Esempio di configurazione di Image and Signature IDS 4.1 con IPS 5.0 e versioni successive (AIP-SSM, NM-IDS, IDSM-2)

Sommario

Introduzione

In questo documento viene descritto come aggiornare l'immagine e la firma per il software Cisco Intrusion Detection Sensor (IDS) dalla versione 4.1 a Cisco Intrusion Prevention System (IPS) 5.0 e versioni successive.

Nota: dalla versione software 5.x e successive, Cisco IPS sostituisce Cisco IDS, che è applicabile fino alla versione 4.1.

Nota: Il sensore non può scaricare gli aggiornamenti software da Cisco.com. È necessario scaricare gli aggiornamenti software da Cisco.com sul server FTP, quindi configurare il sensore per scaricarli dal server FTP.

Per la procedura, consultare la sezione Installazione dell'immagine del sistema AIP-SSM in Aggiornamento, downgrade e installazione delle immagini del sistema.

Per ulteriori informazioni su come ripristinare l'accessorio Cisco Secure IDS (in precedenza NetRanger) e i moduli delle versioni 3.x e 4.x, consultare il documento sulla procedura di recupero della password per i Cisco IDS Sensor e IDS Services Module (IDSM-1, IDSM-2).

Nota: il traffico degli utenti non viene influenzato durante l'aggiornamento nelle impostazioni **inline e fail-open** su ASA - AIP-SSM.

Nota: per ulteriori informazioni sulla procedura di aggiornamento di IPS 5.1 alla versione 6.x, fare riferimento alla sezione Aggiornamento del software Cisco IPS dalla versione 5.1 alla 6.x di Configurazione del sensore Cisco Intrusion Prevention System con l'interfaccia della riga di comando 6.0.

Nota: il sensore non supporta i server proxy per gli aggiornamenti automatici. Le impostazioni proxy sono solo per la funzione Correlazione globale.

Prerequisiti

Requisiti

La versione minima richiesta per l'aggiornamento alla versione 5.0 è la 4.1(1).

Componenti usati

Le informazioni di questo documento si basano sull'hardware Cisco serie 4200 IDS con software versione 4.1 (da aggiornare alla versione 5.0).

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

L'aggiornamento da Cisco 4.1 a 5.0 è disponibile come download sul sito Cisco.com. Per la procedura da utilizzare per accedere ai download del software IPS, consultare il documento sul download del software IPS Cisco sul sito Cisco.com.

Per eseguire l'aggiornamento, è possibile utilizzare uno dei metodi elencati di seguito:

- Dopo aver scaricato il file di aggiornamento 5.0, consultare il file Leggimi per la procedura di installazione del file di aggiornamento 5.0 con il comando **upgrade**. Per ulteriori informazioni, vedere la sezione Uso del comando Upgrade di questo documento.
- Se è stato configurato Aggiornamento automatico per il sensore, copiare il file di aggiornamento 5.0 nella directory del server in cui il sensore esegue il polling per gli aggiornamenti. Per ulteriori informazioni, vedere la sezione Uso del comando auto-upgrade in

questo documento.
- Se si installa un aggiornamento del sensore e il sensore non è utilizzabile dopo il riavvio, è necessario ricreare l'immagine del sensore. L'aggiornamento di un sensore da una versione di Cisco IDS precedente alla 4.1 richiede anche l'uso del comando **recovery** o del CD di ripristino/aggiornamento. Per ulteriori informazioni, vedere la sezione Reimaging the Sensor di questo documento.

Aggiornare il sensore

Nelle sezioni seguenti viene spiegato come usare il comando **upgrade** per aggiornare il software del sensore:

Panoramica

Èpossibile aggiornare il sensore con questi file, tutti con estensione .pkg:

- Aggiornamenti della firma, ad esempio IPS-sig-S150-minreq-5.0-1.pkg
- Aggiornamenti del motore delle firme, ad esempio IPS-engine-E2-req-6.0-1.pkg
- Aggiornamenti principali, ad esempio IPS-K9-maj-6.0-1-pkg
- Aggiornamenti secondari, ad esempio IPS-K9-min-5.1-1.pkg
- Aggiornamenti dei service pack, ad esempio IPS-K9-sp-5.0-2.pkg
- Aggiornamenti delle partizioni di ripristino, ad esempio IPS-K9-r-1.1-a-5.0-1.pkg
- Patch release, ad esempio, IPS-K9-patch-6.0-1p1-E1.pkg
- Aggiornamenti delle partizioni di ripristino, ad esempio IPS-K9-r-1.1-a-6.0-1.pkg

Un aggiornamento del sensore modifica la versione software del sensore.

Comandi e opzioni di aggiornamento

Per configurare gli aggiornamenti automatici, usare il comando **auto-upgrade-option enabled** nella modalità secondaria dell'host del servizio.

Si applicano le seguenti opzioni:

- **default** - Ripristina l'impostazione di default del sistema.
- **directory**: directory in cui si trovano i file di aggiornamento sul file server.
- **file-copy-protocol**: protocollo di copia dei file utilizzato per scaricare i file dal file server. I valori validi sono **ftp** o **scp**.**Nota:** se si usa SCP, è necessario usare il comando **ssh host-key** per aggiungere il server alla lista di host noti SSH in modo che il sensore possa comunicare con esso tramite SSH. Per la procedura, consultare il documento sull'aggiunta di host all'elenco degli host noti.
- **ip-address**: indirizzo IP del file server.
- **password**—Password utente per l'autenticazione sul file server.
- **schedule-option**: programma quando vengono eseguiti aggiornamenti automatici. La pianificazione del calendario avvia gli aggiornamenti a orari specifici in giorni specifici. La

programmazione periodica avvia gli aggiornamenti a intervalli periodici specifici.**calendario-pianificazione**: configura i giorni della settimana e le ore del giorno in cui vengono eseguiti gli aggiornamenti automatici.**giorni della settimana**: giorni della settimana in cui vengono eseguiti gli aggiornamenti automatici. È possibile selezionare più giorni. I valori validi sono da domenica a sabato.**no** - Rimuove una voce o un'impostazione di selezione.**ora del giorno**: ora del giorno in cui ha inizio l'aggiornamento automatico. È possibile selezionare più volte. Il valore valido è hh:mm[:ss].**periodic-schedule**: configura l'ora in cui deve essere eseguito il primo aggiornamento automatico e il tempo di attesa tra gli aggiornamenti automatici.**intervallo**: il numero di ore di attesa tra gli aggiornamenti automatici. I valori validi sono compresi tra 0 e 8760.**start-time** - Ora di inizio del primo aggiornamento automatico. Il valore valido è hh:mm[:ss].

- **user-name**: nome utente per l'autenticazione sul file server.

Per la procedura IDM per l'aggiornamento del sensore, consultare Aggiornamento del sensore.

Utilizzare il comando Upgrade

Se prima dell'aggiornamento a IPS 6.0 non sono stati configurati i parametri della community di sola lettura e di lettura/scrittura, si ricevono errori SNMP. Se si utilizza SNMP set e/o get features, è necessario configurare i parametri della community di sola lettura e di lettura/scrittura prima di eseguire l'aggiornamento a IPS 6.0. In IPS 5.x la community di sola lettura è stata impostata su public per impostazione predefinita e la **community di lettura/scrittura** è stata impostata su private per impostazione predefinita. In IPS 6.0 queste due opzioni non hanno valori predefiniti. Se non sono stati utilizzati get e set SNMP con IPS 5.x, ad esempio, enable-set-get è stato impostato su false, non vi sono problemi con l'aggiornamento a IPS 6.0. Se sono stati utilizzati get e **set** SNMP con IPS 5.x, ad esempio enable-set-get è stato impostato su true, è necessario configurare i parametri **community di sola lettura** e **community di lettura/scrittura** su valori specifici, altrimenti l'aggiornamento a IPS 6.0 non riesce.

Viene visualizzato questo messaggio di errore:

```
Error: execUpgradeSoftware : Notification Application "enable-set-get" value set to true,
but "read-only-community" and/or "read-write-community" are set to null. Upgrade may not
continue with null values in these fields.
```

Nota: per impostazione predefinita IPS 6.0 nega gli eventi ad alto rischio. Si tratta di una modifica rispetto a IPS 5.x. Per modificare l'impostazione predefinita, creare una sostituzione dell'azione evento per l'azione in linea deny packet e configurarla in modo che sia disabilitata. Se l'amministratore non è a conoscenza della community di lettura/scrittura, deve tentare di disabilitare completamente il protocollo SNMP prima di eseguire un tentativo di aggiornamento per rimuovere questo messaggio di errore.

Per aggiornare il sensore, completare i seguenti passaggi:

1. Scaricare il file di aggiornamento principale (IPS-K9-maj-5.0-1-S149.rpm.pkg) in un server FTP, SCP, HTTP o HTTPS accessibile dal sensore.Per la procedura su come individuare il software sul sito Cisco.com, consultare il documento sul reperimento del software Cisco IPS.**Nota:** per scaricare il file, è necessario accedere a Cisco.com utilizzando un account con privilegi di crittografia. Non modificare il nome del file. Per accettare l'aggiornamento, è necessario conservare il nome file originale del sensore.**Nota:** non modificare il nome del file. Per consentire al sensore di accettare l'aggiornamento, è necessario mantenere il nome file

originale.
2. Accedere alla CLI utilizzando un account con privilegi di amministratore.
3. Accedere alla modalità di configurazione:
```
sensor#configure terminal
```

4. Aggiornare il sensore:
```
sensor(config)#upgrade scp://
```

Esempio:Nota: questo comando è su due righe per motivi di spazio.
```
sensor(config)#upgrade scp://tester@10.1.1.1//upgrade/
IPS-K9-maj-5.0-1-S149.rpm.pkg
```

Nota: fare riferimento a Server FTP e HTTP/HTTPS supportati per un elenco dei server FTP e HTTP/HTTPS supportati. Per ulteriori informazioni su come aggiungere il server SCP alla lista degli host noti SSH, consultare il documento sull'aggiunta di host alla lista degli host noti SSH.
5. Immettere la password quando richiesto:
```
Enter password: ********
Re-enter password: ********
```
6. Digitare **yes** per completare l'aggiornamento.**Nota:** aggiornamenti importanti, aggiornamenti secondari e service pack possono forzare il riavvio dei processi IPS o addirittura il riavvio del sensore per completare l'installazione. Il servizio viene interrotto per almeno due minuti. Al termine dell'aggiornamento, tuttavia, non è necessario riavviare gli aggiornamenti delle firme. Fare riferimento a Download Signature Updates (solo utenti registrati) per gli ultimi aggiornamenti.
7. Verificare la nuova versione del sensore:
```
sensor#show version

Application Partition:


Cisco Intrusion Prevention System, Version 5.0(1)S149.0


OS Version 2.4.26-IDS-smp-bigphys

Platform: ASA-SSM-20

Serial Number: 021

No license present

Sensor up-time is 5 days.

Using 490110976 out of 1984704512 bytes of available memory (24% usage)

system is using 17.3M out of 29.0M bytes of available disk space (59% usage)

application-data is using 37.7M out of 166.6M bytes of
available disk space (24 usage)

boot is using 40.5M out of 68.5M bytes of available disk space (62% usage)
```

```
MainApp          2005_Mar_04_14.23 (Release)  2005-03-04T14:35:11-0600  Running

AnalysisEngine   2005_Mar_04_14.23 (Release)  2005-03-04T14:35:11-0600  Running

CLI              2005_Mar_04_14.23 (Release)  2005-03-04T14:35:11-0600


Upgrade History:


  IDS-K9-maj-5.0-1-   14:16:00 UTC Thu Mar 04 2004


Recovery Partition Version 1.1 - 5.0(1)S149


sensor#
```

Nota: Per IPS 5.x, viene visualizzato un messaggio che indica che l'aggiornamento è di tipo sconosciuto. È possibile ignorare questo messaggio.**Nota:** viene ricreata l'immagine del sistema operativo e tutti i file inseriti nel sensore tramite l'account del servizio vengono rimossi.

Fare riferimento a Aggiornamento del sensore per ulteriori informazioni sulla procedura IDM per l'aggiornamento del sensore.

Configurazione degli aggiornamenti automatici

Aggiornamenti automatici

Èpossibile configurare il sensore per cercare automaticamente nuovi file di aggiornamento nella directory di aggiornamento. Ad esempio, diversi sensori possono puntare alla stessa directory remota del server FTP con diverse pianificazioni di aggiornamento, ad esempio ogni 24 ore o lunedì, mercoledì e venerdì alle 23.00.

Per pianificare gli aggiornamenti automatici, specificare le seguenti informazioni:

- Indirizzo IP server
- Percorso della directory sul file server in cui il sensore controlla i file di aggiornamento
- Protocollo di copia file (SCP o FTP)
- Nome utente e password
- Pianificazione aggiornamento

Ènecessario scaricare l'aggiornamento software da Cisco.com e copiarlo nella directory di aggiornamento prima che il sensore possa eseguire il polling per gli aggiornamenti automatici.

Nota: se si utilizza l'aggiornamento automatico con AIM-IPS e altri accessori o moduli IPS, accertarsi di inserire sia il file di aggiornamento 6.0(1), IPS-K9-6.0-1-E1.pkg, che il file di aggiornamento AIM-IPS, IPS-AIM-K9-6.0-4-E1.pkg, sul server di aggiornamento automatico in modo che AIM-IPS possa rilevare correttamente il file da scaricare e installare automaticamente. Se si inserisce solo il file di aggiornamento 6.0(1), IPS-K9-6.0-1-E1.pkg, sul server di aggiornamento automatico, AIM-IPS scarica e tenta di installarlo, ovvero il file errato per AIM-IPS.

Fare riferimento a Aggiornamento automatico del sensore per ulteriori informazioni sulla

procedura IDM per l'aggiornamento automatico del sensore.

Uso del comando auto-upgrade

Per i comandi di **aggiornamento automatico**, vedere la sezione Comandi e opzioni di questo documento.

Per pianificare gli aggiornamenti automatici, completare i seguenti passaggi:

1. Accedere alla CLI con un account con privilegi di amministratore.
2. Configurare il sensore per cercare automaticamente i nuovi aggiornamenti nella directory di aggiornamento.
```
sensor#configure terminal
sensor(config)#service host
sensor(config-hos)#auto-upgrade-option enabled
```

3. Specificare la pianificazione:Per la pianificazione del calendario, che avvia gli aggiornamenti a orari specifici in giorni specifici:
```
sensor(config-hos-ena)#schedule-option calendar-schedule
sensor(config-hos-ena-cal#days-of-week sunday
sensor(config-hos-ena-cal#times-of-day 12:00:00
```

   Per la programmazione periodica, che avvia gli aggiornamenti a intervalli periodici specifici:
```
sensor(config-hos-ena)#schedule-option periodic-schedule
sensor(config-hos-ena-per)#interval 24
sensor(config-hos-ena-per)#start-time 13:00:00
```

4. Specificare l'indirizzo IP del file server:
```
sensor(config-hos-ena-per)#exit
sensor(config-hos-ena)#ip-address 10.1.1.1
```

5. Specificare la directory in cui si trovano i file di aggiornamento sul file server:
```
sensor(config-hos-ena)#directory /tftpboot/update/5.0_dummy_updates
```

6. Specificare il nome utente per l'autenticazione nel file server:
```
sensor(config-hos-ena)#user-name tester
```

7. Specificare la password dell'utente:
```
sensor(config-hos-ena)#password

Enter password[]: ******
Re-enter password: ******
```

8. Specificare il protocollo del file server:
```
sensor(config-hos-ena)#file-copy-protocol ftp
```

   Nota: se si usa SCP, è necessario usare il comando **ssh host-key** per aggiungere il server alla lista di host noti SSH in modo che il sensore possa comunicare con esso tramite SSH. Per la procedura, consultare il documento sull'aggiunta di host all'elenco degli host noti.
9. Verificare le impostazioni:
```
sensor(config-hos-ena)#show settings

    enabled
```

```
    ----------------------------------------------

       schedule-option

       ----------------------------------------------

          periodic-schedule

          ----------------------------------------------

             start-time: 13:00:00

             interval: 24 hours

          ----------------------------------------------

       ----------------------------------------------

       ip-address: 10.1.1.1

       directory: /tftpboot/update/5.0_dummy_updates

       user-name: tester

       password: <hidden>

       file-copy-protocol: ftp default: scp

    ----------------------------------------------

  sensor(config-hos-ena)#
```

10. Uscire dalla modalità secondaria di aggiornamento automatico:

```
sensor(config-hos-ena)#exit
sensor(config-hos)#exit

Apply Changes:?[yes]:
```

11. Premere **Invio** per applicare le modifiche o digitare **no** per ignorarle.

Ricreare l'immagine del sensore

Èpossibile ricreare l'immagine del sensore nei seguenti modi:

- Per gli accessori IDS dotati di unità CD-ROM, utilizzare il CD di ripristino/aggiornamento.Fare riferimento alla sezione Uso del CD di ripristino/aggiornamento in Aggiornamento, downgrade e installazione delle immagini del sistema per la procedura.
- Per tutti i sensori, usare il comando **recovery**.Per la procedura, consultare la sezione Recupero della partizione dell'applicazione in Aggiornamento, downgrade e installazione delle immagini del sistema.
- Per gli IDS-4215, IPS-4240 e IPS 4255, utilizzare ROMMON per ripristinare l'immagine del sistema.Per le procedure, consultare le sezioni Installazione dell'immagine del sistema IDS-4215 e Installazione delle immagini del sistema IPS-4240 e IPS-4255 in Aggiornamento, downgrade e installazione delle immagini del sistema.
- Per NM-CIDS, utilizzare il bootloader.Per la procedura, consultare la sezione Installazione dell'immagine del sistema NM-CIDS in Aggiornamento, downgrade e installazione delle immagini del sistema.

- Per IDSM-2, ricreare l'immagine della partizione applicativa dalla partizione di manutenzione.Per la procedura, consultare la sezione Installazione dell'immagine del sistema IDSM-2 in Aggiornamento, downgrade e installazione delle immagini del sistema.
- Per AIP-SSM, ricreare l'immagine dall'ASA utilizzando il comando **hw-module 1 recovery [configure | boot]**.Per la procedura, consultare la sezione Installazione dell'immagine del sistema AIP-SSM in Aggiornamento, downgrade e installazione delle immagini del sistema.

Informazioni correlate

- Pagina di supporto di Cisco Intrusion Prevention System
- Aggiornamento, downgrade e installazione delle immagini del sistema per IPS 6.0
- Pagina di supporto del modulo Cisco Catalyst serie 6500 Intrusion Detection System (IDSM-2)
- Procedura di recupero della password per i Cisco IDS Sensor e IDS Services Module (1, IDSM-2)
- Risoluzione dei problemi relativi agli aggiornamenti della firma automatica
- Documentazione e supporto tecnico – Cisco Systems