Perguntas mais freqüentes sobre o Cisco Secure Intrusion Detection System (Versões 3.1 e anteriores)

Índice

Introdução

Este documento contém as perguntas mais frequentes (FAQ) sobre o Cisco Secure Intrusion Detection System (IDS), conhecido anteriormente como Netranger, versões 3.1 e anterior.

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

Geral

Q. Onde posso eu encontrar a informação adicional no Cisco Secure IDS?

A. Consulte ao máximo ajustado da documentação do produto para obter mais informações sobre do Cisco Secure IDS.

Q. Como eu atualizo as assinaturas para meu sistema IDS inteiro (sensor de IDS + software de gestão IDS)?

A. Você tem que promover as assinaturas do sensor e da plataforma de gerenciamento separadamente. Note que o software de gestão não pode *aprender* assinaturas do sensor, assim que deve ser atualizado também. Transfira o arquivo de atualização de assinatura o mais atrasado para cada aplicativo dos downloads seguros de Cisco (clientes registrados somente). Os arquivos de leia-me disponíveis no mesmo lugar contêm instruções para o procedimento de upgrade.

Q. Onde posso eu encontrar uma lista completa das assinaturas?

A. A lista de assinaturas de IDS está disponível através da enciclopédia segura de Cisco (clientes registrados somente).

Q. Que é a senha padrão para usuários nos ID DE UNIX e no sensor independente?

A. No sensor independente dos ID DE UNIX e no software de gestão IDS, a senha padrão é “ataque” para o **netrangr** e a **raiz dos** usuários. Quando você emite o **comando su** se transformar o usuário de raiz, a senha padrão é “ataque.” Na lâmina do módulo intrusion detection system (IDSM), a senha padrão é “ataque” para **ciscoids** username.

Q. Como eu consigo uma lâmina do módulo intrusion detection system (IDSM) despejar suas configurações?

A. Você precisa um servidor FTP local assim que você pode transferir arquivos pela rede as configurações.

1. Incorpore este comando do modo do diag na lâmina.

   report systemstatus site *<ftp_target_ip_address>* **user** *<ftpusername>* **dir** *<directoryname>*
2. Datilografe **y** a fim continuar quando perguntado “Continue que gerencie o relatório do sistema?”.
3. Datilografe a senha de FTP de seu usuário especificado quando você é alertado. Quando o processo está completo, você recebe uma mensagem que indique se o processo falhou ou se o arquivo foi enviado.

Q. Quando eu instalo/desinstalar IDS, onde os arquivos de registro estão encontrados?

A. Os logs da instalação/atualização podem ser encontrados nestes lugar:

- Os log de instalação do diretor estão em /var/adm/nrInstall.log.
- Os logs da atualização do pacote de serviços do sensor estão em /usr/nr/sp-update/.
- Os logs da atualização de assinatura estão em /usr/nr/sig-update/.

Q. Que assinaturas estão disponíveis no PIX para o IDS?

A. O IDS está disponível somente para PIX 6.0 e mais atrasado. As assinaturas são contidas nos mensagens do syslog 400000 a 400051, referido como os mensagens de assinatura do Cisco Secure IDS. Refira a documentação dos mensagens de Log de sistema PIX para obter mais informações sobre de cada assinatura.

Q. Posso eu ser notificado quando as atualizações de assinatura são liberadas?

A. Assine acima para Notificações de atualização ativa do Cisco IDS a fim receber alertas do email para as notícias de produto relativas ao Cisco Secure IDS.

Q. Que aplicativos devo eu usar para controlar meu sensor de IDS, e que é a diferença entre eles?

A. Antes da versão 3.1, as opções de gerenciamento são usar o Cisco Secure Policy Manager (CSPM) ou o UNIX Diretor. O principal diferença entre os dois é que o CSPM é executado como

um aplicativo independente em um Windows Server, quando o UNIX Diretor for executado sobre o HP OpenView em um servidor solaris de UNIX. Com IDS 3.1, os sensores podem igualmente ser controlados com o IDS Event Viewer (IEV) instalados em um PC ou que usam o gerenciador de dispositivo ids, que seja parte do sensor da versão 3.1. O gerenciador de dispositivo está permitido à revelia usando o Secure Socket Layer (SSL) depois que você estabelece o sensor.

Q. Onde posso eu obter o software do Software Development Kit (SDK)?

A. O software SDK não está disponível ao público.

Sensor de IDS

Q. Que é a diferença entre as versões do sensor 3.x e 4.x?

A. A versão 4.0 oferece diversos novos recursos. Os novos recursos os mais visíveis são um comando line interface(cli) similar a Cisco IOS®.

Q. Como fazem I duro codificam a velocidade da relação no IDS?

A. O ajuste duro a velocidade/duplex em 3.x e em código 4.0 não é apoiado e há um erro contra o pedido da característica (identificação de bug Cisco CSCdy43054 (clientes registrados somente)). A característica está disponível no código 5.0, que está agora disponível em configurar relações.

Q. Como eu promovo meu software de sensor da versão 3.0 à 3.1?

A. Os clientes podem transferir o arquivo da atualização para a versão 3.1 dos downloads seguros de Cisco (clientes registrados somente).

Q. Como eu promovo meu software de sensor da versão 2.5 à 3.0?

A. Os clientes podem transferir o arquivo da atualização para a versão 3.0 dos downloads seguros de Cisco (clientes registrados somente). Instale a atualização de software da mesma forma que o pacote de serviços e as atualizações de assinatura são instalados na versão 2.5. O procedimento é descrito em detalhe na versão 3.0 da nota da configuração de sensor do Cisco IDS.

Q. Como eu promovo meu software de sensor da versão 2.2 à 3.0?

A. O arquivo da elevação do 3.0 pode ser transferido dos downloads seguros de Cisco (clientes registrados somente), mas este arquivo não pode atualizar versões antes de 2.5. Você deve usar o CD da elevação/recuperação disponível através da ferramenta de upgrade de produto (clientes registrados somente) para promover da versão de software 2.2 ao 3.0. O part number para este CD é IDS-SW-U.

Note: Você deve ter um contrato de suporte válido pedir o CD da elevação/recuperação.

Q. Eu anexei um teclado e um monitor a meu sensor, mas não carreg corretamente. O que devo fazer?

A. Verifique que você está usando um teclado e um monitor apoiados. Alguns tipos e modelos não são compatíveis com Cisco Secure IDS e impedem que o sensor de IDS carreg corretamente. Refira a falha de inicialização do equipamento do Cisco secure IDs para detalhes específicos do tipo.

Q. Na seção IDS dos downloads seguros de Cisco, eu ver dois tipos de arquivos da atualização (pacote de serviços e assinatura). Que é a diferença entre estes arquivos?

A. Cada um destes arquivos contém um grupo específico de atualizações de software ou de adições, como indicado pelas convenções de nomeação explicadas aqui.

- A atualização do pacote de serviços para o software do equipamento do sensor de IDs contém a melhoria ao software assim como às correções de bug do aplicativo central do sensor de IDS. Por exemplo, um arquivo nomeado **IDSk9-sp-3.0-5-S17.bin** inclui atualizações ao número ajustado 17 da assinatura positiva da versão de software 3.0(5).
- O arquivo de atualização de assinatura contém somente atualizações das assinaturas (impressões digitais do ataque). Por exemplo, um arquivo nomeado **IDSk9-sig-3.0-5-S18.bin** contém o número ajustado 18 da assinatura para 3.0(5) o software de sensor.

Os clientes podem transferir estes arquivos do local dos downloads seguros de Cisco (clientes registrados somente).

Q. Como posso eu dizer se um sensor é configurado corretamente para evitar um roteador?

A. Entre ao sensor como o **netrangr do** usuário e execute este comando:

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

Você deve receber uma resposta similar do “ao Active *<IP_address>*”, esse mostras o endereço IP de Um ou Mais Servidores Cisco ICM NT do dispositivo evitando usado para obstruir ataques. Esta saída mostra um exemplo da sintaxe de comando e da resposta esperada:

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

Você pode igualmente entrar ao roteador e emitir o **comando who** ver se o sensor é entrado.

Q. Eu estou recebendo um Mensagem de Erro que indique o " valor não definido " quando eu emito o comando nrconns. Como resolvo esse problema?

A. Este Mensagem de Erro indica problemas potenciais com os arquivos de /usr/nr/etc/routes e/ou de /usr/nr/etc/hosts em seu sensor. … Os arquivos /routes definem comunicações de correspondência entre o sensor e o diretor. … Os arquivos /hosts definem os nomes e os endereços IP de Um ou Mais Servidores Cisco ICM NT dos sensores e dos diretores.

Você pode igualmente entrar como a raiz de usuário, executa o **comando sysconfig-sensor**, e

incorpora sua informação de Infraestrutura de Comunicações de IDS outra vez.

Q. Como eu uso o FTP para copiar arquivos de registro do sensor para os armazenar em outro lugar?

A. Refira o copi dos arquivos de registro IP a ser vistos para obter mais informações sobre deste procedimento.

Q. Que aconteceu ao demônio do configd em versões 2.5 e 3.1 do software de sensor?

A. O configd é o demônio que processa comandos all em diretores assim como em sensores de UNIX na base de código 2.2.x. Na base de código de 2.5 e de 3.0, esta funcionalidade foi absorvida nos outros demônios e o demônio do configd já não existe.

Q. Quando eu atualizo as assinaturas no sensor, eu obtenho o `ERRO: Não podia determinar o tipo de Netranger do arquivo dos demônios. Incapaz de atualizar.`" mensagem de erro. Que devo eu fazer sobre este?

A. Edite o arquivo de /usr/nr/etc/daemons no sensor para assegurar-se de que o nr.packetd esteja na lista do demônio. Então pare e enfie os serviços.

Q. No IDS 4210, que são a interface de controle e que é o farejando interface?

A. A interface de controle na parte superior é **iprb1:** , e o farejando interface na parte inferior é **iprb0:**.

Q. Por que eu ver somente uma relação quando eu emito o `comando ifconfig -a em` meu sensor?

A. **O comando ifconfig** deve mostrar somente a interface de controle. A outra relação (o farejando interface) é usada ainda pelo sensor, mas por usuários não é suposta para poder considerá-lo. Se você precisa de ver esta relação, entre como a raiz e emita o **comando ifconfig -a** determinar os nomes da relação. Emita o **comando ifconfig <interface> plumb** verificar o estado de uma interface particular.

Q. Como posso eu codificar a velocidade da relação no sensor?

A. Codificar a velocidade da relação no sensor não deve ser necessário e não é apoiado pelo Suporte técnico de Cisco. Se o interruptor é ajustado para a negociação automática, a relação negocia a velocidade com o interruptor a que é anexada. O tráfego da rede ao sensor é unidirecional (ou seja o sensor recebe). Consequentemente, é geralmente adequado se o interruptor mostra que 100 metade-frente e verso estiveram negociados (a suposição é que a porta de switch é 100 M).

UNIX Director

Q. Posso eu usar o sensor novo do 3.0 com uma versão do Diretor 2.2.x?

A. Sim, mas você deve promover seu software de diretor à versão 2.2.3 ou mais recente. Os clientes registrados podem transferir estes arquivos dos downloads seguros de Cisco (clientes registrados somente).

Q. Como posso eu dizer que versão do daemon diretor eu estou usando?

A. Emita o comando de **/usr/nr/VERSION do gato** e verifique o número de versão que a saída contém.

Note: A saída do **comando nrvers no** diretor di-lo que a versão dos demônios que executam no diretor, mas não lhe diz a versão do software de diretor própria.

Q. Como eu consigo um diretor despejar sua configuração?

A. Entre como o **netrangr do** usuário e execute o script /usr/nr/bin/director/nrCollectInfo para enviar a informação de configuração a um arquivo nomeado /usr/nr/var/tmp/Report_For_Director.html.

Q. Eu tenho muitos erros (potencialmente mais de 1,000) em meu indicador do HP OpenView. Eu suprimo d, mas mantêm-se voltar. Por quê?

A. Se o IDS diretor obtém inundado com os erros e não pode os indicar todos, começa proteger a um arquivo. Pare os daemons de IDS e retire todos os mapas do OpenView que você tiver aberto a obter livrado do arquivo. Suprima do arquivo **/usr/nr/var/nrDirmap.buffer.default**, a seguir reinicie os daemons de IDS e seu mapa do OpenView.

Q. Eu estou tendo os problemas que obtêm alarmes no mapa do HP OpenView. Eu mantenho-me obter erros em /usr/nr/var/errors.nrdirmap. O que devo fazer?

A. Nas versões de IDS antes de 2.2.2, a coisa a mais fácil a fazer é limpar para fora o base de dados openview. As vidas úteis do base de dados em /var/opt/OV/share/databases/openview. Termine estas etapas para suprimir do base de dados openview.

1. Feche tudo mapas abertos do OpenView com o **comando ovstop**, a seguir pare os serviços IDS com o **comando nrstop**.
2. Entre como a raiz de usuário e a edição **/usr/nr/bin/director/nrDeleteOVwDb**.
3. Remova todos os arquivos “error.*” no diretório de /usr/nr/var (por exemplo, errors.configd).
4. Reinicie os serviços com o **comando nrstart**, a seguir o OpenView do reinício com o **comando ovstart**. **Note**: Na versão de diretor 2.2.2, você pode remover somente o IDS parte do base de dados openview em vez do base de dados inteiro. Este procedimento é descrito no manual de configuração do IDS diretor.

Q. Eu não posso obter alarmes em meu mapa do OpenView. O arquivo de /usr/nr/var/errors.postofficed no diretor contém as mensagens que dizem que o nrdirmap não está licenciado para ser executado nesta máquina. Como posso corrigir este problema?

A. Execute este comando.

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

Assegure-se de que o **netrangr do** usuário possua os arquivos, a seguir reiniciam os serviços IDS.

Q. Quando eu executo o utilitário nrconfigure e o clique duas vezes no diretor, eu recebo esta mensagem: “Incapaz de encontrar o tipo do sensor para o *<diretor_name>*. Certifique-se de por favor o postoffice e o packetd estejam sendo executado”. O que devo fazer?

A. O problema ocorre porque o nrConfigure vê o processo do packetd nos demônios do diretor arquivar (que não deve). Quando o nrConfigure pergunta o diretor para sua versão como se era um sensor, o diretor não pode responder com uma versão do sensor.

Termine estas etapas para resolver esta edição.

1. Edite o arquivo de /usr/nr/etc/daemons e remova as entradas para o nr.packetd, o nr.sensord, e o nr.managed, desde que estes processos devem somente ser executado no sensor.
2. Pare os serviços com o **comando nrstop**, a seguir reinicie os serviços com o **comando nrstart**.
3. Assegure-se de que o nrConfigure esteja fechado.
4. Comece o OpenView com o **comando ovw**.
5. Selecione **Security > Advanced > Nrconfigure Db > Delete** para suprimir do base de dados corrompido do nrConfigure.
6. Entre **sim** quando pedido para continuar.
7. Destaque seu diretor e todos seus sensores na janela principal do OpenView.
8. Selecione a **Segurança > avançou > nrConfigure DB > criam** para criar um base de dados novo do nrConfigure com as versões da configuração atual das máquinas.

Q. Como eu mantenho o aplicativo nrdirmap da possibilidade à revelia em mapas do OpenView?

A. Os usuários que executam o aplicativo de IDS no UNIX Diretor podem igualmente executar outros aplicativos no OpenView. Isto não é recomendado, mas em alguns casos não pode ser evitado. O problema é que o nrdirmap está permitido à revelia para cada mapa do OpenView, que não é desejável quando outros aplicativos são executado no OpenView.

Termine estas etapas no UNIX Diretor para mudar o padrão de modo que você possa escolher que os mapas têm o nrdirmap permitido nelas.

1. Entre como o **netrangr do** usuário.
2. Datilografe o **CD $OV_REGISTRATION/C.** (OV_REGISTRATION é parte de seu variável ambiental. O trajeto usual é /etc/opt/OV/share/registration/C.)
3. Datilografe a **raiz SU**.
4. Edite o arquivo do nrdirmap e mude a linha do “comando” como esta saída mostra:

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

5. Salvar o arquivo do nrdirmap.
6. Recicle o OpenView. Agora, quando um mapa for trazido acima com o **comando ovw**, datilografando o **ps - ef | o dirmap do grep** deve render a saída similar àquela mostrada aqui. Note o `nrdirmap` com `- o` interruptor `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
```

Os mapas novos criados no OpenView agora não têm o nrdirmap permitido à revelia. Se você quer criar um mapa com o nrdirmap instalado, você deve fazê-lo do OpenView GUI, porque este procedimento explica.

1. Do menu OpenView principal, escolha o **mapa > novo** e dê entrada com um nome para o mapa novo.
2. Sob os aplicativos configurávéis, você deve ver Netranger/diretor. Escolha **Netranger/diretor** e o clique **configura para este mapa**.
3. Para a opção que diz “deve o nrdirmap ser permitido para este mapa? ”, escolha **verdadeiro** se você quer permitir o nrdirmap.
4. Escolha **verificam** e clicam a **APROVAÇÃO**.

Q. Eu promovi à versão de diretor 2.2.3, e agora eu não posso ajustar a severidade do evento a um mais alto nivelado do que 5, mesmo que eu poderia fazer assim nas versões anterior. Por que isso ocorre?

A. Os níveis de seriedade foram mudados na versão 2.2.3 do diretor para apoiar somente a escala 1 com o 5.

O CSPM (Cisco Secure Policy Manager) de IDS

Q. Que versão do CSPM devo eu usar para controlar meu sensor de IDS?

A. Atualmente a versão 2.3i do CSPM é essa que pode controlar o sensor de IDS, visto que o 3.0 CSPM não pode. Se você usa o CSPM para controlar o sensor e o outro Cisco fixa dispositivos (tais como PIXes, Roteadores), você deve instalar as duas versões de CSPM diferentes (2.3i e 3.x) em dois server das janelas separadas. Você pode usar cada um dos server para controlar os dispositivos correspondentes: CSPM 2.3i para os sensores e CSPM 3.x para PIXes, Roteadores, e assim por diante.

Q. Como eu configuro o CSPM para controlar meu sensor de IDS e para se certificar de trabalhos de uma comunicação?

A. Refira configurar um sensor do Cisco Secure IDS no CSPM para obter mais informações sobre de como configurar o CSPM para controlar seu sensor de IDS e para assegurar trabalhos de uma comunicação.

Q. Posso eu ajustar as assinaturas para o dispositivo com CSPM?

A. Ajustar envolve mudar o que toma para que uma assinatura ateie fogo (como o número de anfitriões em uma varredura) e não significa ações e níveis de seriedade do ajuste.

O CSPM não pode (em alguma versão) ajustar assinaturas para o dispositivo. Pode somente ajustar as ações e as gravidades de uma assinatura. Ou seja o CSPM pode ajustar-se que severidade e que a ação para associar à assinatura mas não pode se ajustar que fogos que assinatura. O SigWizMenu no sensor tem que ser usado para ajustar os sensores. O SigWizMenu e o CSPM podem ser usados para configurar o mesmo sensor desde que afeta parcelas diferentes da configuração.

Note: Se você usa a versão 2.2.3 ou mais recente do UNIX Diretor, o utilitário nrconfigure pode configurar tudo que o SigWizMenu configura. Depois que você promove a 2.2.3, você deve usar o nrConfigure em vez do SigWizMenu para ajustar as assinaturas.

Informações Relacionadas

- Sustentação do produto do Sistema de prevenção de intrusões da Cisco
- Documentação para Cisco Secure Intrusion Detection System
- Field Notice para o Cisco Secure Intrusion Detection System
- Suporte Técnico e Documentação - Cisco Systems