Forum aux questions sur Cisco Secure Intrusion Detection System (Versions 3.1 et antérieures)

Contenu

Introduction

Ce document contient des forums aux questions (Foires aux questions) au sujet de l'intrusion Cisco Secure Detection System (ID), autrefois connu sous le nom de NetRanger, des versions 3.1 et antérieures.

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Généralités

Q. Où peux-je trouver les informations complémentaires sur le Cisco Secure IDS ?

A. Référez-vous à l'ensemble complet de documentation du produit pour plus d'informations sur le Cisco Secure IDS.

Q. Comment est-ce que je mets à jour les signatures pour mon système IDS entier (capteur d'ID + logiciel de gestion d'ID) ?

A. Vous devez améliorer les signatures de capteur et de plate-forme d'administration séparément. Notez que le logiciel de gestion ne peut pas *apprendre des* signatures du capteur, ainsi il doit être aussi bien mis à jour. Téléchargez le dernier fichier de mise à jour de signature pour chaque application des téléchargements Cisco Secures (clients enregistrés seulement). Les fichiers readmes disponibles au même emplacement contiennent des instructions pour la procédure de mise à niveau.

Q. Où peux-je trouver une liste complète de signatures ?

A. La liste de signatures d'ID est disponible par l'encyclopédie Cisco Secure (clients enregistrés seulement).

Q. Quel est le mot de passe par défaut pour des utilisateurs sur les ID UNIX et le capteur autonome ?

A. Sur le capteur d'ID UNIX et le logiciel de gestion autonomes d'ID, le mot de passe par défaut est « attaque » pour le **netrangr** et la **racine d'**utilisateurs. Quand vous émettez l'ordre du **su** de devenir l'utilisateur de base, le mot de passe par défaut est « attaque. » Sur la lame du module de système de détection d'intrusion (IDSM), le mot de passe par défaut est « attaque » pour des **ciscoids de** nom d'utilisateur.

Q. Comment est-ce que j'obtiens une lame du module de système de détection d'intrusion (IDSM) pour vider ses configurations ?

A. Vous avez besoin d'un ftp server local ainsi vous pouvez télécharger les configurations.

1. Sélectionnez cette commande de mode de diag sur la lame.

   report systemstatus site *<ftp_target_ip_address>* **user** *<ftpusername>* **dir** *<directoryname>*
2. Tapez **y** afin de continuer une fois demandé « continuent de générer l'état de système ? ».
3. Tapez le mot de passe FTP de votre utilisateur spécifié quand vous êtes incité. Quand le processus est complet, vous recevez un message qui énonce si le processus manquait ou si le fichier était envoyé.

Q. Quand j'installe/désinstalle des ID, où les fichiers journal sont-ils localisés ?

A. Les logs d'installation/mise à jour peuvent être trouvés dans ces emplacements :

- Les journaux d'installation de directeur sont dans /var/adm/nrInstall.log.
- Les logs de mise à jour de Service Pack de capteur sont dans /usr/nr/sp-update/.
- Les logs de mise à jour de signature sont dans /usr/nr/sig-update/.

Q. Quelles signatures sont disponibles sur le PIX pour des ID ?

A. Les ID est disponible seulement pour PIX 6.0 et plus tard. Les signatures sont contenues dans les messages de Syslog 400000 à 400051, désigné sous le nom des messages de signature de Cisco Secure IDS. Référez-vous à la documentation de messages du journal système PIX pour plus d'informations sur chaque signature.

Q. Est-ce que je peux être annoncé quand des mises à jour de signature sont libérées ?

A. Inscrivez-vous pour des notifications actives de mise à jour d'ID de Cisco afin de recevoir des alertes par courrier électronique pour des nouvelles de produit liées au Cisco Secure IDS.

Q. Quelles applications est-ce que je devrais est-elle employer pour gérer mon capteur d'ID, et que la différence entre elles ?

A. Avant la version 3.1, les options d'administration sont d'utiliser le Cisco Secure Policy Manager (CSPM) ou le directeur d'UNIX. La principale différence entre les deux est que CSPM fonctionne comme application indépendante sur des Windows Server, alors que le directeur UNIX s'exécute

sur le HP OpenView sur un serveur UNIX Solaris. Avec les ID 3.1, les capteurs peuvent également être gérés par le visualiseur d'événement d'ID (IEV) installé sur un PC ou utiliser le gestionnaire de périphérique d'ID, qui fait partie du capteur de version 3.1. Le gestionnaire de périphériques est activé par défaut utilisant le Protocole SSL (Secure Socket Layer) après que vous installiez le capteur.

Q. Où peux-je obtenir le logiciel du kit de développement logiciel (SDK) ?

A. Le logiciel SDK n'est pas à la disposition du public.

Capteur d'ID

Q. Quelle est la différence entre les versions 3.x et 4.x de capteur ?

A. La version 4.0 offre plusieurs nouvelles caractéristiques. La nouvelle caractéristique la plus apparente est une interface de ligne de commande (CLI) semblable au Cisco IOS®.

Q. Comment font I dur codent la vitesse d'interface sur les ID ?

A. La configuration dure la vitesse/duplex en 3.x et code 4.0 n'est pas prise en charge et il y a une bogue contre la demande de caractéristique (ID de bogue Cisco CSCdy43054 (clients enregistrés seulement)). La caractéristique est disponible en code 5.0, qui est maintenant disponible à configurer des interfaces.

Q. Comment est-ce que j'améliore mon logiciel de capteur des versions 3.0 à 3.1 ?

A. Les clients peuvent télécharger le fichier de mise à jour pour la version 3.1 des téléchargements Cisco Secures (clients enregistrés seulement).

Q. Comment est-ce que j'améliore mon logiciel de capteur des versions 2.5 à 3.0 ?

A. Les clients peuvent télécharger le fichier de mise à jour pour la version 3.0 des téléchargements Cisco Secures (clients enregistrés seulement). Installez la mise à jour logicielle de la même manière que des mises à jour de paquet et de signature de service sont installé dans la version 2.5. La procédure est décrite en détail dans la version 3.0 de note de configuration en capteur d'ID de Cisco.

Q. Comment est-ce que j'améliore mon logiciel de capteur des versions 2.2 à 3.0 ?

A. Le fichier de mise à niveau 3.0 peut être téléchargé des téléchargements Cisco Secures (clients enregistrés seulement), mais ce fichier ne peut pas mettre à jour des versions avant 2.5. Vous devez employer le CD de mise à jour/reprise disponible par l'outil de mise à jour d'un produit (clients enregistrés seulement) pour améliorer la version de logiciel 2.2 3.0. Le numéro de pièce pour ce CD est IDS-SW-U.

Note: Vous devez avoir un contrat valide de support pour commander le CD de mise à jour/reprise.

Q. J'ai relié un clavier et un moniteur à mon capteur, mais il ne démarre pas

correctement. Que dois-je faire ?

A. Vérifiez que vous utilisez un clavier et un moniteur pris en charge. Quelques marques et modèles ne sont pas compatibles avec le Cisco Secure IDS et empêchent le capteur d'ID d'amorcer correctement. Référez-vous à la panne de démarrage d'appareils de Cisco Secure IDS pour les détails spécifiques de marque.

Q. À la section d'ID des téléchargements Cisco Secures, je vois deux types de fichiers de mise à jour (pack de services et signature). Quelle est la différence entre ces fichiers ?

A. Chacun de ces fichiers contient un ensemble spécifique de mises à jour logicielles ou d'ajouts, comme indiqué par les conventions nommantes expliquées ici.

- La mise à jour de pack de services pour le logiciel de capteur d'ID contient l'amélioration au logiciel aussi bien qu'aux correctifs de bogue d'application principale de capteur d'ID. Par exemple, un fichier nommé **IDSk9-sp-3.0-5-S17.bin** inclut des mises à jour à l'ensemble plus 17 de signature de la version de logiciel 3.0(5).
- Le fichier de mise à jour de signature contient seulement des mises à jour des signatures (empreintes digital d'attaque). Par exemple, un fichier nommé **IDSk9-sig-3.0-5-S18.bin** contient l'ensemble 18 de signature pour 3.0(5) le logiciel de capteur.

Les clients peuvent télécharger ces fichiers du site Cisco Secure de téléchargements (clients enregistrés seulement).

Q. Comment est-ce que je peux dire si un capteur est correctement configuré pour éviter un routeur ?

A. Ouvrez une session au capteur comme **netrangr d'**utilisateur et exécutez cette commande :

```
nrgetbulk <appID> <sensorHostID> <sensorOrgID> <priority> <token>
```

Vous devriez recevoir une réponse semblable au « Active de *<IP_address>* », ce des expositions l'adresse IP du périphérique de évitement utilisé pour bloquer des attaques. Cette sortie affiche un exemple de la syntaxe de commande et de la réponse prévue :

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

Vous pouvez également ouvrir une session au routeur et émettre **qui** commandent de voir si le capteur est ouvert une session.

Q. J'obtiens un message d'erreur qui indique la « valeur non réglée » quand j'émets la commande de nrconns. Comment puis-je résoudre ce problème ?

A. Ce message d'erreur indique des problèmes potentiels avec les fichiers de /usr/nr/etc/routes et/ou de /usr/nr/etc/hosts sur votre capteur. … Les fichiers /routes définissent des transmissions

postofficed entre le capteur et le directeur. … Les fichiers /hosts définissent les noms et les adresses IP des capteurs et des directeurs.

Vous pouvez également ouvrir une session comme **racine d'**utilisateur, exécutez la commande de sysconfig-**capteur**, et écrivez vos informations d'Infrastructure de communications d'ID de nouveau.

Q. Comment est-ce que j'emploie le FTP pour copier des fichiers journal du capteur pour les enregistrer ailleurs ?

A. Référez-vous à copier des fichiers journal IP à visualiser pour plus d'informations sur cette procédure.

Q. Qu'est arrivé au démon de configd dans les versions de logiciel 2.5 et 3.1 de capteur ?

A. Configd est le démon qui traite toutes les commandes sur des directeurs aussi bien que des capteurs UNIX dans la base du code 2.2.x. Dans la base du code 2.5 et 3.0, cette fonctionnalité a été absorbée dans les autres démons et le démon de configd n'existe plus.

Q. Quand je mets à jour les signatures sur le capteur, j'obtiens l'**ERREUR : N'a pas pu déterminer le type de NetRanger à partir de fichier de démons. Incapable de mettre à jour. » .** Queest-ce que je devrais faire au sujet de ceci ?

A. Éditez le fichier de /usr/nr/etc/daemons sur le capteur pour s'assurer que nr.packetd est dans la liste de démon. Alors arrêtez et commencez les services.

Q. Sur les ID 4210, qui est l'interface de contrôle et qui est l'interface de reniflement ?

A. L'interface de contrôle sur le dessus est **iprb1 :** , et l'interface de reniflement sur le bas est **iprb0 :**.

Q. Pourquoi est-ce que je vois seulement une interface quand j'émets l'**ifconfig - une** commande sur mon capteur ?

A. La commande d'**ifconfig** devrait afficher seulement l'interface de contrôle. L'autre interface (l'interface de reniflement) est encore utilisée par le capteur, mais des utilisateurs ne sont pas censées pouvoir le voir. Si vous devez voir cette interface, ouvrez une session comme racine et émettez l'**ifconfig - une** commande de déterminer les noms d'interface. Émettez la commande de **plomb de *<interface> d'*ifconfig** de vérifier le statut d'une interface spécifique.

Q. Comment est-ce que je peux coder en dur la vitesse d'interface sur le capteur ?

A. Coder en dur la vitesse d'interface sur le capteur ne devrait pas être nécessaire et n'est pas pris en charge par le support technique de Cisco. Si le commutateur est placé pour la négociation automatique, l'interface est en pourparlers la vitesse avec le commutateur auquel elle est reliée. Le trafic du réseau au capteur est unidirectionnel (en d'autres termes, le capteur reçoit). Par conséquent, il est généralement adéquat si le commutateur affiche que 100 bidirectionnels-

alternés a été négocié (la supposition est que le port de commutateur est 100 M).

Directeur UNIX

Q. Est-ce que je peux utiliser le nouveau capteur 3.0 avec une version 2.2.x de directeur ?

A. Oui, mais vous devrait améliorer votre logiciel de directeur à la version 2.2.3 ou ultérieures. Les clients enregistrés peuvent télécharger ces fichiers des téléchargements Cisco Secures (clients enregistrés seulement).

Q. Comment est-ce que je peux dire quelle version du démon de directeur j'utilise ?

A. Émettez la commande de **/usr/nr/VERSION de cat** et vérifiez le numéro de version que la sortie contient.

Note: La sortie des **nrvers** commandent sur le directeur te dit la version des démons qu'exécuté là-dessus le directeur, mais ne te dit pas la version du logiciel de directeur elle-même.

Q. Comment est-ce que j'oblige un directeur pour vider sa configuration ?

A. Ouvrez une session comme **netrangr d'**utilisateur et exécutez le script /usr/nr/bin/director/nrCollectInfo pour envoyer les informations de configuration à un fichier nommé /usr/nr/var/tmp/Report_For_Director.html.

Q. J'ai beaucoup d'erreurs (potentiellement plus de 1,000) sur mon affichage de HP OpenView. Je les supprime, mais ils continuent le retour. Pourquoi ?

A. Si l'IDS Director obtient inondé avec des erreurs et ne peut pas les afficher toutes, il commence à mettre en mémoire tampon à un fichier. Arrêtez les démons d'ID et quittez toutes les cartes d'OpenView que vous avez ouvert à se débarasser du fichier. Supprimez le fichier **/usr/nr/var/nrDirmap.buffer.default**, puis redémarrez les démons d'ID et votre carte d'OpenView.

Q. J'ai des problèmes obtenant des alarmes sur la carte de HP OpenView. Je maintiens obtenir des erreurs dans /usr/nr/var/errors.nrdirmap. Que dois-je faire ?

A. Dans des versions antérieures à 2.2.2 d'ID, la chose la plus facile à faire est d'éliminer la base de données d'OpenView. Les vies de base de données dans /var/opt/OV/share/databases/openview. Terminez-vous ces étapes pour supprimer la base de données d'OpenView.

1. Clôturez tous les cartes ouvertes d'OpenView avec la commande d'**ovstop**, puis arrêtez les services d'ID avec la commande de **nrstop**.
2. Procédure de connexion comme **racine** et question **/usr/nr/bin/director/nrDeleteOVwDb d'**utilisateur.
3. Retirez tous les fichiers « error.* » dans le répertoire de /usr/nr/var (par exemple, errors.configd).
4. Redémarrez les services avec la commande de **nrstart**, puis la reprise OpenView avec la

commande d'**ovstart**. **Note**: Dans la version 2.2.2 de directeur, vous pouvez enlever seulement la pièce d'ID de la base de données d'OpenView au lieu de la base de données entière. Cette procédure est décrite dans le guide de configuration d'IDS Director.

Q. Je ne peux pas obtenir des alarmes sur ma carte d'OpenView. Le fichier de /usr/nr/var/errors.postofficed sur le directeur contient les messages qui indiquent que le nrdirmap n'est pas autorisé pour fonctionner sur cet ordinateur. Comment résoudre ce problème ?

A. Exécutez cette commande.

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

Assurez-vous que le **netrangr d'**utilisateur possède les fichiers, puis redémarrent les services d'ID.

Q. Quand I exécutent l'utilitaire de nrConfigure et double-cliquer sur le directeur, je reçois ce message : « Incapable de trouver le type du capteur pour le *<director_name>*. Vérifiez s'il vous plaît que le bureau de poste et le packetd s'exécutent ». Que dois-je faire ?

A. Le problème se pose parce que le nrConfigure voit le processus de packetd dans les démons du directeur classer (qu'il ne devrait pas). Quand le nrConfigure questionne le directeur pour sa version comme si c'étaient un capteur, le directeur ne peut pas répondre avec une version de capteur.

Terminez-vous ces étapes pour résoudre ce problème.

1. Éditez le fichier de /usr/nr/etc/daemons et retirez les entrées pour nr.packetd, nr.sensord, et nr.managed, puisque ces processus devraient seulement fonctionner sur le capteur.
2. Arrêtez les services avec la commande de **nrstop**, puis redémarrez les services avec la commande de **nrstart**.
3. Assurez-vous que le nrConfigure a été arrêté.
4. Début OpenView avec la commande d'**ovw**.
5. **La Sécurité** choisie **> a avancé > DB > effacement de nrConfigure** pour supprimer la base de données corrompue de nrConfigure.
6. Entrez **oui** une fois demandé à poursuivre.
7. Mettez en valeur votre directeur et tous vos capteurs dans la fenêtre principale d'OpenView.
8. **La Sécurité** choisie **> a avancé > DB de nrConfigure > créent** pour créer une nouvelle base de données de nrConfigure avec les versions de configuration en cours des ordinateurs.

Q. Comment est-ce que je garde l'application de nrdirmap de l'activation par défaut sur des cartes d'OpenView ?

A. Les utilisateurs qui exécutent l'application d'ID sur le directeur UNIX peuvent également exécuter d'autres applications sur OpenView. Ceci n'est pas informé, mais parfois il ne peut pas être évité. Le problème est que le nrdirmap est activé par défaut pour chaque carte d'OpenView, qui n'est pas desirable quand d'autres applications fonctionnent sur OpenView.

Terminez-vous ces étapes sur le directeur UNIX pour changer le par défaut de sorte que vous puissiez choisir que les cartes ont le nrdirmap activé sur elles.

1. Procédure de connexion comme **netrangr d'**utilisateur.
2. **Cd $OV_REGISTRATION/C. de** type (OV_REGISTRATION fait partie de votre variable environnementale. Le chemin habituel est /etc/opt/OV/share/registration/C.)
3. Le type **su s'enracinent**.
4. Éditez le fichier de nrdirmap et changez la ligne de « commande » comme cette sortie affiche :

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

5. Sauvegardez le fichier de nrdirmap.
6. Réutilisez OpenView. Maintenant, quand une carte est apportée avec la commande d'**ovw**, tapant la **picoseconde - E-F | le dirmap de grep** devrait rapporter la sortie semblable à cela affichée ici. Notez le `nrdirmap` avec `- le` commutateur `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
   ```

Les nouvelles cartes créées dans OpenView maintenant n'ont pas le nrdirmap activé par défaut. Si vous voulez créer une carte avec le nrdirmap installé, vous devez le faire du GUI d'OpenView, car cette procédure explique.

1. Du menu principal d'OpenView, choisissez la **carte > nouveau** et écrivez un nom pour la nouvelle carte.
2. Sous les applications configurables, vous devriez voir NetRanger/directeur. Choisissez **NetRanger/directeur** et cliquez sur Configure **pour cette carte**.
3. Pour l'option qui indique « le nrdirmap devrait-il être activé pour cette carte ? », choisissez **vrai** si vous voulez activer le nrdirmap.
4. Choisissez **vérifient** et cliquent sur OK.

Q. J'ai amélioré à la version 2.2.3 de directeur, et maintenant je ne peux pas placer la sévérité de l'événement à un supérieur à de niveau 5, quoique je pourrais faire ainsi dans les versions antérieures. Pourquoi cela ?

A. Les niveaux d'importance ont été changés dans la version 2.2.3 du directeur pour prendre en charge seulement la plage 1 à 5.

Cisco Secure Policy Manager d'ID (CSPM)

Q. Quelle version de CSPM est-ce que je devrais employer pour gérer mon capteur d'ID ?

A. Actuellement la version 2.3i de CSPM est celle qui peut gérer le capteur d'ID, tandis que CSPM 3.0 ne peut pas. Si vous employez CSPM pour gérer le capteur et d'autres périphériques Cisco Secures (tels que PIXes, des Routeurs), vous devez installer les deux versions différentes CSPM (2.3i et 3.x) sur deux serveurs de fenêtres séparées. Vous pouvez utiliser chacun des serveurs pour gérer les périphériques correspondants : CSPM 2.3i pour les capteurs et CSPM 3.x pour

PIXes, Routeurs, et ainsi de suite.

Q. Comment est-ce que je configure CSPM pour gérer mon capteur d'ID et pour m'assurer des travaux de transmission ?

A. Référez-vous à configurer un capteur de Cisco Secure IDS dans CSPM pour plus d'informations sur la façon configurer CSPM pour gérer votre capteur d'ID et pour assurer des travaux de transmission.

Q. Est-ce que je peux accorder les signatures pour l'appliance avec CSPM ?

A. L'accord implique de changer ce qu'il prend pour qu'une signature se déclenche (comme le nombre d'hôtes dans un champ) et ne signifie pas des actions et des niveaux d'importance de configuration.

CSPM ne peut pas (dans toute version) accorder des signatures pour l'appliance. Il peut seulement placer les actions et les severities d'une signature. En d'autres termes, CSPM peut placer qui sévérité et que l'action de s'associer à la signature mais ne peut pas placer ce qui se déclenche cette signature. Le SigWizMenu sur le capteur doit être utilisé pour accorder les capteurs. SigWizMenu et CSPM peuvent être utilisés pour configurer le même capteur puisqu'ils affectent différentes parties de la configuration.

Note: Si vous utilisez la version 2.2.3 ou ultérieures de directeur d'UNIX, l'utilitaire de nrConfigure peut configurer tout que SigWizMenu configure. Après que vous amélioriez à 2.2.3, vous devriez employer le nrConfigure au lieu de SigWizMenu pour accorder les signatures.

Informations connexes

- Support produit de Système de protection contre les intrusions Cisco
- Documentation pour le système de détection d'intrusion Cisco Secure
- Notes de terrain pour le système de détection d'intrusion Cisco Secure
- Support et documentation techniques - Cisco Systems