

CSM 3.x -向資產中增加IDS感測器和模組

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[將裝置增加到安全管理器資產](#)

[增加IDS感測器和模組的步驟](#)

[提供裝置資訊-新裝置](#)

[疑難排解](#)

[錯誤消息](#)

[相關資訊](#)

簡介

本文檔提供有關如何在思科安全管理器(CSM)中增加入侵檢測系統(IDS)感測器和模組 (包括 Catalyst 6500交換機上的IDSM、路由器上的NM-CIDS和ASA上的AIP-SSM) 的資訊。

注意：CSM 3.2不支援IPS 6.2。CSM 3.3支援此功能。

必要條件

需求

本文檔假設CSM和IDS裝置已安裝並正常工作。

採用元件

本檔案中的資訊是根據CSM 3.0.1。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

將裝置增加到安全管理器資產

當您將裝置增加到安全管理器時，您將引入裝置的標識資訊範圍，例如裝置的DNS名稱和IP地址。

增加裝置後，它會顯示在安全管理器裝置資產中。僅當將裝置增加到資產中後，才能在安全管理器中管理該裝置。

您可以使用以下方法將裝置增加到安全管理器資產：

- 從網路新增裝置。
- 新增尚未連線到網路上的裝置
- 從裝置和憑證儲存庫(DCR)中增加一個或多個裝置。
- 從配置檔案中增加一個或多個裝置。

注意：本文檔重點介紹方法：增加尚未在網路中運行的新裝置。

增加IDS感測器和模組的步驟

使用Add New Device選項可將單個裝置增加到安全管理器資產中。您可以使用此選項進行預配置。您可以在系統中建立裝置、將原則指定給裝置，並在收到裝置硬體之前產生組態檔。

收到裝置硬體時，必須準備由安全管理器管理的裝置。有關詳細資訊，請參閱[準備供安全管理器管理的裝置](#)。

此過程顯示如何增加新的IDS感測器和模組：

1. 按一下工具欄中的Device View按鈕。

系統將顯示Devices頁面。

2. 在裝置選擇器中，按一下Add按鈕。

系統將顯示New Device - Choose Method頁面，其中包含四個選項。

3. 選擇Add New Device，然後按一下Next。

系統將顯示New Device - Device Information頁面。

4. 在相應的欄位中輸入裝置資訊。

有關詳細資訊，請參閱[提供裝置資訊-新裝置](#)部分。

5. 按一下「Finish」（結束）。

系統執行裝置驗證任務：

- 如果資料不正確，系統會產生錯誤訊息，並顯示發生錯誤的頁面，並顯示對應的紅色錯誤圖示。
- 如果資料正確，裝置會增加到資產中，並顯示在裝置選擇器中。

提供裝置資訊-新裝置

請完成以下步驟：

1. 選擇新裝置的裝置型別：

- a. 選擇頂級裝置型別資料夾以顯示支援的裝置系列。
- b. 選擇裝置系列資料夾以顯示支援的裝置型別。
 - a. 選擇Cisco Interfaces and Modules > Cisco Network Modules 以增加Cisco IDS Access Router Network Module。同樣地，選擇Cisco Interfaces and Modules > Cisco Services Modules 以增加所示的AIP-SSM和IDSM模組。
 - b. 選擇Security and VPN > Cisco IPS 4200 Series Sensors以將Cisco IDS 4210感測器增加到CSM清單。
- c. 選擇裝置型別。

注意：增加裝置後，您無法更改裝置型別。

該裝置型別的系統對象ID顯示在SysObjectId欄位中。依預設會選取第一個系統物件ID。如果需要，您可以選取另一個選項。

2. 輸入裝置身份資訊，如IP型別（靜態或動態）、主機名、域名、IP地址和顯示名稱。
3. 輸入裝置作業系統資訊，如作業系統型別、映像名稱、目標作業系統版本、上下文和操作模式。
4. 系統將顯示Auto Update或CNS-Configuration Engine欄位，具體取決於您選擇的裝置型別：
 - Auto Update -為PIX防火牆和ASA裝置顯示。
 - CNS-Configuration Engine -針對Cisco IOS®路由器顯示。

注意：此欄位對於Catalyst 6500/7600和FWSM裝置處於非活動狀態。

5. 請完成以下步驟：

- 自動更新-按一下箭頭以顯示伺服器清單。選擇管理裝置的伺服器。如果伺服器沒有出現在清單中，請完成以下步驟：
 - a. 按一下箭頭，然後選擇+增加伺服器...出現「Server Properties (伺服器屬性)」對話方塊。
 - b. 在必要欄位中輸入資訊。
 - c. 按一下「OK」(確定)。新伺服器會新增至可用伺服器清單。
- CNS-Configuration Engine -顯示不同的資訊，具體取決於您選擇的是靜態IP型別還是動態IP型別：

Static -點選箭頭顯示配置引擎清單。選擇管理裝置的配置引擎。如果Configuration

Engine未出現在清單中，請完成以下步驟：

- a. 點選箭頭，然後選擇+增加配置引擎...系統將顯示Configuration Engine屬性對話方塊。
 - b. 在必要欄位中輸入資訊。
 - c. 按一下「OK」（確定）。新的配置引擎會增加到可用配置引擎清單中。
- Dynamic -點選箭頭以顯示伺服器清單。選擇管理裝置的伺服器。如果伺服器沒有出現在清單中，請完成以下步驟：
 - a. 按一下箭頭，然後選擇+增加伺服器...出現「Server Properties（伺服器屬性）」對話方塊。
 - b. 在必填欄位中輸入資訊。
 - c. 按一下「OK」（確定）。新伺服器會新增至可用伺服器清單。

6. 請完成以下步驟：

- 要在安全管理器中管理裝置，請選中Manage in Cisco Security Manager覈取方塊。這是預設值。
- 如果要增加的裝置的唯一功能是充當VPN終端，請取消選中Manage in Cisco Security Manager覈取方塊。

安全管理器將不在此裝置上管理配置或上載或下載配置。

7. 選中Security Context of Unmanaged Device覈取方塊以管理其父裝置（PIX防火牆、ASA或FWSM）不由安全管理器管理的安全上下文。

您可以將PIX防火牆、ASA或FWSM劃分為多個安全防火牆，也稱為安全情景。每個情景都是獨立的系統，具有自己的配置和策略。您可以在安全管理器中管理這些獨立上下文，即使父級（PIX防火牆、ASA或FWSM）不由安全管理器管理。

注意：僅當您在裝置選擇器中選擇的裝置是支援安全情景的防火牆裝置（例如PIX防火牆、ASA或FWSM）時，此欄位才處於活動狀態。

8. 選中在IPS Manager中管理覈取方塊以便在IPS Manager中管理Cisco IOS路由器。

僅當從裝置選擇器中選擇了Cisco IOS路由器時，此欄位才處於活動狀態。

注意：IPS Manager只能在具有IPS功能的Cisco IOS路由器上管理IPS功能。有關詳細資訊，請參閱IPS文檔。

如果選中Manage in IPS Manager覈取方塊，則必須同時選中Manage in Cisco Security Manager覈取方塊。

如果所選裝置是IDS，則此欄位處於非活動狀態。但是，由於IPS Manager管理IDS感測器，因此該覈取方塊處於選中狀態。

如果所選裝置是PIX防火牆、ASA或FWSM，則此欄位處於非活動狀態，因為IPS管理器不管理這些裝置型別。

9. 按一下「Finish」（結束）。

系統執行裝置驗證任務：

- 如果輸入的資料不正確，系統將生成錯誤消息並顯示發生錯誤的頁面。
- 如果輸入的資料正確，裝置會增加到資產中，並顯示在裝置選擇器中。

疑難排解

使用本節內容，對組態進行疑難排解。

錯誤消息

將IPS增加到CSM時，會顯示Invalid device: Could not deduce the SysObjId for the platform type錯誤消息。

解決方案

完成以下步驟即可解決此錯誤訊息。

1. 在Windows中停止CSM守護程式服務，然後選擇Program Files > CSCOPx > MDC > athena > config > Directory，您可在其中找到VMS-SysObjID.xml。
2. 在CSM系統上，將預設情況下位於C:\Program Files\CSCOPx\MDC\athena\config\directory中的原始VMS-SysObjID.xml檔案替換為最新的VMS-SysObjID.xml檔案。
3. 重新啟動CSM協助程式管理員服務(CRMDmgtd)，然後再次嘗試新增或探索受影響的裝置。

相關資訊

- [Cisco Security Manager支援頁面](#)
- [Cisco Intrusion Detection System支援頁](#)
- [技術支援與文件 - Cisco Systems](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。