連線事件似乎從FireSIGHT管理中心消失

目錄

簡介

本文檔介紹如何確定根本原因，以及如何解決系統運行幾天後連線事件從FireSIGHT管理中心消失的問題。這可能是由於管理中心的配置設定造成的。

必要條件

需求

思科建議您瞭解FireSIGHT管理中心。

採用元件

本檔案中的資訊是根據以下硬體和軟體版本：

- FireSIGHT管理中心
- 軟體版本5.2或更高版本

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。

疑難排解

第1步：確定儲存事件的數量

要確定FireSIGHT管理中心上儲存的連線事件數，

1. 選擇**Analysis > Connections > Table View of Connection Events**。
2. 將「時間視窗」擴展為包含所有當前事件的範圍，例如12個月。
3. 請注意頁面底部的總行數。按一下最後一頁並記下上次可用連線事件的時間戳。

此資訊可讓您瞭解使用當前配置可以保留連線事件的數量和持續時間。

第2步：確定日誌記錄選項

檢視正在記錄的連線，以及連線記錄到的流中的位置。您應該根據組織的安全和合規性需求記錄連線。如果您的目標是限制生成的事件數，則僅對分析至關重要的規則啟用日誌記錄。但是，如果您希望獲得網路流量的廣泛檢視，則可以啟用其他訪問控制規則或預設操作的日誌記錄。您可以禁用非基本流量的連線日誌記錄，以幫助將連線事件保留更長時間。

提示：為了最佳化效能，思科建議您記錄連線的開始或結束，但不能同時記錄兩者。

註：對於單個連線，連線結束事件包含連線開始事件中的所有資訊以及在會話期間收集的資訊。對於信任和允許規則，建議使用連線終止。

此圖表說明了每個規則操作可用的不同日誌記錄選項：

規則操作或日誌記錄選項	開始時登入	結束時登入
信任 預設操作：信任	X	X
允許 預設操作：入侵	X	X
預設操作：發現 監視		X（必需）
封鎖 封鎖並重設	X	
預設操作：阻止 互動式封鎖 互動式封鎖並重設	X	X（如果繞過）
安全情報	X	

第3步：調整連線資料庫的大小

根據系統策略中的Maximum Connection Events設定修剪連線事件。要更改設定，請：

1. 選擇**System > Local > System Policy**。
2. 按一下*pencil*圖示以編輯當前應用的策略。
3. 選擇**Database > Connection Database > Maximum Connection Events**。
4. 更改**Maximum Connection Events**的值。
5. 按一下**Save Policy and Exit**，然後按一下**Apply**策略到裝置。

可儲存的最大連線事件數取決於管理中心模型：

注意：最大事件限制在連線事件和安全情報事件之間共用；為兩個事件配置的最大值的總和不

能超過最大事件限制。

管理中心型號	最大事件數
FS750、DC750	五千萬
FS1500、DC1500	1億
FS2000	3億
FS3500、DC3500	5億
FS4000	10億
虛擬裝置	1000萬

注意：資料庫限制增加可能會對裝置效能產生不利影響。為了改善效能，您應該定製事件限制來限制定期處理的事件數量。

對於在時間範圍內顯示事件計數的小元件，事件總數可能無法反映出事件檢視器中可以提供其詳細資料的事件數。出現這種情況是因為系統有時會修剪較舊的事件詳細資訊以管理磁碟空間使用情況。為了最大限度地減少事件詳細資訊修剪的發生，您可以微調事件日誌記錄，以只記錄對部署最重要的那些事件。

相關資訊

- 配置資料庫事件限制
- 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）。