Upgrade von Image und Signature IDS 4.1 auf IPS 5.0 und höher (AIP-SSM, NM-IDS, IDSM-2) - Konfigurationsbeispiel

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie das Image und die Signatur der Cisco Intrusion Detection Sensor (IDS)-Software von Version 4.1 auf das Cisco Intrusion Prevention System (IPS) 5.0 und höher aktualisieren.

Hinweis: Von der Softwareversion 5.x und höher ersetzt Cisco IPS das Cisco IDS, das bis zur Version 4.1 gültig ist.

Hinweis: Der Sensor kann keine Software-Updates von Cisco.com herunterladen. Sie müssen die Software-Updates von Cisco.com auf Ihren FTP-Server herunterladen und anschließend den Sensor konfigurieren, um sie von Ihrem FTP-Server herunterzuladen.

Das Verfahren finden Sie im Abschnitt Installation des AIP-SSM-Systemabbilds im Abschnitt Upgrading, Downgrade and Installing System Images (Aktualisierung, Downgrade und Installieren von Systemabbildern).

Weitere Informationen zur Wiederherstellung der Cisco IDS Sensor- und IDS Services-Module (IDSM-1, IDSM-2) und der Module für die Versionen 3.x und 4.x finden Sie unter Password Recovery Procedure for the Cisco IDS Sensor and IDS Services Modules (IDSM-1, IDSM-2).

Hinweis: Der Benutzerdatenverkehr wird während des Upgrades in der **Inline- und Fail-Open-**Einstellung auf ASA - AIP-SSM nicht beeinträchtigt.

Hinweis: Im Abschnitt Upgrade der Cisco IPS-Software von 5.1 auf 6.x unter Konfigurieren des Cisco Intrusion Prevention System-Sensors mithilfe der Befehlszeilenschnittstelle 6.0 finden Sie weitere Informationen zum Upgrade von IPS 5.1 auf Version 6.x.

Hinweis: Der Sensor unterstützt keine Proxyserver für automatische Updates. Die Proxyeinstellungen gelten nur für die Funktion "Global Correlation".

Voraussetzungen

Anforderungen

Die mindestens erforderliche Softwareversion für ein Upgrade auf 5.0 ist 4.1(1).

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco IDS-Hardware der Serie 4200, auf der Softwareversion 4.1 ausgeführt wird (auf Version 5.0 aktualisiert werden muss).

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Konfiguration

In diesem Abschnitt erfahren Sie, wie Sie die in diesem Dokument beschriebenen Funktionen konfigurieren können.

Das Upgrade von Cisco 4.1 auf 5.0 steht als Download von Cisco.com zur Verfügung. Informationen zum Zugriff auf IPS-Software-Downloads finden Sie unter Erhalten der Cisco IPS-Software auf Cisco.com.

Sie können eine der folgenden Methoden verwenden, um das Upgrade durchzuführen:

- Nachdem Sie die 5.0-Aktualisierungsdatei heruntergeladen haben, lesen Sie die Readme-Datei, um zu erfahren, wie Sie die 5.0-Aktualisierungsdatei mit dem Befehl **upgrade** installieren. Weitere Informationen finden Sie im Abschnitt Aktualisierungsbefehl verwenden in diesem Dokument.
- Wenn Sie die automatische Aktualisierung für Ihren Sensor konfiguriert haben, kopieren Sie die Upgrade-Datei für 5.0 in das Verzeichnis auf dem Server, auf dem der Sensor eine Abfrage nach Updates ausführt. Weitere Informationen finden Sie im Abschnitt Auto-Upgrade-

Befehl verwenden dieses Dokuments.
- Wenn Sie ein Upgrade auf Ihrem Sensor installieren und der Sensor nach dem Neustart nicht mehr verwendbar ist, müssen Sie das Image Ihres Sensors erneut erstellen. Bei einem Upgrade eines Sensors von einer Cisco IDS-Version vor 4.1 müssen Sie außerdem den **Befehl "restore"** oder die Wiederherstellungs-/Upgrade-CD verwenden. Weitere Informationen finden Sie im Abschnitt Re-Image des Sensors in diesem Dokument.

Aktualisieren des Sensors

In diesen Abschnitten wird erklärt, wie Sie mit dem **Upgrade-**Befehl die Software auf dem Sensor aktualisieren:

Übersicht

Sie können den Sensor mit diesen Dateien aktualisieren, die alle die Erweiterung .pkg haben:

- Signatur-Updates, z. B. IPS-sig-S150-minreq-5.0-1.pkg
- Signature-Engine-Updates, z. B. IPS-engine-E2-req-6.0-1.pkg
- Wichtigste Updates, z. B. IPS-K9-maj-6.0-1-pkg
- Kleinere Updates, z. B. IPS-K9-min-5.1-1.pkg
- Service Pack-Updates, z. B. IPS-K9-sp-5.0-2.pkg
- Aktualisierte Wiederherstellungspartitionen, z. B. IPS-K9-r-1.1-a-5.0-1.pkg
- Patch-Versionen, z. B. IPS-K9-Patch-6.0-1p1-E1.pkg
- Aktualisierte Wiederherstellungspartitionen, z. B. IPS-K9-r-1.1-a-6.0-1.pkg

Bei einem Sensor-Upgrade wird die Softwareversion des Sensors geändert.

Befehl und Optionen zum Aktualisieren

Verwenden Sie den Befehl **auto-upgrade-option enabled** im Service-Host-Submodus, um automatische Upgrades zu konfigurieren.

Diese Optionen gelten für:

- **default**: Setzt den Wert auf die Standardeinstellung des Systems zurück.
- **directory**: Verzeichnis, in dem sich Aktualisierungsdateien auf dem Dateiserver befinden.
- **file-copy-protocol** - Dateikopierprotokoll zum Herunterladen von Dateien vom Dateiserver. Die gültigen Werte sind **ftp** oder **scp**.**Hinweis:** Wenn Sie SCP verwenden, müssen Sie den Befehl **ssh host-key** verwenden, um den Server der Liste der bekannten SSH-Hosts hinzuzufügen, damit der Sensor über SSH mit ihm kommunizieren kann. Das Verfahren finden Sie unter Hinzufügen von Hosts zur Liste bekannter Hosts.
- **ip-address**: IP-Adresse des Dateiservers.
- **password** - Benutzerkennwort für die Authentifizierung auf dem Dateiserver.
- **schedule-option**: Zeitplanung bei automatischen Upgrades. Die Kalenderplanung startet Upgrades zu bestimmten Zeiten an bestimmten Tagen. Die regelmäßige Planung startet

Upgrades in bestimmten regelmäßigen Abständen.**Kalender-Scheduler** - Konfiguriert die Wochentage und Tageszeiten, an denen automatische Upgrades durchgeführt werden.**Wochentage**: Wochentage, an denen automatische Upgrades durchgeführt werden. Sie können mehrere Tage auswählen. Sonntag bis Samstag sind die gültigen Werte.**no** - Entfernt eine Eingabe- oder Auswahleinstellung.**times-of-Day** (Zeiten des Tages, an dem die automatischen Upgrades beginnen) Sie können mehrere Male auswählen. Der gültige Wert ist hh:mm[:ss].**periodischer Zeitplan** - Konfiguriert die Zeit, in der das erste automatische Upgrade durchgeführt werden soll, und die Wartezeit zwischen automatischen Upgrades.**interval** - Die Anzahl der Stunden, die zwischen automatischen Upgrades gewartet werden. Gültige Werte sind 0 bis 8760.**start-time** (Startzeit): Die Uhrzeit, zu der die erste automatische Aktualisierung gestartet wird. Der gültige Wert ist hh:mm[:ss].

- **user-name** (Benutzername): Benutzername für die Authentifizierung auf dem Dateiserver.

Informationen zum IDM-Verfahren zum Aktualisieren des Sensors finden Sie unter Aktualisieren des Sensors.

Verwenden des Befehls Upgrade

Sie erhalten SNMP-Fehler, wenn Sie vor dem Upgrade auf IPS 6.0 nicht über die Parameter **Read-Only Community** und **Read-Write-Community** verfügen. Wenn Sie SNMP-**set** und/oder **get**-Funktionen verwenden, müssen Sie vor dem Upgrade auf IPS 6.0 die **Read-Only-Community** und **Lese-Schreib-Community**-Parameter konfigurieren. In IPS 5.x wurde die **schreibgeschützte Community** standardmäßig auf "public" (Öffentlich) und die **Lese-/Schreib-Community** standardmäßig auf "private" (Privat) festgelegt. In IPS 6.0 haben diese beiden Optionen keine Standardwerte. Wenn Sie beispielsweise **für** SNMP **get** and **sets** mit IPS 5.x nicht verwendet haben, wurde enable-set-get auf false festgelegt, dann besteht kein Problem beim Upgrade auf IPS 6.0. Wenn Sie SNMP **erhalten** und mit IPS 5.x **festlegen**, wurde enable-set-get beispielsweise auf true festgelegt, müssen Sie die **schreibgeschützten Community-** und **Lese-Schreib-Community-**Parameter auf bestimmte Werte konfigurieren oder das IPS 6.0-Upgrade schlägt fehl.

Sie erhalten diese Fehlermeldung:

```
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.
```

Hinweis: IPS 6.0 verweigert standardmäßig Ereignisse mit hohem Risiko. Dies ist eine Änderung von IPS 5.x. Um den Standardwert zu ändern, erstellen Sie eine Ereignisaktionsüberschrift für die Inline-Aktion "deny Packet", und konfigurieren Sie sie so, dass sie deaktiviert wird. Wenn dem Administrator die Lese- und Schreibgemeinschaft nicht bekannt ist, sollte er versuchen, SNMP vollständig zu deaktivieren, bevor ein Upgrade durchgeführt wird, um diese Fehlermeldung zu entfernen.

Führen Sie die folgenden Schritte aus, um den Sensor zu aktualisieren:

1. Laden Sie die Hauptaktualisierungsdatei (IPS-K9-maj-5.0-1-S149.rpm.pkg) auf einen FTP-, SCP-, HTTP- oder HTTPS-Server herunter, auf den Sie von Ihrem Sensor zugreifen können.Unter Erhalten der Cisco IPS-Software finden Sie Informationen zum Suchen von Software auf Cisco.com.**Hinweis:** Sie müssen sich bei Cisco.com über ein Konto mit kryptografischen Berechtigungen anmelden, um die Datei herunterzuladen. Ändern Sie den Dateinamen nicht. Sie müssen den ursprünglichen Dateinamen beibehalten, damit der Sensor die Aktualisierung akzeptiert.**Hinweis:** Ändern Sie den Dateinamen nicht. Sie müssen

den ursprünglichen Dateinamen beibehalten, damit der Sensor die Aktualisierung akzeptiert.
2. Melden Sie sich mit einem Konto mit Administratorrechten bei der CLI an.
3. Rufen Sie den Konfigurationsmodus auf:
```
sensor#configure terminal
```

4. Aktualisieren Sie den Sensor:
```
sensor(config)#upgrade scp://
```

Beispiel:Hinweis: Dieser Befehl ist aus räumlichen Gründen auf zwei Zeilen beschränkt.
```
sensor(config)#upgrade scp://tester@10.1.1.1//upgrade/
IPS-K9-maj-5.0-1-S149.rpm.pkg
```

Hinweis: Eine Liste der unterstützten FTP- und HTTP/HTTPS-Server finden Sie unter Unterstützte FTP- und HTTP/HTTPS-Server. Unter Hinzufügen von Hosts zur Liste der bekannten SSH-Hosts finden Sie weitere Informationen zum Hinzufügen des SCP-Servers zur Liste der bekannten SSH-Hosts.
5. Geben Sie bei Aufforderung das Kennwort ein:
```
Enter password: ********
Re-enter password: ********
```
6. Geben Sie **yes** ein, um das Upgrade abzuschließen.**Hinweis:** Wichtige Updates, kleinere Updates und Service Packs können einen Neustart der IPS-Prozesse erzwingen oder sogar einen Neustart des Sensors erzwingen, um die Installation abzuschließen. Es besteht also eine Unterbrechung des Service für mindestens zwei Minuten. Signatur-Updates erfordern jedoch keinen Neustart, nachdem die Aktualisierung abgeschlossen ist. Unter Signature-Updates herunterladen (nur registrierte Kunden) finden Sie die aktuellsten Updates.
7. Überprüfen Sie Ihre neue Sensorversion:
```
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#
```

Hinweis: Für IPS 5.x erhalten Sie eine Meldung, dass das Upgrade von unbekannter Art ist. Sie können diese Nachricht ignorieren.**Hinweis:** Das Betriebssystem wird neu erstellt und alle Dateien, die über das Dienstkonto auf dem Sensor gespeichert wurden, werden entfernt.

Unter Aktualisieren des Sensors finden Sie weitere Informationen zum IDM-Verfahren für das Upgrade des Sensors.

Konfigurieren automatischer Upgrades

Automatische Upgrades

Sie können den Sensor so konfigurieren, dass er automatisch nach neuen Upgrade-Dateien im Upgrade-Verzeichnis sucht. Beispielsweise können mehrere Sensoren auf dasselbe FTP-Serververzeichnis mit unterschiedlichen Aktualisierungsplänen verweisen, z. B. alle 24 Stunden oder Montag, Mittwoch und Freitag um 23:00 Uhr.

Sie geben diese Informationen an, um automatische Upgrades zu planen:

- Server-IP-Adresse
- Pfad des Verzeichnisses auf dem Dateiserver, in dem der Sensor nach Aktualisierungsdateien sucht
- File Copy Protocol (SCP oder FTP)
- Benutzername und Kennwort
- Upgrade-Zeitplan

Sie müssen das Software-Upgrade von Cisco.com herunterladen und in das Upgrade-Verzeichnis kopieren, bevor der Sensor automatische Upgrades abfragen kann.

Hinweis: Wenn Sie ein automatisches Upgrade mit AIM-IPS und anderen IPS-Appliances oder -Modulen durchführen, stellen Sie sicher, dass Sie sowohl die 6.0(1)-Upgrade-Datei IPS-K9-6.0-1-E1.pkg als auch die AIM-IPS-Upgrade-Datei IPS-AIM-K9-6.0-4-E1.pkg auf dem automatischen IPServer zur Verfügung stellen. S kann korrekt erkennen, welche Datei automatisch heruntergeladen und installiert werden muss. Wenn Sie nur die 6.0(1)-Aktualisierungsdatei IPS-K9-6.0-1-E1.pkg auf den automatischen Aktualisierungsserver legen, lädt AIM-IPS die Datei herunter und versucht sie zu installieren, was die falsche Datei für AIM-IPS ist.

Unter Automatisches Aktualisieren des Sensors finden Sie weitere Informationen zum IDM-Verfahren für das automatische Upgrade des Sensors.

Auto-Upgrade-Befehl verwenden

Informationen zu den Befehlen für **automatische Updates finden Sie** im Abschnitt Upgrade-Befehl und -Optionen dieses Dokuments.

Gehen Sie wie folgt vor, um automatische Upgrades zu planen:

1. Melden Sie sich bei der CLI mit einem Konto an, das über Administratorrechte verfügt.
2. Konfigurieren Sie den Sensor, um automatisch nach neuen Upgrades in Ihrem Upgrade-Verzeichnis zu suchen.
   ```
   sensor#configure terminal
   sensor(config)#service host
   sensor(config-hos)#auto-upgrade-option enabled
   ```
3. Angeben der Planung:Für die Kalenderplanung, die Upgrades zu bestimmten Zeiten an bestimmten Tagen startet:
   ```
   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
   ```

   Für die periodische Planung, bei der Upgrades in bestimmten regelmäßigen Abständen gestartet werden:
   ```
   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. Geben Sie die IP-Adresse des Dateiservers an:
   ```
   sensor(config-hos-ena-per)#exit
   sensor(config-hos-ena)#ip-address 10.1.1.1
   ```
5. Geben Sie das Verzeichnis an, in dem sich die Aktualisierungsdateien auf dem Dateiserver befinden:
   ```
   sensor(config-hos-ena)#directory /tftpboot/update/5.0_dummy_updates
   ```
6. Geben Sie den Benutzernamen für die Authentifizierung auf dem Dateiserver an:
   ```
   sensor(config-hos-ena)#user-name tester
   ```
7. Geben Sie das Kennwort des Benutzers an:
   ```
   sensor(config-hos-ena)#password

   Enter password[]: ******
   Re-enter password: ******
   ```
8. Geben Sie das Dateiserverprotokoll an:
   ```
   sensor(config-hos-ena)#file-copy-protocol ftp
   ```

   Hinweis: Wenn Sie SCP verwenden, müssen Sie den Befehl **ssh host-key** verwenden, um den Server der Liste der bekannten SSH-Hosts hinzuzufügen, damit der Sensor über SSH mit ihm kommunizieren kann. Das Verfahren finden Sie unter Hinzufügen von Hosts zur Liste bekannter Hosts.

9. Überprüfen Sie die Einstellungen:

```
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. Beenden Sie den Submodus Auto-Upgrade:

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

Apply Changes:?[yes]:
```

11. Drücken Sie die **Eingabetaste**, um die Änderungen anzuwenden oder **no** einzugeben, um sie zu verwerfen.

Erneutes Abbild des Sensors

Sie haben folgende Möglichkeiten, ein neues Bild Ihres Sensors zu erstellen:

- Für IDS-Appliances mit einem CD-ROM-Laufwerk verwenden Sie die Wiederherstellungs-/Upgrade-CD.Das Verfahren finden Sie im Abschnitt Verwenden der Wiederherstellungs-/Upgrade-CDs Upgrading, Downgrading and Installing System Images (Aktualisierung, Downgrade und Installieren von Systemabbildern).
- Verwenden Sie für alle Sensoren den Befehl **restore**.Weitere Informationen finden Sie im Abschnitt Wiederherstellen der Anwendungspartition unter Aktualisieren, Downgraden und Installieren von Systembildern.
- Verwenden Sie für IDS-4215, IPS-4240 und IPS 4255 ROMMON, um das Systemabbild

wiederherzustellen.In den Abschnitten Installation des IDS-4215-Systemabbilds und Installation des IPS-4240- und IPS-4255-Systemabbilds unter Upgrading, Downgrade und Installieren von Systemabbildern finden Sie die erforderlichen Schritte.
- Verwenden Sie für NM-CIDS den Bootloader.Das Verfahren finden Sie im Abschnitt Installation des NM-CIDS-Systemabbilds unter Aktualisieren, Downgraden und Installieren von Systemabbildern.
- Für IDSM-2 müssen Sie die Anwendungspartition von der Wartungspartition neu abbilden.Weitere Informationen finden Sie im Abschnitt Installation des IDSM-2-Systemabbilds im Abschnitt Upgrading, Downgrade and Installing System Images (Aktualisieren, Downgrade und Installieren von Systemabbildern).
- Für AIP-SSM erstellen Sie mithilfe des **hw-module-Moduls 1** ein neues Image von der ASA **[konfigurieren | boot]**-Befehl.Das Verfahren finden Sie im Abschnitt Installation des AIP-SSM-Systemabbilds im Abschnitt Upgrading, Downgrade and Installing System Images (Aktualisierung, Downgrade und Installieren von Systemabbildern).

Zugehörige Informationen

- Support-Seite für das Cisco Intrusion Prevention System
- Aktualisieren, Downgrade und Installieren von Systemabbildern für IPS 6.0
- Modulunterstützung für das Cisco Catalyst Intrusion Detection System (IDSM-2) der Serie 6500
- Verfahren zur Kennwortwiederherstellung für Cisco IDS-Sensor und IDS-Dienstmodule 1, IDSM-2
- Fehlerbehebung bei Updates für automatische Signaturen
- Technischer Support und Dokumentation für Cisco Systeme