Procedura di configurazione di AMP Update Server

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Fasi di installazione](#)
[Tutte le piattaforme](#)
[IIS di Windows](#)
[Creazione directory](#)
[Aggiorna creazione attività](#)
[Configurazione Gestione IIS](#)
[Apache/Nginx](#)
[Configurazione criteri](#)
[Verifica](#)
[Informazioni correlate](#)

Introduzione

In questo documento viene descritta in dettaglio la configurazione di Cisco Advanced Malware Protection (AMP) TETRA Update Server.

Prerequisiti

- Conoscenza degli host server, ad esempio Windows 2012R2 o CentOS 6.9 x86_64.
- Conoscenza di software di hosting come IIS (solo Windows), Apache, Nginx
- Host del server configurati con HTTPS abilitato e certificato attendibile valido installato.
- Opzione del server di aggiornamento locale HTTPS configurata.

Nota: Per informazioni dettagliate sull'abilitazione della configurazione e dei requisiti di Local Update Server, fare riferimento al capitolo 25 della Guida per l'utente di AMP for Endpoints, disponibile qui. (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf)

Nota: Gli host server (IIS, Apache, Nginx) sono prodotti di terze parti e non sono supportati da Cisco. Per domande che esulano dalle procedure fornite, fare riferimento ai team di supporto dei rispettivi prodotti.

Avviso: Se AMP è configurato con un server proxy, tutto il traffico di aggiornamento (incluso TETRA) continuerà a essere inviato tramite il server proxy al server locale. Accertarsi che il traffico possa passare al proxy senza modifiche mentre è in transito.

Fasi di installazione

Tutte le piattaforme

1. Confermare il sistema operativo del server di hosting.
2. Confermare il portale AMP for Endpoints Dashboard, scaricare il pacchetto software dell'Updater e il file di configurazione.

AMP for Endpoints Console:

STATI UNITI - 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

IIS di Windows

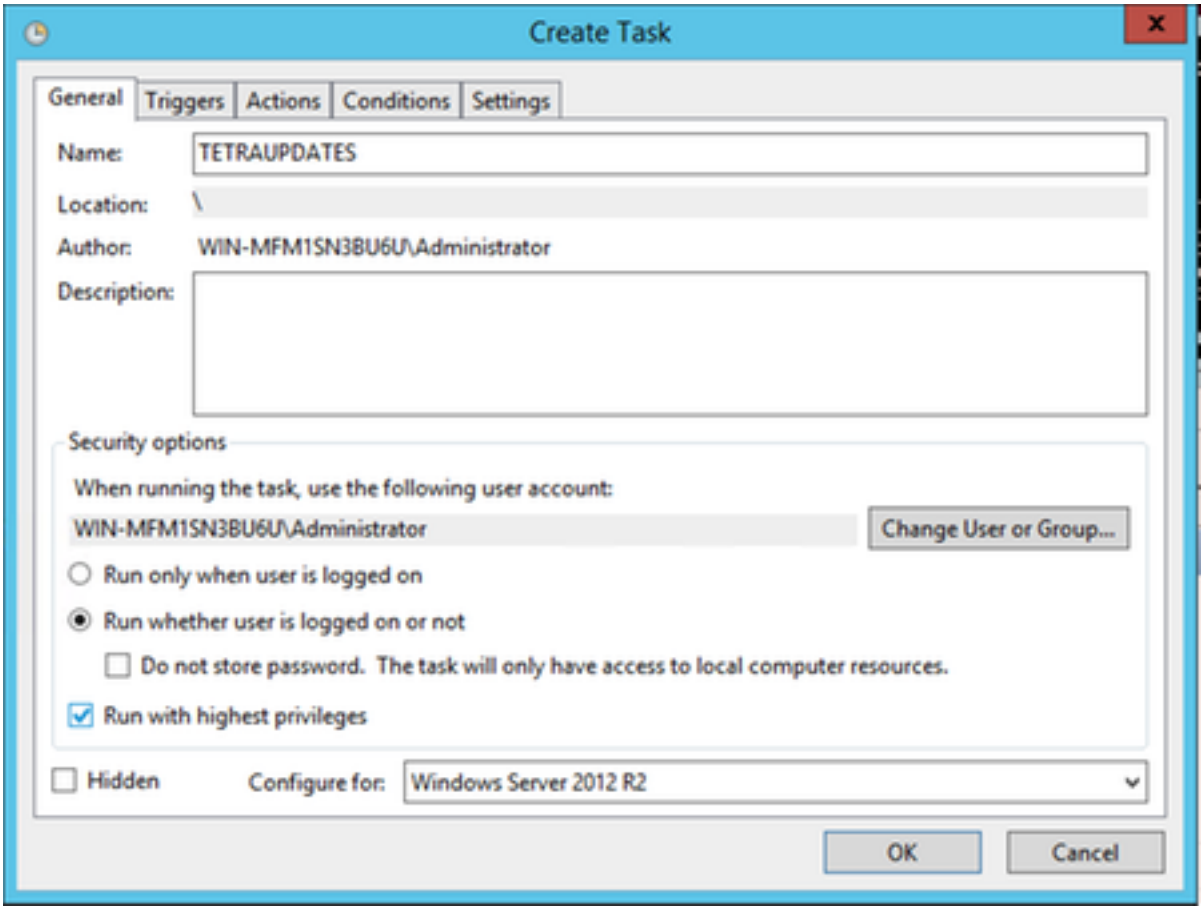
> **Nota:** I passaggi seguenti si basano sul nuovo pool di applicazioni di IIS per ospitare le firme, **non** sul pool di applicazioni predefinito. Per utilizzare il pool predefinito, modificare la cartella **—mirror** nei passaggi forniti in modo che rifletta il percorso di hosting Web predefinito (**C:\inetpub\wwwroot**)

Creazione directory

1. Creare una nuova cartella sull'unità principale, denominandola **TETRA**.
2. Copiare il pacchetto del software di aggiornamento dell'AMP compresso e il file di configurazione nella cartella **TETRA** creata.
3. Decomprimere il pacchetto software in questa cartella.
4. Creare una nuova cartella denominata **Signatures** all'interno della cartella TETRA.

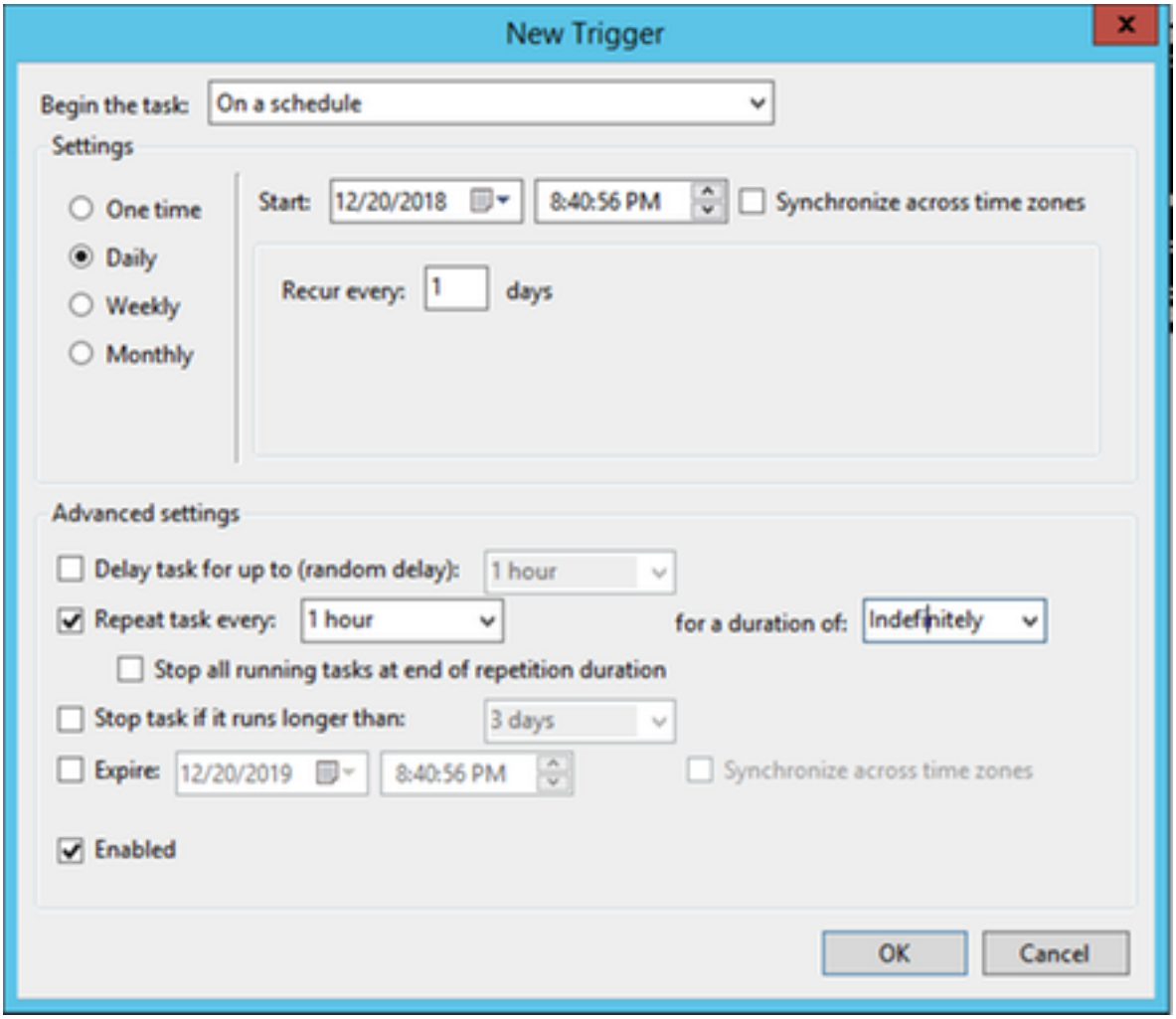
Aggiorna creazione attività

1. Aprire la riga di comando e passare alla cartella *C:\TETRA.**cd C:\TETRA***
2. Eseguire il comando ***update-win-x86-64.exe fetch —config="C:\TETRA\config.xml" —once —mirror C:\TETRA\Signatures***
3. Aprire l'Utilità di pianificazione e creare una nuova attività. (Azione > Crea task) per eseguire automaticamente il software di aggiornamento con le seguenti opzioni, se necessario:
4. Selezionare la scheda Generale. Immettere un nome per il task.Selezionare **Esegui indipendentemente dal fatto che l'utente sia connesso o meno**.Selezionare **Esegui con i privilegi più elevati.**Selezionare **sistema operativo** dall'elenco a discesa **Configura.**



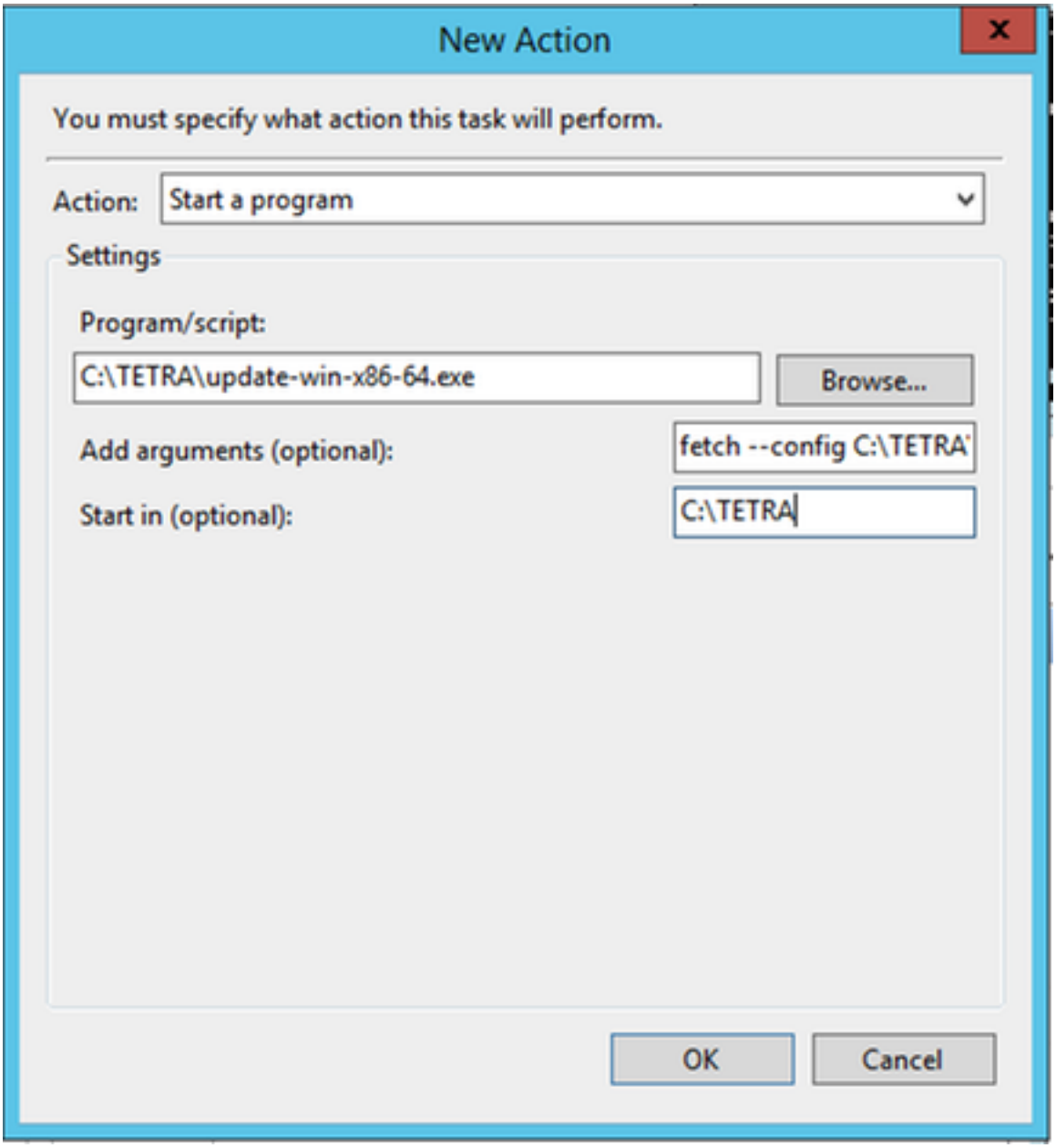
5. Selezionare la scheda Trigger.

- Fare clic su New.
- Selezionare **In base a una pianificazione** dall'elenco a discesa **Inizia il task**.
- Selezionare **Daily** in Settings (Impostazioni).
- Selezionare **Ripeti attività ogni**, **selezionare 1 ora** dall'elenco a discesa e scegliere **Indefinito** dal menu "**per una durata di:"**
- Verificare che l'opzione **Enabled** sia **selezionata**.
- Fare clic su **OK**.



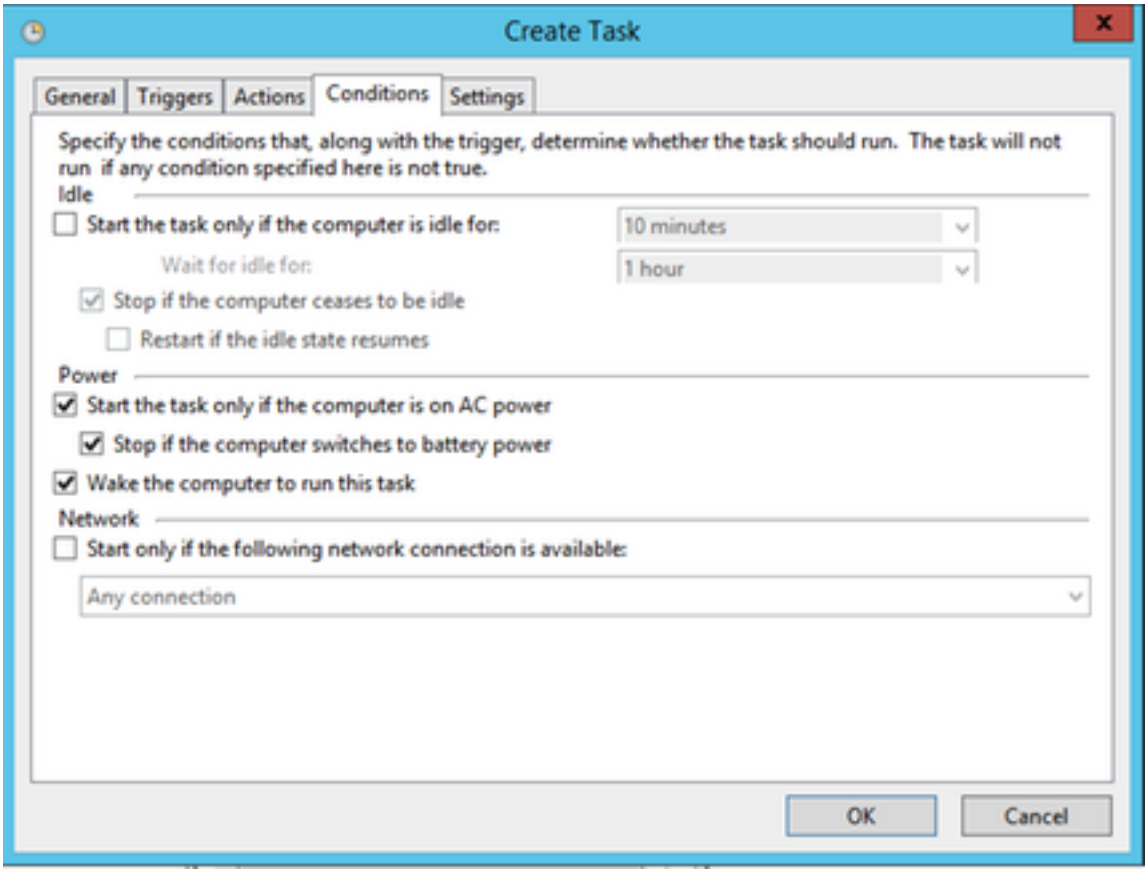
6. Selezionare la scheda Azioni

- Fare clic su **New**.
- Selezionare **Avvia un programma** dal menu a discesa **Azione**.
- Immettere ***C:\TETRA\update-win-x86-64.exe*** nel campo **Programma/script**.
- Immettere ***fetch —config C:\TETRA\config.xml —once —mirror C:\TETRA\Signatures*** nel campo **Aggiungi argomenti**.
- Immettere ***C:\TETRA*** nel campo **Inizia** in
- Fare clic su **OK.**



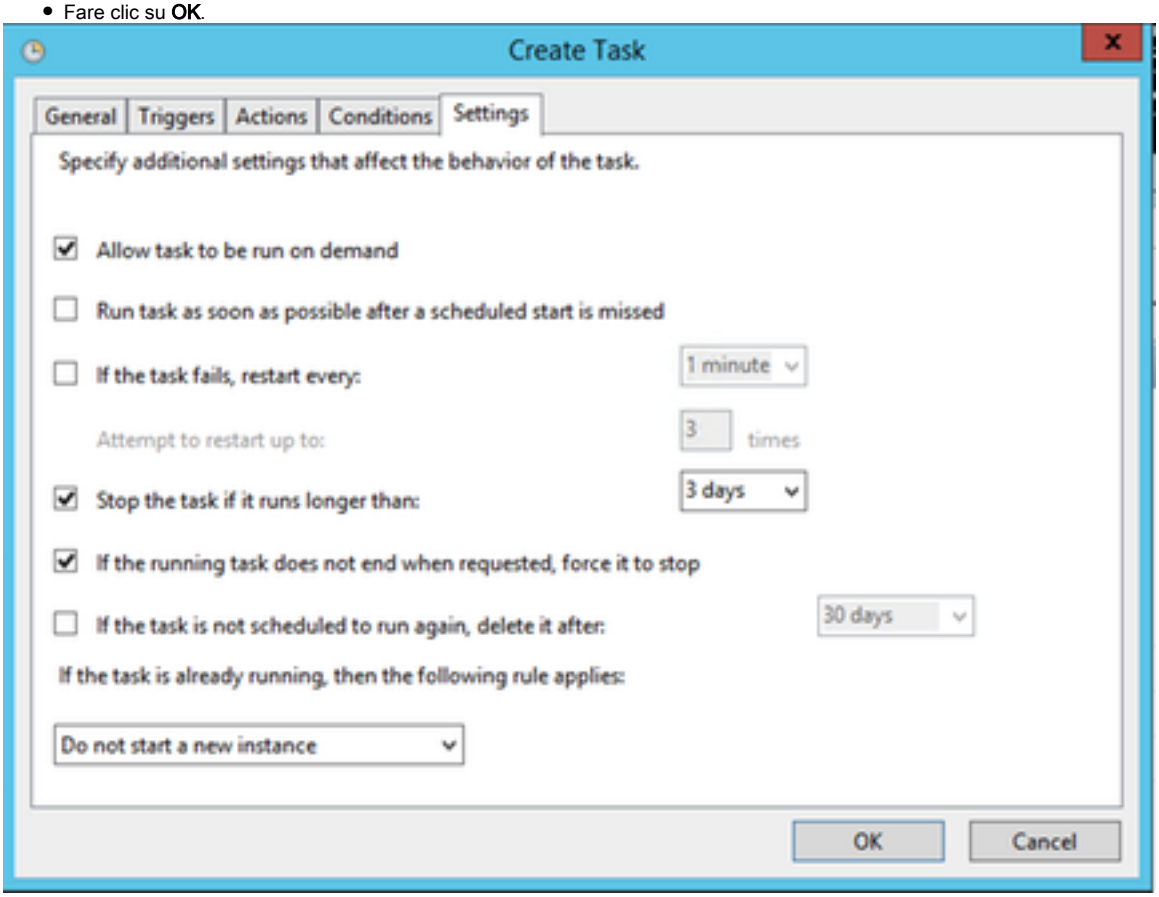
7. *[Facoltativo]* Selezionare la scheda Condizioni.

Selezionare l'opzione Riattiva il computer per eseguire questa attività.



8 Selezionare la scheda Settings.

- Verificare che l'opzione **Non avviare una nuova istanza** sia selezionata *in* Se l'attività è già in esecuzione.
- Fare clic su **OK**.



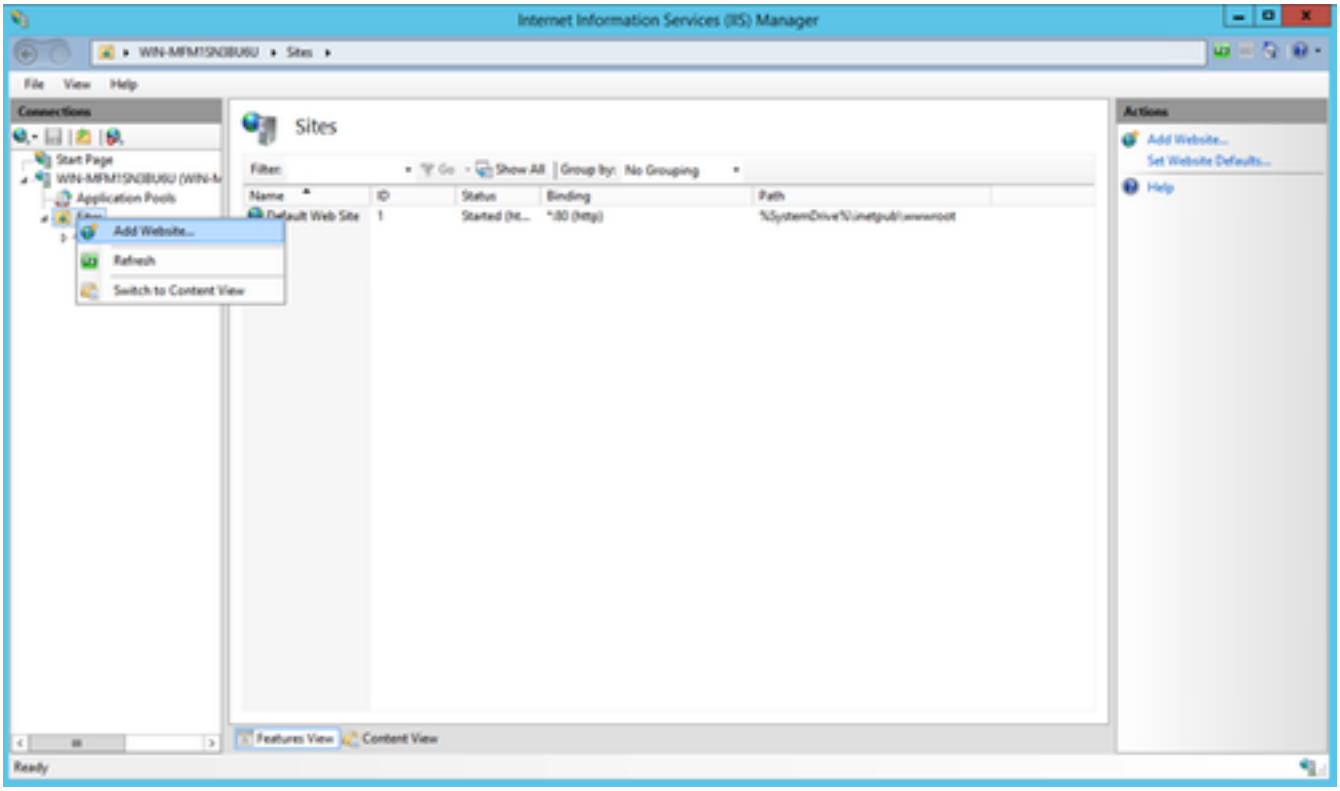
9. Immettere le credenziali per **l'account che eseguirà il task**.

Configurazione Gestione IIS

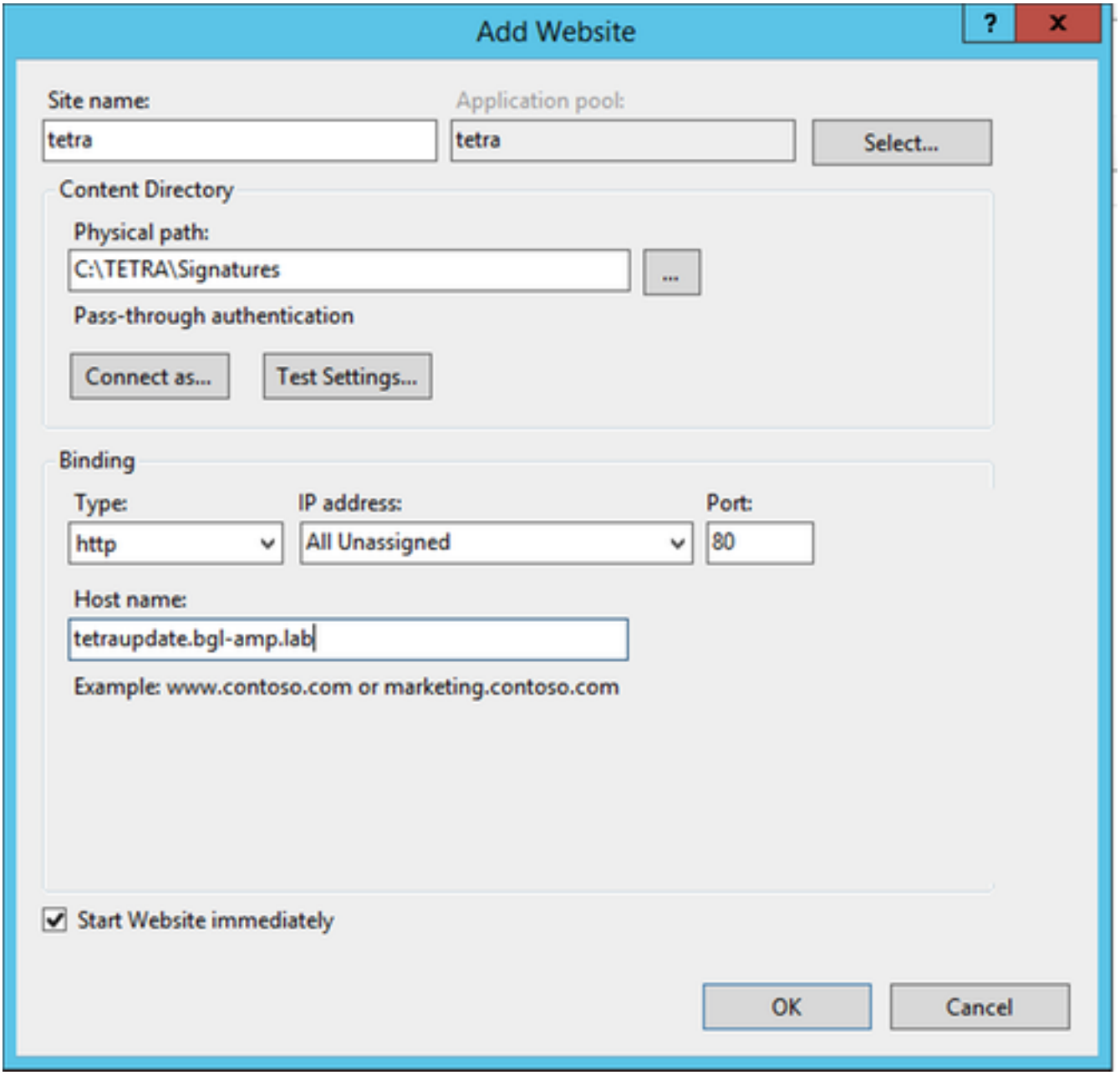
Nota: Andare al passaggio 5 quando è configurato il pool di applicazioni predefinito.

1. Passare a (IIS) Manager (**In Server Manager > Strumenti**)

2. Espandere la colonna destra fino a quando la **cartella Siti** è visibile, **Fare clic con il pulsante destro del mouse e selezionare Aggiungi sito Web**.



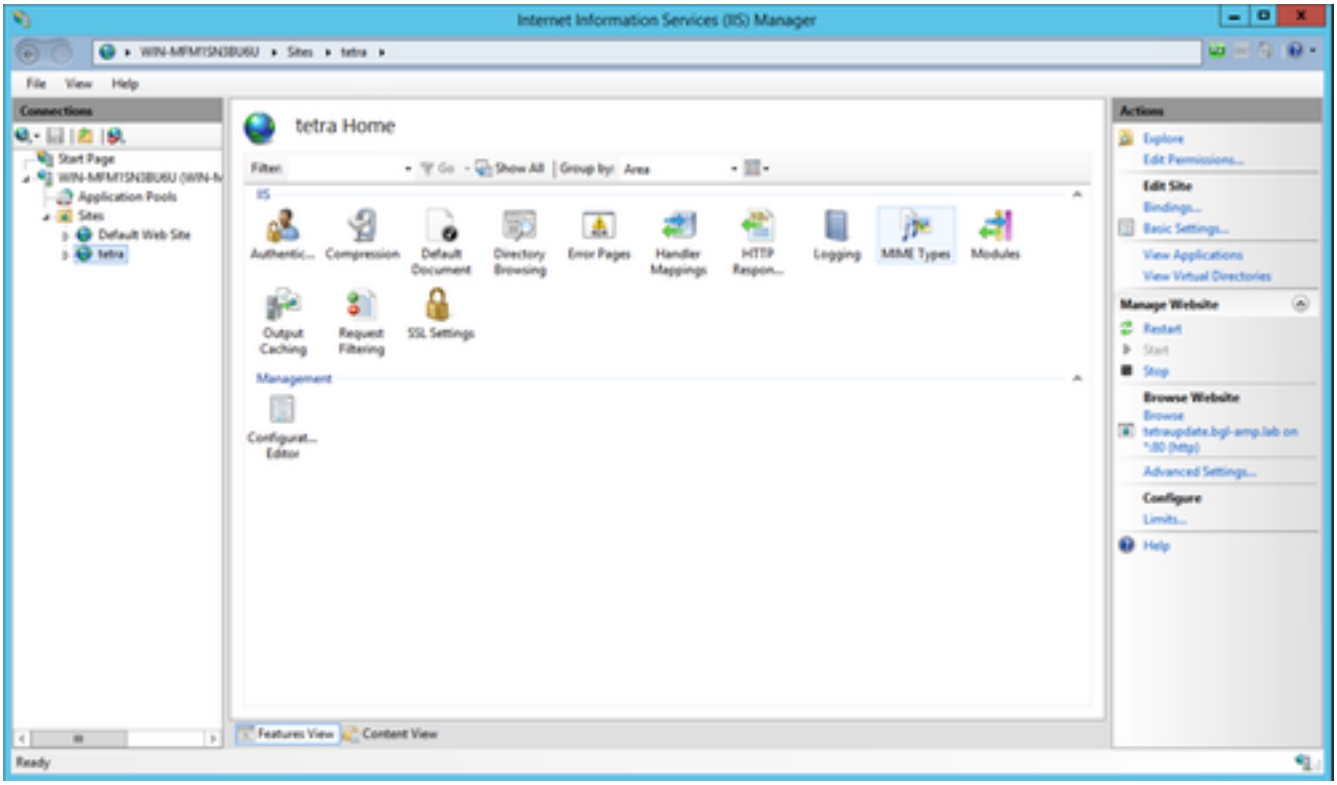
3. Scegliere un nome. Per Percorso fisico selezionare la cartella *C:\TETRA\Signatures* in cui sono state scaricate le firme.



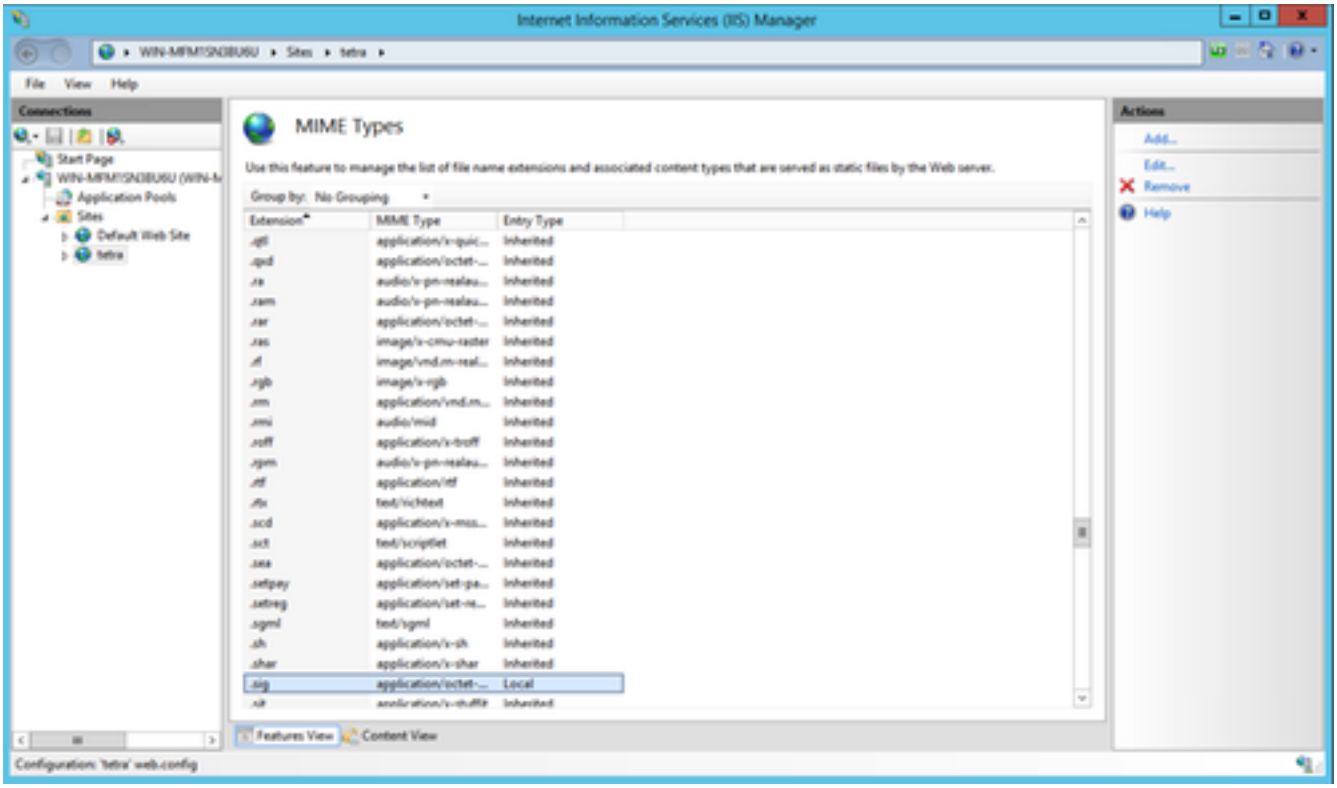
4. Non modificare le associazioni. **Configurare un nome host** e un nome server **separati**. I nomi scelti devono essere risolvibili dai client. URL che verrà configurato nel criterio.

5. Selezionare il sito, passare a **Tipi MIME** e **aggiungere i seguenti tipi MIME**:

- .gzip, flusso di applicazioni/ottetti
- .dat, flusso di applicazioni/ottetti
- .id, flusso-applicazione/ottetto
- .sig, Application/octet-stream



6. Passare al **file web.config** (che si trova nella cartella mirror), aggiungere le seguenti righe all'inizio del file.



Al termine, il contenuto del file *C:\TETRA\Signatures\web.config* apparirà come tale quando visualizzato in un editor di testo. La sintassi e la spaziatura devono rimanere invariate rispetto all'esempio fornito.

> **Nota:** AMP for Endpoints Connector richiede la presenza dell'intestazione HTTP del server nella risposta per il corretto funzionamento. Se l'intestazione HTTP del server è stata disattivata, è possibile che il server Web richieda una configurazione aggiuntiva specificata di seguito.

Ènecessario installare l'estensione per la riscrittura dell'URL. Aggiungere il seguente frammento XML alla configurazione del server in /[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>
  </rules>
</rewrite>
```

> **Nota:** Eseguire questa modifica manualmente con un editor di testo o con Gestione IIS utilizzando il modulo URL Rewrite. Il modulo Rewrite può essere installato dal seguente URL (https://www.iis.net/downloads/microsoft/url-rewrite)

Al termine, il contenuto del file *C:\TETRA\Signatures\web.config* apparirà come tale quando visualizzato in un editor di testo. La sintassi e la spaziatura devono rimanere invariate rispetto all'esempio fornito.

Apache/Nginx

> **Nota:** I passaggi forniti presuppongono che le firme vengano fornite dalla directory predefinita del software di hosting Web.

1. **Creare una nuova cartella** sull'unità *radice* denominata **TETRA.**
2. **Decomprimere** il pacchetto di script scaricato in questa cartella.
3. Eseguire il comando ***Chmod +x update-linux**** per concedere agli script l'autorizzazione di esecuzione.
4. Eseguire il comando per recuperare i file di aggiornamento 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. Per automatizzare il processo di aggiornamento del server, aggiungere un processo cron al server:

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

6. Continuare a seguire la procedura descritta in **Configurazione dei criteri** per configurare i criteri in modo che utilizzino il server di aggiornamento.

Configurazione criteri

1. Passare al criterio per utilizzare il server di aggiornamento e in ***Impostazioni avanzate > TETRA*** selezionare: Casella di controllo per il server di aggiornamento AMP localeIl nome host o l'indirizzo IP del server di aggiornamento nel formato <hostname.domain.root> o indirizzo IP.

Attenzione: Non includere alcun protocollo prima o dopo le sottodirectory; in caso contrario, si verificherà un errore durante il download.

[Facoltativo] Casella di controllo **Usa HTTPS per gli aggiornamenti della definizione TETRA:** se il server locale è configurato con un certificato corretto e per i connettori per usare HTTPS.

Verifica

Passare alla **directory C:\inetpub\wwwroot\, C:\TETRA\Signature** o **/var/www/html** e verificare che le firme aggiornate siano visibili. Le firme verranno scaricate dal server al client finale in attesa del successivo ciclo di sincronizzazione oppure in attesa dell'eliminazione manuale delle firme esistenti e del download. L'impostazione predefinita è un intervallo di 1 ora per la verifica della disponibilità di un aggiornamento.

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems
- Cisco AMP for Endpoints - Note tecniche
- Cisco AMP for Endpoints - Guida per l'utente

.