Domande frequenti sul Cisco Secure Intrusion Detection System (versione 3.1 e precedenti)

Sommario

Introduzione

Questo documento contiene le domande frequenti (FAQ) sul Cisco Secure Intrusion Detection System (IDS), noto in precedenza come NetRanger, versione 3.1 e precedenti.

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

Generale

D. Dove posso trovare ulteriori informazioni su Cisco Secure IDS?

R. Per ulteriori informazioni su Cisco Secure IDS, consultare la documentazione completa del prodotto.

D. Come posso aggiornare le firme per l'intero sistema IDS (sensore IDS + software di gestione IDS)?

R. È necessario aggiornare le firme di Sensor e Management Platform separatamente. Si noti che il software di gestione non è in grado di *apprendere* le firme dal sensore, pertanto deve essere aggiornato. Scaricare il file dell'aggiornamento della firma più recente per ciascuna applicazione dai Cisco Secure Downloads (solo utenti registrati). I file Leggimi disponibili nello stesso percorso contengono istruzioni per la procedura di aggiornamento.

D. Dove posso trovare un elenco completo delle firme?

R. L'elenco delle firme IDS è disponibile su Cisco Secure Encyclopedia (solo utenti registrati).

D. Qual è la password predefinita per gli utenti su UNIX IDS e Standalone Sensor?

R. Sul software di gestione IDS UNIX standalone Sensor and IDS, la password predefinita è "attack" per gli utenti **netrangr** e **root**. Quando si esegue il comando **su** per diventare l'utente root, la password predefinita è "attack". Sul blade IDSM (Intrusion Detection System Module), la password predefinita è "attack" per i **ciscoid** di nome utente.

D. Come è possibile ottenere un blade IDSM (Intrusion Detection System Module) per eseguire il dump delle configurazioni?

R. È necessario un server FTP locale per poter caricare le configurazioni.

1. Immettere questo comando dalla modalità diag sul pannello.

   ```
   report systemstatus site user dir
   ```
2. Digitare **y** per continuare quando viene richiesto di continuare la generazione del report di sistema?.
3. Digitare la password FTP dell'utente specificato quando richiesto. Al termine del processo, viene visualizzato un messaggio che indica se il processo non è riuscito o se il file è stato inviato.

D. Quando si installa/disinstalla IDS, dove si trovano i file di registro?

R. I registri di installazione/aggiornamento sono disponibili nei seguenti percorsi:

- I log di installazione di Director si trovano in /var/adm/nrInstall.log.
- I registri di aggiornamento del Service Pack dei sensori si trovano in /usr/nr/sp-update/.
- I log di aggiornamento della firma si trovano in /usr/nr/sig-update/.

D. Quali firme sono disponibili sul PIX per IDS?

R. IDS è disponibile solo per PIX 6.0 e versioni successive. Le firme sono contenute nei messaggi syslog da 400000 a 400051, definiti messaggi di firma Cisco Secure IDS. Fare riferimento alla documentazione dei PIX System Log Messages per ulteriori informazioni su ciascuna firma.

D. È possibile ricevere una notifica quando vengono rilasciati aggiornamenti della firma?

A. Iscriviti alle notifiche di aggiornamento attivo di Cisco IDS per ricevere avvisi e-mail relativi a notizie sui prodotti correlate a Cisco Secure IDS.

D. Quali applicazioni si devono utilizzare per gestire il sensore IDS e qual è la differenza tra di esse?

R. Nelle versioni precedenti alla 3.1, le opzioni di gestione sono Cisco Secure Policy Manager (CSPM) o UNIX Director. La differenza principale tra i due è che CSPM viene eseguito come applicazione indipendente su un server Windows, mentre UNIX Director viene eseguito su HP OpenView su un server UNIX Solaris. Con IDS 3.1, i Sensori possono anche essere gestiti tramite IDS Event Viewer (IEV) installato su un PC o tramite IDS Device Manager, che fa parte della versione 3.1 Sensor. Gestione periferiche è attivato per impostazione predefinita mediante SSL (Secure Sockets Layer) dopo l'impostazione del sensore.

D. Dove è possibile ottenere il software Software Development Kit (SDK)?

R. Il software SDK non è disponibile al pubblico.

Sensore IDS

D. Qual è la differenza tra le versioni 3.x e 4.x dei sensori?

R. La versione 4.0 offre diverse nuove funzioni. La nuova funzionalità più evidente è un'interfaccia della riga di comando (CLI) simile a Cisco IOS®.

D. Come posso impostare la velocità dell'interfaccia sull'IDS?

R. L'impostazione della velocità/duplex sui codici 3.x e 4.0 non è supportata e c'è un bug nella richiesta della funzione (ID bug Cisco CSCdy43054 (solo utenti registrati)). La funzione è disponibile nella versione 5.0 del codice, ora disponibile in Configurazione delle interfacce.

D. Come aggiornare il software del sensore dalla versione 3.0 alla 3.1?

R. I clienti possono scaricare il file dell'aggiornamento alla versione 3.1 da Cisco Secure Downloads (solo utenti registrati).

D. Come aggiornare il software del sensore dalla versione 2.5 alla 3.0?

R. I clienti possono scaricare il file di aggiornamento per la versione 3.0 da Cisco Secure Downloads (solo utenti registrati). Installare l'aggiornamento software nello stesso modo in cui gli aggiornamenti di service pack e firme sono installati nella versione 2.5. La procedura è descritta in dettaglio nella nota sulla configurazione del sensore Cisco IDS versione 3.0.

D. Come aggiornare il software del sensore dalla versione 2.2 alla 3.0?

R. Il file di aggiornamento della versione 3.0 può essere scaricato dal sito Cisco Secure Downloads (solo utenti registrati), ma non può essere aggiornato prima della versione 2.5. Per eseguire l'aggiornamento dalla versione 2.2 alla versione 3.0, è necessario utilizzare il CD di aggiornamento/ripristino disponibile tramite il Product Upgrade Tool (solo utenti registrati). Il numero di parte del CD è IDS-SW-U.

Nota: per ordinare il CD di aggiornamento/ripristino è necessario disporre di un contratto di assistenza valido.

D. Dopo aver collegato una tastiera e un monitor al sensore, il sistema non si avvia correttamente. Cosa devo fare?

R. Verificare che la tastiera e il monitor utilizzati siano compatibili. Alcuni marchi e modelli non sono compatibili con Cisco Secure IDS e impediscono il corretto avvio del sensore IDS. Per ulteriori informazioni sul marchio, fare riferimento al documento Cisco Secure IDS Appliance Boot Failure.

D. Nella sezione IDS di Cisco Secure Downloads, vedo due tipi di file di aggiornamento (service pack e firma). Qual è la differenza tra questi file?

R. Ognuno di questi file contiene una serie specifica di aggiornamenti o aggiunte software, come indicato dalle convenzioni di denominazione qui descritte.

- L'aggiornamento del service pack per il software IDS Sensor Appliance contiene miglioramenti al software dell'applicazione principale IDS Sensor e correzioni di bug. Ad esempio, un file denominato **IDSk9-sp-3.0-5-S17.bin** include gli aggiornamenti alla versione software 3.0(5) più il set di firme numero 17.
- Il file di aggiornamento della firma contiene solo gli aggiornamenti delle firme (impronte digitali degli attacchi). Ad esempio, un file denominato **IDSk9-sig-3.0-5-S18.bin** contiene il set di firme numero 18 per il software 3.0(5) Sensor.

I clienti possono scaricare questi file dal sito Cisco Secure Downloads (solo utenti registrati).

D. Come è possibile stabilire se un sensore è configurato correttamente per evitare un router?

R. Accedere al sensore come utente **netranger** ed eseguire questo comando:

```
nrgetbulk
```

Si dovrebbe ricevere una risposta simile a "*<IP_address>* Active", che mostra l'indirizzo IP del dispositivo di shun usato per bloccare gli attacchi. Questo output mostra un esempio della sintassi del comando e della risposta prevista:

```
netrangr@sensor:/usr/nr
>nrgetbulk 10003 38 1000 1 NetDeviceStatus
10.48.66.68 Active
Success
```

Èinoltre possibile accedere al router e usare il comando **who** per verificare se il sensore è collegato.

D. Quando si esegue il comando nrconns viene visualizzato un messaggio di errore che indica che il valore non è impostato. Come risolvere il problema?

R. Questo messaggio di errore indica potenziali problemi con i file /usr/nr/etc/route e/o /usr/nr/etc/hosts del sensore. Il...I file /route definiscono le comunicazioni postofficed tra il sensore e il director. Il...I file /hosts definiscono i nomi e gli indirizzi IP di Sensori e Director.

Èinoltre possibile accedere come utente **root**, eseguire il comando **sysconfig-sensor** e immettere nuovamente le informazioni sull'infrastruttura di comunicazione IDS.

D. Come utilizzare FTP per copiare i file di registro dal sensore e memorizzarli in un'altra posizione?

R. Per ulteriori informazioni su questa procedura, consultare il documento sulla copia dei file di

registro IP da visualizzare.

D. Cosa è successo al daemon configurato nelle versioni software dei sensori 2.5 e 3.1?

R. Configd è il daemon che elabora tutti i comandi sia sui director UNIX che sui sensori nella base di codice 2.2.x. Nella base di codice 2.5 e 3.0, questa funzionalità è stata assorbita negli altri daemon e il daemon configurato non esiste più.

D. Quando si aggiornano le firme sul sensore, viene visualizzato il messaggio di `ERRORE: Impossibile determinare il tipo di NetRanger dal file daemons. Impossibile aggiornare.`" x Cosa dovrei fare a riguardo?

R. Modificare il file /usr/nr/etc/daemons sul sensore per assicurarsi che nr.packetd sia presente nell'elenco dei daemon. Quindi arrestare e avviare i servizi.

D. Sull'IDS 4210, che è l'interfaccia di controllo e che è l'interfaccia di sniffing?

A. L'interfaccia di controllo in alto è **iprb1:**, mentre l'interfaccia di sniffing in basso è **iprb0:**.

D. Perché quando si usa il comando `ifconfig -a` sul sensore viene visualizzata una sola interfaccia?

R. Il comando **ifconfig** deve restituire solo l'interfaccia di controllo. L'altra interfaccia (l'interfaccia di sniffing) è ancora utilizzata dal sensore, ma gli utenti non sono in grado di vederla. Se è necessario visualizzare questa interfaccia, eseguire il login come root e usare il comando **ifconfig -a** per determinare i nomi dell'interfaccia. Utilizzare il comando **ifconfig** *<interface>* **plumb** per controllare lo stato di un'interfaccia specifica.

D. Come è possibile codificare la velocità dell'interfaccia sul sensore?

R. L'hardcode della velocità dell'interfaccia sul sensore non deve essere necessario e non è supportato dal supporto tecnico Cisco. Se lo switch è impostato per la negoziazione automatica, l'interfaccia negozia la velocità con lo switch a cui è collegato. Il traffico tra la rete e il sensore è unidirezionale (in altre parole, il sensore riceve). Pertanto, in genere è adeguato se lo switch mostra che è stata negoziata la modalità 100 half-duplex (si presume che la porta dello switch sia 100 M).

UNIX Director

D. È possibile utilizzare il nuovo sensore 3.0 con una versione 2.2.x di Director?

R. Sì, ma è necessario aggiornare il software Director alla versione 2.2.3 o successiva. Gli utenti registrati possono scaricare questi file da Cisco Secure Downloads (solo utenti registrati).

D. Come è possibile stabilire quale versione del daemon Director si sta utilizzando?

A. Utilizzare il comando **cat /usr/nr/VERSION** e controllare il numero di versione contenuto

nell'output.

Nota: l'output del comando **nrvers** su Director indica la versione dei daemon eseguiti su Director, ma non la versione del software Director stesso.

D. Come fare in modo che un Director scarichi la configurazione?

R. Accedere come utente **netranger** ed eseguire lo script /usr/nr/bin/director/nrCollectInfo per inviare le informazioni di configurazione a un file denominato /usr/nr/var/tmp/Report_For_Director.html.

D. Il display HP OpenView contiene molti errori (potenzialmente più di 1.000). Le cancello, ma continuano a tornare. Perché?

R. Se IDS Director è pieno di errori e non è in grado di visualizzarli tutti, inizia a inserire un buffer in un file. Arrestare i daemon IDS e chiudere tutte le mappe OpenView aperte per eliminare il file. Eliminare il file **/usr/nr/var/nrDirmap.buffer.default**, quindi riavviare i daemon IDS e la mappa OpenView.

D. Si verificano problemi durante l'invio di allarmi sulla mappa OpenView di HP. Continuo a ricevere errori in /usr/nr/var/errors.nrdirmap. Cosa devo fare?

R. Nelle versioni IDS precedenti alla 2.2.2, la cosa più semplice da fare è eliminare il database OpenView. Il database si trova in /var/opt/OV/share/databases/openview. Completare la procedura seguente per eliminare il database OpenView.

1. Chiudere tutte le mappe OpenView aperte con il comando **ovstop**, quindi arrestare i servizi IDS con il comando **nrstop**.
2. Accedere come utente **root** e **/usr/nr/bin/director/nrDeleteOVwDb**.
3. Rimuovere tutti i file "error.*" nella directory /usr/nr/var (ad esempio, errors.configd).
4. Riavviare i servizi con il comando **nrstart**, quindi riavviare OpenView con il comando **ovstart**.
   Nota: in Director versione 2.2.2 è possibile rimuovere solo la parte IDS del database OpenView anziché l'intero database. Questa procedura è descritta nella Guida alla configurazione di IDS Director.

D. Non è possibile ricevere avvisi sulla mappa OpenView. Il file /usr/nr/var/errors.postofficed in Director contiene messaggi che indicano che nrdirmap non è concesso in licenza per l'esecuzione su questo computer. Come risolvere il problema?

R. Eseguire questo comando.

```
cp /usr/nr/etc/.lt/license-all.lic /usr/nr/etc/licenses
```

Verificare che l'utente **netranger** sia il proprietario dei file, quindi riavviare i servizi IDS.

D. Quando si esegue l'utility nrConfigure e si fa doppio clic su Director, viene

visualizzato questo messaggio: "Impossibile trovare il tipo di sensore per *<director_name>*. Verificare che Postoffice e packed siano in esecuzione". Cosa devo fare?

R. Il problema si verifica perché nrConfigure riconosce il processo inserito nel file daemons di Director (che non deve essere rilevato). Quando nrConfigure chiede a Director la versione come se si trattasse di un sensore, Director non può rispondere con una versione del sensore.

Completare questi passaggi per risolvere il problema.

1. Modificare il file /usr/nr/etc/daemons e rimuovere le voci per nr.packetd, nr.sensord e nr.managed, poiché questi processi devono essere eseguiti solo sul sensore.
2. Arrestare i servizi con il comando **nrstop**, quindi riavviare i servizi con il comando **nrstart**.
3. Assicurarsi che nrConfigure sia stato chiuso.
4. Avviare OpenView con il comando **ovw**.
5. Selezionare **Protezione > Avanzate > nrConfigura DB > Elimina** per eliminare il database nrConfigure danneggiato.
6. Alla richiesta di procedere, immettere **yes**.
7. Evidenziare Director e tutti i Sensori nella finestra principale di OpenView.
8. Selezionare **Protezione > Avanzate > nrConfigura DB > Crea** per creare un nuovo database nrConfigure con le versioni di configurazione correnti dei computer.

D. Come è possibile evitare che l'applicazione nrdirmap venga attivata per impostazione predefinita sulle mappe OpenView?

R. Gli utenti che eseguono l'applicazione IDS in UNIX Director possono eseguire anche altre applicazioni in OpenView. Ciò non è consigliabile, ma in alcuni casi non può essere evitato. Il problema è che nrdirmap è attivato per impostazione predefinita per ogni mappa OpenView, il che non è consigliabile quando altre applicazioni vengono eseguite su OpenView.

Completare questi passaggi in UNIX Director per modificare l'impostazione predefinita in modo da poter scegliere le mappe per le quali è abilitato nrdirmap.

1. Accedere come utente **netranger**.
2. Digitare **cd $OV_REGISTRATION/C**. (OV_REGISTRATION è parte della variabile di ambiente. Il percorso abituale è /etc/opt/OV/share/registration/C.)
3. Digitare **su root**.
4. Modificare il file nrdirmap e modificare la riga di comando come mostrato nell'output:

```
Command -Shared -Initial "nrdirmap";
!--- Changes to: Command -Shared -Initial "nrdirmap -d";
```

5. Salvare il file nrdirmap.
6. Riciclare OpenView. Quando viene visualizzata una mappa con il comando **ovw**, digitare **ps -ef | grep dirmap** dovrebbe produrre risultati simili a quelli mostrati qui. Prendere nota della `mappa` del router con lo switch `-d`.

```
>ps -ef | grep dirmap
netrangr 7175 6820 0 09:50:47 pts/2 0:00 grep dirmap
netrangr 7158 7152 0 09:50:21 ? 0:00 nrdirmap -d
```

Per impostazione predefinita, per le nuove mappe create in OpenView non è attivato nrdirmap. Se

si desidera creare una mappa con nrdirmap installato, è necessario farlo dall'interfaccia utente di OpenView, come illustrato in questa procedura.

1. Dal menu principale di OpenView, scegliere **Mappa > Nuovo** e immettere un nome per la nuova mappa.
2. Sotto le applicazioni configurabili, dovrebbe essere visualizzato NetRanger/Director. Scegliere **NetRanger/Director** e fare clic su **Configura per questa mappa**.
3. Per l'opzione "Attivare nrdirmap per questa mappa?", scegliere **True** per attivare nrdirmap.
4. Selezionate **Verifica (Verify)** e fate clic su **OK**.

D. Dopo aver eseguito l'aggiornamento a Director versione 2.2.3, non è possibile impostare la gravità dell'evento su un livello superiore a 5, anche se era possibile farlo nelle versioni precedenti. Perché?

R. I livelli di gravità sono stati modificati nella versione 2.2.3 del Director per supportare solo l'intervallo da 1 a 5.

IDS Cisco Secure Policy Manager (CSPM)

D. Quale versione di CSPM utilizzare per gestire il sensore IDS?

R. Attualmente CSPM versione 2.3i è in grado di gestire IDS Sensor, mentre CSPM 3.0 no. Se si utilizza CSPM per gestire il sensore e altri dispositivi Cisco Secure (ad esempio PIX, router), è necessario installare le due diverse versioni di CSPM (2.3i e 3.x) su due server Windows separati. È possibile utilizzare ognuno dei server per gestire i dispositivi corrispondenti: CSPM 2.3i per i sensori e CSPM 3.x per PIX, router e così via.

D. Come configurare CSPM per gestire il sensore IDS e verificare che la comunicazione funzioni?

R. Fare riferimento a Configurazione di un sensore Cisco Secure IDS in CSPM per ulteriori informazioni su come configurare CSPM in modo da gestire il sensore IDS e garantire il funzionamento della comunicazione.

D. È possibile regolare le firme per l'accessorio con CSPM?

R. Il tuning implica la modifica di ciò che è necessario affinché una firma venga attivata (ad esempio il numero di host in una sweep) e non implica l'impostazione di azioni e livelli di gravità.

CSPM non è in grado di ottimizzare le firme per l'accessorio in alcuna versione. È possibile impostare solo le azioni e le severità di una firma. In altre parole, CSPM consente di impostare il livello di gravità e l'azione da associare alla firma, ma non di impostare il tipo di firma da attivare. Il SigWizMenu del sensore deve essere utilizzato per sintonizzare i sensori. SigWizMenu e CSPM possono essere entrambi utilizzati per configurare lo stesso sensore in quanto influiscono su parti diverse della configurazione.

Nota: se si utilizza UNIX Director versione 2.2.3 o successiva, l'utilità nrConfigure è in grado di configurare tutte le configurazioni di SigWizMenu. Dopo l'aggiornamento alla versione 2.2.3, utilizzare nrConfigure invece di SigWizMenu per ottimizzare le firme.

Informazioni correlate

- Supporto dei prodotti Cisco Intrusion Prevention System
- Documentazione per Cisco Secure Intrusion Detection System
- Notifiche sul campo per Cisco Secure Intrusion Detection System
- Documentazione e supporto tecnico – Cisco Systems