Cisco Secure Intrusion Detection System (Versions 3.1 and Earlier) Frequently Asked Questions

Contents

Introduction

This document contains frequently asked questions (FAQs) about the Cisco Secure Intrusion Detection System (IDS), formerly known as NetRanger, versions 3.1 and earlier.

Refer to Cisco Technical Tips Conventions for more information on document conventions.

General

Q. Where can I find additional information on Cisco Secure IDS?

A. Refer to the full set of product documentation for more information on Cisco Secure IDS.

Q. How do I update the signatures for my entire IDS system (IDS Sensor + IDS Management Software)?

A. You have to upgrade the Sensor and Management Platform signatures separately. Note that the Management Software is not able to *learn* signatures from the Sensor, so it must be updated as well. Download the latest signature update file for each application from the Cisco Secure Downloads (registered customers only) . The readme files available at the same location contain instructions for the upgrade procedure.

Q. Where can I find a complete list of signatures?

A. The list of IDS signatures is available through the Cisco Secure Encyclopedia (registered customers only) .

Q. What is the default password for users on the UNIX IDS and standalone

Sensor?

A. On the UNIX IDS standalone Sensor and IDS Management Software, the default password is "attack" for users **netrangr** and **root**. When you issue the **su** command to become the root user, the default password is "attack." On the Intrusion Detection System Module (IDSM) blade, the default password is "attack" for username **ciscoids**.

Q. How do I get an Intrusion Detection System Module (IDSM) blade to dump its configurations?

A. You need a local FTP server so you can upload the configurations.

1. Enter this command from diag mode on the blade.

   report systemstatus site *<ftp_target_ip_address>* **user** *<ftpusername>* **dir** *<directoryname>*
2. Type **y** in order to continue when asked to "Continue generating the System Report?".
3. Type the FTP password of your specified user when you are prompted. When the process is complete, you receive a message that states if the process failed or if the file was sent.

Q. When I install/uninstall IDS, where are the log files located?

A. The installation/update logs can be found in these locations:

- Director installation logs are in /var/adm/nrInstall.log.
- Sensor Service Pack update logs are in /usr/nr/sp-update/.
- Signature update logs are in /usr/nr/sig-update/.

Q. What signatures are available on the PIX for IDS?

A. IDS is available only for PIX 6.0 and later. The signatures are contained in syslog messages 400000 through 400051, referred to as the Cisco Secure IDS signature messages. Refer to the PIX System Log Messages documentation for more information about each signature.

Q. Can I be notified when signature updates are released?

A. Sign up for Cisco IDS Active Update Notifications in order to receive e-mail alerts for product news related to Cisco Secure IDS.

Q. Which applications should I use to manage my IDS Sensor, and what is the difference between them?

A. Prior to version 3.1, the management options are to use Cisco Secure Policy Manager (CSPM) or UNIX Director. The main difference between the two is that CSPM runs as an independent application on a Windows server, while UNIX Director runs on top of HP OpenView on a UNIX Solaris server. With IDS 3.1, the Sensors can also be managed through IDS Event Viewer (IEV) installed on a PC or using IDS Device Manager, which is part of the version 3.1 Sensor. Device Manager is enabled by default using Secure Socket Layer (SSL) after you set up the Sensor.

Q. Where can I obtain the Software Development Kit (SDK) software?

A. The SDK software is not available to the public.

IDS Sensor

Q. What is the difference between Sensor versions 3.x and 4.x?

A. Version 4.0 offers several new features. The most noticeable new feature is a command-line interface (CLI) similar to Cisco IOS®.

Q. How do I hard code the Interface speed on the IDS?

A. Hard setting the speed/duplex in 3.x and 4.0 code is not supported and there is a bug against the feature request (Cisco bug ID CSCdy43054 (registered customers only)). The feature is available in 5.0 code, which is now available at Configuring Interfaces.

Q. How do I upgrade my Sensor software from version 3.0 to 3.1?

A. Customers can download the update file for version 3.1 from the Cisco Secure Downloads (registered customers only) .

Q. How do I upgrade my Sensor software from version 2.5 to 3.0?

A. Customers can download the update file for version 3.0 from the Cisco Secure Downloads (registered customers only) . Install the software update in the same way that service pack and signature updates are installed in version 2.5. The procedure is described in detail in Cisco IDS Sensor Configuration Note Version 3.0.

Q. How do I upgrade my Sensor software from version 2.2 to 3.0?

A. The 3.0 upgrade file can be downloaded from the Cisco Secure Downloads (registered customers only) , but this file is not able to update versions before 2.5. You must use the Upgrade/Recovery CD available through the Product Upgrade Tool (registered customers only) to upgrade from software version 2.2 to 3.0. The part number for this CD is IDS-SW-U.

Note: You must have a valid support contract to order the Upgrade/Recovery CD.

Q. I have attached a keyboard and monitor to my Sensor, but it does not boot properly. What should I do?

A. Verify that you are using a supported keyboard and monitor. Some brands and models are not compatible with Cisco Secure IDS and prevent the IDS Sensor from booting properly. Refer to Cisco Secure IDS Appliance Boot Failure for specific brand details.

Q. At the IDS section of the Cisco Secure Downloads, I see two types of update files (service pack and signature). What is the difference between these files?

A. Each of these files contains a specific set of software updates or additions, as indicated by the

naming conventions explained here.

- The service pack update for the IDS Sensor Appliance software contains improvement to the IDS Sensor core application software as well as bug fixes. For example, a file named **IDSk9-sp-3.0-5-S17.bin** includes updates to software version 3.0(5) plus signature set number 17.
- The signature update file contains only updates of the signatures (attack fingerprints). For example, a file named **IDSk9-sig-3.0-5-S18.bin** contains signature set number 18 for the 3.0(5) Sensor software.

Customers can download these files from the Cisco Secure Downloads (registered customers only) site.

Q. How can I tell if a Sensor is correctly configured to shun a router?

A. Log in to the Sensor as user **netrangr** and execute this command:

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

You should receive a response similar to "<*IP_address*> Active", that shows the IP address of the shunning device used to block attacks. This output shows an example of the command syntax and expected response:

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

You can also log in to the router and issue the **who** command to see if the Sensor is logged in.

Q. I am getting an error message that indicates "value not set" when I issue the nrconns command. How can I resolve this issue?

A. This error message indicates potential problems with the /usr/nr/etc/routes and/or /usr/nr/etc/hosts files on your Sensor. The .../routes files define postofficed communications between the Sensor and the Director. The .../hosts files define the names and IP addresses of Sensors and Directors.

You can also log in as user **root**, run the **sysconfig-sensor** command, and enter your IDS Communications Infrastructure information again.

Q. How do I use FTP to copy log files from the Sensor to store them somewhere else?

A. Refer to Copying IP Log Files to Be Viewed for more information on this procedure.

Q. What happened to the configd daemon in Sensor software versions 2.5 and 3.1?

A. Configd is the daemon that processes all commands on both UNIX Directors as well as Sensors in the 2.2.x code base. In the 2.5 and 3.0 code base, this functionality has been absorbed into the other daemons and the configd daemon no longer exists.

Q. When I update the signatures on the Sensor, I get the `ERROR: Could not determine the type of NetRanger from daemons file. Unable to update.`" error message. What should I do about this?

A. Edit the /usr/nr/etc/daemons file on the Sensor to ensure that nr.packetd is in the daemon list. Then stop and start the services.

Q. On the IDS 4210, which is the control interface and which is the sniffing interface?

A. The control interface on the top is **iprb1:**, and the sniffing interface on the bottom is **iprb0:**.

Q. Why do I only see one interface when I issue the `ifconfig -a` command on my Sensor?

A. The **ifconfig** command should show only the control interface. The other interface (the sniffing interface) is still used by the Sensor, but users are not supposed to be able to see it. If you need to see this interface, log in as root and issue the **ifconfig -a** command to determine the interface names. Issue the **ifconfig *<interface>* plumb** command to check the status of a particular interface.

Q. How can I hardcode the interface speed on the Sensor?

A. Hardcoding the interface speed on the Sensor should not be necessary and is not supported by Cisco Technical Support. If the switch is set for autonegotiation, the interface negotiates speed with the switch to which it is attached. Traffic from the network to the Sensor is unidirectional (in other words, the Sensor receives). Therefore, it is generally adequate if the switch shows that 100 half-duplex has been negotiated (assumption is that the switch port is 100 M).

UNIX Director

Q. Can I use the new 3.0 Sensor with a 2.2.x version of Director?

A. Yes, but you should upgrade your Director software to version 2.2.3 or later. Registered customers can download these files from the Cisco Secure Downloads (registered customers only) .

Q. How can I tell what version of the Director daemon I am using?

A. Issue the **cat /usr/nr/VERSION** command and check the version number that the output contains.

Note: Output of the **nrvers** command on the Director tells you the version of the daemons that run on the Director, but it does not tell you the version of the Director software itself.

Q. How do I get a Director to dump its configuration?

A. Log in as user **netrangr** and execute the script /usr/nr/bin/director/nrCollectInfo to send configuration information to a file named /usr/nr/var/tmp/Report_For_Director.html.

Q. I have many errors (potentially more than 1,000) on my HP OpenView display. I delete them, but they keep coming back. Why?

A. If IDS Director gets flooded with errors and cannot display them all, it starts to buffer to a file. Stop the IDS daemons and exit any OpenView maps that you have open to get rid of the file. Delete the file **/usr/nr/var/nrDirmap.buffer.default**, then restart the IDS daemons and your OpenView map.

Q. I am having problems getting alarms onto the HP OpenView map. I keep getting errors in /usr/nr/var/errors.nrdirmap. What should I do?

A. In IDS versions prior to 2.2.2, the easiest thing to do is to wipe out the OpenView database. The database lives in /var/opt/OV/share/databases/openview. Complete these steps to delete the OpenView database.

1. Close all open OpenView maps with the **ovstop** command, then stop the IDS services with the **nrstop** command.
2. Log in as user **root** and issue **/usr/nr/bin/director/nrDeleteOVwDb**.
3. Remove all "error.*" files in the /usr/nr/var directory (for example, errors.configd).
4. Restart the services with the **nrstart** command, then restart OpenView with the **ovstart** command. **Note:** In Director version 2.2.2, you can remove only the IDS part of the OpenView database instead of the entire database. This procedure is described in the IDS Director Configuration Guide.

Q. I cannot get alarms on my OpenView map. The /usr/nr/var/errors.postofficed file on the Director contains messages that say nrdirmap is not licensed to run on this machine. How do I fix this?

A. Execute this command.

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

Ensure that user **netrangr** owns the files, then restart the IDS services.

Q. When I run the nrConfigure utility and double-click on Director, I get this message: "Unable to find the type of the sensor for <*director_name*>. Please check that Postoffice and packetd are running". What should I do?

A. The problem occurs because nrConfigure sees the packetd process in the Director's daemons file (which it should not). When nrConfigure queries the Director for its version as if it were a Sensor, the Director cannot respond with a Sensor version.

Complete these steps to resolve this issue.

1. Edit the /usr/nr/etc/daemons file and remove entries for nr.packetd, nr.sensord, and nr.managed, since these processes should only run on the Sensor.
2. Stop the services with the **nrstop** command, then restart the services with the **nrstart** command.
3. Ensure that nrConfigure has been shut down.
4. Start OpenView with the **ovw** command.
5. Select **Security > Advanced > nrConfigure DB > Delete** to delete the corrupted nrConfigure database.
6. Enter **yes** when asked to proceed.
7. Highlight your Director and all of your Sensors in the main OpenView window.
8. Select **Security > Advanced > nrConfigure DB > Create** to create a new nrConfigure database with the current configuration versions from the machines.

Q. How do I keep the nrdirmap application from being enabled by default on OpenView maps?

A. Users who run the IDS application on UNIX Director can also run other applications on OpenView. This is not advised, but in some instances it cannot be avoided. The problem is that nrdirmap is enabled by default for every OpenView map, which is not desirable when other applications run on OpenView.

Complete these steps on the UNIX Director to change the default so that you can choose which maps have nrdirmap enabled on them.

1. Log in as user **netrangr**.
2. Type **cd $OV_REGISTRATION/C**. (OV_REGISTRATION is part of your environmental variable. The usual path is /etc/opt/OV/share/registration/C.)
3. Type **su root**.
4. Edit the nrdirmap file and change the "Command" line as this output shows:

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

5. Save the nrdirmap file.
6. Recycle OpenView. Now, when a map is brought up with the **ovw** command, typing **ps -ef | grep dirmap** should yield output similar to that shown here. Note the `nrdirmap` with the `-d` switch.

```
>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
```

New maps created in OpenView now do not have nrdirmap enabled by default. If you want to create a map with nrdirmap installed, you must do it from the OpenView GUI, as this procedure explains.

1. From the main OpenView menu, choose **Map > New** and enter a name for the new map.
2. Under the configurable applications, you should see NetRanger/Director. Choose **NetRanger/Director** and click **Configure For this Map**.
3. For the option that says "Should nrdirmap be enabled for this map?", choose **True** if you

want to enable nrdirmap.
4. Choose **Verify** and click **OK**.

Q. I upgraded to Director version 2.2.3, and now I cannot set severity of event to a level higher than 5, even though I could do so in earlier versions. Why is this?

A. The severity levels have been changed in version 2.2.3 of the Director to support only the range 1 through 5.

IDS Cisco Secure Policy Manager (CSPM)

Q. Which version of CSPM should I use to manage my IDS Sensor?

A. Currently version 2.3i of CSPM is the one that can manage IDS Sensor, whereas CSPM 3.0 cannot. If you use CSPM to manage the Sensor and other Cisco Secure devices (such as PIXes, routers), you must install the two different CSPM versions (2.3i and 3.x) on two separate Windows servers. You can use each of the servers to manage the corresponding devices: CSPM 2.3i for the Sensors and CSPM 3.x for PIXes, routers, and so forth.

Q. How do I configure CSPM to manage my IDS Sensor and make sure communication works?

A. Refer to Configuring a Cisco Secure IDS Sensor in CSPM for more information on how to configure CSPM to manage your IDS Sensor and ensure communication works.

Q. Can I tune the signatures for the appliance with CSPM?

A. Tuning involves changing what it takes for a signature to fire (such as the number of hosts in a sweep) and does not mean setting actions and severity levels.

CSPM cannot (in any version) tune signatures for the appliance. It can only set a signature's actions and severities. In other words, CSPM can set which severity and which action to associate to the signature but cannot set what fires that signature. The SigWizMenu on the Sensor has to be used to tune the Sensors. SigWizMenu and CSPM can both be used to configure the same Sensor since they affect different portions of the configuration.

Note: If you use UNIX Director version 2.2.3 or later, the nrConfigure utility is able to configure everything that SigWizMenu configures. After you upgrade to 2.2.3, you should use nrConfigure instead of SigWizMenu to tune the signatures.

Related Information

- **Cisco Intrusion Prevention System Product Support**
- **Documentation for Cisco Secure Intrusion Detection System**
- **Field Notices for Cisco Secure Intrusion Detection System**
- **Technical Support & Documentation - Cisco Systems**