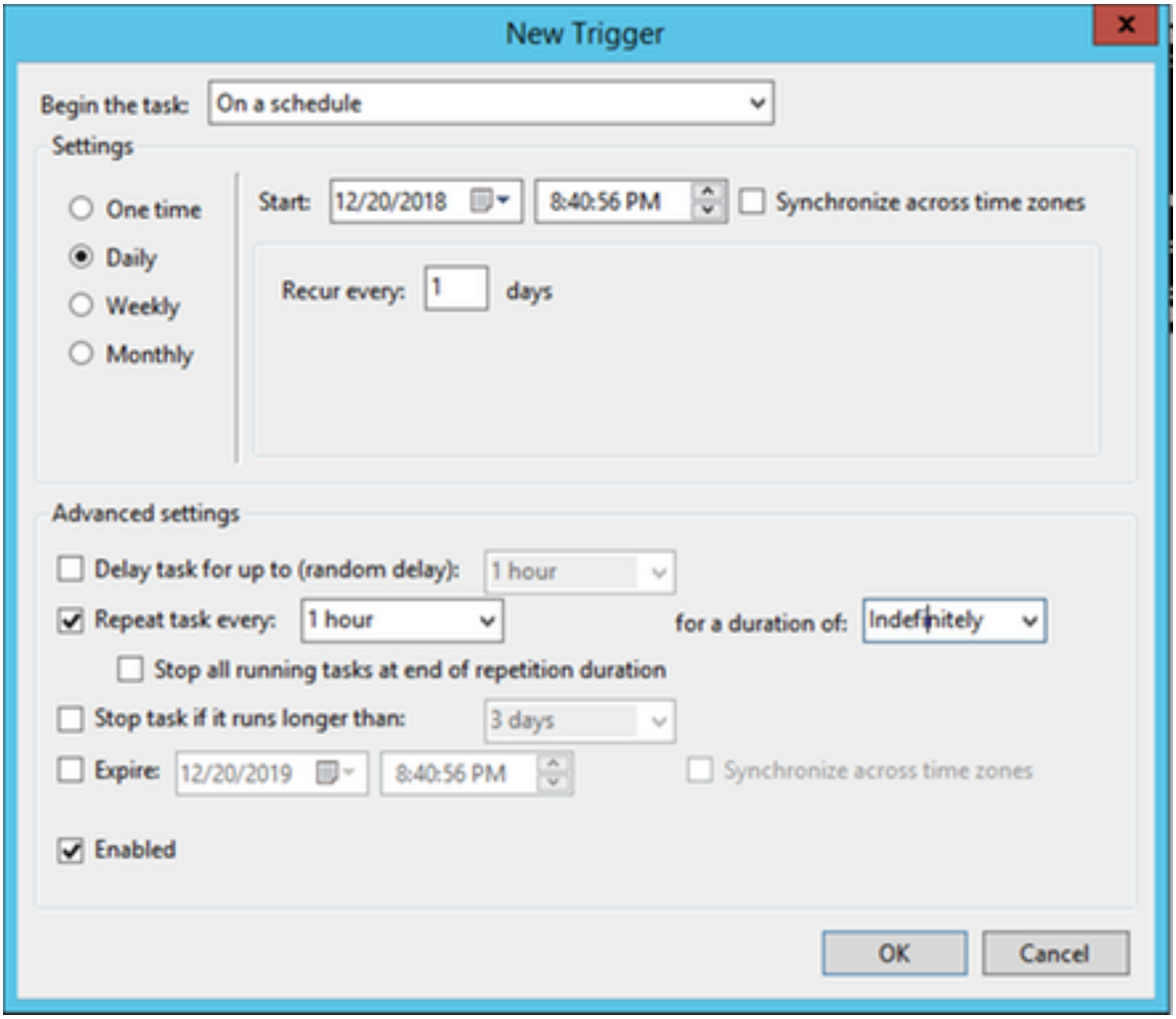
更新タスクの作成

1. コマンドラインを開き、*C:\TETRA*フォルダ.***cd C:\TETRAに移動します***
2. ***update-win-x86-64.exe fetch —config="C:\TETRA\config.xml" —once —mirror C:\TETRA\Signaturesコマンドを実行します***
3. タスクスケジューラを開き、新しいタスクを作成します。([アクション(Action)] > [タスクの作成(Create Task)])を選択して、必要に応じて次のオプションを使用してアップデータソフトウェアを自動的に実行します。
4. [General]タブを選択します。 タスクの名前を入力します。[ユーザー***がログオンしているかどうかを実行]を選択します。「最高の権限で実行」を選択します。***[構成]ド**ロップダウン**ダウンからオペレーティ**ングシステ**ムを選択します**。**



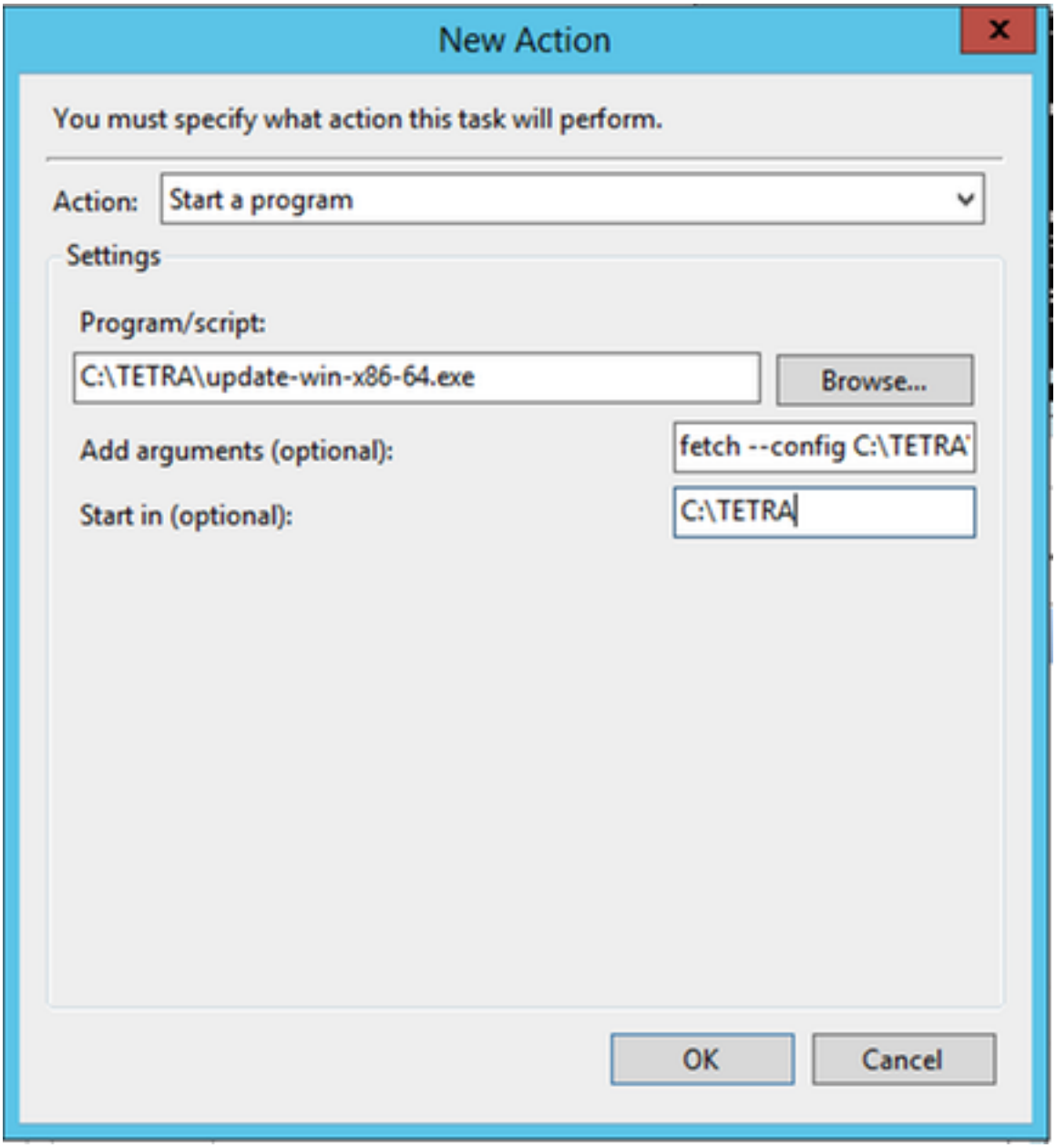
5. 「トリガー」タブを選択します。

- [New] をクリックします。
- [タスクの開始]ドロップダウンから[スケジュール]を選択します。
- [設定]の[日次]を選択します。
- [Repeat task every]をオンにして、ドロップダウンから[1 hour]を選択し、[duration of:]から[Indefinitely]を選択します。
- [有効]にチェックマークが付いていることを確認します。
- [OK] をクリックします。



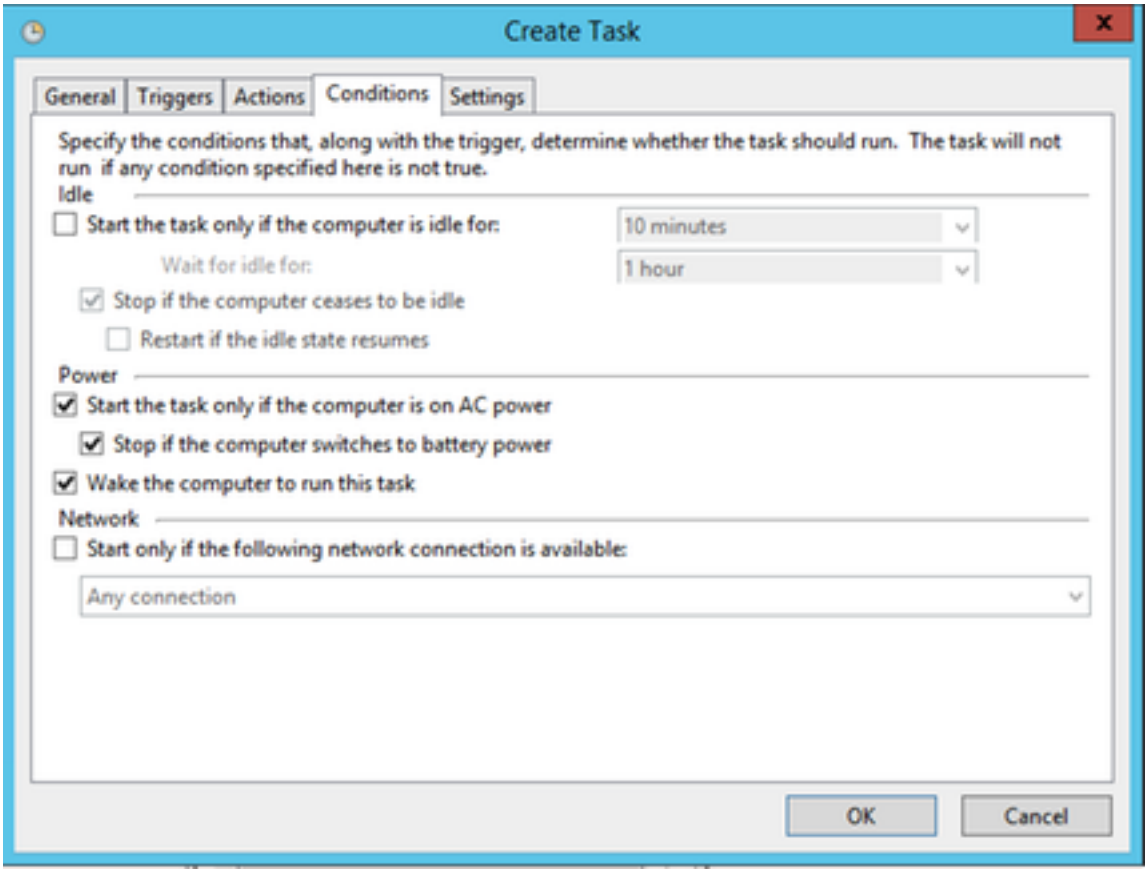
6. 「処理」タブの選択

- [New] をクリックします。
- [アクション]ドロップダウンから[プログラムの開始]を選択します。
- [プログラム/スクリプト]フィールドにC:\TETRA\update-win-x86-64.exeと入力します。
- [Add arguments]フィールドに*fetch —config C:\TETRA\config.xml —once —mirror C:\TETRA\Signatures*と入力します。
- [Start *in]*フィールドにC:\TETRAと入力します。
- [OK] をクリックします。



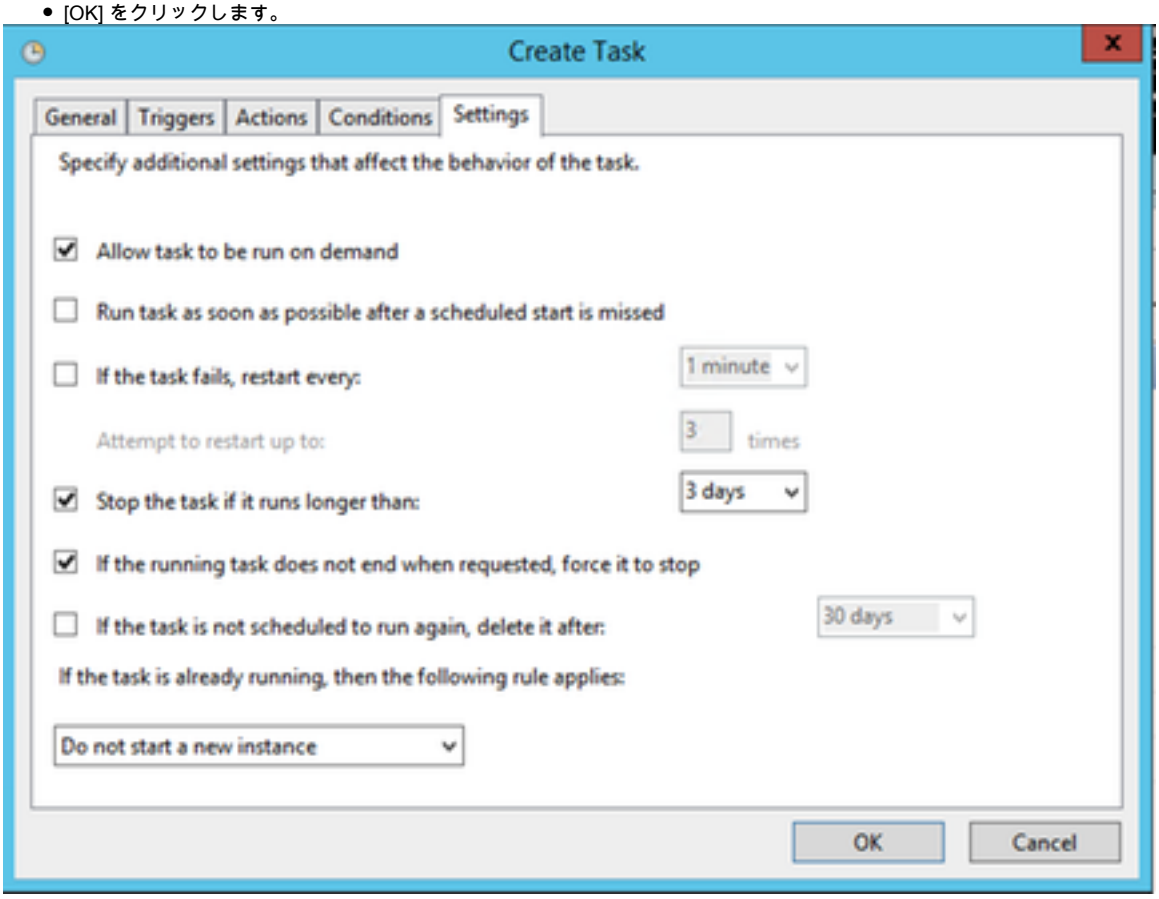
7. [オプション] [条件]タブを選択します。

   [Wake the computer to run this task]オプションをオンにします。



8 [Settings]タブを選択します。

- [タスクが既に実**行中の場合]で[新しいイ**ンスタンスを*開始しない*]**が選択されていることを確認します。**
- [OK] をクリックします。



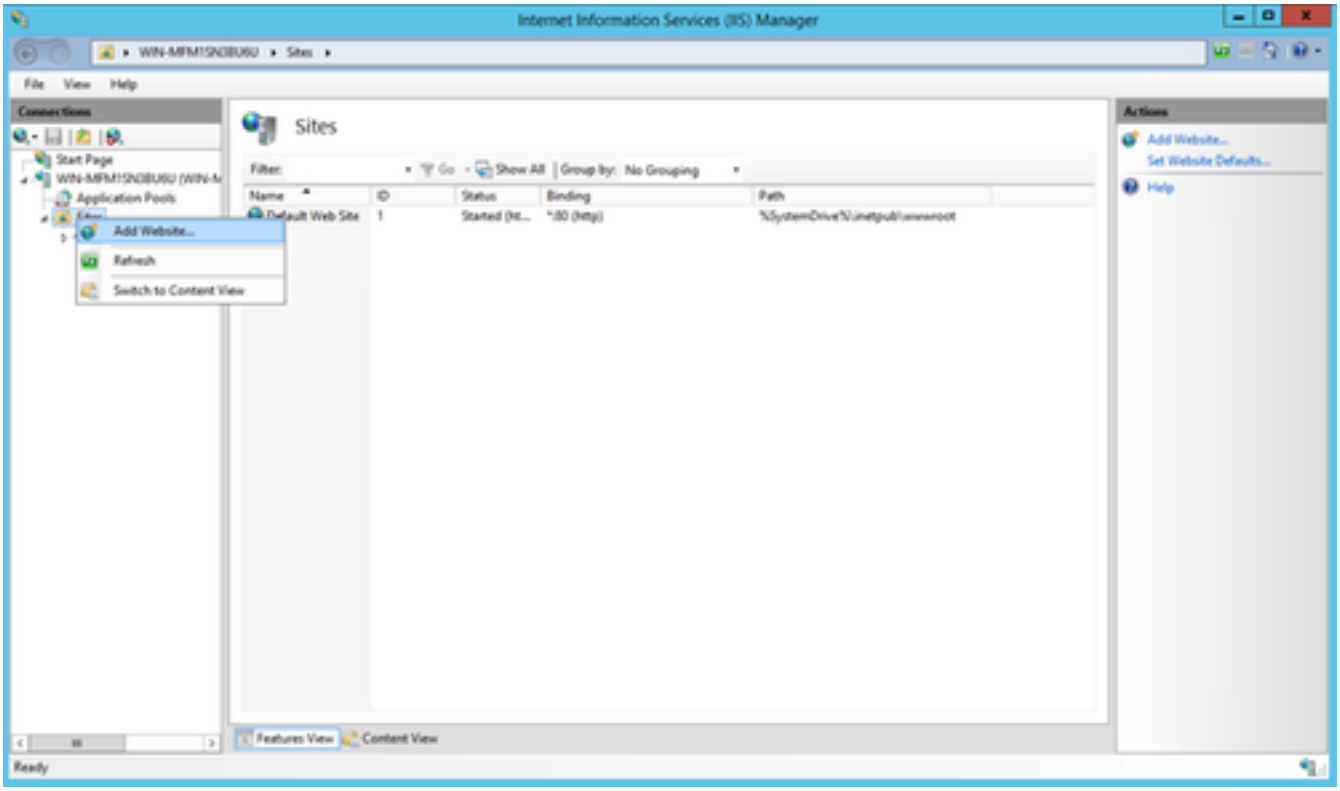
9.タスクを実行するアカ**ウントの資格証明を入力します。**

IISマネージャの設定

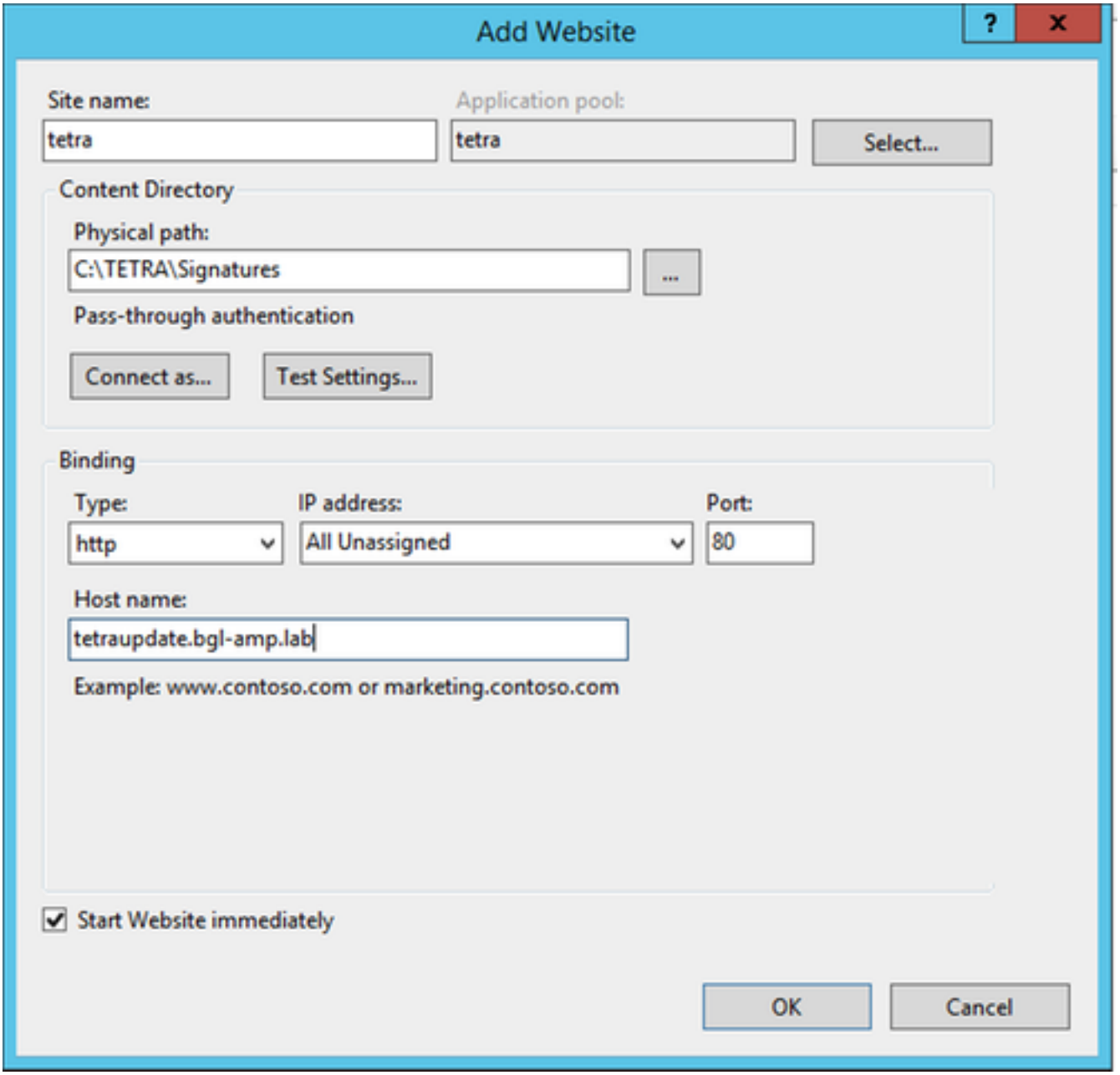
注：デフォルトアプリケーションプールが設定されている場合は、ステップ5に進みます。

1. (IIS) Managerに移動します([サー**バーマネージャ] > [ツール]で**)

2. 「サイト」フォルダが表示されるまで右側の列を展開し、「右クリック」を選択して、「**Webサイトの追加」を選択します。**



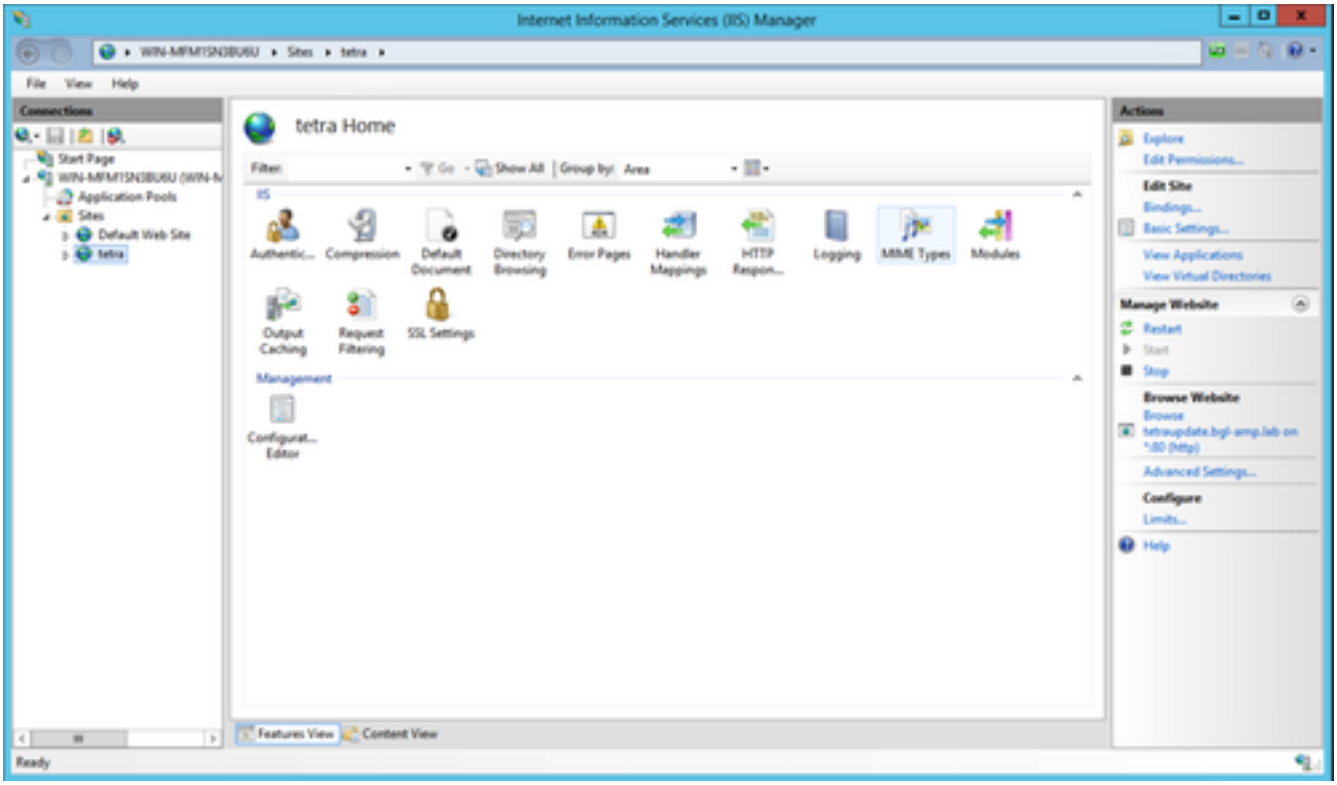
3.任意の名前を選択します。[Physical Path]で、署名がダウンロードさ***れた C:\TETRA\Signatures***フォルダを選択します。



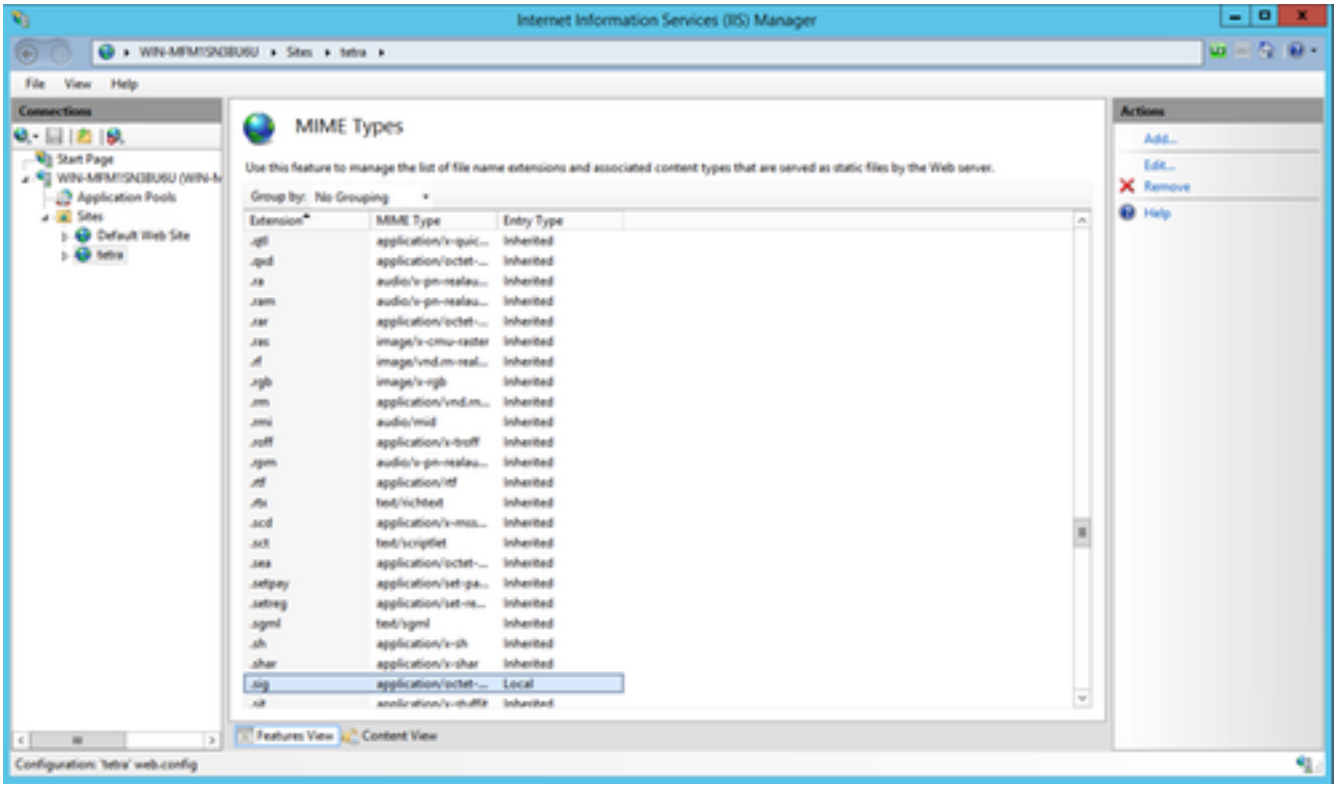
4.バインディングは単独で行います。**ホスト名とサーバー名を別**々に構成してください。選択した名前はクライアントで解決できる必要があります。これは、ポリシーで設定するURLです。

5.サイトを選択し、「MIMEタイプ」にナビゲートし、**次の**MIME**タイプを追加します。**

- .gzip、Application/octet-stream
- .dat、Application/octet-stream
- .id、Application/octet-stream
- .sig、Application/octet-stream



6.ミラーフォルダにあるweb.configファイルに移動し、ファイルの先頭に次の行を追加します。



終了すると、*C:\TETRA\Signatures\web.configファイル*の内容は、テキストエディタで表示すると、そのように表示されます。（構文と間隔は、指定した例と同じままにする必要があります）。

注：エンドポイント用AMPコネクタが正常に動作するには、応答にサーバHTTPヘッダーが存在する必要があります。サーバのHTTPヘッダーが無効になっている場合、Webサーバでは次に示す追加の設定が必要になる場合があります。

url-rewrite拡張をインストールする必要があります。次のXMLスニペットを/[MIRROR_DIRECTORY]/web.configのサーバ設定に追加します。

```
<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：テキストエディタまたはIISマネージャを使用して、URLリライトモジュールを使用して、この変更を手動で実行します。Rewriteモジュールは、次のURL(https://www.iis.net/downloads/microsoft/url-rewrite)からインストールできます

終了すると、*C:\TETRA\Signatures\web.configファイル*の内容は、テキストエディタで表示すると、そのように表示されます。（構文と間隔は、指定した例と同じままにする必要があります）。

Apache/Nginx

注：この手順では、Webホスティングソフトウェアのデフォルトディレクトリからシグニチャを提供していることを前提としています。

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. [Policy configuration]

1. > AMP<hostname.domain.root>IPIP

注意：それ以外の場合は、前のプロトコルやサブディレクトリを含めないと、ダウンロード中にエラーが発生します。

*[]***TETRAHTTPS**HTTPS

C:\inetpub\wwwroot\、C:\TETRA\Signature、または/var/www/htmlディレクトリに移動して、更新されたシグニチャが表示されていることを確認します。次の同期サイクルまで待つか、既存のシグニチャを手動で削除し、シグニチャのダウンロードを待機して、サーバからエンドクライアントにシグニチャををダウンロードします。デフォルトでは、更新を確認するための1時間インターバルです。

関連情報

- テクニカル サポートとドキュメント – Cisco Systems
- エンドポイント向けCisco AMP – テクニカルノート
- エンドポイント向けCisco AMP – ユーザガイド

.