Cisco Secure Inbraakdetectiesysteem (versies 3.1 en eerder) - veelgestelde vragen

Inhoud

Inleiding

Dit document bevat vaak gestelde vragen (FAQ's) over het Cisco Secure Inbraakdetectiesysteem (IDS), voorheen bekend als NetRanger, versies 3.1 en eerder.

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Algemeen

Q. Waar kan ik extra informatie op Cisco Secure IDS vinden?

A. Raadpleeg de volledige reeks productdocumentatie voor meer informatie over Cisco Secure IDS.

V. Hoe update ik de handtekeningen voor mijn hele IDS-systeem (IDS Sensor + IDS Management Software)?

A. U moet de handtekeningen van het Sensor- en Management Platform afzonderlijk upgraden. Merk op dat de Management Software geen handtekeningen van de Sensor kan *leren*, en dat deze dus ook moet worden bijgewerkt. Download het nieuwste bestand voor het bijwerken van handtekeningen voor elke toepassing van de Cisco Secure Downloads (alleen geregistreerde klanten). De leesbestanden op dezelfde locatie bevatten instructies voor de upgradeprocedure.

Waar kan ik een volledige lijst van handtekeningen vinden?

A. De lijst met IDS-handtekeningen is beschikbaar via Cisco Secure Encyclopedia (alleen geregistreerde klanten).

Q. Wat is het standaardwachtwoord voor gebruikers op de UNIX IDS en de

standalone sensor?

A. Op de standalone UNIX IDS-sensor en IDS Management Software is het defaultwachtwoord "aanval" voor gebruikers **in netwerk** en **wortel**. Wanneer u de opdracht SU geeft om de basisgebruiker te worden, is het standaardwachtwoord "aanval". Op het lemma van de Inbraakdetectiesysteem Module (IDSM) is het standaardwachtwoord "aanval" voor **ciscoïden** van de gebruikersnaam.

Q. Hoe krijg ik een IDSM-blad (Inbraakdetectiesysteem Module) om zijn configuraties te dumpen?

A. U hebt een lokale FTP server nodig zodat u de configuraties kunt uploaden.

1. Voer deze opdracht in vanuit de diagelmodus op het blad.

   ```
   report systemstatus site user dir
   ```
2. Typ **y** om verder te gaan wanneer u wordt gevraagd "Doorgaan met het genereren van het systeemrapport?".
3. Typ het FTP-wachtwoord van de opgegeven gebruiker wanneer u een waarschuwing krijgt. Wanneer het proces is voltooid, ontvangt u een bericht waarin staat of de procedure is mislukt of of het bestand is verzonden.

Q. Wanneer ik IDS installeer/verwijder, waar zijn de logbestanden gelokaliseerd?

A. De installatie/update logbestanden zijn op deze locaties te vinden:

- De installatielogbestanden van de directeur zijn in /var/adm/nrInstall.log.
- Sensor Service Pack update-logbestanden zijn in /usr/nr/sp-update/.
- Handtekeningen voor update-logbestanden zijn te vinden in /usr/nr/sig-update/.

Welke handtekeningen zijn op de PIX beschikbaar voor IDS?

A. IDS is alleen beschikbaar voor PIX 6.0 en later. De handtekeningen zijn vervat in syslog-berichten 400000 tot en met 400051, die de Cisco Secure IDS-handtekeningen worden genoemd. Raadpleeg de documentatie bij het PIX-systeem voor logberichten voor meer informatie over elke handtekening.

Kan ik op de hoogte worden gesteld als er updates voor handtekeningen worden vrijgegeven?

A. Meld u aan voor Cisco IDS Active Update Notes om e-mailwaarschuwingen te ontvangen voor productnieuws dat betrekking heeft op Cisco Secure IDS.

Vraag. Welke applicaties zou ik moeten gebruiken om mijn IDS-sensor te beheren, en wat is het verschil tussen deze?

A. Vóór versie 3.1 moeten de beheeropties Cisco Secure Policy Manager (CSPM) of UNIX Director gebruiken. Het belangrijkste verschil tussen deze twee is dat CSPM als een onafhankelijke toepassing op een Windows server draait, terwijl UNIX Director boven HP

OpenView op een UNIX Solaris server draait. Met IDS 3.1 kunnen de sensoren ook worden bestuurd via het IDS Event Viewer (IEV), die op een pc is geïnstalleerd of gebruik maakt van IDS ApparaatManager, dat deel uitmaakt van de versie 3.1 Sensor. Apparaatbeheer is standaard ingeschakeld met Secure Socket Layer (SSL) nadat u de Sensor hebt ingesteld.

V. Waar kan ik de software voor de softwareontwikkelingskit (SDK) verkrijgen?

A. De SDK-software is niet voor het publiek beschikbaar.

IDS-sensor

Wat is het verschil tussen Sensor versies 3.x en 4.x?

A. Versie 4.0 biedt verschillende nieuwe functies. De opmerkelijkste nieuwe functie is een opdracht-lijn interface (CLI) gelijkend op Cisco IOS®.

Vraag. Hoe codeer ik de interfacesnelheid op de IDS?

A. Harde instelling van de snelheid/duplex in 3.x en 4.0 code wordt niet ondersteund en er is een bug tegen het functieverzoek (Cisco bug ID CSCdy43054 (alleen geregistreerde klanten)). Deze optie is beschikbaar in 5.0-code, die nu beschikbaar is bij Interfaces configureren.

Vraag: Hoe kan ik mijn Sensor-software upgraden van versie 3.0 naar 3.1?

A. Klanten kunnen het update-bestand voor versie 3.1 downloaden van de Cisco Secure Downloads (alleen geregistreerde klanten).

Vraag. Hoe kan ik mijn Sensor-software upgraden van versie 2.5 naar 3.0?

A. Klanten kunnen het update-bestand voor versie 3.0 downloaden van de Cisco Secure Downloads (alleen geregistreerde klanten). Installeer de software update op dezelfde manier dat het servicepakket en de updates van de handtekening zijn geïnstalleerd in versie 2.5. De procedure wordt in detail beschreven in Cisco IDS Sensor Configuration Notes versie 3.0.

Vraag: Hoe kan ik mijn Sensor-software upgraden van versie 2.2 naar 3.0?

A. Het upgradebestand 3.0 kan van de Cisco Secure Downloads (alleen geregistreerde klanten) worden gedownload, maar dit bestand kan versies niet vóór 2.5 bijwerken. U moet de upgrade-cd gebruiken die via het product-upgrade-**programma** (alleen geregistreerde klanten) beschikbaar is, maar van softwareversie 2.2.2.2 U.

Opmerking: U moet een geldig ondersteuningscontract hebben voor het bestellen van de CD voor upgrade/herstel.

Ik heb een toetsenbord en monitor aan mijn sensor bevestigd, maar het start niet goed. Wat moet ik doen?

A. Controleer dat u een ondersteund toetsenbord en monitor gebruikt. Sommige merken en

modellen zijn niet compatibel met Cisco Secure IDS en voorkomen dat de IDS-sensor wordt gestart. Raadpleeg Cisco Secure IDS-applicatie en opblaasfout voor specifieke merkdetails.

Q. In het gedeelte IDS van de Cisco Secure Downloads, zie ik twee typen update bestanden (servicepakket en handtekening). Wat is het verschil tussen deze bestanden?

A. Elk van deze bestanden bevat een specifieke reeks softwareupdates of toevoegingen, zoals aangegeven door de hier beschreven naamgevingsconventies.

- Het servicepakket waarmee de software van de IDS Sensor-applicatie wordt bijgewerkt, bevat verbetering van de belangrijkste toepassingssoftware van de IDS-sensor en bug-fixes. Een bestand met de naam **IDSk9-sp-3.0-5-S17.bin** bevat bijvoorbeeld updates voor softwareversie 3.0(5) plus signatuur ingesteld nummer 17.
- Het bestand voor de bijwerking van de handtekening bevat alleen updates van de handtekeningen (vingerafdrukken). Een bestand met de naam **IDSk9-sig-3.0-5-S18.bin** bevat bijvoorbeeld voor de software van de 3.0(5) Sensor het instelnummer 18.

Klanten kunnen deze bestanden downloaden van de Cisco Secure Downloads (alleen geregistreerde klanten).

Q. Hoe kan ik vertellen of een sensor correct is ingesteld om een router te vernietigen?

A. Meld u aan bij de Sensor als **gebruikersnetwerk** en voert u deze opdracht uit:

```
nrgetbulk
```

U zou een reactie gelijkend op "*<IP_adres>* Active" moeten ontvangen die het IP-adres van het shunning-apparaat weergeeft dat wordt gebruikt om aanvallen te blokkeren. Deze uitvoer toont een voorbeeld van de opdrachtsyntaxis en de verwachte respons:

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

U kunt ook inloggen op de router en de **who**-opdracht uitgeven om te zien of de sensor is inlogd.

Q. Ik krijg een foutbericht dat aangeeft dat "waarde niet ingesteld" is als ik de fout geef. Hoe kan ik deze kwestie oplossen?

A. Deze foutmelding geeft aan dat er problemen zijn met de bestanden /usr/nr/etc/routes en/of /usr/nr/etc/hosts/bestanden op uw sensor. De.../routebestanden definiëren gestoffeerde communicatie tussen de sensor en de directeur. De.../hosts bestanden definiëren de namen en IP-adressen van sensoren en directeuren.

U kunt ook inloggen als **wortel van de** gebruiker, de **systeem-configuratie-sensor** opdracht uitvoeren en de informatie over de infrastructuur van de IDS-communicatie opnieuw invoeren.

Vraag. Hoe gebruik ik FTP om logbestanden van de Sensor te kopiëren om ze ergens anders op te slaan?

A. Raadpleeg IP-logbestanden kopiëren die moeten worden bekeken voor meer informatie over deze procedure.

Wat is er gebeurd met de ingestelde daemon in de Sensor-softwareversies 2.5 en 3.1?

A. Configureer is de datum die alle opdrachten op zowel UNIX-directors als sensoren in de 2.2.x-codebasis verwerkt. In de 2.5 en 3.0 codebasis is deze functionaliteit opgenomen in de andere datums en bestaat de ingestelde datum niet langer.

Q. Wanneer ik de handtekeningen op de sensor update, krijg ik de `FOUT: Kan het type NetRanger niet bepalen uit daemons-bestand. Kan niet bijwerken.`" (Het stuurprogramma van de VPN-client heeft een fout aangetroffen.) getoond. Wat moet ik hieraan doen?

A. Bewerk het bestand /usr/nr/etc/daemons in de Sensor om er zeker van te zijn dat nr.packetd in de daemon-lijst staat. Stop en start de diensten.

Q. Op de IDS 4210, de interface voor controle en de interface voor snuiven?

A. De controle-interface bovenaan is **iprb1:** en de snuifinterface onderaan is **iprb0:**.

Q. Waarom zie ik slechts één interface wanneer ik de `iffig -een` opdracht op mijn sensor geef?

A. Het opdracht **iffig** dient alleen de regelinterface te tonen. De andere interface (de snuifinterface) wordt nog steeds gebruikt door de sensor, maar de gebruikers zouden het niet moeten kunnen zien. Als u deze interface wilt zien, logt u in als wortel en geeft **de** opdracht **iffig -** om de interfacenamen te bepalen. Geef het **iffig** *<interface>***plumb** opdracht uit om de status van een bepaalde interface te controleren.

Hoe kan ik de interfacesnelheid op de sensor coderen?

A. De interfacesnelheid op de sensor moet niet nodig zijn en wordt niet ondersteund door Cisco Technical Support. Als de schakelaar voor autonome onderhandeling wordt ingesteld, onderhandelt de interface snelheid met de schakelaar waar het aan is verbonden. Het verkeer van het netwerk naar de sensor is uniek (met andere woorden: de sensor ontvangt). Daarom is het in het algemeen toereikend als de switch aantoont dat 100 halfduplex is onderhandeld (aangenomen wordt dat de switchpoort 100 M is).

UNIX-directeur

Kan ik de nieuwe 3.0-sensor gebruiken met een 2.2.x versie van Director?

A. Ja, maar u dient de Director-software te upgraden naar versie 2.2.3 of hoger. Geregistreerde klanten kunnen deze bestanden downloaden van de Cisco Secure Downloads (alleen

geregistreerde klanten).

Vraag. Hoe kan ik weten welke versie van de directeur-generaal ik gebruik?

A. Geef de opdracht **cat/usr/nr/VERSIE uit** en controleer het versienummer dat de uitvoer bevat.

Opmerking: Uitvoer van de opdracht van de nrvers op de Director vertelt u de versie van de daders op de Director-software, maar hij vertelt u niet de versie van de Director-software zelf.

Hoe krijg ik een directeur om zijn configuratie te dumpen?

A. Meld u aan als gebruikersnetwerk en voer het script/usr/nr/bin/regisseur/nrCollectInfo uit om configuratieinformatie naar een bestand met de naam /usr/nr/var/tmp/Report_For_Director.html te verzenden.

Q. Ik heb veel fouten (potentieel meer dan 1.000) op mijn HP OpenView display. Ik verwijder ze, maar ze blijven terugkomen. Waarom?

A. Als IDS Director overstroomd wordt met fouten en niet alle fouten kan weergeven, wordt er begonnen met de buffer van een bestand. Stop de IDS-datums en verlaat alle OpenView-kaarten die u hebt geopend om het bestand te verwijderen. Verwijdert het bestand **/usr/nr/var/nrDirmap.buffer.standaard**, start de IDS-datums en uw OpenView-kaart opnieuw.

Q. Ik heb problemen met alarmen op de HP OpenView kaart. Ik krijg fouten in /usr/nr/var/errors.nrdirmap. Wat moet ik doen?

A. In IDS versies eerder dan 2.2.2, is het makkelijkste om te doen het OpenView gegevensbestand uit te wissen. De databank leeft in /var/opt/OV/sharing/databases/open view. Voltooi deze stappen om de OpenView database te verwijderen.

1. Sluit alle open OpenView kaarten met de **ovstop**-opdracht en stop de IDS-services met de opdracht.
2. Meld u aan als **wortel** van de gebruiker en geeft u**/usr/nr/bin/director/nr DeleteOVwDb**.
3. Verwijder alle "error.*" bestanden in de /usr/nr/var folder (bijvoorbeeld foutmelding.configuratie).
4. Start de services opnieuw met de opdracht **Start** en start OpenView opnieuw met de opdracht **ovstart**. **Opmerking:** In Director versie 2.2.2 kunt u alleen het IDS-gedeelte van de OpenView-database verwijderen in plaats van de gehele database. Deze procedure wordt beschreven in de IDS Director Configuration Guide.

Q. Ik kan geen alarm halen op mijn OpenView-kaart. Het /usr/nr/var/errors.postofficed-bestand op de Director bevat berichten die aangeven dat nrdirmap niet is toegestaan om op deze machine te draaien. Hoe los ik dit op?

A. Voer deze opdracht uit.

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

Zorg ervoor dat het **gebruikersnetwerk** de bestanden bezit, en start de IDS-services opnieuw.

Q. Wanneer ik de nrConfigure voorziening en dubbelklik op Directeur, krijg ik dit bericht: "Kan het type sensor niet vinden voor *<director_name>*. Controleer of Postoffice en packed in bedrijf zijn." Wat moet ik doen?

A. Het probleem doet zich voor omdat geenConfigure het verpakte proces in het daemonbestand van de Directeur ziet (wat het niet zou moeten). Wanneer nrConfigure de Director voor zijn versie zoekt alsof het een Sensor is, kan de Director niet reageren met een Sensor-versie.

Voltooi deze stappen om dit probleem op te lossen.

1. Bewerk het bestand/usr/nr/etc/daemons en verwijder de gegevens voor nr.packetd, nr.sensord, en nr.managed, aangezien deze processen alleen op de Sensor mogen lopen.
2. Stop de services met de opdracht Instop en start de services opnieuw met de opdracht **nrstart**.
3. Zorg ervoor dat nrConfigure is afgesloten.
4. Start OpenView met de **ovw-**opdracht.
5. Selecteer **Beveiliging > Geavanceerd > Stationele DB > Verwijderen** om de gecorrumpeerde database te verwijderen en te configureren.
6. Voer **ja in** wanneer u wilt doorgaan.
7. Markeer uw Director en al uw sensoren in het hoofdvenster van OpenView.
8. Selecteer **Beveiliging > Geavanceerd > Stormd OB > Maken** om een nieuwe nrConfigure database te maken met de huidige configuratie versies van de machines.

Vraag. Hoe kan ik voorkomen dat de nrdirmap-toepassing standaard op OpenView-kaarten wordt ingeschakeld?

A. Gebruikers die de IDS-toepassing uitvoeren op UNIX Director kunnen ook andere toepassingen uitvoeren op OpenView. Dit wordt niet aangeraden, maar kan in sommige gevallen niet worden vermeden. Het probleem is dat nrdirmap door standaard voor elke OpenView map is ingeschakeld. Dit is niet wenselijk wanneer andere toepassingen op OpenView worden uitgevoerd.

Voltooi deze stappen op de UNIX Director om het standaard te veranderen zodat je kunt kiezen welke kaarten op die kaarten staan.

1. Meld u aan als **gebruikersnetwerk**.
2. Type **cd $OV_REGISTRATION/C**. (OV_REGISTRATION is onderdeel van uw milieuvariabele. Het gebruikelijke pad is /etc/opt/OV/share/registration/C.)
3. Typ **su root**.
4. Bewerk het filmbestand en wijzig de regel "Opdracht" zoals in deze uitvoer wordt weergegeven:

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

5. Bewaar het nrdirmap-bestand.

6. OpenView recyclen. Wanneer een kaart met de **ovw** opdracht is, typt hij **ps-ef | grep dirmap** moet een productie opleveren die vergelijkbaar is met de resultaten die hier worden getoond. Merk op dat de `nrdirmap` met de `d`-schakelaar is gebruikt.

```
>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
```

Nieuwe kaarten die in OpenView zijn gemaakt, hebben standaard geen verstrooikaart ingeschakeld. Als u een kaart wilt maken met geïnstalleerde nrmap, moet u dit doen vanuit de OpenView GUI, zoals deze procedure uitlegt.

1. Kies in het hoofdmenu OpenView **Kaart > Nieuw** en voer een naam voor de nieuwe map in.
2. Onder de configureerbare toepassingen moet u NetRanger/Director bekijken. Kies **NetRanger/Director** en klik op **Configureren voor deze map**.
3. Voor de optie die zegt "Zou nrdirmap moeten worden ingeschakeld voor deze kaart?", kies **True** als u nrdirmap wilt inschakelen.
4. Kies **Verifiëren** en klik op **OK**.

Q. Ik heb een upgrade uitgevoerd naar Director versie 2.2.3, en nu kan ik de ernst van de gebeurtenis niet meer dan 5 instellen, ook al kon ik dat in eerdere versies doen. Waarom is dit?

A. De ernst is gewijzigd in versie 2.2.3 van de directeur om alleen het bereik 1 tot en met 5 te ondersteunen.

IDS Cisco Secure Policy Manager (CSPM)

Welke versie van CSPM moet ik gebruiken om mijn IDS-sensor te beheren?

A. Momenteel is versie 2.3i van CSPM degene die IDS-sensor kan beheren, terwijl CSPM 3.0 dat niet kan. Als u CSPM gebruikt om de sensor en andere Cisco Secure-apparaten (zoals PIX's, routers) te beheren, moet u de twee verschillende CSPM-versies (2.3i en 3.x) op twee afzonderlijke Windows-servers installeren. U kunt elk van de servers gebruiken om de corresponderende apparaten te beheren: CSPM 2.3i voor de sensoren en CSPM 3.x voor PIX's, routers, enzovoort.

Vraag. Hoe vorm ik CSPM om mijn IDS-sensor te beheren en ervoor te zorgen dat de communicatie werkt?

A. Raadpleeg Een Cisco beveiligde IDS-sensor in CSPM configureren voor meer informatie over hoe u CSPM kunt configureren om uw IDS-sensor te beheren en communicatie te garanderen.

Kan ik de handtekeningen voor het apparaat afstemmen op CSPM?

A. Tuning betekent het veranderen van wat nodig is voor het branden van een handtekening (zoals het aantal hosts tijdens een veger) en betekent niet het instellen van acties en ernst.

CSPM kan (in geen enkele versie) de handtekeningen voor het apparaat aanpassen. Het kan alleen maar een handtekening zetten en een handtekening plaatsen. Met andere woorden: CSPM kan de ernst van de brand bepalen en welke actie er wordt ondernomen om de handtekening te

koppelen, maar kan niet vaststellen welke branden die handtekening hebben. Het SigWiz-menu op de Sensor moet worden gebruikt om de sensor aan te passen. SigWizMenu en CSPM kunnen beide worden gebruikt om dezelfde sensor te configureren, aangezien ze verschillende delen van de configuratie beïnvloeden.

Opmerking: Als u UNIX Director versie 2.2.3 of hoger gebruikt, kan de nrConfigure alle configuratie applicatie aanpassen die SigWizMenu aansluit. Nadat u hebt geupgrade naar 2.2.3, kunt u beter de optie Configuration in plaats van SigWizMenu gebruiken om de handtekeningen af te stemmen.

Gerelateerde informatie

- Productondersteuning voor Cisco-inbraakpreventiesysteem
- Documentatie voor Cisco Secure Inbraakdetectiesysteem
- Veldmeldingen voor Cisco Secure Inbraakdetectiesysteem
- Technische ondersteuning en documentatie – Cisco Systems