IDS 4.0/AIP-SSM/IPS 5.0 e FAQ mais atrasado

Índice

Introdução

Este documento responde mais frequentemente às perguntas feitas (FAQ) relativas ao Cisco Secure Intrusion Detection System (IDS) 4.0, inspeção avançada e módulo de Serviços de segurança da prevenção (AIP SS), e Sistema de prevenção de intrusões da Cisco (IPS) 5.0 e mais atrasado.

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

IDS 4.0

Q. Eu instalei IDS MC e SecMon sobre um server novo e agora eu quero ao import all configurações (usuário, dispositivo, e assim por diante) do server velho ao novo. Como eu faço este?

A. A maneira a mais fácil de executar isto é trazer acima seu servidor VMS novo, e descobre então os sensores com esta caixa nova.

Nota: Quando você adiciona o sensor, não o adicionar manualmente. Verifique a caixa dos **ajustes da descoberta**.

Uma vez que o sensor é descoberto, importe-o no **SecMon**. Todas as configurações salvar no sensor. Os ajustes da assinatura, filtros, e assim por diante devem vir transversalmente depois que você constrói seu server novo. Certifique-se de você a atualização IDS MC às assinaturas as mais atrasadas.

Q. O IDS-4215 recebe o `idsPackageMgr: Mensagem de Erro do argumento inválido` quando tentar promover a separação da recuperação IDS. Que eu preciso de fazer para resolver esta edição?

A. Este é um problema de fabricação. Alguns clientes receberam IDS-4215 com uma imagem de base ruim (4.0). Termine estas etapas.

1. Transfira a imagem de partição de recuperação (clientes registrados somente).

2. Aplique a elevação da imagem de partição de recuperação com o CLI: `sensor#configure terminal sensor(config)#upgrade METHOD://USERNAME@SERVER/PATH/ IDS-4215-K9-r-1.1-a-4.1-1-S47.tar.pkg`
3. Uma vez que a imagem de partição de recuperação é aplicada, os 4215 estão restaurados a uma base do 4.1(1) 4215 da execução normal. `sensor(config)#recover application-partition`

Q. Quando eu promovo de um 2-digit aos sig 3-digit nivele pacotes, tais como S100 ou mais tarde, por exemplo, 4.1(4)S99 a 4.1(4)S100, a funcionalidade da atualização automática falha. Como posso corrigir este problema?

Nota: Cisco VMS e clientes CLI não experimenta esta edição.

A causa do problema é a lógica de classificação que é usada quando o nome de arquivo é analisado gramaticalmente. É um tipo alfanumérico quando deve ser numérico. A ação alternativa é usar o CLI (ou o VMS) para promover aos pacotes do nível dos sig 3-digit, tais como S100 ou mais tarde. Uma vez que isto é terminado, a atualização automática começa a funcionar outra vez. Refira a identificação de bug Cisco CSCef07999 (clientes registrados somente) para mais informação.

Q. O que faz do `"o erro da manipulação token de autenticação".` meio do Mensagem de Erro?

A. A fim resolver esta edição, use a senha padrão (Cisco) duas vezes e mude então a senha do modo de configuração. O IDS exige a senha padrão ser incorporado duas vezes.

Por exemplo:

```
login:cisco
Password:cisco
Enter current password:cisco
Enter new password: ***
Re-enter new password: ***
```

Q. Como eu removo o IDSM do interruptor?

A. O módulo deve ser removido somente depois que você desabilita a potência. Conclua estes passos:

1. Do sensor CLI, emita o comando do **powerdown da restauração**.
2. Uma vez que o sensor termina a parada programada, do interruptor CLI, edição ou **nenhuma potência permita o** comando do **módulo (module_number)** para o Cisco IOS ou a **potência do módulo do grupo para baixo (module_number)** comanda para Cactos.
3. Pressione o botão da parada programada na lâmina.
4. Põe fisicamente para baixo o chassi. Quando a luz de status indica um verde mais longo, você pode remover o módulo de forma segura.

IPS 5.0 e mais atrasado

Q. Eu tenho evitar configurado mas eu sou confundido sobre como configurar a obstrução nas assinaturas. Que é a diferença entre o host do bloco e a conexão do

bloco?

A. O host do bloco obstrui todos os pacotes desse endereço de origem. A conexão do bloco obstrui somente a uma conexão baseada na fonte e no destino IP/port. O PIX trabalha em uma maneira levemente diferente. Para automático evita, o sensor envia o IP da fonte, o IP de destino, a porta de origem, e a porta do destino. O PIX obstrui todos os pacotes que originam desse endereço IP de Um ou Mais Servidores Cisco ICM NT. A informação adicional é usada pelo PIX para remover essa uma conexão de suas tabelas de conexão. Se a conexão não foi removida da tabela de conexão, a seguir é teoricamente possível que se evitar é removido shortly after é aplicado, a seguir a conexão original não pôde ter cronometrado para fora ainda. Isto permite que o atacante continue o ataque na conexão original. A remoção da conexão da tabela assegura-se de que a conexão original não possa ser usada para continuar o ataque depois que evitar é removido. O sensor não pode evitar uma conexão única no PIX porque o PIX não apoia o uso do **comando shun** a fim evitar uma conexão única. **O comando shun** PIX evita sempre o endereço de origem apesar de mesmo se a informação de conexão adicional esteja fornecida.

Q. O que faz o **"erro: Não podia reiniciar os serviços de rede. O erro fatal ocorreu. O nó DEVE ser recarregado para permitir o alarme".** meio do Mensagem de Erro?

A. Este erro significa que seu gateway padrão é incorreto ou um Mensagem de Erro genérico que signifique que o IP, o netmask, ou o gateway padrão estão incorretos. `O fatal` parte da mensagem significa que após a primeira falha, a configuração precedente era aplicada e igualmente falhada. O sensor emite configuração se e os **comandos route** e esse ou os ambos eles falham.

Q. Autoupdate falha com o **erro de HTTP response:500" do errSystemError "mainApp[343] Cid/E.** mensagem de erro. Que este Mensagem de Erro significa?

A. Esta edição pôde ser a auto característica da atualização, que não trabalha, porque é ajustada para transferir mesmo em uma hora. Tente ajustar a auto atualização a um tempo aleatório; mesmo um offset pequeno de oito ou os minutos da noite podem fixar este problema.

Geralmente, a edição é resolved e o `erro: resposta de erro de HTTP: 500 que o` Mensagem de Erro é sejam vistos se você muda o tempo de recuperação a um limite NON-de hora em hora.

Nota: O IPS falha a atualização automática das assinaturas e retorna com este Mensagem de Erro:

```
Exceção de AutoUpdate: Name=errSystemError falhado conexão de HTTP [1,110]
```

Verifique estes artigos a fim resolver esta edição:

- Verifique se um Firewall está impedindo o sensor do cisco.com de alcance.
- Verifique se distribuir se transforma uma edição.
- Verifique se o NATing é configurado corretamente no dispositivo de gateway para o dispositivo de downstream.
- Verifique se as credenciais do usuário estão corretas.
- Mude as horas inicial da atualização às horas impares.

Q. O que faz o **"erro: execUpgradeSoftware: AnalysisEngine é atualmente ocupado e incapaz de processar esta atualização. Espere por favor diversos minutos antes de tentar a atualização**

outra vez.”. meio do Mensagem de Erro?

A. A fim resolver esta edição, tente recarregar o sensor ou a nova imagem o sensor.

Q. Como faço eu resolva o **aviso do** Mensagem de Erro **Cid/W - o DNS ou o proxy HTTP são exigidos para a inspeção global e a reputação da correlação que filtram mas nenhum DNS ou servidor proxy são definidos. Adicionar um servidor proxy ou o servidor DNS HTTP na configuração de serviço do “host”**?

A. Termine estas tarefas a fim resolver esta edição:

- Desabilite a correlação global.
- Adicionar a configuração do proxy/dns.

Q. Como faço eu resolva estes erros que o IPS recebe para problemas de saúde globais da correlação: “**23Jan2010 15:50:39.831 38.001 atualização global da correlação collaborationApp[655] rep/E A falhou: Não abrem uma conexão TLS ao Server do HTTP em X.X.82.127:443: Conexão TLS falhada**” e “**atualização global da correlação collaborationApp[459] rep/E A falhada: Falha de download de ibrs/1.1/drop/default/1296529950: URI não contém um endereço IP válido**”?

A. O IPS é incapaz de obter ao Internet devido a uma questão de porta, por exemplo, um Firewall em um trajeto que não tenha as portas direitas abertas para o acesso ao Internet ou nele pode ser uma edição NAT.

Para que a correlação global funcione completamente, o sensor contacta primeiramente através dos https **update-manifests.ironport.com** a fim autenticar o usuário e uma conexão de HTTP transferir então atualizações do GC. Os arquivos que as transferências do sensor do HTTP (updates.ironport.com) são os dados da reputação que a correlação global usa. Os https update-manifests.ironport.com devem sempre resolver ao endereço X.X.82.127, mas o **endereço IP de Um ou Mais Servidores Cisco ICM NT** HTTP updates.ironport.com **pode mudar**, que depende do Internet que você alcança. Assim você deve verificar o endereço IP de Um ou Mais Servidores Cisco ICM NT. Se a Filtragem URL é permitida, adicionar uma exceção para o IP da relação do Gerenciamento de IPS no filtro URL, de modo que o IPS possa conectar ao Internet.

Este erro ocorre quando há uma corrupção em uma atualização precedente do GC:

```
atualização global da correlação collaborationApp[459] rep/E A falhada: Falha de download de
ibrs/1.1/drop/default/1296529950: O URI não contém um endereço IP válido
```

Esta edição pode geralmente ser corrigida desligando o serviço do GC e então girando o para trás sobre. No IDM, escolha a **configuração > as políticas > correlação > inspeção/reputação globais**, ajuste a inspeção global da correlação (e a **reputação que filtra** se **sobre**) a **fora**, aplique as mudanças, espere os minutos 10, gire as características sobre, e monitore-as.

Q. **A atualização global da correlação A falhada: openConnection: IpAddrException travado que badAddrString. Incapaz de usar o proxy HTTP global da correlação e ajustes DNS. Verifique a conexão e a tentativa outra vez.** o Mensagem de Erro é recebido da “na categoria da falha da atualização reputação”. Como eu resolvo esse problema?

A. Verifique estes artigos:

- Você deve ter uma licença válida IPS a fim permitir que as características globais da correlação funcionem.
- Você deve ter um servidor proxy HTTP ou um servidor DNS configurado a fim permitir que as características globais da correlação funcionem.
- Porque as atualizações globais da correlação ocorrem através da interface de gerenciamento do sensor, os Firewall devem permitir o tráfego tcp 443/80 e UDP 53.
- Certifique-se que seu sensor apoia as características globais da correlação. Se você não quer este, desabilite a característica global da Colaboração do IDM:Vão à **configuração** > às **políticas** > a **correlação** > a **inspeção/reputação globais**, e ajustam a inspeção global da correlação (e a reputação que filtra se **sobre**) a **fora**.

Q. Como faço eu resolva **"a atualização global da correlação falhada: openConnection:** Erro **badAddrString travado de IpAddrException"** que o IPS recebe para o problema de saúde global da correlação?

A. Se você usa a correlação global (GC) então certifique-se de que a resolução de nome trabalha, por exemplo, o DNS é alcançável. Igualmente verifique se há um porto bloqueado 53 do Firewall. Se não, você pode desligar a característica do GC se você deseja obter livrado desta mensagem.

Q. Como eu resolvo a **exceção ao inicializar a conexão ao** Mensagem de Erro de **MySQL** que eu recebo quando eu lanço IME do navegador?

A. Esta edição ocorrer geralmente quando tentativa do cliente de executar IME em sistemas operacionais unsupported, tais como Windows 7.

Q. Como faço eu resolva o **"título: IDM no vendedor 88-nsmc-c1: Cisco Systems, Inc. Categoria: Os recursos do FRASCO do erro do arquivo do lançamento no arquivo JNLP não são assinados pelo mesmo certificado". ou "erro que conecta ao sensor, não são criados o sensor x.x.x.x:443 que retira** erro do **idm"** que o IDM recebe, que acontece durante o lançamento do aplicativo?

A. Cancele o cache de navegador a fim resolver esta edição.

Q. É o modo assimétrico no IPS configurável se você usa o GUI?

A. Na versão 6.0, modo assimétrico no IPS que é configurável usando o CLI somente e não disponível no GUI. Mas, na versão 6.1 esta característica está igualmente disponível no GUI.

Q. Como eu resolvo a edição da latência com o sensor IPS?

A. A fim resolver esta edição, permita o modo assimétrico que processa a fim permitir que o sensor sincronize o estado com o fluxo e mantenha a inspeção para aqueles motores que não exigem ambos sentidos. Use esta configuração:

```
IPS_Sensor#configure terminal IPS_Sensor(config)#service analysis-engine IPS_Sensor(config-
ana)#virtual-sensor vs0 IPS_Sensor(config-ana-vir)#inline-TCP-evasion-protection-mode asymmetric
```

A edição da latência ocorrer quando a ação da negação inline e negar o pacote é permitida para cada assinatura em VS0. Permitir todas as assinaturas conduzirá à latência como o IPS inspeciona cada pacote único que passa completamente. É bom permitir somente a assinatura

específica exigida conforme o fluxo de tráfego de rede a fim resolver a edição da latência.

Q. AIP-SSM ajuda a obstruir Skype?

A. O PIX/ASA não pode obstruir o tráfego do skype. Skype tem a capacidade negociar portas dinâmica, e usar o tráfego criptografado. Com tráfego criptografado, é virtualmente impossível detectá-lo porque não há nenhum teste padrão a procurar.

Você poderia eventualmente usar um ips Cisco (sistema) da prevenção de intrusão /AIP-SSM. Tem algumas assinaturas que podem detectar um cliente de Windows Skype que conecte a Skype o server para sincronizar sua versão. Isto é feito geralmente quando o cliente é iniciado a conexão. Quando o sensor pegara a conexão inicial de Skype, você pode poder encontrar a pessoa que usa o serviço, e obstrui todas as conexões iniciadas de seu endereço IP de Um ou Mais Servidores Cisco ICM NT.

Q. Por que faz o `flap de` detecção da relação ou vão frequentemente ao estado inativo no IPS?

A. Durante uma atualização de assinatura e reconfigurações, as paradas do sensorApp para processar pacotes como ela processam as assinaturas novas na atualização. O driver de rede detecta que o sensorApp parou e puxa todos os pacotes novos do buffer. Assim o driver de rede faz coisas diferentes, que depende da configuração e do modelo do sensor:

Relação promíscuo — Traz o link para baixo nas relações, e traz o apoio do link uma vez que o sensorApp começa monitorar outra vez.

Relação Inline ou pares Inline de Vlan — Depende do ajuste do desvio:

- **Automóvel do desvio** — O direcionador mantém o link ascendente e começa a passar completamente pacotes sem análise. Reverte então de volta a enviar os pacotes através do sensorApp uma vez que o sensorApp começa monitorar outra vez.
- **Desvio fora** — O direcionador traz o link para baixo nas relações, que reage o mesmo que do modo misturado, e trá-las alternativas uma vez que o sensorApp começa monitorar outra vez.

Assim, se o app do sensor não puxa pacotes do buffer, que ocorre possivelmente porque não há nenhuma relação configurada para processar pacotes, a seguir o direcionador pode pôr a relação em um `estado inativo`.

Estes logs são considerados quando a relação de detecção bate:

```
28Jun2011 09:03:09.483 6050.885 interface[409] Cid/W errWarning Inline
    databypass has started.
28Jun2011 09:03:13.639 4.156 interface[409] Cid/W errWarning Inline databypass
    has stopped.
28Jun2011 09:19:23.922 970.283 interface[409] Cid/W errWarning Inline databypass
    has started.
28Jun2011 09:19:27.486 3.564 interface[409] Cid/W errWarning Inline databypass
    has stopped.
```

Q. O sensor IDS ou de Intrusion Prevention System (IPS) mantém uma história da senha?

A. Não, o sensor não mantém uma história da senha. As senhas não são visualizável a qualquer hora.

Q. O sensor IDS ou de Intrusion Prevention System (IPS) apoia o servidor de SYSLOG para enviar logs?

A. Não.

Q. Que é o limite máximo de armazenar eventos no IPS?

A. O evento local do sensor armazena somente o 30 MB e começa a overwrite uma vez que o limite do 30 MB é alcançado. Este limite é não-configurável.

Q. Como eu escrevo uma assinatura para detectar o [a-z] do foto \ arquivo do .zip em algum email entrante ou que parte?

A. Use o STRING.TCP a fim escrever uma assinatura que detecte o acessório. Procure algo similar a este:

```
Engine STRING.TCP
Enabled True
Severity informational
AlarmThrottle Summarize
CapturePacket False
Direction ToService
MinHits 1
Protocol =TCP
RegexString [Ff][Ii][Ll][Ee][Nn][Aa][Mm][Ee][=]["][Ff][Oo]
             [Tt][Oo][a-zA-Z][.][Zz][Ii][Pp]["]
ResetAfterIdle 15
ServicePorts 25
StorageKey =STREAM
```

Q. Como você configura o intervalo do cliente de FTP?

A. Execute estes comandos:

```
configure terminal
service host
networkParams
ftpTimeout 300 <timeout is in seconds>
```

Q. Como você converte as horas inicial e as termina tempo no iplog-estado a um formato legível?

A. Esta saída é uma representação decimal das horas atual desde o UNIX epoc. Use uma Calculadora UNIX epoc tal como essa encontrada no local da calculadora da data/hora de UNIX. Incorpore os primeiros dígitos 10 porque esta calculadora é granulada somente aos segundos, e os IDS armazena nanossegundo. Isto significa que os últimos nove dígitos estão descascados. Desde o início tempo nesta saída, `1084798479 = segunda-feira o 17 de maio 12:54:39 2004 (GMT)` são o que você recebe.

Do CLI, incorpore o iplog-**estado** a fim receber esta saída:

```
"
Log ID:             138343946
IP Address:         xxx.xxx.xxx.xxx
Group:              0
Status:             completed
```

Start Time: 1084798479512524000 End Time: 1084798510136582000 Bytes Captured: 2833 Packets Captured: 14 "

Q. **O "IOException quando tentativa para obter o certificado: java.security.cert.CertificateExpiredException".** é exibida a mensagem de erro. Como isto pode ser resolved?

A. A fim resolver este Mensagem de Erro, início de uma sessão no AIP-SSM e emitir o comando da gerar-chave dos tls no modo de exec privilegiado segundo as indicações deste exemplo:

```
sensor#tls generate-key
```

Nota: Esta definição de usar a gerar-chave dos tls do comando igualmente resolve a introdução de AIP-SSM que não pode conectar ao IME.

Q. **O "IOException: Conexão recusada: conecte. O server IME IME não está respondendo. Verifique por favor se está executando o"** Mensagem de Erro aparece quando eu adicionar o IPS em IME. Como pode esta edição ser resolved?

A. A fim resolver este Mensagem de Erro, escolha o **> serviços do Control Panel > das ferramentas administrativas** e reinicie serviços IME.

Q. **Não poderia verificar que** Mensagem de Erro do **[IOException - connect timed out] username/senha da configuração** está recebida quando eu adiciono um sensor IPS ao IME. Como pode esta edição ser resolved?

A. Isto indica uma comunicação quebrada entre o IME e o sensor IPS. Certifique-se de que não há nenhum software que obstrui o SDEE.

Q. **A "resposta de erro do server IME: Erro desconhecido (arquivo de registro da verificação no diretório do log da instalação)".** é exibida a mensagem de erro. Como pode esta edição ser resolved?

A. A fim resolver este Mensagem de Erro, verifique que o endereço IP de Um ou Mais Servidores Cisco ICM NT correto está usado quando você adiciona o IPS em IME e igualmente verifica todo o firewall de software que está sendo executado no computador IME, que pode obstruir a conexão.

Q. Pode o sensor IDS ou de Intrusion Prevention System (IPS) enviar alertas do email?

A. O sensor de IDS não tem a capacidade para enviar alertas do email no seus próprios. O monitor da Segurança quando usado com IDS tem a capacidade para enviar notificações de Email quando uma regra do evento é provocada pelo sensor.

Consulte para configurar notificações de E-mail para obter mais informações sobre de como configurar notificações de Email com monitor da Segurança.

O gerente do ips Cisco expresso (IME) pode ser configurado para enviar a mensagem da notificação de Email (alertas) quando as regras do evento são provocadas por sensores do ips

Cisco. Refira IPS 6.X e mais tarde: Notificações de Email usando o exemplo de configuração IME para mais informação.

Q. `O erro: Não pode comunicar-se com o mainApp (getVersion). Contacte por favor seu administrador de sistema.` o Mensagem de Erro aparece quando eu tento conectar a meu sensor. Como pode esta edição ser resolved?

A. Recarregue o sensor a fim resolver esta edição.

Q. `O aviso: AVISO: Recursos insuficientes disponíveis para combinar todos os regexes feitos sob encomenda atualmente ativos. Alguns alertas não atearão fogo. As assinaturas reservadas Consider até esta mensagem já não ocorrem.` o Mensagem de Erro aparece assinatura que ajusta em meu sensor. Como pode esta edição ser resolved?

A. Aposente-se as assinaturas que não são dentro uso a fim resolver esta edição e igualmente o número de assinaturas do cliente com regexes deve ser reduzido. Também, não se recomenda usar-se ***** e **+** metacharacters nos regexes.

Q. Por que as edições da latência ocorrem em sensores do Sistema de prevenção de intrusões da Cisco (IPS)? Como pode esta edição ser resolved?

A. A edição da latência pode ocorrer devido ao roteamento assimétrico. Tente desabilitar a assinatura 1330 a fim resolver esta edição.

Q. É possível desabilitar SSHv1 e deixar somente o SSHv2 permitido nos sensores do Sistema de prevenção de intrusões da Cisco (IPS)?

A. Agora não é possível desabilitar SSHv1 e deixar somente SSHv2 permitido. SSHv1 e SSHv2 são permitidos junto e não podem ser desabilitados individualmente.

Q. `O erro: Um erro ocorreu no sensor durante a atualização, mensagem do sensor = a atualização exige 115000 KB em /usr/cids/idsRoot/var, lá tem somente 110443 KB disponível.` a mensagem aparece quando eu promovo o sensor à versão 4.1(5). Como pode esta edição ser resolved?

A. Este Mensagem de Erro ocorre devido à memória insuficiente no sensor.

Termine estas tarefas a fim resolver esta edição:

1. Log na conta de serviço e na raiz tornada
2. Remova os seguintes diretórios como mostrado abaixo: `# rm -rf /usr/cids/idsRoot/var/updates/files/S69`
   ```
   # rm -rf /usr/cids/idsRoot/var/updates/files/common
   # rm /usr/cids/idsRoot/var/virtualSensor/*
   # rm /usr/cids/idsRoot/var/.tmp/*
   ```
3. Tente agora promover o sensor. Refira a identificação de bug Cisco CSCsb81288 (clientes registrados somente) para mais informação.

Q. Eu obtenho o `erro mainApp[396] cplane/E - o atendimento do accept() retornou o`

Mensagem de Erro `-1 no` fazer logon ASA. Como pode este erro ser resolved?

A. `O erro mainApp[396] cplane/E - o atendimento do accept() retornou o` Mensagem de Erro `-1` indica que o servidor de Web não pode ler o arquivo, e o programa do accept() falhado, que rende descritores de arquivo quando as conexões TLS existem. Mas este arquivo não é precisado para o comportamento normal. É inofensivo.

Q. Como faço eu resolva o `errTransport WebSession tls/W:: exceção da conexão TLS do sessionTask:` Mensagem de Erro `incompleto do aperto de mão`?

A. Este Mensagem de Erro indica que o certificado é já não válido no módulo. Siga estas etapas para resolver o problema:

1. Regenere o certificado do CLI:Entre à linha de comando do sensor.Emita os **tls gerenciem o** comando, e pressionam-no **entram**. Note as impressões digitais que são indicadas.
2. Puxe o certificado novo dentro para IME:Abra o IME e encontre o nome do sensor na lista no Home Page.Clicar com o botão direito o sensor, e o clique **edita**.Quando você alcança a tela de dispositivo da edição, clique a **APROVAÇÃO**. Contorneie todo o aviso sobre não poder recuperar o tempo do sensor.Você será alertado com o Security Certificate novo (esse que você apenas gerou). Verifique para certificar-se que as impressões digitais combinam, e clicam **sim**.Após diversos segundos, o sensor deve mostrar “conectado” no estado do evento outra vez.

Q. Quando eu tento entrar ao IPS, eu recebo este Mensagem de Erro: `errSystemError-ct-sensorAPP.450 que não responde, clientpipe falhado.` Como eu posso solucionar esse erro?

A. A fim resolver este erro, use o comando reset a fim recarregar o IPS.

Q. O tempo em AIP-SSM difere do tempo na ferramenta de segurança adaptável de Cisco (ASA). Como pode esta edição ser resolved?

A. A fim resolver esta edição, use o servidor de NTP para sincronizar o tempo na Segurança adaptável Appliance(ASA) e AIP-SSM de Cisco.

Refira configurar o NTP em sensores IPS para mais informação.

Q. Como posso eu aplicar sensores virtuais múltiplos em AIP-SSM?

A. Os sensores virtuais em AIP-SSM não podem ser aplicados pela relação porque o AIP-SSM tem somente uma relação. Quando você cria sensores virtuais múltiplos, você deve atribuir esta relação a somente um sensor virtual. Você não precisa de designar uma relação para os outros sensores virtuais.

Depois que você cria sensores virtuais, você deve traçá-los a um contexto de segurança na ferramenta de segurança adaptável (ASA) que usa o comando atribuir-**IP**. Você pode traçar muitos contextos de segurança a muitos sensores virtuais. Refira os *sensores virtuais de atribuição à* seção *adaptável dos contextos da ferramenta de segurança de* configurar AIP-SSM para mais informação.

Q. Que é o número máximo de sensores virtuais apoiados por AIP-SSM?

A. Um número máximo de quatro sensores virtuais pode ser apoiado.

Q. Se eu me uso o SSH ou o IDM a fim entrar ao IPS a seguir são ele possível configurar o IPS 4240/IDSM/IDSM2 a fim validar usuários administrativos contra um server RADIUS/TACACS+?

A. Não é possível com um server TACACS+ mas o RAIO é apoiado da liberação IPS 7.0.(4)E4. Refira as seções *novas e da informação alterada* e das *limitações e das limitações dos* Release Note para o Sistema de prevenção de intrusões da Cisco 7.0(4)E4 para mais informação. Também, refira IPS 7.X: Autenticação de login de usuário usando ACS 5.X como o exemplo da configuração de servidor RADIUS para uma configuração de exemplo.

Q. Que é o impacto da licença expirada no funcationality IPS?

A. O único impacto que uma licença expirada tem no sensor é que para as atualizações de assinatura.

Q. As atualizações de assinatura IPS têm um impacto nos serviços ou na conectividade de rede?

A. Não. As atualizações de assinatura IPS não têm um impacto nos serviços ou na conectividade de rede.

Q. Que é a URL que exata eu preciso de incorporar para que o módulo ips atualize automaticamente com as assinaturas as mais atrasadas?

A. O link exigido para permitir que o módulo ips atualize automaticamente com a assinatura a mais atrasada é: https://198.133.219.25/cgi-bin/front.x/ida/locator/locator.pl.

Você deve usar seu usuário de Cisco - identificação e senha para terminar a atualização do módulo ips.

Nota: No trem 6.x do código, as atualizações automáticas do cisco.com não são apoiadas. Você deve manualmente transferir os arquivos de assinatura e aplicá-los ao sensor. Há uma função da atualização automática no código 6.x; contudo, isto é possível somente de um servidor de arquivo local em que os arquivos de assinatura devem manualmente ser transferidos também.

Q. O sensor IPS vulnerável à sessão da transmissão da porta X11 sequestra a vulnerabilidade?

A. Não. Não é vulnerável por estas razões:

- O sensor não tem as bibliotecas X11. Consequentemente não há nenhuma sessão a sequestrar.
- A transmissão da porta X11 não é permitida na configuração SSH.
- O IPv6 não é compilado no núcleo do sensor. Isto é exigido a fim explorar a vulnerabilidade.

Q. Por que o AIP-SSM não mostra nenhuns logs quando o ASA mostra a abundância de logs do aviso e do ataque?

A. Isto acontece porque quando o ASA obstrui algo, não é passado ao IPS para a inspeção duplicada. Consequentemente, você não pode ver que a duplicata entra o ASA e o IPS.

Q. Depois que um usuário distribui o grupo da assinatura S518, o "**invalidValue: O sig de Editng corda-XL-TCP não tem NENHUM efeito** Mensagem de Erro **n**esta versão" ocorre. Por quê?

A. Este é o Mensagem de Erro completo:

```
evError: eventId=1284051856322985135 vendor=Cisco severity=warning
  originator:
    hostId: vbintestids03
    appName: sensorApp
    appInstanceId: 700
  time: offset=-240 timeZone=GMT-05:00 1286305251136551000
errorMessage: name=errWarning invalidValue:Editing string-xl-tcp
sig 21619 has NO effect
```

Esta edição vem acima porque o motor corda-XL-TCP ou corda-TCP-XL não é apoiado no hardware. Para mais detalhes, refira os Release Note do motor E4 IPS.

Q. Quando eu atualizo automaticamente assinaturas em um ASA-SSM-10 com a auto característica da atualização, eu recebo este Mensagem de Erro: **Auto pacote não instalável da atualização encontrado no status=true do server.** Como resolvo esse problema?

A. Esta saída mostra o Mensagem de Erro completo:

```
autoUpgradeServerCheck:
    uri: https://XX.XX.XX.XX//cgi-bin/front.x/ida/locator/locator.pl
    packageFileName:
    result: No installable auto update package found on server  status=true
```

Este erro foi gerado e as assinaturas não atualizam automaticamente porque as atualizações da definição da assinatura após S479 exigem o motor E4. A fim resolver isto, você precisa de promover manualmente o sensor a 7.0(2)E4.

Nota: O sensor não pode promover-se automaticamente ao E4 porque exige 7.0(2) e uma repartição do sensor.

Q. O auto feauture da atualização no IPS 5.0 para o módulo NID não está trabalhando. Como resolvo esse problema?

A. Esta saída mostra o Mensagem de Erro completo:

```
autoUpgradeServerCheck:
    uri: ftp://hfcu-inet01@192.168.1.12//ips-update/
    packageFileName:
    result: No installable auto update package found on server  status=true
```

Esta edição ocorre devido a um estilo impróprio da listagem de diretórios com o servidor FTP. A fim resolver isto, comute listagens de diretórios do Unix-estilo das listagens de diretórios

existentes do estilo de MS-DOS.

A fim alterar os ajustes da listagem de diretórios, > arquivos de programa seleto do **começo > ferramentas administrativas** a fim abrir o gerente de serviços de Internet. Então vá à aba do diretório home e mude o estilo da listagem de diretórios de MS-DOS a UNIX.

Q. O IPS-4255 recebe o SensorApp falha em TcpRootNode:: Mensagem de Erro do expireNow() durante uma elevação. Como eu resolvo esse problema?

A. Esta edição é devido à falha do motor da análise e é endereçada na identificação de bug Cisco CSCtb39179 (clientes registrados somente). Promova o sensor à versão 7.0(4)E4 a fim fixar esta edição.

Q. Quando eu tentar executar uma atualização da licença depois que o purchanse l um novo licencia os relatórios do dispositivo este erro: **"Não atualizam a licença no sensor." o "errExpiredLicense-The que a licença nova expira data é mais velho do que a licença atual expira data."** Como resolvo esse problema?

A. Esta edição ocorre quando o arquivo de licença recebido é inválido. Para obter um arquivo da licença válida, entre ao cisco.com como um usuário registrado, e transfira o arquivo de licença apropriado. Uma vez que você obtém o arquivo da licença válida, instale-o em seu sensor.

Se você o instala o arquivo de licença novo e ainda receba um erro, pôde haver uma edição com o arquivo existente da licença inválida. A fim resolver esta edição, termine estas etapas para suprimir do arquivo existente da licença inválida:

1. Entre à conta de serviço datilografando seu nome de usuário da conta de serviço.Se você não tem uma conta de serviço, abra a linha de comando IPS, incorpore o modo de configuração, e incorpore este comando**senha senha do serviço do privilégio do** *nome* **username**
```
ciscoasa# session 1
Opening command session with slot 1.

Connected to slot 1. Escape character sequence is 'CTRL-^X'.
login:
Password:

IPS#
IPS#conf t
IPS(config)# username name privilege service password password
```
2. Uma vez que você entra a sua conta de serviço, inscreva o **comando su** a fim ir enraizar (usando a mesma senha que a conta de serviço).
3. Suprima dos arquivos no diretório de /usr/cids/idsRoot/shared/.**Nota:** Não suprima do arquivo host.conf.Incorpore o comando de **/usr/cids/idsRoot/shared/ do CD** a fim ir ao diretório compartilhado.Inscreva o **comando ls** a fim ver os arquivos no diretório.Incorpore o comando do *file_name do* **rm** a fim remover os arquivos.**Nota:** Não suprima do arquivo host.conf.
4. Incorpore o comando do **reinício de /etc/init.d/cids** reiniciar o sensor.
5. Instale a licença nova.

Um Bug da Cisco foi arquivado para endereçar este comportamento. Para mais informação, refira CSCtg76339 (clientes registrados somente).

Q. O que faz o **errorMessage: IpLog 1712041197 terminou devido adiantado faltar dos**

identificadores de arquivo. meio **name=ErrLimitExceeded do** Mensagem de Erro? Como eu resolvo esse problema?

A. Este erro é causado por uma quantidade excessiva de pacotes no registro IP. Desabilite os recursos de registro IP a fim resolver esta edição. O registro IP é significado pesquisando defeitos somente; Cisco recomenda que você não o permite para todas as assinaturas.

Q. Eu recebo este erro quando eu atualizo o sensor de s550 a s551: **Não pode analisar gramaticalmente o config. atual para o "signatureDefinition componente" e o exemplo "sig0".** Como resolvo esse problema?

A. A alteração da assinatura 23899.0 causa esta edição. Refira a identificação de bug Cisco CSCtn84552 (clientes registrados somente) para mais informação.

Q. Eu recebo este erro no sensor: **Erro: o autoUpdate selecionou com sucesso um pacote do serviço do localizador do cisco.com, contudo, transferência do pacote falhada: Não recebem a resposta HTTP.** Como resolvo esse problema?

A. Verifique se há Filtragem URL, filtragem de conteúdo, ou um presente do servidor proxy que esteja obstruindo o autoUpdate do acontecimento. Certifique-se de que autoUpdate não está sendo obstruído e igualmente verifique que as credenciais do usuário fornecidas estão corretas.

Q. Eu recebo esta mensagem de erro de XML no sensor IPS que é executado com versão 6.2(3)E4: **errorMessage: O IPS do software tentou redigir dados inválidos XML para (token). Os caráteres inválidos XML foram substituídos com "*".** Como resolvo esse problema?

A. Este comportamento foi endereçado pela identificação de bug Cisco CSCsq50873 (clientes registrados somente). Este é um problema cosmético e não cria nenhumas despesas gerais operacionais a não ser que a quantidade excessiva de logs que estão sendo recebidos. Uma solução temporária é remover a configuração relacionada NTP no sensor. Para uma solução permanente, elevação a uma versão em que este erro é fixo.

Q. Por que a estação de trabalho IME faz conexões constante aos server controlados apesar do cliente que está sendo fechado?

A. IME funciona como dois serviços de Windows e o cliente GUI. Quando o cliente é fechado, os dois serviços de Windows (gerente do ips Cisco expresso e MySQL-IME) continuam a executar e recolher eventos dos sensores controlados e a armazená-los no base de dados de MySQL local; isto permite o relatório histórico ocorrer.

O cliente IME deve abrir uma única assinatura SDEE ao sensor controlado, e reutiliza esta assinatura para a atividade subsequente da recuperação do evento. A Conectividade constante da estação de trabalho IME aos sensores controlados é comportamento esperado.

Q. Pode o módulo AIP-SSM ser usado como um alvo do PERÍODO?

A. Não. O módulo AIP-SSM não pode ser usado porque um alvo do PERÍODO como é usado para monitorar somente o tráfego que corre através da relação ASA.

Q. Por que o uso da alta utilização da CPU é observado depois que o IPS é promovido ao motor E3?

A. Com atualizações do motor E3, o IPS usa um algoritmo diferente controlando seu tempo ocioso e gasta mais votação do tempo para que os pacotes reduzam a latência. Isto verificação aumentada causa um aumento de correspondência no USO de CPU. A maneira correta medir o CPU no E3 é não pelo USO de CPU, mas pela **porcentagem da carga de pacote** que mostra a utilização CPU correta.

Q. Por que é o gerencio do LED de status da saúde VERMELHO intermitentemente em meu dispositivo IPS?

A. Isto podia acontecer devido a um certificado incorreto na estação remota do maanagement, a software running tal como CS-MARS, a CS, a IEV, a VMS-IDS/IPSMC, etc. a fim resolver esta edição, termina estas etapas:

1. Aplique o certificado TLS do sensor na estação de gerenciamento remota.
2. Configurar um server dos DN válidos.

Q. Como pode o IPS ser parado de atrasar o tráfego do HTTP ao atravessar suas relações?

A. Configurar o sensor para trabalhar no modo assimétrico resolverá a edição. A fim pôr o sensor na proteção assimétrica do modo, termine estas etapas:

1. Vá à **configuração** > às **políticas** > às **políticas IPS**.
2. Fazer duplo clique o **sensor virtual**.
3. Vá **avançar opções**.
4. Sob normalize o modo, selecionam a **proteção assimétrica do modo**.
5. Clique em **OK**.
6. Recarregue a unidade para que as mudanças tomem o efeito.

Informações Relacionadas

- Página segura do suporte de sistema da prevenção de intrusão de Cisco
- Pesquise defeitos AIP-SSM
- Field Notice de produto de segurança (que incluem a intrusion detection do CiscoSecure)
- Suporte Técnico e Documentação - Cisco Systems