Cisco Secure Intrusion Detection System（3.1及更低版本）常見問題

目錄

簡介

本文檔包含有關Cisco Secure Intrusion Detection System(IDS)（以前稱為NetRanger，3.1及更低版本）的常見問題(FAQ)。

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

一般

問：在哪裡可以找到有關Cisco Secure IDS的其他資訊？

A.有關 Cisco Secure IDS的詳細信息，請參閱全套產品文檔。

問：如何更新整個IDS系統（IDS感測器+ IDS管理軟體）的簽名？

A.您必須分別升級感測器和管理平台簽名。請注意，管理軟體無法從*感測器*獲取簽名，因此也必須對其進行更新。從Cisco Secure Downloads（僅限註冊客戶）下載每個應用的最新簽名更新檔案（僅限註冊客戶）。 同一位置提供的自述檔案包含升級過程的說明。

問：在哪裡可以找到完整的簽名清單？

A.IDS簽名清單可通過Cisco Secure Encyclopedia**(僅限**註冊客戶)獲得。

問： UNIX IDS和獨立感測器上的使用者的預設密碼是什麼？

A.在UNIX IDS獨立感測器和IDS管理軟體上，使用者的預設密碼為「attack」（攻擊）**Netrangr**和**root**。當您發出**su**命令成為根使用者時，預設密碼為「attack」。 在入侵檢測系統模組(IDSM)刀片上，使用者名稱**ciscoids**的預設密碼為「attack」。

問：如何獲得入侵檢測系統模組(IDSM)刀片來轉儲其配置？

A.您需要一個本地FTP伺服器，以便可以上傳配置。

1. 在刀片式伺服器的診斷模式下輸入此命令。

   ```
   report systemstatus site user dir
   ```
2. 當系統詢問「Continue generating the System Report？（繼續生成系統報告？）」時，鍵入**y**以繼續。
3. 當系統提示時，鍵入指定使用者的FTP密碼。當進程完成時，您會收到一條消息，指明進程是否失敗或檔案是否傳送。

問：安裝/解除安裝IDS時，日誌檔案位於何處？

A.可在以下位置找到安裝/更新日誌：

- 控制器安裝日誌位於/var/adm/nrInstall.log。
- 感測器Service Pack更新日誌位於/usr/nr/sp-update/中。
- 簽名更新日誌位於/usr/nr/sig-update/中。

PIX for IDS上有哪些可用簽名？

A. IDS僅適用於PIX 6.0及更高版本。簽名包含在400000至400051的系統日誌消息中，稱為Cisco Secure IDS簽名消息。有關每個簽名的詳細資訊，請參閱PIX系統日誌消息文檔。

問：簽名更新發佈後是否可以通知我？

A.註冊Cisco IDS Active Update Notifications，以接收與Cisco Secure IDS相關的產品新聞的電子郵件警報。

問：我應該使用哪些應用程式來管理IDS感測器？它們之間有什麼區別？

A. 3.1之前的版本中，管理選項是使用Cisco Secure Policy Manager(CSPM)或UNIX Director。兩者之間的主要區別是CSPM在Windows伺服器上作為獨立的應用程式運行，而UNIX Director在UNIX Solaris伺服器上運行在HP OpenView之上。在IDS 3.1中，還可以通過PC上安裝的IDS事件檢視器(IEV)或使用3.1版感測器中的IDS裝置管理器來管理感測器。設定感測器後，預設情況下會使用安全套接字層(SSL)啟用裝置管理器。

問：在哪裡可以獲取軟體開發套件(SDK)軟體？

A. SDK軟體不向公眾提供。

IDS感應器

問：感測器版本3.x和4.x有何區別？

A. 4.0版提供了幾個新功能。最顯著的新功能是類似於Cisco IOS®的命令列介面(CLI)。

如何對IDS上的介面速度進行硬編碼？

A.不支援在3.x和4.0代碼中硬式設定速度/雙工，且功能要求有錯誤(思科錯誤ID CSCdy43054**(僅限**註冊客戶))。 該功能以5.0代碼形式提供，現在可以在配置介面中找到。

問：如何將感測器軟體從3.0版升級到3.1版？

答：客戶可以從Cisco Secure Downloads(僅限註冊客戶)下載3.1版更新檔案。

問：如何將感測器軟體從2.5版升級到3.0版？

答：客戶可以從Cisco Secure Downloads(僅限註冊客戶)下載3.0版更新檔案。 安裝軟體更新時，應採用2.5版中安裝Service Pack和特徵碼更新的方式。此過程在Cisco IDS感測器配置說明3.0版中詳述。

問：如何將感測器軟體從2.2版升級到3.0版？

答：3.0升級檔案可以從Cisco Secure Downloads(僅限註冊客戶)**下載，但此檔案無法更新2.5之前的版本。您必須使用通過**產品升級工具(註冊客戶僅)提供的升級/恢復CD將軟體版本2.2升級到3.0。此CD的部件號為IDS-SW-U。

注意：您必須擁有有效的支援合約才能訂購升級/恢復光碟。

問：我已將鍵盤和顯示器連線到感測器上，但無法正確啟動。我該怎麼辦？

A.驗證您使用的是受支援的鍵盤和顯示器。某些品牌和型號與Cisco Secure IDS不相容，並阻止IDS感測器正確啟動。有關特定品牌的詳細資訊，請參閱Cisco Secure IDS裝置引導失敗。

問：在Cisco安全下載的IDS部分，我看到兩種型別的更新檔案（服務包和簽名）。這些檔案之間有何區別？

A.每個檔案都包含一組特定的軟體更新或附加內容，如此處所述的命名規則所示。

- IDS Sensor Appliance軟體的Service Pack更新包含IDS Sensor核心應用程式軟體的改進以及錯誤修復。例如，名為**IDSk9-sp-3.0-5-S17.bin** 的檔案包含軟體版本3.0(5)的更新以及簽名集編號17。
- 特徵碼更新檔案僅包含特徵碼（攻擊指紋）的更新。 例如，名為**IDSk9-sig-3.0-5-S18.bin** 的檔案包含用於3.0(5)感測器軟體的特徵碼集編號18。

客戶可從Cisco Secure Downloads(僅限註冊客戶)網站下載這些檔案。

問：如何判斷感測器是否正確配置為避開路由器？

A.以使用者身份登入感測器並**執**行以下命令：

```
nrgetbulk
```

您應該會收到類似於「*<IP_address>* Active」的響應，該響應顯示用於阻止攻擊的規避裝置的IP地址。以下輸出顯示命令語法和預期響應的示例：

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

您也可以登入到路由器並發出**who**命令，檢視感測器是否已登入。

問：當我發出nrconns命令時，我收到一條錯誤消息，指示「value not set」。如何解決此問題？

A.此錯誤消息表示感測器上的/usr/nr/etc/routes和/或/usr/nr/etc/hosts檔案可能存在問題。其.../routes檔案定義感測器和導向器之間的內部通訊。其.../hosts檔案定義感測器和控制器的名稱和IP地址。

您還可以以使用者**root**身份登入，運行**sysconfig-sensor**命令，然後再次輸入IDS通訊基礎設施資訊。

問：如何使用FTP從感測器複製日誌檔案並將其儲存在其他位置？

A.有關此過程的詳細信息，請參閱複製要檢視的IP日誌檔案。

問：感測器軟體2.5和3.1版中的configd守護程式發生了什麼情況？

A. Configd是處理UNIX控制器和2.2.x代碼庫中的感測器上的所有命令的守護程式。在2.5和3.0代碼庫中，此功能已被其他守護程式吸收，configd守護程式不再存在。

問：更新感測器上的特徵碼時，我收到`ERROR:NetRanger」` 錯誤消息。我該怎麼辦？

A.編輯感測器上的/usr/nr/etc/daemons檔案，以確保nr.packetd在守護程式清單中。然後停止並啟動服務。

在IDS 4210上，哪個是控制介面，哪個是監聽介面？

A.頂部的控制介面是**iprb1:**，底部的監聽介面是**iprb0:**。

問：為什麼在感測器上發出`ifconfig -a`命令時只看到一個介面？

A. ifconfig命令應僅顯示控制介面。感測器仍在使用另一個介面（監聽介面），但使用者應該無法看到它。如果需要檢視此介面，請以root使用者身份登入並發出**ifconfig -a**命令以確定介面名稱。發出**ifconfig** ***<interface>*** **plumb**命令以檢查特定介面的狀態。

問：如何對感測器上的介面速度進行硬編碼？

A.無需對感測器介面速度進行硬編碼，思科技術支援也不支援這種方法。如果交換器設定為自動交涉，介面就會與所連線的交換器交涉速度。從網路到感測器的通訊量是單向的（換句話說，感測器接收）。 因此，如果交換器顯示已交涉100半雙工，這通常就足夠了（假設交換器連線埠為100 M）。

UNIX Director

問：能否將新的3.0感測器與2.2.x版本的Director配合使用？

答：是，但您應將控制器軟體升級到2.2.3版或更高版本。註冊客戶可以從Cisco Secure Downloads下載這些檔案(僅限註冊客戶)。

問：如何得知我使用的導向器守護程式的版本？

A.發出**cat /usr/nr/VERSION 命令，並檢查輸出包含的版本號。**

注意：Director上的nrvers命令的輸出會顯示Director上運行的守護程式的版本，但不會顯示Director軟體本身的版本。

問：如何讓控制器轉儲其配置？

A.以使用者網路身份**登入**，然後執行指令碼/usr/nr/bin/director/nrCollectInfo將配置資訊傳送到名為/usr/nr/var/tmp/Report_For_Director.html的檔案。

問：我的HP OpenView顯示屏上有很多錯誤（可能超過1000個）。我刪除了他們，但是他們一直回來。為什麼？

A.如果IDS Director出現大量錯誤，並且無法全部顯示，它會開始緩衝到檔案。停止IDS守護程式並退出已開啟以刪除檔案的所有OpenView對映。刪除檔案**/usr/nr/var/nrDirmap.buffer.default**，然後重新啟動IDS守護程式和OpenView對映。

問：在HP OpenView地圖上獲取警報時遇到問題。我經常在/usr/nr/var/errors.nrdirmap中出錯。我該怎麼辦？

A.在2.2.2之前的IDS版本中，最簡單的方法就是刪除OpenView資料庫。資料庫位於/var/opt/OV/share/databases/openview中。完成以下步驟以刪除OpenView資料庫。

1. 使用**ovstop**命令關閉所有開啟的OpenView對映，然後使用**nrstop**命令停止IDS服務。
2. 以使用者**root**身份登入，並發出**/usr/nr/bin/director/nrDeleteOVwDb**。
3. 刪除/usr/nr/var目錄中的所有"error.*"檔案（例如errors.configd）。
4. 使用**nrstart**命令重新啟動服務，然後使用**ovstart**命令重新啟動OpenView。 **注意**：在Director版本2.2.2中，只能刪除OpenView資料庫的IDS部分，而不能刪除整個資料庫。IDS Director Configuration Guide中介紹了此過程。

問：我無法在OpenView地圖上收到警報。Director上的/usr/nr/var/errors.postofficed檔案包含消息，指出nrdirmap未授權在此電腦上運行。如何修復此問題？

A.執行此命令。

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

確保使用者**網路**擁有檔案，然後重新啟動IDS服務。

問：運行nrConfigure實用程式並按兩下Director時，會收到以下消息："找不到<director_name>的傳*感器型別*。請檢查Postoffice和資料包是否正在運行」。 我該怎麼辦？

A.出現此問題的原因是nrConfigure在導向器的守護程式檔案（它不應看到此進程）中看到打包的進程。 當nrConfigure像查詢感測器一樣查詢控制器的版本時，控制器不能響應感測器版本。

完成以下步驟以解決此問題。

1. 編輯/usr/nr/etc/daemons檔案並刪除nr.packetd 、 nr.sensord和nr.managed的條目，因為這些進程應僅在感測器上運行。
2. 使用**nrstop**命令停止服務，然後使用**nrstart**命令重新啟動服務。
3. 確保nrConfigure已關閉。
4. 使用**ovw**命令啟動OpenView。
5. 選擇**Security > Advanced > nrConfigure DB > Delete**以刪除損壞的nrConfigure資料庫。
6. 當要求繼續時，請輸入**yes**。
7. 在OpenView主視窗中突出顯示您的控制器和所有感測器。
8. 選擇**Security > Advanced > nrConfigure DB > Create**以使用電腦的當前配置版本建立新的nrConfigure資料庫。

問：如何防止在OpenView對映上預設啟用nrdirmap應用程式？

A.在UNIX Director上運行IDS應用程式的使用者也可以在OpenView上運行其他應用程式。這並非建議，但在某些情況下無法避免。問題在於每個OpenView對映預設啟用nrdirmap，當其他應用程式在OpenView上運行時，這是不可取的。

在UNIX Director上完成以下步驟以更改預設值，以便可以選擇哪些對映上啟用了nrdirmap。

1. 以使用者網路身**份登入**。
2. 鍵入**cd $OV_REGISTRATION/C**。(OV_REGISTRATION是環境變數的一部分。通常的路徑是/etc/opt/OV/share/registration/C。)
3. 鍵入**su root**。
4. 編輯nrdirmap檔案並更改「命令」行，如下輸出所示：

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

5. 儲存nrdirmap檔案。
6. 回收OpenView。現在，當使用**ovw**命令啟動對映時，鍵入**ps -ef | grep dirmap應產**生類似於此處所示的輸出。使用-d開關注意nrdirmap。

```
>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
```

現在，在OpenView中建立的新對映在預設情況下沒有啟用nrdirmap。如果要建立已安裝nrdirmap的對映，必須按照以下過程所述，從OpenView GUI執行該操作。

1. 在OpenView主選單中，選擇**Map > New**，然後輸入新對映的名稱。
2. 在可配置的應用程式下，您應該看到NetRanger/Director。選擇**NetRanger/Director**，然後點選此對映的**配置**。
3. 對於「是否應該為此對映啟用nrdirmap？」選項，如果要啟用nrdirmap，請選擇**True**。

4. 選擇**Verify**，然後按一下**OK**。

問：我升級到導向器2.2.3版，但現在，我不能將事件的嚴重性設定為高於5的級別，即使我能在較早版本中這樣做。為什麼會這樣？

A.在Director的2.2.3版中，嚴重性級別已更改，僅支援1到5範圍。

IDS思科安全原則管理員(CSPM)

問：我應該使用哪個版本的CSPM來管理我的IDS感測器？

A.目前的CSPM 2.3i版是可以管理IDS感測器的版本，而CSPM 3.0不能。如果使用CSPM管理感測器和其他Cisco安全裝置（例如PIX、路由器），則必須在兩個獨立的Windows伺服器上安裝兩個不同的CSPM版本（2.3i和3.x）。可以使用每個伺服器來管理相應的裝置：感測器的CSPM 2.3i和用於PIX、路由器等的CSPM 3.x。

問：如何配置CSPM以管理IDS感測器並確保通訊正常？

A.有關如何配置CSPM以管理IDS感測器並確保通訊正常工作的詳細資訊，請參閱在CSPM中配置Cisco Secure IDS感測器。

問：是否可以使用CSPM調整裝置的簽名？

A.調優涉及更改特徵碼激發所需的條件（如掃描中的主機數量），並不意味著設定操作和嚴重性級別。

CSPM無法（在任何版本中）調整裝置的簽名。它只能設定簽名的操作和嚴重性。換句話說，CSPM可以設定與簽名關聯的嚴重性和操作，但不能設定觸發該簽名的操作。必須使用感測器上的SigWizMenu來調整感測器。SigWizMenu和CSPM都可用於配置同一感測器，因為它們會影響配置的不同部分。

注意：如果使用UNIX導向器2.2.3版或更高版本，nrConfigure實用程式可以配置SigWizMenu配置的所有內容。升級到2.2.3後，應使用nrConfigure而不是SigWizMenu來調整簽名。

相關資訊

- **思科入侵防禦系統產品支援**
- **思科安全入侵檢測系統文檔**
- **思科安全入侵檢測系統的現場通知**
- **技術支援與文件 - Cisco Systems**