IDS 4.0/AIP-SSM/IPS 5.0 e domande frequenti (FAQ) successive

Sommario

Introduzione

Questo documento risponde alle domande più frequenti (FAQ) relative a Cisco Secure Intrusion Detection System (IDS) 4.0, Advanced Inspection and Prevention Security Services Module (AIP SSM) e Cisco Intrusion Prevention System (IPS) 5.0 e versioni successive.

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

IDS 4.0

D. Dopo aver installato IDS MC e SecMon su un nuovo server, si desidera importare tutte le configurazioni (utente, dispositivo e così via) dal server precedente a quello nuovo. Come posso fare?

R. Il modo più semplice per eseguire questa operazione consiste nell'attivare il nuovo server VMS e quindi scoprire i sensori con questa nuova scatola.

Nota: non aggiungere il sensore manualmente. Selezionare la casella **impostazioni individuazione**.

Una volta individuato il sensore, importarlo in **SecMon**. Tutte le configurazioni vengono salvate sul sensore. Le impostazioni della firma, i filtri e così via dovrebbero essere visualizzati dopo la creazione del nuovo server. Assicurarsi di aggiornare IDS MC alle firme più recenti.

D. IDS-4215 riceve `idsPackageMgr:` messaggio di errore di `argomento non valido` durante il tentativo di aggiornare la partizione di ripristino IDS. Cosa devo fare per risolvere il problema?

R. Si tratta di un problema di produzione. Alcuni clienti hanno ricevuto IDS-4215s con un'immagine di base errata (4.0). Attenersi alla seguente procedura.

1. Scaricare l'immagine della partizione di ripristino (solo utenti registrati).
2. Applicare l'aggiornamento dell'immagine della partizione di ripristino dalla 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. Una volta applicata l'immagine della partizione di ripristino, lo switch 4215 viene ripristinato a una base normale in esecuzione 4.1(1) 4215.
```
sensor(config)#recover application-partition
```

D. Quando si esegue l'aggiornamento da pacchetti di livello di firma a 2 cifre a 3 cifre, ad esempio S100 o versioni successive, ad esempio da 4.1(4)S99 a 4.1(4)S100, la funzionalità di aggiornamento automatico non riesce. Come risolvere il problema?

Nota: i clienti Cisco VMS e CLI non riscontrano questo problema.

La causa del problema è la logica di ordinamento utilizzata quando si analizza il nome del file. Si tratta di un ordinamento alfanumerico quando deve essere numerico. La soluzione è utilizzare CLI (o VMS) per aggiornare i pacchetti a 3 cifre del livello di firma, come S100 o versioni successive. Al termine, l'aggiornamento automatico riprende a funzionare. per ulteriori informazioni, fare riferimento all'ID bug Cisco CSCef07999 (solo utenti registrati).

D. Qual è l'"Errore di modifica del token di autenticazione"? messaggio di errore?

R. Per risolvere il problema, usare due volte la password predefinita (cisco) e quindi modificare la password dalla modalità di configurazione. L'IDS richiede che la password predefinita sia immessa due volte.

Ad esempio:

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

D. Come rimuovere IDSM dallo switch?

R. Rimuovere il modulo solo dopo aver disattivato l'alimentazione. Attenersi alla seguente procedura:

1. Dalla CLI del sensore, usare il comando **reset powerdown**.
2. Una volta che il sensore ha completato lo spegnimento, dalla CLI dello switch, usare il comando **no power enable module (module_number)** per Cisco IOS o il comando **set module power down (module_number)** per CatOS.
3. Premere il pulsante di arresto sul pannello.
4. Spegnere fisicamente lo chassis. Quando la spia di stato è più verde, è possibile rimuovere il modulo in modo sicuro.

IPS 5.0 e versioni successive

D. La configurazione di shunning è stata eseguita, ma non è chiaro come configurare il blocco delle firme. Qual è la differenza tra l'host a blocchi e la connessione a blocchi?

R. Blocca l'host blocca tutti i pacchetti provenienti dall'indirizzo di origine specificato. Blocca connessione blocca solo una connessione in base all'indirizzo IP/porta di origine e di destinazione. Il PIX funziona in modo leggermente diverso. Per gli shun automatici, il sensore invia l'IP di origine, l'IP di destinazione, la porta di origine e la porta di destinazione. Il PIX blocca tutti i pacchetti provenienti da quell'indirizzo IP. Le informazioni aggiuntive vengono utilizzate dal PIX per rimuovere quella connessione dalle relative tabelle di connessione. Se la connessione non è stata rimossa dalla tabella delle connessioni, è possibile che, in teoria, se la connessione shun viene rimossa poco dopo l'applicazione, la connessione originale non sia ancora scaduta. Ciò consente all'autore dell'attacco di continuare l'attacco alla connessione originale. La rimozione della connessione dalla tabella garantisce che la connessione originale non possa essere utilizzata per continuare l'attacco dopo la rimozione dello shun. Il sensore non può evitare una singola connessione sul PIX perché il PIX non supporta l'uso del comando **shun** per evitare una singola connessione. Il comando PIX **shun** evita sempre l'indirizzo di origine, a prescindere dal fatto che vengano fornite o meno le informazioni aggiuntive sulla connessione.

D. Cosa fa il **"Errore: Impossibile riavviare i servizi di rete. Errore irreversibile. Il nodo DEVE essere riavviato per abilitare la modalità "allarmante".** messaggio di errore?

R. Questo errore indica che il gateway predefinito non è corretto o un messaggio di errore generico indica che l'indirizzo IP, la netmask o il gateway predefinito non sono corretti. La parte `Fatal` del messaggio indica che dopo il primo errore, la configurazione precedente è stata applicata ed è anche fallita. Il sensore emette i comandi **ifconfig** e **route** e uno o entrambi hanno esito negativo.

D. L'aggiornamento automatico non riesce con il messaggio di errore **"mainApp[343] Cid/E errSystemError http error response:500"**. Qual è il significato di questo messaggio di errore?

R. Questo problema potrebbe essere dovuto alla funzione di aggiornamento automatico, che non funziona, perché è impostata per il download a un'ora pari. Provare a impostare l'aggiornamento automatico su un tempo casuale; anche un piccolo offset di otto o minuti di notte può risolvere questo problema.

In generale, il problema è risolto e viene visualizzato il messaggio di `errore: risposta di errore http:` Se modificate il tempo di recupero in un limite non orario, viene visualizzato il messaggio di errore `500`.

Nota: IPS non esegue l'aggiornamento automatico delle firme e restituisce questo messaggio di errore:

```
Eccezione AutoUpdate: Connessione HTTP non riuscita [1,110] name=errSystemError
```

Per risolvere il problema, verificare quanto segue:

- Verificare se un firewall impedisce al sensore di raggiungere Cisco.com.
- Verificare se il routing diventa un problema.
- Verificare che NATing sia configurato correttamente sul dispositivo gateway per il dispositivo

downstream.
- Verificare che le credenziali utente siano corrette.
- Modificare l'ora di inizio dell'aggiornamento in ore dispari.

D. Cosa fa il **"Errore: Software execUpgrade: AnalysisEngine è attualmente occupato e non è in grado di elaborare l'aggiornamento. Attendere qualche minuto prima di tentare di nuovo l'aggiornamento."**. messaggio di errore

R. Per risolvere il problema, provare a ricaricare il sensore o a ricrearne l'immagine.

D. Come risolvere il messaggio di errore **Avviso Cid/W - Il proxy DNS o HTTP è necessario per l'ispezione della correlazione globale e il filtro della reputazione, ma non sono stati definiti server DNS o proxy.Aggiungere un server proxy HTTP o un server DNS nella configurazione del servizio 'host'**?

R. Per risolvere il problema, completare i seguenti task:

- Disabilita correlazione globale.
- Aggiungere la configurazione proxy/DNS.

D. Come risolvere gli errori ricevuti da IPS per i problemi di integrità della correlazione globale: "**23Jan2010 15:50:39.831 38.001 collaborationApp[655] rep/E Un aggiornamento della correlazione globale non è riuscito: Impossibile aprire una connessione TLS al server HTTP in X.X.82.127:443: Connessione TLS non riuscita**" e "**collaborationApp[459] rep/E Aggiornamento della correlazione globale non riuscito: Download di ibrs/1.1/drop/default/1296529950 non riuscito: L'URI non contiene un indirizzo IP valido**"?

R. IPS non è in grado di accedere a Internet a causa di un problema della porta, ad esempio un firewall in un percorso che non dispone delle porte corrette per l'accesso a Internet o può essere un problema NAT.

Affinché la correlazione globale funzioni completamente, il sensore contatta prima https **update-manifests.ironport.com** per autenticare l'utente e quindi una connessione HTTP per scaricare gli aggiornamenti GC. I file scaricati dal sensore dal sito HTTP (updates.ironport.com) sono i dati di reputazione utilizzati dalla correlazione globale. L'indirizzo https update-manifests.ironport.com deve sempre essere risolto nell'indirizzo X.X.82.127, ma l'indirizzo IP **updates.ironport.com** può cambiare, a seconda di Internet a cui si accede. Quindi è necessario controllare l'indirizzo IP. Se il filtro URL è abilitato, aggiungere un'eccezione per l'IP dell'interfaccia di gestione IPS nel filtro URL, in modo che IPS possa connettersi a Internet.

Questo errore si verifica in caso di danneggiamento in un precedente aggiornamento GC:

```
collaborationApp[459] rep/E Aggiornamento della correlazione globale non riuscito: Download di
ibrs/1.1/drop/default/1296529950 non riuscito: L'URI non contiene un indirizzo IP valido
```

Questo problema può in genere essere risolto disattivando e riattivando il servizio di catalogo globale. In IDM, scegliere **Configurazione > Criteri > Correlazione globale > Ispezione/Reputazione**, impostare Ispezione correlazione globale (e **Filtro reputazione** se **Attivato**) su **Disattivato**, applicare le modifiche, attendere 10 minuti, attivare le funzionalità e monitorare.

D. **Aggiornamento correlazione globale A non riuscito: apriConnessione: Rilevato IpAddrException**

badAddrString. Impossibile utilizzare il proxy HTTP di correlazione globale e le impostazioni DNS. Verificare la connessione e riprovare. Viene ricevuto un messaggio di errore nella categoria "Errore di aggiornamento reputazione". Come posso risolvere questo problema?

A. Verificare quanto segue:

- Per consentire il funzionamento delle funzionalità di correlazione globale, è necessario disporre di una licenza IPS valida.
- Per consentire il funzionamento delle funzionalità di correlazione globale, è necessario che sia configurato un server proxy HTTP o un server DNS.
- Poiché gli aggiornamenti di correlazione globale vengono eseguiti tramite l'interfaccia di gestione dei sensori, i firewall devono consentire il traffico tcp 443/80 e udp 53.
- Assicurati che il sensore supporti le funzioni di correlazione globale. In caso contrario, disattivare la funzionalità di collaborazione globale da IDM:Selezionare Configurazione > Criteri > Correlazione globale > Ispezione/Reputazione, quindi impostare Ispezione correlazione globale (e Filtro reputazione se attivato) su Disattivato.

D. Come risolvere il problema **"Aggiornamento di correlazione globale non riuscito: apriConnessione: Rilevato** errore **IpAddrException badAddrString"** ricevuto da IPS per un problema di integrità di correlazione globale.

R. Se si utilizza la correlazione globale (GC), verificare che la risoluzione dei nomi funzioni, ad esempio che il DNS sia raggiungibile. Verificare inoltre se è presente una porta 53 bloccata dal firewall. In caso contrario, è possibile disattivare la funzionalità GC per eliminare il messaggio.

D. Come risolvere l'**eccezione durante l'inizializzazione della connessione al** messaggio di errore **MySQL** ricevuto all'avvio dell'IME dal browser?

R. Questo problema si verifica in genere quando il cliente tenta di eseguire l'IME su sistemi operativi non supportati, ad esempio Windows 7.

D. Come risolvere il problema **" Titolo: IDM su 88-nsmc-c1 Fornitore: Cisco Systems, Inc. Categoria: Avvia errore file Le risorse JAR nel file JNLP non sono firmate con lo stesso certificato". o "Errore di connessione al sensore, Impossibile creare il sensore x.x.x:443 uscita da IDM"** errore ricevuto da IDM, che si verifica durante l'avvio dell'applicazione?

R. Per risolvere il problema, cancellare la cache del browser.

D. La modalità asimmetrica su IPS è configurabile se si utilizza la GUI?

R. Nella versione 6.0, modalità asimmetrica su IPS configurabile solo con CLI e non disponibile sulla GUI. Tuttavia, nella versione 6.1 questa funzione è disponibile anche nella GUI.

D. Come risolvere il problema di latenza con il sensore IPS?

R. Per risolvere il problema, abilitare l'elaborazione in modalità asimmetrica per consentire al sensore di sincronizzare lo stato con il flusso e mantenere l'ispezione per i motori che non

richiedono entrambe le direzioni. Utilizzare questa configurazione:

```
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
```

Il problema di latenza si verifica quando l'azione di negazione in linea e il pacchetto di negazione sono abilitati per ogni firma in VS0. L'abilitazione di tutte le firme determinerà una latenza quando IPS controlla ogni singolo pacchetto trasmesso. È consigliabile abilitare solo la firma specifica richiesta in base al flusso del traffico di rete per risolvere il problema di latenza.

D. AIP-SSM aiuta a bloccare Skype?

R. Il PIX/ASA non è in grado di bloccare il traffico Skype. Skype ha la capacità di negoziare porte dinamiche e di utilizzare traffico crittografato. Con il traffico crittografato, è virtualmente impossibile rilevarlo poiché non vi sono modelli da cercare.

Èpossibile infine utilizzare un Cisco IPS (Intrusion Prevention System)/AIP-SSM. Ha alcune firme che sono in grado di rilevare un client Windows Skype che si connette al server Skype per sincronizzarne la versione. Questa operazione viene in genere eseguita quando il client avvia la connessione. Quando il sensore rileva la connessione iniziale Skype, puoi trovare la persona che usa il servizio e bloccare tutte le connessioni avviate dal loro indirizzo IP.

D. Perché l'interfaccia di rilevamento `flap` o passa frequentemente allo stato down in IPS?

R. Durante un aggiornamento e una riconfigurazione della firma, sensorApp si interrompe per elaborare i pacchetti mentre elabora le nuove firme nell'aggiornamento. Il driver di rete rileva che sensorApp si è arrestato e preleva eventuali nuovi pacchetti dal buffer. Il driver di rete esegue diverse operazioni, che dipendono dalla configurazione e dal modello del sensore:

Interfaccia promiscua: abbassa il collegamento sulle interfacce e lo riattiva una volta che sensorApp ricomincia a monitorare.

Interfaccia inline o coppia di Vlan inline - Dipende dall'impostazione di Bypass:

- **Ignora auto (Bypass Auto)** - Il driver mantiene attivo il collegamento e inizia a passare i pacchetti senza eseguire l'analisi. Quindi torna a inviare i pacchetti tramite sensorApp quando sensorApp ricomincia a monitorare.
- **Bypass Off**: il driver disattiva il collegamento sulle interfacce, come nella modalità promiscua, e lo riattiva una volta che sensorApp ricomincia a monitorare.

Quindi, se l'app del sensore non preleva i pacchetti dal buffer, cosa che probabilmente accade perché non c'è un'interfaccia configurata per elaborare i pacchetti, il driver può mettere l'interfaccia in stato `down`.

I seguenti registri vengono visualizzati quando l'interfaccia di rilevamento lampeggia:

```
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.
```

D. Il sensore IDS o Intrusion Prevention System (IPS) conserva una cronologia delle password?

R. No, il sensore non conserva la cronologia delle password. Le password non sono visualizzabili in alcun momento.

D. Il sensore IDS o IPS (Intrusion Prevention System) supporta il server syslog per l'invio dei registri?

R. No.

D. Qual è il limite massimo di archiviazione degli eventi in IPS?

R. L'evento locale del sensore memorizza solo 30 MB e inizia a sovrascrivere se stesso una volta raggiunto il limite di 30 MB. Questo limite non è configurabile.

D. Come si scrive una firma per rilevare il file foto[a-z]\.zip nei messaggi di posta elettronica in arrivo o in uscita?

R. Utilizzare STRING.TCP per scrivere una firma che rilevi l'allegato. Cerca una soluzione simile alla seguente:

```
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
```

D. Come si configura il timeout del client FTP?

A. Utilizzare i seguenti comandi:

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

D. Come è possibile convertire l'ora di inizio e l'ora di fine nello stato iplog-status in un formato leggibile?

R. Questo output è una rappresentazione decimale dell'ora corrente dall'epoc UNIX. Utilizzare una calcolatrice epoc UNIX, ad esempio quella disponibile nel sito Calcolatrice data/ora UNIX . Immettere le prime 10 cifre perché la calcolatrice è granulare solo a secondi e IDS memorizza nanosecondi. Ciò significa che le ultime nove cifre vengono eliminate. Dall'ora di inizio in questo output, `1084798479 = lun 17 maggio 12:54:39 2004 (GMT)` è ciò che si riceve.

Dalla CLI, immettere **iplog-status** per ricevere questo output:

```
"
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
"
```

D. La **"IOException when try to get certificate: java.security.cert.CertificateExpiredException"** viene visualizzato un messaggio di errore. Come risolvere il problema?

A. Per risolvere questo messaggio di errore, accedere a AIP-SSM e usare il comando tls generate-key in modalità di esecuzione privilegiata, come mostrato nell'esempio:

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

Nota: questa risoluzione dell'uso del comando tls generate-key risolve anche il problema di AIP-SSM che non è in grado di connettersi all'IME.

D. La **"IOException: Connessione rifiutata: connessione. Il server IME non risponde. Verificare che sia in esecuzione"** viene visualizzato il messaggio di errore durante l'aggiunta di IPS in IME. Come risolvere il problema?

A. Per risolvere il problema, scegliere **Pannello di controllo > Strumenti di amministrazione > Servizi** e riavviare i servizi IME.

D. Il messaggio di errore **Impossibile verificare nome utente/password di configurazione[IOEXception - timeout connessione]** viene ricevuto quando si aggiunge un sensore IPS all'IME. Come risolvere il problema?

R. Indica una comunicazione interrotta tra l'IME e il sensore IPS. Assicurarsi che non vi sia software che blocchi il SDEE.

D. La **"Risposta di errore dal server IME: Unknown error (check log file in installation's log directory)" (Errore sconosciuto (verificare il file di log nella directory di log dell'installazione).** Viene visualizzato il messaggio di errore. Come risolvere il problema?

R. Per risolvere questo messaggio di errore, verificare che venga utilizzato l'indirizzo IP corretto quando si aggiungono gli indirizzi IP in IME e controllare anche eventuali firewall software in esecuzione sul computer IME che possano bloccare la connessione.

D. Il sensore IDS o Intrusion Prevention System (IPS) può inviare avvisi tramite e-mail?

R. Il sensore IDS non è in grado di inviare da solo avvisi e-mail. Quando utilizzato con IDS, Security Monitor consente di inviare notifiche tramite posta elettronica quando il sensore attiva una regola di evento.

Per ulteriori informazioni su come configurare le notifiche tramite posta elettronica con Security Monitor, fare riferimento a Configurazione delle notifiche tramite posta elettronica.

Èpossibile configurare Cisco IPS Manager Express (IME) per inviare il messaggio di notifica e-mail (avvisi) quando le regole degli eventi vengono attivate dai sensori Cisco IPS. Fare riferimento a IPS 6.X e versioni successive: Invia notifiche tramite posta elettronica utilizzando l'esempio di configurazione IME per ulteriori informazioni.

D. L'`errore: Impossibile comunicare con mainApp (getVersion). Contattare l'amministratore di sistema.` Quando si tenta di connettersi al sensore viene visualizzato un messaggio di errore. Come risolvere il problema?

R. Riavviare il sensore per risolvere il problema.

D. L'`avvertimento: AVVISO: Risorse insufficienti per combinare tutti i regex personalizzati attualmente attivi. Alcuni avvisi non verranno attivati. Si consiglia di ritirare le firme finché il messaggio non verrà più visualizzato.` viene visualizzato il messaggio di errore Signature tuning sul sensore. Come risolvere il problema?

R. Ritirare le firme non utilizzate per risolvere il problema e ridurre il numero di firme dei clienti con regex. Inoltre, si sconsiglia di utilizzare metacaratteri ***** e **+** nei regex.

D. Perché si verificano problemi di latenza sui sensori Cisco Intrusion Prevention System (IPS)? Come risolvere il problema?

R. Il problema della latenza può essere dovuto al routing asimmetrico. Per risolvere il problema, provare a disabilitare la firma 1330.

D. È possibile disabilitare SSHv1 e lasciare abilitato solo SSHv2 sui sensori Cisco Intrusion Prevention System (IPS)?

R. Al momento non è possibile disabilitare SSHv1 e lasciare solo SSHv2 abilitato. SSHv1 e SSHv2 sono entrambi abilitati e non possono essere disabilitati singolarmente.

D. L'`errore: Errore del sensore durante l'aggiornamento. Messaggio del sensore = L'aggiornamento richiede 115000 KB in /usr/cids/idsRoot/var. Sono disponibili solo 110443 KB.` viene visualizzato un messaggio quando si aggiorna il sensore alla versione 4.1(5). Come risolvere il problema?

R. Questo messaggio di errore viene visualizzato quando la memoria del sensore è insufficiente.

Per risolvere il problema, completare le seguenti attività:

1. Accedere all'account del servizio e diventare root
2. Rimuovere le seguenti directory come indicato di seguito:
   ```
   # 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. Ora provate ad aggiornare il sensore. per ulteriori informazioni, fare riferimento all'ID bug Cisco CSCsb81288 (solo utenti registrati).

D. Viene visualizzato il messaggio di errore `mainApp[396] cplane/E Error - accept() call returns -1` nell'accesso all'appliance ASA. Come risolvere l'errore?

R. Il messaggio di errore `mainApp[396] cplane/E Error - accept() ha restituito -1` indica che il server Web non è in grado di leggere il file e il programma accept() non è riuscito, il che produce descrittori di file quando esistono connessioni TLS. Questo file non è tuttavia necessario per un comportamento normale. È innocuo.

D. Come risolvere l'`eccezione di connessione TLS tls/W errTransport WebSession::sessionTask? handshake` messaggio di errore `incompleto`?

R. Questo messaggio di errore indica che il certificato non è più valido nel modulo. Per risolvere il problema, completare i seguenti passaggi:

1. Rigenerare il certificato dalla CLI:Accedere alla riga di comando del sensore.Eseguire il comando **tls generate** e premere **Invio**. Prendere nota delle impronte digitali visualizzate.
2. Esegui il pull del nuovo certificato nell'IME:Aprire l'IME e individuare il nome del sensore nell'elenco della home page.Fare clic con il pulsante destro del mouse sul sensore e scegliere **Modifica**.Quando viene visualizzata la schermata Edit Device (Modifica dispositivo), fare clic su **OK**. Ignorare gli avvisi che indicano che non è possibile recuperare l'ora del sensore.Verrà richiesto il nuovo certificato di protezione (quello appena generato). Verificare che le impronte digitali corrispondano e fare clic su **Sì**.Dopo alcuni secondi, il sensore dovrebbe visualizzare di nuovo "Connesso" in Stato evento.

D. Quando si tenta di accedere a IPS, viene visualizzato questo messaggio di errore: `errSystemError-ct-sensorAPP.450 non risponde. Errore di clientpipe.` Come risolvere l'errore?

A. Per risolvere il problema, usare il comando **reset** per riavviare l'IPS.

D. L'ora su AIP-SSM è diversa da quella su Cisco Adaptive Security Appliance (ASA). Come risolvere il problema?

R. Per risolvere il problema, usare il server NTP per sincronizzare l'ora su Cisco Adaptive Security Appliance (ASA) e AIP-SSM.

Per ulteriori informazioni, fare riferimento a Configurazione dell'NTP sui sensori IPS.

D. Come è possibile applicare più sensori virtuali su AIP-SSM?

R. Impossibile applicare i sensori virtuali su AIP-SSM per interfaccia perché AIP-SSM ha una sola interfaccia. Quando si creano più sensori virtuali, è necessario assegnare questa interfaccia a un solo sensore virtuale. Non è necessario designare un'interfaccia per gli altri sensori virtuali.

Dopo aver creato i sensori virtuali, è necessario mapparli a un contesto di sicurezza sull'appliance ASA (Adaptive Security Appliance) utilizzando il comando **allocate-ips**. È possibile mappare molti contesti di sicurezza a molti sensori virtuali. Per ulteriori informazioni, consultare la sezione *Assegnazione di sensori virtuali ai contesti adattivi dell'appliance di sicurezza* in Configurazione di AIP-SSM.

D. Qual è il numero massimo di sensori virtuali supportati da AIP-SSM?

R. È possibile supportare un massimo di quattro sensori virtuali.

D. Se si utilizza SSH o IDM per accedere a IPS, è possibile configurare IPS 4240/IDSM/IDSM2 per convalidare gli utenti amministrativi su un server RADIUS/TACACS+?

R. Non è possibile usare un server TACACS+, ma RADIUS è supportato dalla versione IPS 7.0(4)E4. Per ulteriori informazioni, consultare le sezioni *Informazioni nuove e modificate* e *Limitazioni e limitazioni* delle Note di rilascio per Cisco Intrusion Prevention System 7.0(4)E4. Inoltre, fare riferimento a IPS 7.X: Autenticazione di accesso utente tramite ACS 5.X come esempio di configurazione del server Radius per una configurazione di esempio.

D. Qual è l'impatto della licenza scaduta sulla funzionalità IPS?

R. L'unico impatto che una licenza scaduta ha sul sensore è l'interruzione degli aggiornamenti della firma.

D. Gli aggiornamenti delle firme IPS hanno un impatto sui servizi o sulla connettività di rete?

R. No. Gli aggiornamenti delle firme IPS non hanno alcun impatto sui servizi o sulla connettività di rete.

D. Qual è l'URL esatto da immettere per l'aggiornamento automatico del modulo IPS con le firme più recenti?

R. Il collegamento necessario per consentire l'aggiornamento automatico del modulo IPS con l'ultima firma è: https://198.133.219.25/cgi-bin/front.x/ida/locator/locator.pl.

Per completare l'aggiornamento del modulo IPS, è necessario usare l'ID utente e la password Cisco.

Nota: nella sequenza di codici 6.x, gli aggiornamenti automatici da Cisco.com non sono supportati.

È necessario scaricare manualmente i file di firma e applicarli al sensore. Nel codice 6.x è presente una funzione di aggiornamento automatico; tuttavia, ciò è possibile solo da un file server locale in cui i file di firma devono essere scaricati manualmente.

D. Il sensore IPS è vulnerabile alla vulnerabilità del dispositivo di inoltro delle porte X11?

R. No. Non è vulnerabile per le seguenti ragioni:

- Il sensore non dispone di librerie X11. Non ci sono quindi sessioni da dirottare.
- L'inoltro della porta X11 non è abilitato nella configurazione SSH.
- IPv6 non è compilato nel kernel del sensore. Ciò è necessario per sfruttare la vulnerabilità.

D. Perché AIP-SSM non visualizza alcun log quando l'ASA mostra una quantità elevata di log di avvisi e attacchi?

R. Questo accade perché quando l'ASA blocca un elemento, questo non viene passato all'IPS per una doppia ispezione. Pertanto, non è possibile visualizzare log duplicati sull'appliance ASA e sull'interfaccia IPS.

D. Dopo che un utente ha distribuito il set di firme S518, viene visualizzato il messaggio di errore "**invalidValue:Editing string-xl-tcp sig XXXX has NO effect in this version**". Perché?

R. Questo è il messaggio di errore 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
```

Questo problema si verifica perché il motore string-xl-tcp o string-tcp-xl non è supportato sull'hardware. Per ulteriori informazioni, consultare le note sulla versione di IPS Engine E4.

D. Quando si aggiornano automaticamente le firme su un'ASA-SSM-10 con la funzione di aggiornamento automatico, viene visualizzato questo messaggio di errore: **Nessun pacchetto di aggiornamento automatico installabile trovato sul server status=true.** Come risolvere il problema?

R. Questo output visualizza il messaggio di errore 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
```

Questo errore è stato generato e le firme non vengono aggiornate automaticamente perché gli

aggiornamenti delle definizioni delle firme dopo S479 richiedono il motore E4. Per risolvere questo problema, è necessario aggiornare manualmente il sensore a 7.0(2)E4.

Nota: il sensore non può aggiornarsi automaticamente a E4 perché richiede la versione 7.0(2) e il riavvio del sensore.

D. La funzione di aggiornamento automatico su IPS 5.0 per il modulo NIDS non funziona. Come risolvere il problema?

R. Questo output visualizza il messaggio di errore completo:

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

Questo problema si verifica a causa di uno stile di elenco delle directory non corretto con il server FTP. Per risolvere questo problema, passare agli elenchi di directory di tipo UNIX dagli elenchi di directory di tipo MS-DOS esistenti.

Per modificare le impostazioni dell'elenco delle directory, selezionare **Start > Programmi > Strumenti di amministrazione** per aprire Gestione servizi Internet. Passare quindi alla scheda Home directory e modificare lo stile dell'elenco delle directory da MS-DOS a UNIX.

Q. IPS-4255 riceve il messaggio di errore SensorApp fail in TcpRootNode::expireNow() durante un aggiornamento. Come posso risolvere questo problema?

R. Questo problema è dovuto a un errore del motore di analisi ed è risolto nell'ID bug Cisco CSCtb39179 (solo utenti registrati). Per risolvere il problema, aggiornare il sensore alla versione 7.0(4)E4.

D. Quando si tenta di aggiornare la licenza dopo l'acquisto di una nuova licenza, il dispositivo segnala questo errore: **"Impossibile aggiornare la licenza sul sensore." "errExpiredLicense-La nuova data di scadenza della licenza è precedente alla data di scadenza corrente."** Come risolvere il problema?

R. Questo problema si verifica quando il file di licenza ricevuto non è valido. Per ottenere un file di licenza valido, accedere a Cisco.com come utente registrato e scaricare il file di licenza appropriato. Una volta ottenuto il file di licenza valido, installarlo sul sensore.

Se si installa il nuovo file di licenza e si riceve ancora un errore, è possibile che si sia verificato un problema con il file di licenza non valido esistente. Per risolvere il problema, completare la procedura seguente per eliminare il file di licenza non valido esistente:

1. Accedere all'account del servizio digitando il nome utente dell'account del servizio.Se non si dispone di un account del servizio, aprire la riga di comando IPS, accedere alla modalità di configurazione e immettere questo comando**nome utente *nome* privilegio servizio password *password***
   ```
   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. Una volta eseguito l'accesso all'account del servizio, immettere il comando **su** per passare alla directory principale (utilizzando la stessa password dell'account del servizio).
3. Eliminare i file nella directory /usr/cids/idsRoot/shared/.**Nota:** non eliminare il file host.conf.Immettere il comando **cd /usr/cids/idsRoot/shared/** per passare alla directory condivisa.Immettere il comando **ls** per visualizzare i file nella directory.Immettere il comando **rm *nome_file*** per rimuovere i file.**Nota:** non eliminare il file host.conf.
4. Immettere il comando **/etc/init.d/cids restart** per riavviare il sensore.
5. Installare la nuova licenza.

Per risolvere questo problema, è stato archiviato un bug Cisco. Per ulteriori informazioni, fare riferimento a CSCtg76339 (solo utenti registrati).

D. Qual è la funzione di **errorMessage: IpLog 1712041197 terminato in anticipo per mancanza di handle di file. name=ErrLimitExceeded** messaggio di errore? Come posso risolvere questo problema?

R. Questo errore è causato da una quantità eccessiva di pacchetti sulla registrazione IP. Per risolvere il problema, disattivare la funzione di registrazione IP. La registrazione su reti IP è riservata esclusivamente alla risoluzione dei problemi; Cisco consiglia di non attivarla per tutte le firme.

D. Quando si aggiorna il sensore da s550 a s551, viene visualizzato questo messaggio di errore: **Impossibile analizzare la configurazione corrente per il componente "signatureDefinition" e l'istanza "sig0".** Come risolvere il problema?

R. La modifica della firma 23899.0 causa questo problema. per ulteriori informazioni, fare riferimento all'ID bug Cisco CSCtn84552 (solo utenti registrati).

D. Viene visualizzato questo messaggio di errore sul sensore: **Errore: autoUpdate: selezione di un pacchetto dal servizio di localizzazione cisco.com completata. Download del pacchetto non riuscito: Impossibile ricevere la risposta HTTP.** Come risolvere il problema?

R. Verificare se il filtro URL, il filtro contenuti o un server proxy presente impediscono l'esecuzione dell'aggiornamento automatico. Verificare che AutoUpdate non sia bloccato e che le credenziali utente specificate siano corrette.

D. Viene visualizzato questo messaggio di errore XML sul sensore IPS in esecuzione con la versione 6.2(3)E4: **messaggio di errore: Tentativo del software IPS di scrivere dati XML non validi per (token). I caratteri XML non validi sono stati sostituiti con '*'.** Come risolvere il problema?

R. Questo comportamento è stato risolto dall'ID bug Cisco CSCsq50873 (solo utenti registrati). Si tratta di un problema estetico e non crea alcun sovraccarico operativo, ad eccezione della quantità

eccessiva di registri ricevuti. Una soluzione temporanea consiste nel rimuovere la configurazione NTP sul sensore. Per una soluzione permanente, aggiornare la versione in cui il bug è stato risolto.

D. Perché la workstation IME effettua connessioni costanti ai server gestiti nonostante la chiusura del client?

R. L'IME funziona come due servizi Windows e il client GUI. Quando il client viene chiuso, i due servizi Windows (Cisco IPS Manager Express e MySQL-IME) continuano a eseguire e raccogliere eventi dai sensori gestiti e li memorizzano nel database MySQL locale; in questo modo è possibile generare report cronologici.

Il client IME deve aprire una singola sottoscrizione SDEE al sensore gestito e riutilizzare questa sottoscrizione per attività successive di recupero degli eventi. La connettività costante dalla workstation IME ai sensori gestiti è prevista.

D. Il modulo AIP-SSM può essere utilizzato come destinazione SPAN?

R. No. Il modulo AIP-SSM non può essere usato come destinazione SPAN in quanto è usato solo per monitorare il traffico che attraversa l'interfaccia ASA.

D. Perché si osserva un elevato utilizzo della CPU dopo l'aggiornamento dell'IPS al motore E3?

R. Con gli aggiornamenti del motore E3, l'IPS utilizza un algoritmo diverso per la gestione del tempo di inattività e impiega più tempo per il polling dei pacchetti per ridurre la latenza. L'aumento dei controlli determina un corrispondente aumento dell'utilizzo della CPU. Il modo corretto per misurare la CPU in E3 non è l'utilizzo della CPU, ma la **percentuale di carico del pacchetto** che mostra l'utilizzo corretto della CPU.

D. Perché il LED dello stato di salute si accende in modo intermittente sul dispositivo IPS?

R. Il problema potrebbe essere dovuto a un certificato errato sulla stazione di gestione remota, all'esecuzione di software quali CS-MARS, CSM, IEV, VMS-IDS/IPSMC, ecc. Per risolvere il problema procedere come segue:

1. Applicare il certificato TLS del sensore sulla stazione di gestione remota.
2. Configurare un server DNS valido.

D. Come impedire all'IPS di ritardare il traffico HTTP mentre attraversa le sue interfacce?

R. Configurando il sensore in modo che funzioni in modalità asimmetrica il problema verrà risolto. Per impostare la protezione in modalità asimmetrica per il sensore, attenersi alla seguente procedura:

1. Andare a **Configurazione > Criteri > Criteri IPS**.
2. Fare doppio clic su **sensore virtuale**.

3. Passare alle **opzioni avanzate**.
4. In modalità normalizzazione, selezionare **Protezione in modalità asimmetrica**.
5. Fare clic su **OK**.
6. Riavviare l'unità per rendere effettive le modifiche.

Informazioni correlate

- Pagina di supporto di Cisco Secure Intrusion Prevention System
- Risoluzione dei problemi di AIP-SSM
- Avvisi sui prodotti per la sicurezza (incluso Cisco Secure Intrusion Detection)
- Documentazione e supporto tecnico – Cisco Systems