Cisco Secure Intrusion Detection System（3.1及更早版本）常见问题

目录

简介

本文包含常见问题(常见问题)以前叫作Netranger (IDS)的Cisco安全入侵监测系统，版本3.1和以下。

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

一般问题

Q. 在哪里能找到关于Cisco Secure IDS的其他信息？

A. 参考全套产品文档关于Cisco Secure IDS的更多信息。

Q. 如何更新整个IDS系统的(IDS传感器签名+ IDS管理软件) ？

A. 您必须分开升级传感器和管理平台签名。注意管理软件不能学习从传感器的签名，因此必须更新。下载每应用程序的最新的签名更新文件从Cisco Secure下载(仅限注册用户)。README文件可用在同一个位置包含升级程序的说明。

Q. 在哪里能找到签名完整列表？

A. IDS签名列表通过Cisco Secure百科全书(仅限注册用户)是可用的。

Q. 什么是用户的默认密码UNIX IDS和独立传感器的？

A. 在UNIX IDS独立传感器和IDS管理软件上，默认密码是“攻击”用户**netrangr**和**根的**。当您发出**su命令**变为root用户时，默认密码是“攻击”。在入侵检测系统模块(IDSM)刀片，默认密码是“攻击”用户名**ciscoids的**。

Q. 如何获得入侵检测系统模块(IDSM)刀片转存其配置？

A. 您需要一个本地FTP服务器，因此您能上传配置。

1. 输入从diag模式的此命令在刀片。
   report systemstatus site *<ftp_target_ip_address>* **user** *<ftpusername>* **dir** *<directoryname>*
2. 键入**y**为了继续，当询问"持续生成系统报告？"。
3. 当提示时，请键入您的指定的用户FTP密码您。当进程完成时，您收到陈述的消息进程是否失败或文件是否发送。

Q. 当我安装/时在哪里卸载IDS，日志文件查找？

A. 安装/更新日志可以在这些位置找到：

- 导向器安装日志在/var/adm/nrInstall.log。
- 传感器服务包更新日志在/usr/nr/sp-update/。
- 签名更新日志在/usr/nr/sig-update/。

Q. 什么签名是可用的在PIX为IDS ？

A. IDS仅可用为PIX 6.0和以后。签名在系统消息400000至400051包含，指Cisco Secure IDS签名消息。参考PIX系统日志信息文档关于每个签名的更多信息。

Q. 当签名更新发布时，能通知？

A. 为Cisco IDS活动更新通知签字为了收到与Cisco Secure IDS涉及的产品新闻的电子邮件告警。

Q. 应该使用哪些应用程序管理IDS传感器，并且他们有何区别？

A. 在版本3.1之前，管理选项是Cisco Secure Policy Manager使用或UNIX向导。两个之间的主要区别是CSPM运行作为在Windows服务器的一独立应用程序，而UNIX向导运作在它上面在UNIX Solaris服务器的HP OpenView。使用IDS 3.1，传感器可能通过安装在PC或使用IDS服务管理器的IDS Event Viewer (IEV)也被管理，是版本3.1传感器的一部分。在您设置传感器后，默认情况下设备管理器启用使用安全套接字层SSL。

Q. 在哪里能得到软件开发工具(SDK)软件？

A. SDK软件不供给公共。

IDS 传感器

Q. 传感器版本3.x和4.x有何区别？

A. 版本4.0提供几新特性。最显而易见的新特性是命令行界面(CLI)类似于Cisco IOS。

Q. I hard code在IDS的接口速度？

A. 速度/双工用3.x和4.0代码不支持硬设置，并且有bug功能请求(Cisco Bug ID CSCdy43054 (仅限注册用户))。功能是可用的用5.0代码，当前是可用的在配置接口。

Q. 如何升级从版本3.0到3.1的传感器软件？

A. 客户能下载版本3.1的更新文件从Cisco Secure下载(仅限注册用户)。

Q. 如何升级从版本2.5到3.0的传感器软件？

A. 客户能下载版本3.0的更新文件从Cisco Secure下载(仅限注册用户)。相似地安装服务包和签名更新在版本2.5安装的软件更新。步骤在Cisco IDS传感器配置说明版本3.0详细描述。

Q. 如何升级从版本2.2到3.0的传感器软件？

A. 3.0升级文件可以从Cisco Secure下载(仅限注册用户)下载，但是此文件不能在2.5前更新版本。您必须通过产品升级工具(仅限注册用户)使用升级/恢复CD联机升级从软件版本2.2到3.0。此CD的部件号是IDS-SW-U。

注意： 您必须有有效支持合同定购升级/恢复CD。

Q. 我附加键盘和监视器对我的传感器，但是不适当地启动。我该怎么办？

A. 验证您使用一支持的键盘和监视器。一些品牌和型号不是与Cisco Secure IDS兼容并且防止IDS传感器适当启动。参考的Cisco Secure IDS器具引导失败关于特定品牌详细信息。

Q. 在Cisco Secure下载的IDS部分，我看到更新文件的两种类型(服务包和签名)。这些文件有何区别？

A. 这些文件中的每一个包含特定的软件更新或新增内容，如表示的是由解释的命名规则此处。

- 为IDS传感器工具软件的服务包更新包含改进对IDS传感器核心应用程序软件以及bug修复。例如，名为**IDSk9-sp-3.0-5-S17.bin的**文件包括更新到软件版本3.0(5)正签名集合第17。
- 签名更新文件包含签名(攻击指纹)的仅更新。例如，名为**IDSk9-sig-3.0-5-S18.bin的**文件包含3.0(5)传感器软件的签名集合第18。

客户能下载从Cisco Secure下载(仅限注册用户)站点的这些文件。

Q. 如何能告诉传感器是否正确地配置避开路由器？

A. 登陆对传感器作为用户**netrangr**并且执行此命令：

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

您应该收到答复类似于“*<ip_address>*激活”，那显示用于的避开设备的IP地址拦截攻击。此输出显示命令语法和期望的响应的示例：

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

您能也登陆到路由器和发出**who命令**发现传感器是否登陆。

Q. 我收到指示"value not set"的错误消息，当我发出nrconns命令时。如何能解决此问题？

A. 此错误消息指示潜在问题用在您的传感器的/usr/nr/etc/routes和/usr/nr/etc/hosts文件。… /routes文件定义了传感器和导向器之间的postofficed通信。… /hosts文件定义了传感器和导向器的名称和IP地址。

您能也登陆作为用户根，运行**sysconfig-sensor命令**，并且再输入您的IDS通信基础架构信息。

Q. 如何使用FTP复制从传感器的日志文件存储他们其他地方？

A. 参考复制将查看的IP日志文件关于此步骤的更多信息。

Q. 什么发生在传感器软件版本2.5和3.1的configd守护？

A. 处理所有on命令UNIX向导以及传感器在2.2.x代码基址的Configd是守护程序。在2.5和3.0代码基址，此功能被吸收了到其他守护程序，并且configd守护不再存在。

Q. 当我更新在传感器时的签名，我获得ERROR:Netranger"。错误消息。对此我该做什么?

A. 编辑在传感器的/usr/nr/etc/daemons文件保证nr.packetd在守护程序列表。然后请终止并且开始服务。

Q. 在IDS 4210，是控制接口，并且是探测接口？

A. 在上面的控制接口是**iprb1** ：和在底部的探测接口是**iprb0** ：。

Q. 当我发出`ifconfig - a`在我的传感器时，为什么只看到一个接口？

A. **ifconfig命令**应该显示仅控制接口。传感器，但是用户仍然使用另一个接口(探测接口)不应该能发现它。如果需要发现此接口，请登陆作为根并且发出**ifconfig - a命令**确定接口名称。发出**ifconfig <interface> plumb命令**检查特定接口的状况。

Q. 如何能硬编码在传感器的接口速度？

A. 在传感器的接口速度不应该是必要的和思科技术支持不支持硬编码。如果交换机为自动协商设置，接口协商速度用附加的交换机。从网络的流量到传感器是单向的(换句话说，传感器接收)。所以，它是通常适当的，如果交换机显示100半双工协商(假定是交换机端口是100 M)。

UNIX Director

Q. 能否以导向器2.2.x版本使用新的3.0传感器？

A. 是，但是您应该升级您的导向器软件到版本2.2.3或以上。注册用户能下载从Cisco Secure下载(仅限注册用户)的这些文件。

Q. 如何能告诉控制器程序的什么版本我使用？

A. 发出**cat /usr/nr/VERSION**命令并且检查输出包含的版本号。

注意： 输出**nrvers命令**在导向器告诉您在导向器运行守护程序的版本，但是不告诉您导向器软件的

版本。

Q. 如何使导向器转存其配置？

A. 登陆作为用户**netrangr**并且执行脚本/usr/nr/bin/director/nrCollectInfo发送配置信息到名为/usr/nr/var/tmp/Report_For_Director.html的文件。

Q. 我有许多错误(潜在超过1,000)在我的HP OpenView显示。我删除他们，但是他们继续回来。为什么？

A. 如果IDS控制器充斥与错误，并且不能显示他们全部，它开始缓冲到文件。终止IDS守护程序并且退出您有开放摆脱文件的所有OpenView地图。删除文件**/usr/nr/var/nrDirmap.buffer.default**，然后重新启动IDS守护程序和您的OpenView地图。

Q. 我有获得在HP OpenView地图上的问题报警。我在/usr/nr/var/errors.nrdirmap保留收到错误。我该怎么办？

A. 在2.2.2之前的IDS版本中，要执行的最容易的事是消除OpenView数据库。在/var/opt/OV/share/databases/openview的数据库寿命。完成这些步骤删除OpenView数据库。

1. 结束所有开放OpenView地图用**ovstop命令**，然后终止IDS服务用**nrstop命令**。
2. 登陆作为用户根并且发出**/usr/nr/bin/director/nrDeleteOVwDb**。
3. 删除在/usr/nr/var目录的所有“error.*”文件(例如， errors.configd)。
4. 重新启动服务用**nrstart命令**，然后重新启动OpenView用**ovstart命令**。 **注意**： 在导向器版本2.2.2，您能取消OpenView数据库的仅IDS零件而不是整个数据库。此步骤在IDS控制器配置指南描述。

Q. 我不能获得在我的OpenView地图的报警。在导向器的/usr/nr/var/errors.postofficed文件包含说的消息nrdirmap在此计算机没有准许运行。如何解决此问题？

A. 执行此命令。

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

保证用户**netrangr**拥有文件，然后重新启动IDS服务。

Q. 当我在导向器时运行nrConfigure软件并且双击，我收到此消息：“无法查找传感器的种类*<director_name>*的。请检查Postoffice和packetd运行”。我该怎么办？

A. 问题发生，因为nrConfigure看到在的packetd进程不应该)的控制器程序文件(。当nrConfigure查询导向器其版本时，好象它传感器，导向器不能回应传感器版本。

完成这些步骤解决此问题。

1. 因为这些进程在传感器，应该只运行编辑/usr/nr/etc/daemons文件并且删除nr.packetd、nr.sensord和nr.managed的条目。
2. 终止服务用**nrstop命令**，然后重新启动服务用**nrstart命令**。
3. 保证nrConfigure被关闭了。

4. 开始OpenView用**ovw命令**。
5. 选择**Security > Advanced > nrConfigure DB > Delete**删除损坏的nrConfigure数据库。
6. 输入**是**，当询问继续。
7. 突出显示您的导向器和所有您的在主要OpenView窗口的传感器。
8. 选择**安全>Advanced > nrConfigure DB >创建**创建与当前配置版本的一个新的nrConfigure数据库从机器。

Q. 默认情况下如何保持从启用的nrdirmap应用程序在OpenView地图？

A. 运行在UNIX向导的IDS应用程序的用户能也运行在OpenView的其他应用程序。这没有建议，但是不可能例如避免。问题是默认情况下nrdirmap为每张OpenView地图启用，不是理想，当其他应用程序在OpenView时运行。

完成在UNIX向导的这些步骤更改默认，以便地图有在他们启用的nrdirmap的您能选择。

1. 登陆作为用户**netrangr**。
2. 键入**cd $OV_REGISTRATION/C.** (OV_REGISTRATION是您的环境变量的一部分。通常路径是/etc/opt/OV/share/registration/C。)
3. 类型**su根**。
4. 编辑nrdirmap文件并且更换“命令”线路，此输出显示：
```
Command -Shared -Initial "nrdirmap";
!--- Changes to: Command -Shared -Initial "nrdirmap -d";
```
5. 保存nrdirmap文件。
6. 回收OpenView。现在，当地图用**ovw命令**启动，键入的**ps - ef|grep dirmap**应该产生输出类似于显示的那此处。注释nrdirmap用- d交换机。 >**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
```

在OpenView创建的默认情况下新的地图当前没有启用的nrdirmap。如果要创建有安装的nrdirmap的一张地图，您必须从OpenView GUI执行它，因为此步骤解释。

1. 从主要OpenView菜单，请选择**地图>New**并且输入一名称对于新的地图。
2. 在可配置应用程序下，您应该看到Netranger/导向器。选择**Netranger/导向器**并且单击**为此地图配置**。
3. 对于说“的选项应该为此地图启用nrdirmap ？如果要启用nrdirmap”，请选择**真**。
4. 选择**验证**并且点击OK键。

Q. 我升级对导向器版本2.2.3，并且我不能当前设置事件严重性到级高于5，即使我在更早版本可能如此执行。为什么会这样？

A. 严重级别在导向器的版本2.2.3更改支持仅范围1至5。

IDS Cisco Secure Policy Manager (CSPM)

Q. 应该使用CSPM哪个版本管理IDS传感器？

A. 目前CSPM版本2.3i是能管理IDS传感器的那个，而CSPM 3.0不能。如果使用CSPM管理传感器和其他Cisco Secure设备(例如PIXes，路由器)，您必须安装两个不同的CSPM版本(2.3i和3.x)在两个单独的窗口服务器。您能使用其中每一个服务器管理对应设备：传感器的PIXes的CSPM 2.3i和CSPM 3.x，路由器，等等。

Q. 如何配置CSPM管理IDS传感器和确保通信工作？

A. 参考配置在CSPM的Cisco Secure IDS传感器关于如何配置CSPM的更多信息管理您的IDS传感器和保证通信工作。

Q. 能否调整设备的签名有CSPM的？

A. 调整介入更改什么采取为了签名能射击(例如主机数量在清除的)和不含义设置操作和严重级别。

CSPM不能(在任何版本)调整设备的签名。它能只设置签名的操作和严重性。换句话说，严重性，并且操作联合到签名，但是不能放的CSPM能设置什么火签名。在传感器的SigWizMenu必须用于调整传感器。因为他们影响配置的不同的部分SigWizMenu和CSPM可能用于配置同样传感器。

注意： 如果使用UNIX向导版本2.2.3或以上， nrConfigure软件能配置SigWizMenu配置的一切。在您升级到2.2.3后，您应该使用nrConfigure而不是SigWizMenu调整签名。

相关信息

- 思科入侵防御系统产品支持
- Cisco安全入侵监测系统的文档
- Cisco安全入侵监测系统的问题信息通告(Field Notice)
- 技术支持和文档 - Cisco Systems