IDS 4.0/AIP-SSM/IPS 5.0及更高版本常見問題

目錄

簡介

本文回答與Cisco Secure Intrusion Detection System(IDS)4.0、Advanced Inspection and Prevention Security Services Module(AIP SSM)和Cisco Intrusion Prevention System(IPS)5.0及更高版本相關的最常見問題(FAQ)。

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

IDS 4.0

問：我已在新伺服器上安裝了IDS MC和SecMon，現在我想將所有配置（使用者、裝置等）從舊伺服器匯入新伺服器。我該怎麼做？

A.執行此操作的最簡單方法是啟動您的新VMS伺服器，然後使用此新框發現感測器。

注意：新增感測器時，不要手動新增感測器。選中**discover settings**框。

發現感測器後，將其匯入**SecMon**。所有配置都儲存在感測器上。在您構建新伺服器後，應該會遇到特徵碼設定、過濾器等。確保將IDS MC更新為最新簽名。

Q. IDS-4215收到**idsPackageMgr:**級IDS恢復分割槽時，出現無效引數錯誤消息。要解決此問題，需要做什麼？

這是一個製造業的問題。某些客戶收到的IDS-4215帶有錯誤的基礎映像(4.0)。 請完成以下步驟。

1. 下載恢復分割槽映像(僅限註冊客戶)。
2. 通過CLI應用恢復分割槽映像升級：
   ```
   sensor#configure terminal
   sensor(config)#upgrade METHOD://USERNAME@SERVER/PATH/
       IDS-4215-K9-r-1.1-a-4.1-1-S47.tar.pkg
   ```
3. 一旦應用恢復分割槽映像，4215將恢復為正常運行的4.1(1)4215 base。
   ```
   sensor(config)#recover application-partition
   ```

問：當我從2位訊號級別包升級到3位訊號級別包時，例如S100或更高版本，如4.1(4)S99到4.1(4)S100，自動更新功能失敗。如何修復此問題？

注意：Cisco VMS和CLI客戶不會遇到此問題。

問題的原因是分析檔名時使用的排序邏輯。它是字母數字排序，但應當是數字。解決方法是使用CLI（或VMS）升級到3位特徵碼級別軟體包，例如S100或更高版本。完成此操作後，自動更新將再次開始運行。如需詳細資訊，請參閱Cisco錯誤ID CSCef07999(僅限註冊客戶)。

問：「身份驗證令錯誤資訊表示什麼？

A.為了解決此問題，請兩次使用預設密碼(cisco)，然後從配置模式更改密碼。IDS要求輸入預設密碼兩次。

例如：

```
login:cisco
Password:cisco
Enter current password:cisco
Enter new password: ***
Re-enter new password: ***
```

問：如何從Switch中刪除IDSM?

A.只有在禁用電源後才能刪除該模組。請完成以下步驟：

1. 在感測器CLI上，發出**reset power down**命令。
2. 感測器完成關機後，從交換機CLI發出**no power enable module(module_number)**命令（對於Cisco IOS）或**set module power down(module_number)**命令（對於CatOS）。
3. 按刀片式伺服器上的「shutdown（關機）」按鈕。
4. 關閉機箱的物理電源。當狀態指示燈顯示較長的綠色時，可以安全地移除模組。

IPS 5.0及更高版本

問：我已配置迴避，但不知道如何配置阻止簽名功能。塊主機和塊連線有何區別？

A.阻止主機阻止來自該源地址的所有資料包。Block connection only blocks the one connection based on source and destination IP/port。PIX的工作方式略有不同。對於自動迴避，感測器會傳送來源IP、目的地IP、來源連線埠和目的地連線埠。PIX阻止來自該IP地址的所有資料包。PIX使用該附加資訊從其連線表中刪除該連線。如果連線尚未從連線表中刪除，則在理論上如果應用後不久即刪除shun，則原始連線可能尚未超時。這使得攻擊者能夠繼續對原始連線發起攻擊。從表中刪除連線可確保原來的連線不能用於在刪除shun後繼續攻擊。感測器無法對PIX上的單個連線進行迴避，因為PIX不支援使用**shun**命令來迴避單個連線。無論是否提供附加連線資訊，PIX **shun**命令始終避開源地址。

問：「錯誤資訊表示什麼？

A.此錯誤表示您的預設網關不正確，或者表示該IP、網路掩碼或預設網關不正確的通用錯誤消息。消息的`Fatal`部分表示在第一次失敗後，應用了先前的配置，但同樣失敗。感測器發出**ifconfig**和**route**命令，但這兩個命令中的一個或兩個都失敗。

Q.自動更新失敗，mainApp[343] Cid/E errSystemError http error response:500誤消息。此錯誤消息表示什麼意思？

答：此問題可能是自動更新功能，該功能不起作用，因為它設定為在偶數小時下載。嘗試將自動更新設定為隨機時間；即使只是八分鐘或晚上一小段時間，也可以解決此問題。

通常，問題會得到解決，並出現Error:http將檢索時間更改為非小時邊界，則會出現500錯誤消息。

注意：IPS無法自動更新簽名，並返回以下錯誤消息：

```
AutoUpdateHTTP[1,110] name=errSystemError
```

驗證以下專案以解決此問題：

- 驗證防火牆是否阻止感測器訪問Cisco.com。
- 驗證路由是否出現問題。
- 驗證是否已在網關裝置上為下游裝置正確配置NATing。
- 驗證使用者憑據是否正確。
- 將更新開始時間更改為奇數小時。

問：「execUpgradeSoftware:AnalysisEngine"誤消息表示嗎？

答：要解決此問題，請嘗試重新載入感測器或重新映像感測器。

問：如何解析錯誤消息Cid/W – DNSHTTPDNSProxyHTTPDNS?

A.完成以下任務以解決此問題：

- 禁用全域性關聯。
- 新增代理/DNS配置。

問：如何解決IPS因全球關聯運行狀況問題而收到的這些錯誤：「201012315:50:39.831 38.001 collaborationApp[655] rep/EX.X.82.127:443HTTPTLSTLS敗」和「collaborationApp[459] rep/Eibrs/1.1/drop/default/1296529950:URIIP「 」？

答：IPS無法訪問Internet，原因是埠問題，例如，路徑中的防火牆沒有為Internet訪問開啟正確的埠，或者可能是NAT問題。

為使全域性關聯功能完全正常，感測器首先通過https **update-manifests.ironport.com**聯絡以驗證使用者，然後通過HTTP連線下載GC更新。感測器從HTTP(updates.ironport.com)下載的檔案是全域性關聯使用的信譽資料。https update-manifests.ironport.com應始終解析為X.X.82.127地址，但http **updates.ironport.com的IP地址可能更改，這取決於您訪問的網際網路。**因此您必須檢查IP地址。如果啟用URL過濾，請在URL過濾器中為IPS管理介面IP新增一個例外，以便IPS可以連線到網際網路。

在以前的GC更新中發生損壞時，會發生此錯誤：

```
collaborationApp[459] rep/Eibrs/1.1/drop/default/1296529950:URIIP
```

通常，可以通過關閉GC服務然後重新開啟來更正此問題。在IDM中，選擇**Configuration > Policies**

> Global Correlation > Inspection/Reputation，將Global Correlation Inspection(和Reputation Filtering if On)設定為Off，應用更改，等待10分鐘，開啟功能並進行監視。

問：A**openConnection:IpAddrException badAddrStringHTTPDNS**在「信譽更新失敗」類別中收到錯誤消息。如何解決此問題？

A.驗證以下專案：

- 您必須擁有有效的IPS許可證，才能使全域性關聯功能發揮作用。
- 您必須配置HTTP Proxy伺服器或DNS伺服器，才能讓全域關聯功能運作。
- 由於全域性關聯更新通過感測器管理介面進行，因此防火牆必須允許tcp 443/80和udp 53通訊量。
- 確保您的感測器支援全域性關聯功能。如果不希望這樣做，請從IDM禁用全域性合作功能：轉至Configuration > Policies > Global Correlation > Inspection/Reputation，並將Global Correlation Inspection(和Reputation Filtering if**On**)設定為**Off。**

問：如何解決「**A global correlation update failed:openConnection:IPSIpAddrException badAddrString**」錯誤，是否有全域性關聯運行狀況問題？

A.如果您使用全域關聯(GC)，請確保名稱解析有效，例如DNS可訪問。此外，請檢查是否存在防火牆阻止的埠53。否則，如果要清除此消息，可以關閉GC功能。

問：如何解決從瀏覽**IME**初始化到MySQL的連線時出現異常錯誤消息？

答：當客戶嘗試在不支援的作業系統（例如Windows 7）上運行IME時，通常會出現此問題。

問：如何解決「**88-nsmc-c1IDMCisco Systems Inc.JNLPJAR IDM**的「**error connecting to sensor Failed to create sensor x.x.x.x:443 exuting idmx.x.x.x:443idm**

A.清除瀏覽器快取以解決此問題。

問：如果使用GUI，IPS上的非對稱模式是否可配置？

A.在6.0版中，IPS上的非對稱模式，該模式只能使用CLI進行配置，不能在GUI上使用。但是，在6.1版中，此功能也在GUI中提供。

問：如何使用IPS感測器解決延遲問題？

A.要解決此問題，請啟用非對稱模式處理，以允許感測器與流保持同步狀態，並維護對不需要兩個方向的引擎的檢查。使用以下設定：

```
IPS_Sensor#configure terminal
IPS_Sensor(config)#service analysis-engine
IPS_Sensor(config-ana)#virtual-sensor vs0
IPS_Sensor(config-ana-vir)#inline-TCP-evasion-protection-mode asymmetric
```

當VS0中的每個簽名都啟用內聯拒絕操作和拒絕資料包時，就會發生延遲問題。啟用所有簽名將產生延遲，因為IPS會檢查通過的所有單個資料包。最好根據網路流量僅啟用所需的特定簽名，以便解決延遲問題。

問： AIP-SSM是否幫助阻止Skype?

A. PIX/ASA無法阻止Skype流量。Skype能夠協商動態埠並使用加密流量。對於加密流量，幾乎不可能檢測到它，因為沒有要查詢的模式。

您最終可以使用Cisco IPS（入侵防禦系統）/AIP-SSM。它有一些簽名，可以檢測連線到Skype伺服器以同步其版本的Windows Skype客戶端。這通常在客戶端發起連線時完成。當感測器獲取最初的Skype連線時，您可以找到使用該服務的人員，並阻止從其IP地址啟動的所有連線。

問：為什麼感應介面IPS

A.在特徵碼更新和重新配置期間，sensorApp在處理更新中的新特徵碼時會停止處理資料包。網路驅動程式檢測到sensorApp已停止並從緩衝區提取任何新資料包。因此，網路驅動程式會執行不同的操作，具體取決於配置和感測器型號：

混雜接口 — 它使介面上的連結關閉，並在sensorApp再次開始監視時使連結重新開啟。

內嵌介面或內嵌VLAN對 — 取決於旁路設定：

- Bypass Auto — 驅動程式保持鏈路正常運行並開始通過資料包而不進行分析。在sensorApp重新開始監控後，它會恢復為通過sensorApp傳送資料包。
- Bypass Off — 驅動程式關閉介面上的連結（與混雜模式相同），並在sensorApp再次開始監視時將其重新開啟。

因此，如果感測器應用不從緩衝區提取資料包（這可能是因為沒有配置處理資料包的介面），則驅動程式可以將該介面置於down狀態。

感應介面擺動時會顯示以下日誌：

```
28Jun2011 09:03:09.483 6050.885 interface[409] Cid/W errWarning Inline
    databypass has started.
28Jun2011 09:03:13.639 4.156 interface[409] Cid/W errWarning Inline databypass
    has stopped.
28Jun2011 09:19:23.922 970.283 interface[409] Cid/W errWarning Inline databypass
    has started.
28Jun2011 09:19:27.486 3.564 interface[409] Cid/W errWarning Inline databypass
    has stopped.
```

問： IDS或入侵防禦系統(IPS)感測器是否維護密碼歷史記錄？

答：不，感測器不維護密碼歷史記錄。密碼隨時不可檢視。

問： IDS或入侵防禦系統(IPS)感測器是否支援系統日誌伺服器傳送日誌？

A.不。

問：在IPS中儲存事件的最大限制是什麼？

A.傳感器的本地事件僅儲存30 MB，一旦達到30 MB的限制，便會開始覆蓋自己。此限制不可配置。

問：如何編寫簽名以檢測傳入或傳出電子郵件中的foto[a-z]\.zip檔案？

A.使用STRING.TCP編寫檢測附件的簽名。請尋找類似以下內容：

```
Engine STRING.TCP
Enabled True
Severity informational
AlarmThrottle Summarize
CapturePacket False
Direction ToService
MinHits 1
Protocol =TCP
RegexString [Ff][Ii][Ll][Ee][Nn][Aa][Mm][Ee][=]["][Ff][Oo]
             [Tt][Oo][a-zA-Z][.][Zz][Ii][Pp]["]
ResetAfterIdle 15
ServicePorts 25
StorageKey =STREAM
```

問：如何配置FTP客戶端超時？

A.發出以下命令：

```
configure terminal
service host
networkParams
ftpTimeout 300 <timeout is in seconds>
```

問：如何將iplog狀態中的開始時間和結束時間轉換為可讀格式？

A.此輸出是自UNIX epoc以來的當前時間的十進位制表示。使用UNIX epoc計算器，例如位於UNIX日期/時間計算器站點的 計算器。輸入前10位數，因為此計算器是粒度到只有幾秒的，並且IDS儲存納秒。這表示最後九位數字已去除。從此輸出中的開始時間起，1084798479 = 51712:54:39 2004(GMT)就是您收到的時間。

在CLI中輸入iplog-status以接收此輸出：

```
"
Log ID:              138343946
IP Address:          xxx.xxx.xxx.xxx
Group:               0
Status:              completed
Start Time:          1084798479512524000
End Time:            1084798510136582000
Bytes Captured:      2833
Packets Captured:    14
"
```

問：「IOException when try to get certificate:java.security.cert.CertificateExpiredException"出現錯誤消息。如何解決這個問題？

A.要解決此錯誤消息，請登入到AIP-SSM，並在特權EXEC模式下發出tls generate-key 命令，如以下示例所示：

```
sensor#tls generate-key
```

注意：使用命令tls generate-key的此解決方案還解決了AIP-SSM無法連線到IME的問題。

問：「IOException:connectIME IME在IME中新增IPS時顯示錯誤消息。如何解決此問題？

A.為解決此錯誤消息，請選擇**控制面板>管理工具>服務，然**後重新啟動IME服務。

問：IPSIMECould not verify config username/password[IOEXception - connect timed out]如何解決此問題？

A.這表示IME和IPS感測器之間的通訊中斷。確保沒有軟體阻止SDEE。

問：「IME" 錯誤消息。如何解決此問題？

A.要解決此錯誤消息，請確認在IME中新增IPS時使用了正確的IP地址，並且還要檢查在IME電腦上運行的任何軟體防火牆，該防火牆可以阻止連線。

問：IDS或入侵防禦系統(IPS)感測器是否可以傳送電子郵件警報？

A. IDS感測器無法單獨傳送電子郵件警報。與IDS一起使用時，Security Monitor能夠在感測器觸發事件規則時傳送電子郵件通知。

有關如何使用安全監控器配置電子郵件通知的詳細資訊，請參閱配置電子郵件通知。

可以將Cisco IPS Manager Express(IME)配置為在Cisco IPS感測器觸發事件規則時傳送電子郵件通知消息（警報）。請參閱IPS 6.X及更高版本：使用IME的電子郵件通知配置示例以瞭解詳細資訊。

問：錯mainApp(getVersion) 當我嘗試連線到感測器時，出現錯誤消息。如何解決此問題？

A.重新啟動感測器以解決此問題。

問：警錯誤資訊顯示我的感測器上的特徵碼調整。如何解決此問題？

A.註銷未使用的簽名，以解決此問題，還應減少與註冊機構的客戶簽名數量。此外，建議不要在正規表示式中使用*和+元字元。

問：為什麼思科入侵防禦系統(IPS)感測器會發生延遲問題？如何解決此問題？

A.延遲問題可能由於非對稱路由而發生。嘗試禁用簽名1330以解決此問題。

問：是否可以在思科入侵防禦系統(IPS)感測器上禁用SSHv1並僅啟用SSHv2?

A.目前無法禁用SSHv1並僅啟用SSHv2。SSHv1和SSHv2同時啟用，不能單獨禁用。

問：錯=115000 KB/usr/cids/idsRoot/var110443 KB將感測器升級到版本4.1(5)時會顯示資訊。如何解決此問題？

A.此錯誤資訊是由於感測器記憶體不足而出現的。

完成以下任務即可解決此問題：

1. 登入到服務帳戶並成為根帳戶
2. 按如下所示刪除以下目錄：
```
# rm -rf /usr/cids/idsRoot/var/updates/files/S69
# rm -rf /usr/cids/idsRoot/var/updates/files/common
# rm /usr/cids/idsRoot/var/virtualSensor/*
# rm /usr/cids/idsRoot/var/.tmp/*
```
3. 現在嘗試升級感測器。如需詳細資訊，請參閱Cisco錯誤ID CSCsb81288(僅限註冊客戶)。

問：我收到mainApp[396] plane/E Error - accept()ASA-1錯誤消息。如何解決此錯誤？

A. mainApp[396] `plane/E Error - accept()-1`錯誤消息，指示Web伺服器無法讀取檔案，accept()程式失敗，當存在TLS連線時會產生檔案描述符。但正常行為不需要此檔案。這是無害的。

問：如何解決tls/W errTransport WebSession::sessionTask TLS錯誤消息？

A.此錯誤消息表示證書在模組上不再有效。完成以下步驟即可解決問題：

1. 從CLI重新生成證書：登入到感測器命令列。發出**tls generate**命令，然後按**enter**。注意顯示的指紋。
2. 將新證書拉入IME:開啟IME，在首頁的清單中找到感測器名稱。按一下右鍵感測器，然後按一下**Edit**。進入「Edit Device（編輯裝置）」螢幕後，按一下**OK**。忽略有關無法檢索感測器時間的任何警告。系統將提示您輸入新的安全證書（剛剛生成的證書）。 檢查以確保指紋匹配，然後按一下**Yes**。幾秒鐘後，感測器應再次在Event Status（事件狀態）中顯示Connected（已連線）。

問：當我嘗試登入IPS時，我收到以下錯誤消息：errSystemError-ct-sensorAPP.450 clientpipe。 如何解決此錯誤？

A.若要解決此錯誤，請使用**reset命令重新啟動IPS。**

問：AIP-SSM上的時間與思科自適應安全裝置(ASA)上的時間不同。 如何解決此問題？

A.要解決此問題，請使用NTP伺服器同步思科自適應安全裝置(ASA)和AIP-SSM上的時間。

有關詳細資訊，請參閱在IPS感測器上配置NTP。

問：如何在AIP-SSM上應用多個虛擬感測器？

A.AIP-SSM上的虛擬感測器無法應用到每個介面，因為AIP-SSM只有一個介面。建立多個虛擬感測器時，必須僅將此介面分配給一個虛擬感測器。您無需為其他虛擬感測器指定介面。

建立虛擬感測器後，必須使用**allocate-ips**命令將其對映到自適應安全裝置(ASA)上的安全上下文。您可以將多個安全情景對映到多個虛擬感測器。有關詳細資訊，請參閱配置AIP-SSM的*將虛擬感測器分配給自適應安全裝置環境*部分。

問： AIP-SSM支援的虛擬感測器的最大數量是多少？

A.最多可以支援四個虛擬感測器。

問：如果我使用SSH或IDM登入IPS，是否可以配置IPS 4240/IDSM/IDSM2，以便根據RADIUS/TACACS+伺服器驗證管理使用者？

A. TACACS+伺服器無法使用，但IPS 7.0.(4)E4版本支援RADIUS。如需詳細資訊，請參閱思科入侵防禦系統7.0(4)E4版本說明的*新增和變更資訊*以及*限制和限制*一節。此外，請參閱IPS 7.X:使用ACS 5.X作為Radius伺服器配置的使用者登入身份驗證示例配置。

問：許可證過期對IPS功能有何影響？

A.過期許可證對感測器的唯一影響是它會暫停特徵碼更新。

問：IPS簽名更新是否對服務或網路連線產生影響？

答：否。IPS簽名更新對服務或網路連線沒有影響。

問：要用最新簽名自動更新IPS模組，我需要輸入哪個URL?

A.允許IPS模組使用最新簽名自動更新所需的連結為：https://198.133.219.25/cgi-bin/front.x/ida/locator/locator.pl。

您必須使用思科使用者ID和密碼來完成IPS模組的更新。

注意：在6.x系列代碼中，不支援從Cisco.com進行自動更新。您必須手動下載特徵碼檔案並將其應用於感測器。6.x代碼中有一個自動更新功能；但是，這只能從本地檔案伺服器進行，而且必須手動下載簽名檔案。

問：IPS感測器是否易受X11埠轉發會話劫持漏洞的影響？

不，出於以下原因，它並不脆弱：

- 感測器沒有X11庫。因此，沒有可劫持的會話。
- SSH配置中未啟用X11埠轉發。
- IPv6未編譯到感測器核心中。攻擊該漏洞時需要執行此操作。

問：當ASA顯示大量警告和攻擊日誌時，為什麼AIP-SSM不顯示任何日誌？

A.發生這種情況的原因是，當ASA阻止某事物時，它不會傳遞到IPS進行重複檢測。因此，您在ASA和IPS上看不到重複的日誌。

問：使用者部署S518簽名集後，出現「`invalidValue:Edit string-xl-tcp sig XXXX has NO effect in this version`」錯誤消息。為什麼？

A.這是完整的錯誤消息：

```
evError: eventId=1284051856322985135 vendor=Cisco severity=warning
  originator:
```

```
    hostId: vbintestids03
    appName: sensorApp
    appInstanceId: 700
  time: offset=-240 timeZone=GMT-05:00 1286305251136551000
errorMessage: name=errWarning invalidValue:Editing string-xl-tcp
sig 21619 has NO effect
```

出現此問題是因為硬體上不支援string-xl-tcp或string-tcp-xl引擎。有關詳細資訊，請參閱IPS引擎E4發行說明。

問：當我使用自動更新功能自動更新ASA-SSM-10上的簽名時，我收到以下錯誤消息：**status=true。** 如何解決此問題？

A.此輸出顯示完整的錯誤消息：

```
autoUpgradeServerCheck:
    uri: https://XX.XX.XX.XX//cgi-bin/front.x/ida/locator/locator.pl
    packageFileName:
    result: No installable auto update package found on server  status=true
```

已生成此錯誤，並且簽名不會自動更新，因為S479之後的簽名定義更新需要E4引擎。為了解決此問題，您需要手動將感測器升級到7.0(2)E4。

註：感測器無法自動升級到E4，因為它需要7.0(2)並重新啟動感測器。

問：IPS 5.0 for NIDS模組上的自動更新功能無法正常工作。如何解決此問題？

A.此輸出顯示完整的錯誤消息：

```
autoUpgradeServerCheck:
    uri: ftp://hfcu-inet01@192.168.1.12//ips-update/
    packageFileName:
    result: No installable auto update package found on server  status=true
```

之所以會出現此問題，是因為FTP伺服器的目錄清單樣式不正確。為了解決此問題，請從現有的MS-DOS樣式目錄清單切換到UNIX樣式目錄清單。

若要修改目錄清單設定，請選擇**開始 > 程式檔案 > 管理工具**以開啟Internet服務管理器。然後轉到「主目錄」頁籤，將目錄清單樣式從MS-DOS更改為UNIX。

問：IPS-4255在升級期間收到TcpRootNode::expireNow()錯誤消息中的SensorApp fails。如何解決此問題？

答：此問題是由分析引擎故障導致的，已在思科錯誤ID CSCtb39179(**僅限**註冊客戶)中解決。 將感測器升級到版本7.0(4)E4以解決此問題。

問：在購買新許可證後嘗試執行許可證更新時，裝置報告以下錯誤：**errExpiredLicense – 如何解決此問題？**

A.當收到的許可證檔案無效時會發生此問題。要獲取有效的許可證檔案，請以註冊使用者身份登入Cisco.com，然後下載相應的許可證檔案。獲得有效的許可證檔案後，將其安裝在感測器上。

如果安裝新的許可證檔案，但您仍然收到一個錯誤，則可能是因為現有許可證檔案無效。為了解決

此問題，請完成以下步驟以刪除現有的無效許可證檔案：

1. 通過鍵入服務帳戶使用者名稱登入到服務帳戶。如果您沒有服務帳戶，請開啟IPS命令列，進入配置模式，然後輸入以下命令**使用者名稱*名稱*許可權服務密碼密*碼***
```
ciscoasa# session 1
Opening command session with slot 1.

Connected to slot 1. Escape character sequence is 'CTRL-^X'.
login:
Password:

IPS#
IPS#conf t
IPS(config)# username name privilege service password password
```
2. 登入到服務帳戶後，輸入**su**命令以轉至root（使用與服務帳戶相同的密碼）。
3. 刪除/usr/cids/idsRoot/shared/目錄中的檔案。**註：**請勿刪除host.conf檔案。輸入**cd /usr/cids/idsRoot/shared/**命令以轉至共用目錄。輸入**ls**命令以檢視目錄中的檔案。輸入**rm *file_name*** 命令以刪除檔案。**註：**請勿刪除host.conf檔案。
4. 輸入**/etc/init.d/cids restart**命令重新啟動感測器。
5. 安裝新許可證。

思科錯誤已歸檔以解決此行為。如需詳細資訊，請參閱CSCtg76339(僅限註冊客戶)。

問：錯誤消息是什`IpLog1712041197name=ErrLimitExceeded`誤消息表示什麼？如何解決此問題？

A.此錯誤是由IP日誌記錄中的資料包數量過多引起的。停用IP記錄功能以解決此問題。IP日誌記錄僅用於故障排除；思科建議您不要對所有簽名啟用此功能。

問：將感測器從s550更新到s551時，收到此錯誤：`signatureDefinitionsig0`。 如何解決此問題？

A.修改簽名23899.0會導致此問題。如需詳細資訊，請參閱Cisco錯誤ID CSCtn8452(僅限註冊客戶)。

問：我在感測器上收到以下錯誤：`autoUpdatecisco.com locatorHTTP`。 如何解決此問題？

A.檢查是否存在URL過濾、內容過濾或代理伺服器阻止自動更新發生。確保未阻止自動更新，並驗證提供的使用者憑據是否正確。

問：在運行版本6.2(3)E4的IPS感測器上收到以下XML錯誤消息：`IPSXML XML*`。 如何解決此問題？

A.此行為已由Cisco錯誤ID CSCsq50873(僅限註冊客戶)修正。 這是一個無關緊要的問題，除了接收過多的日誌之外，不會產生任何操作開銷。臨時解決方法是刪除感測器上的NTP相關配置。若要尋找永久解決方案，請升級至修正此錯誤的版本。

問：為什麼IME工作站在關閉客戶端的情況下仍會持續連線到受管伺服器？

A. IME可充當兩個Windows服務和GUI客戶端。關閉客戶端後，兩個Windows服務（Cisco IPS Manager Express和MySQL-IME）將繼續運行並收集來自受管感測器的事件，並將它們儲存在本地MySQL資料庫中；這樣就可以進行歷史報告。

IME客戶端應開啟對受管感測器的單一SDEE預訂，並再次使用此預訂進行後續事件檢索活動。從IME工作站到受管感測器的持續連線是預期行為。

問：是否可以將AIP-SSM模組用作SPAN目標？

答：不能。AIP-SSM模組不能用作SPAN目標，因為它僅用於監控通過ASA介面的流量。

問：為什麼在IPS升級到E3引擎後發現高CPU使用率？

答：通過E3引擎更新，IPS使用不同的演算法管理其空閒時間，並花費更多時間輪詢資料包，以減少延遲。增加的檢查會導致CPU使用率相應增加。在E3中測量CPU的正確方法不是根據CPU使用率，而是根據**Packet load percentage**（顯示正確的CPU使用率）。

問：為什麼我的IPS裝置上的運行狀況指示燈間歇性地變為紅色？

A.發生這種情況的原因是，遠端管理站上的證書不正確，運行諸如CS-MARS、CSM、IEV、VMS-IDS/IPSMC等軟體。為了解決此問題，請完成以下步驟：

1. 在遠端管理站上應用感測器的TLS證書。
2. 配置有效的DNS伺服器。

問：如何阻止IPS通過其介面來延遲HTTP的流量？

A.將感測器配置為在非對稱模式下工作可以解決此問題。為了將感測器置於非對稱模式保護，請完成以下步驟：

1. 轉至**Configuration > Policies > IPS policies**。
2. 按兩下虛擬**感測器**。
3. 轉至高級**選項**。
4. 在normalize mode下，選擇**Asymmetric mode protection**。
5. 按一下「**OK**」（確定）。
6. 重新啟動裝置以使更改生效。

相關資訊

- 思科安全入侵防禦系統支援頁面
- AIP-SSM故障排除
- 安全產品現場通知（包括CiscoSecure Intrusion Detection）
- 技術支援與文件 - Cisco Systems