Exemplo de Configuração de Upgrade do IDS de Imagem e Assinatura 4.1 para IPS 5.0 e Posterior (AIP-SSM, NM-IDS, IDSM-2)

Contents

Introdução

Este documento descreve como atualizar a imagem e a assinatura do software Cisco Intrusion Detection Sensor (IDS) da versão 4.1 para o Cisco Intrusion Prevention System (IPS) 5.0 e posterior.

Observação: a partir da versão 5.x e posterior do software, o Cisco IPS substitui o Cisco IDS, que é aplicável até a versão 4.1.

Observação: o sensor não pode baixar atualizações de software de Cisco.com. Você deve baixar as atualizações de software de Cisco.com para o servidor FTP e, em seguida, configurar o sensor para baixá-las do servidor FTP.

Consulte a seção Instalando a Imagem de Sistema do AIP-SSM de Fazendo Upgrades e Downgrades e Instalando Imagens de Sistema para saber como proceder.

Consulte o Procedimento de Recuperação de Senhas para o Cisco IDS Sensor e os IDS Services Modules (IDSM-1, IDSM-2) para obter mais informações sobre como recuperar o Cisco Secure IDS (antigo NetRanger) Appliance e os módulos das versões 3.x e 4.x.

Observação: o tráfego do usuário não é afetado durante a atualização na configuração inline e fail-open no ASA - AIP-SSM.

Observação: consulte a seção Atualização do Cisco IPS Software de 5.1 para 6.x de Configuração do Cisco Intrusion Prevention System Sensor Usando a Command Line Interface 6.0 para obter mais informações sobre o procedimento de atualização do IPS 5.1 para a versão 6.x.

Observação: o sensor não suporta servidores proxy para atualizações automáticas. As configurações de proxy são somente para o recurso Correlação global.

Pré-requisitos

Requisitos

A versão mínima do software necessária para o upgrade para a versão 5.0 é a 4.1(1).

Componentes Utilizados

As informações deste documento são baseadas no hardware Cisco 4200 Series IDS com a versão 4.1 do software (para upgrade para a versão 5.0).

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

A atualização do Cisco 4.1 para 5.0 está disponível para download em Cisco.com. Consulte Obtendo o Software IPS da Cisco para saber como acessar os downloads do Software IPS em Cisco.com.

Você pode usar qualquer um dos métodos relacionados aqui para executar a atualização:

- Após fazer o download do arquivo de upgrade para a versão 5.0, consulte o arquivo Readme para saber como instalar o arquivo de upgrade para a versão 5.0 com o comando upgrade. Consulte a seção Uso do Comando Upgrade deste documento para obter mais informações.

- Se você configurou a atualização automática para seu sensor, copie o arquivo de upgrade para a versão 5.0 para o diretório no servidor em que seu sensor procura as atualizações. Consulte a seção Uso do Comando Auto-Upgrade deste documento para obter mais informações.
- Se você instalar uma atualização em seu sensor e não for possível utilizá-lo após a reinicialização, será necessário reaplicar a imagem no sensor. Um upgrade de um sensor de qualquer versão de Cisco IDS anterior à 4.1 também necessita que você use o comando recover no CD de recuperação/atualização. Consulte a seção Reaplicação da Imagem no Sensor deste documento para obter mais informações.

Upgrade do Sensor

Estas seções explicam como usar o comando upgrade para atualizar o software no sensor:

Overview

Você pode fazer o upgrade do sensor com os seguintes arquivos, todos eles com a extensão .pkg:

- Atualizações de assinatura, por exemplo, IPS-sig-S150-minreq-5.0-1.pkg
- Atualizações do mecanismo de assinatura, por exemplo, IPS-engine-E2-req-6.0-1.pkg
- Atualizações importantes, por exemplo, IPS-K9-maj-6.0-1-pkg
- Atualizações secundárias, por exemplo, IPS-K9-min-5.1-1.pkg
- Atualizações de Service Packs, por exemplo, IPS-K9-sp-5.0-2.pkg
- Atualizações de partição de recuperação, por exemplo, IPS-K9-r-1.1-a-5.0-1.pkg
- Versões de patch, por exemplo, IPS-K9-patch-6.0-1p1-E1.pkg
- Atualizações de partição de recuperação, por exemplo, IPS-K9-r-1.1-a-6.0-1.pkg

O upgrade do sensor altera a versão do software do sensor.

Comando e Opções de Upgrade

Use o comando autoupgrade-option enabled no submodo de host de serviço para configurar upgrades automáticos.

As seguintes opções se aplicam:

- default — Define o valor de volta para a configuração padrão do sistema.
- directory — Diretório em que os arquivos de upgrade estão localizados no servidor de arquivos.
- file-copy-protocol — Protocolo de cópia de arquivos usado para baixar arquivos do servidor de arquivos. Os valores válidos são ftp ou scp.

  Nota:Se você usa o SCP, é necessário usar o comando ssh host-key para adicionar o servidor à lista de hosts conhecidos pelo SSH para que o sensor possa se comunicar com ele via SSH. Consulte Adicionando Hosts à Lista de Hosts Conhecidos para saber como proceder.
- ip-address — O endereço IP do servidor de arquivos.
- password — Senha de usuário para autenticação no servidor de arquivos.
- schedule-option — Agenda quando os upgrades automáticos ocorrem. O agendamento de calendário inicia os upgrades em horários e dias específicos. O agendamento periódico inicia os upgrades em intervalos periódicos específicos.
  - calendar-schedule — Configura os dias da semana e as horas do dia em que os upgrades automáticos são executados.
    - days-of-week — Dias da semana em que os upgrades automáticos são executados. É possível selecionar vários dias. Domingo a sábado são valores válidos.
    - no — Remove uma entrada ou configuração de seleção.
    - times-of-day — As horas do dia em que as atualizações automáticas são iniciadas. É possível selecionar vários horários. O formato válido é hh:mm[:ss].
  - periodic-schedule — Configura a hora em que a primeira atualização automática deve ocorrer e o tempo decorrido entre upgrades automáticos sucessivos.
    - interval — O número de horas decorridas entre upgrades automáticos. Os valores válidos são de 0 a 8760.
    - start-time — A hora do dia em que o primeiro upgrade automático é iniciado. O formato válido é hh:mm[:ss].
- user-name — O nome de usuário para autenticação no servidor de arquivos.

Para obter o procedimento IDM para atualizar o sensor, consulte Atualizando o sensor.

Uso do Comando Upgrade

Você receberá erros de SNMP se não tiver os parâmetros read-only-community e read-write-community configurados antes da atualização para o IPS 6.0. Se estiver usando os recursos set e/ou get do SNMP, você deve configurar os parâmetros read-only-community e read-write-community antes de atualizar para o IPS 6.0. No IPS 5.x, a comunidade somente leitura foi definida como pública por padrão, e a comunidade de leitura e gravação foi definida como privada por padrão. No IPS 6.0, essas duas opções não têm valores padrão. Se você não usou gets e sets SNMP com IPS 5.x, por exemplo, enable-set-get foi definido como falso, então não há problema para atualizar para IPS 6.0. Se você usou gets e sets SNMP com IPS 5.x, por exemplo, enable-set-get foi definido como verdadeiro, você deve configurar os parâmetros read-only-community e read-write-community para valores específicos ou a atualização do IPS 6.0 falhará.

Você recebe esta mensagem de erro:

```
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.
```

Observação: o IPS 6.0 nega eventos de alto risco por padrão. Esta é uma alteração do IPS 5.x. Para alterar o padrão, crie uma substituição de ação de evento para a ação em linha deny packet e configure-a para ser desativada. Se o administrador não estiver ciente da comunidade de leitura e gravação, ele deve tentar desabilitar completamente o SNMP antes de fazer uma tentativa de atualização para remover essa mensagem de erro.

Conclua estas etapas para fazer o upgrade do sensor:

1. Baixe o arquivo de atualização importante (IPS-K9-maj-5.0-1-S149.rpm.pkg) para um servidor FTP, SCP, HTTP ou HTTPS que possa ser acessado pelo seu sensor.

   Consulte Obtendo o Cisco IPS Software para saber como encontrar software no site Cisco.com.

   Nota:É necessário fazer login no site Cisco.com usando uma conta com privilégios criptográficos para baixar o arquivo. Não altere o nome do arquivo. Você deve preservar o nome de arquivo original para que o sensor aceite a atualização.

   Observação: não altere o nome do arquivo. Você deve preservar o nome de arquivo original para que o sensor aceite a atualização.

2. Faça logon na CLI usando uma conta com privilégios de administrador.

3. Entre no modo de configuração:

   <#root>

   ```
   sensor#
   ```

   configure terminal

4. Faça o upgrade do sensor:

<#root>

```
sensor(config)#
upgrade scp://
```

@

//upgrade/

Exemplo:

Nota:Este comando é mostrado em duas linhas por questões de espaço.

<#root>

```
sensor(config)#
upgrade scp://tester@10.1.1.1//upgrade/
IPS-K9-maj-5.0-1-S149.rpm.pkg
```

Observação: consulte Servidores FTP e HTTP/HTTPS Suportados para obter uma lista de servidores FTP e HTTP/HTTPS suportados. Consulte Adicionando hosts à lista de hosts conhecidos SSH para obter mais informações sobre como adicionar o servidor SCP à lista

de hosts conhecidos SSH.

5. Insira a senha quando avisado:

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

6. Digite yes para concluir o upgrade.

   Nota:As atualizações importantes e secundárias e os Service Packs podem forçar o reinício dos processos do IPS ou até mesmo uma reinicialização do sensor para concluir a instalação. Assim, há uma interrupção dos serviços por pelo menos dois minutos. No entanto, as atualizações de assinatura não necessitam de reinicialização após a conclusão. Consulte Download de Atualizações de Assinatura (somente clientes registrados) para obter as atualizações mais recentes.

7. Verifique a nova versão do seu sensor:

```
<#root>

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#
```

Observação: para o IPS 5.x, você recebe uma mensagem que indica que a atualização é de tipo desconhecido. Você pode ignorar esta mensagem.

Observação: o sistema operacional é recriado e todos os arquivos que foram colocados no sensor através da conta de serviço são removidos.

Consulte Atualizando o sensor para obter mais informações sobre o procedimento IDM para a atualização do sensor.

Configurando atualizações automáticas

Atualizações automáticas

Você pode configurar o sensor para procurar novos arquivos de atualização no diretório de atualização automaticamente. Por exemplo, vários sensores podem apontar para o mesmo diretório de servidor FTP remoto com diferentes programações de atualização, como a cada 24 horas, ou segunda, quarta e sexta às 23h.

Você especifica estas informações para programar atualizações automáticas:

- Endereço IP do servidor
- Caminho do diretório no servidor de arquivos onde o sensor verifica se há arquivos de atualização
- Protocolo de cópia de arquivo (SCP ou FTP)
- Nome de usuário e senha
- Agenda de atualização

Você deve fazer o download da atualização de software de Cisco.com e copiá-la para o diretório

de atualização antes que o sensor possa pesquisar atualizações automáticas.

Observação: se você usar a atualização automática com o AIM-IPS e outros dispositivos ou módulos IPS, certifique-se de colocar o arquivo de atualização do 6.0(1), IPS-K9-6.0-1-E1.pkg, e o arquivo de atualização do AIM-IPS, IPS-AIM-K9-6.0-4-E1.pkg, no servidor de atualização automática para que o AIM-IPS possa detectar corretamente qual arquivo precisa ser baixado e instalado automaticamente. Se você colocar apenas o arquivo de atualização do 6.0(1), IPS-K9-6.0-1-E1.pkg, no servidor de atualização automática, o AIM-IPS fará o download e tentará instalá-lo, que é o arquivo incorreto para o AIM-IPS.

Consulte Atualizando o sensor automaticamente para obter mais informações sobre o procedimento IDM para a atualização automática do sensor.

Uso do Comando Auto-Upgrade

Consulte a seção Comando e Opções de Upgrade deste documento para obter os comandos de auto-update.

Conclua estes passos para agendar upgrades automáticos:

1. Faça login na CLI com uma conta que tenha privilégios de administrador.
2. Configure o sensor para procurar automaticamente por novas atualizações em seu diretório de atualização.

```
<#root>

sensor#

configure terminal

sensor(config)#

service host

sensor(config-hos)#

auto-upgrade-option enabled
```

3. Especifique o agendamento:
   - Para o agendamento de calendário, o qual inicia os upgrades em horas e dias específicos:

```
<#root>

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
```

- Para o agendamento periódico, o qual inicia os upgrades em intervalos periódicos específicos:

```
<#root>
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. Especifique o endereço IP do servidor de arquivos:

```
<#root>
sensor(config-hos-ena-per)#
exit
sensor(config-hos-ena)#
ip-address 10.1.1.1
```

5. Especifique o diretório em que os arquivos de upgrade estão localizados no servidor de arquivos:

```
<#root>
sensor(config-hos-ena)#
directory /tftpboot/update/5.0_dummy_updates
```

6. Especifique o nome de usuário para autenticação no servidor de arquivos:

```
<#root>
```

```
sensor(config-hos-ena)#
user-name tester
```

7. Especifique a senha do usuário:

```
<#root>
sensor(config-hos-ena)#
password

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

8. Especifique o protocolo do servidor de arquivos:

```
<#root>
sensor(config-hos-ena)#
file-copy-protocol ftp
```

Observação: Se você usar o SCP, deverá usar o comando ssh host-key para adicionar o servidor à lista de hosts conhecidos SSH para que o Sensor possa se comunicar com ele através do SSH. Consulte Adicionando Hosts à Lista de Hosts Conhecidos para saber como proceder.

9. Verifique as configurações:

```
<#root>
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. Saia do submodo de upgrade automático:

    <#root>

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

    Apply Changes:?
    [yes]:
    ```

11. Pressione Enter para aplicar as alterações ou digite no para descartá-las.

Reaplicação da Imagem no Sensor

Você pode reaplicar a imagem no sensor destas formas:

- Para IDS Appliances com unidade de CD-ROM, use o CD de recuperação/upgrade.

  Consulte a seção Usando o CD de Recuperação/Upgrade de Fazendo Upgrades e Downgrades e Instalando Imagens de Sistema para saber como proceder.

- Para todos os sensores, use o comando recover.

  Consulte a seção Recuperando a Partição de Aplicativos de Fazendo Upgrades e Downgrades e Instalando Imagens de Sistema para saber como proceder.

- Para o IDS-4215, IPS-4240 e IPS 4255, use o ROMMON para restaurar a imagem do sistema.

  Consulte as seções Instalando a Imagem de Sistema do IDS-4215 e Instalando a Imagem de Sistema do IPS-4240 e do IPS-4255 de Fazendo Upgrades e Downgrades e Instalando Imagens de Sistema para saber como proceder.

- Para o NM-CIDS, use o bootloader.

  Consulte a seção Instalando a Imagem de Sistema do NM-CIDS de Fazendo Upgrades e Downgrades e Instalando Imagens de Sistema para saber como proceder.

- Para o IDSM-2, reaplique a partição de aplicativos via partição de manutenção.

  Consulte a seção Instalando a Imagem de Sistema do IDSM-2 de Fazendo Upgrades e Downgrades e Instalando Imagens de Sistema para saber como proceder.

- Para AIP-SSM, recrie a imagem do ASA usando o hw-module module 1 recover [configure | boot].

  Consulte a seção Instalando a Imagem de Sistema do AIP-SSM de Fazendo Upgrades e Downgrades e Instalando Imagens de Sistema para saber como proceder.

Informações Relacionadas

- Página de suporte do Sistema de prevenção de intrusão da Cisco
- Atualizando, baixando e instalando imagens do sistema para IPS 6.0
- Página de suporte do módulo Sistema de detecção de intrusão Cisco Catalyst 6500 Series (IDSM-2)
- Procedimento de recuperação de senha para o Cisco IDS Sensor e IDS Services Modules 1, IDSM-2)
- Troubleshooting de Atualizações de Assinatura Automática
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.