– Cisco Secure Intrusion Detection System Frequently Asked C

Table of Contents

Cisco Secure Intrusion Detection System Frequently Asked Questions

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

Questions

General

- Where can I find additional information on CiscoSecure IDS?
- How do I update the signatures for my entire IDS system (IDS Sensor + IDS Management Software)?
- Where can I find a complete list of signatures?
- What is the default password for users on the UNIX IDS and standalone Sensor?
- How do I get an Intrusion Detection System Module (IDSM) blade to dump its configurations?
- When I install/uninstall IDS, where are the log files located?
- What signatures are available on the PIX for IDS?
- Can I be notified when signature updates are released?
- Which applications should I use to manage my IDS Sensor, and what is the difference between them?

IDS Sensor

- How do I upgrade my Sensor software from version 2.5 to 3.0?
- How do I upgrade my Sensor software from version 2.2 to 3.0?
- I have attached a keyboard and monitor to my Sensor, but it does not boot properly. What should I do?
- At the IDS section of the Cisco Secure Software Center, I see two types of update files (service pack and signature). What is the difference between these files?
- How can I tell if a Sensor is correctly configured to shun a router?
- I am getting an error message indicating "value not set" when issuing the **nrconns** command. How can I resolve this issue?
- How do I use FTP to take log files from the Sensor to store them somewhere else?
- What happened to the configd daemon in Sensor software versions 2.5 and later?
- When I update the signatures on the Sensor, I get an error message that says, "ERROR: Could not determine the type of NetRanger from daemons file. Unable to update." What should I do about this?
- On the IDS 4210, which interface is which?
- Why do I only see one interface when I issue the **ifconfig −a** command on my Sensor?
- I upgraded my Sensor to version 3.0, and my managed routers have different access control lists (ACLs) on them. Why?

UNIX Director

- Can I use the new 3.0 Sensor with a 2.2.x version of Director?
- How can I tell what version of the Director daemon I am using?
- How do I get a Director to dump its configuration?
- I have many errors (potentially more than 1,000) on my HP OpenView display. I delete them, but they keep coming back. Why?
- I'm having problems getting alarms onto the HP OpenView map; I keep getting errors in /usr/nr/var/errors.nrdirmap. What should I do?

- I can't get alarms on my OpenView map. The /usr/nr/var/errors.postofficed file on the Director contains messages saying that nrdirmap is not licensed to run on this machine. How do I fix this?
- When I run the nrConfigure utility and double−click on Director, I get the following message: "Unable to find the type of the sensor for <*director_name*>. Please check that Postoffice and packetd are running". What should I do?
- How do I keep the nrdirmap application from being enabled by default on OpenView maps?
- 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?

IDS Cisco Secure Policy Manager (CSPM)

- Which version of CSPM should I use to manage my IDS Sensor?
- How do I configure CSPM to manage my IDS Sensor and make sure communication is working?
- Can I tune the signatures for the appliance using CSPM?

Tools Information
Related Information

General IDS

Q. Where can I find additional information on CiscoSecure IDS?

A. For further information on CiscoSecure IDS, refer to the full set of product documentation.

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 Cisco Secure Policy Manager (CSPM)/Director signatures separately. Note that the Management Software will not be able to "learn" signatures from the Sensor, so it must be updated as well.

Please download the latest signature update file for each application from the Cisco Secure Software Center (linked from Cisco TAC Tools for Security Technologies). 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.

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**. 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. Note that you will need a local FTP server so you can upload the configurations.

1. From diag mode on the blade, enter the following command.

   report systemstatus site <*ftp_target_ip_address*> user <*ftpusername*> dir <*directoryname*>

2. When asked to "Continue generating the System Report?", type **y** to continue.

3. When prompted, type your specified user's FTP password.

When the process is complete, you will receive a message 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 the following 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. For details about each signature, refer to documentation on PIX System Log Messages.

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

A. Sign up for Cisco IDS Active Update Notifications 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. You can use either 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.

IDS Sensor

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

A. Registered users can download the update file for version 3.0 from the Cisco Secure Software Center (linked from Cisco TAC Tools for Security Technologies).

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 Software Center (linked from Cisco TAC Tools for Security Technologies), but this file is not able to update versions prior to 2.5. To upgrade from software version 2.2 to 3.0, you must use the Upgrade/Recovery CD available through the Product Upgrade Tool. The part number for this CD is IDS−SW−U.

Note: To order the Upgrade/Recovery CD, you must have a valid support contract.

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 will prevent the IDS Sensor from booting properly. For specific brand details, refer to Cisco Secure IDS Appliance Boot Failure.

Q. At the IDS section of the Cisco Secure Software Center, 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 below.

- 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.

Registered users can download the theses files from the Cisco Secure Software Center (linked from Cisco TAC Tools for Security Technologies).

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 the following command.

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

You should receive a response like "<*IP_address*> Active", showing the IP address of the shunning device used to block attacks. An example of the command syntax and expected response is shown below.

```
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 indicating "value not set" when issuing 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 take log files from the Sensor to store them somewhere else?

A. For details on this procedure, please refer to Exporting Log Files to a Remote FTP Server.

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

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, so the configd daemon no longer exists.

Q. When I update the signatures on the Sensor, I get an error message that says, "ERROR: Could not determine the type of NetRanger from daemons file. Unable to update." 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 interface is which?

A. The control interface on top is **iprb1:**, and the sniffing interface on 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. To check the status of a particular interface, issue the **ifconfig <*interface*> plumb** command.

Q. I upgraded my Sensor to version 3.0, and my managed routers have different access control lists (ACLs) on them. Why?

A. After an upgrade to 3.0, the ACLs from 2.5 and 2.2.1 are left on the router. When a Sensor that is controlling a router is updated to 3.0, the ACLs from the old version (199 and 198 by default) are left on the router because the ACL names in 3.0 have changed to use the new format of "IDS_*interface_in*|*out*_[0|1]". You can safely remove the old ACLs from the router without affecting the Sensor.

This change in ACL names will also affect users who are using the 10000 Policy Violation signature to fire alarms on ACLs created by the "managed" process. The ACL names in these signatures will need to change from the old numbers to the new name format.

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 users can download the theses files from the Cisco Secure Software Center (linked from Cisco TAC Tools for Security Technologies).

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 will tell you the version of the daemons running on the Director, but it will 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 can't display them all, it will start buffering to a file. To get rid of the file, stop the IDS daemons and exit any OpenView maps that you have open. Delete the file /usr/nr/var/nrDirmap.buffer.default, then restart the IDS daemons and your OpenView map.

Q. I'm 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 OpenView database. The database lives in /var/opt/OV/share/databases/openview. To delete the OpenView database, complete the following steps.

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

A. Execute the following 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 the following 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.

To resolve this issue, complete the steps below.

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 are running on OpenView.

Complete the steps below 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 shown below.

   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 below; 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 will not have nrdirmap enabled by default. If you want to create

a map with nrdirmap installed, you must to do it from the OpenView GUI, as explained below.

1. From the main OpenView menu, select **Map > New** and enter a name for the new map.
2. Under the configurable applications, you should see NetRanger/Director. Select this item and click **Configure For this Map**.
3. For the option that says "Should nrdirmap be enabled for this map?", select **True** if you want to enable nrdirmap.
4. Select **Verify** and then **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 1−5.

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 will be able to use each of the servers to manage the corresponding devices: CSPM 2.3i for the Sensors and CSPM 3.x for PIXes, routers, etc.

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

A. For details on how to do this, refer to Configuring a Cisco Secure IDS Sensor in CSPM.

Q. Can I tune the signatures for the appliance using 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 are using UNIX Director version 2.2.3 or later, the nrConfigure utility will be able to configure everything that SigWizMenu configures. After upgrading to 2.2.3, you should use nrConfigure instead of SigWizMenu to tune the signatures.

Tools Information

For additional resources, refer to Cisco TAC Tools for Security Technologies.

Related Information

- **Documentation for CiscoSecure Intrusion Detection**
- **More Technical Tips for CiscoSecure Intrusion Detection System**
- **Security Product Field Notices (including CiscoSecure Intrusion Detection System)**
- **Product Support Page for CiscoSecure Intrusion Detection System**

Updated: Jun 06, 2002 Document ID: 4163