記錄器重新啟動生成舊的SNMP陷阱

目錄

簡介

本檔案介紹Cisco Unified Intelligent Contact Management(ICM)企業環境中的過時簡單網路管理協定(SNMP)陷阱消息，並提供了兩種可能的方法來防止報告這些資訊性消息。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco ICM企業版
- 瞭解SNMP

採用元件

本文件所述內容不限於特定軟體和硬體版本。

慣例

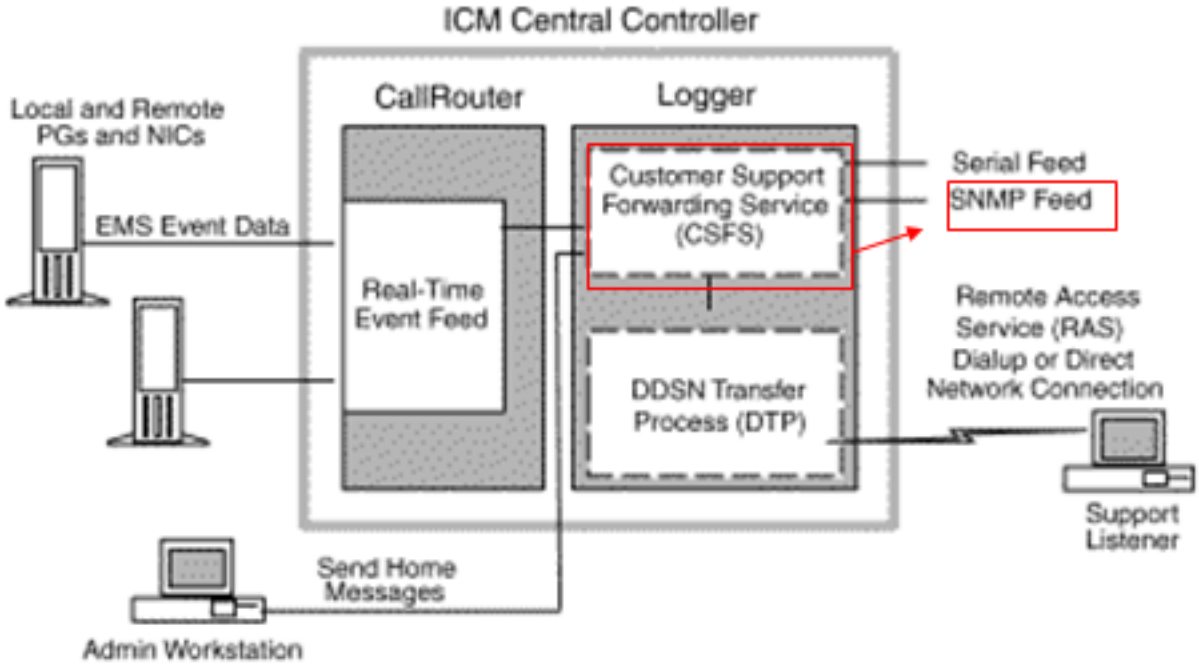
如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

背景資訊

ICM的記錄器收集來自系統所有元件的事件和消息。記錄器將此資訊傳遞給客戶支援轉發服務(CSFS)進程，該進程接收事件、過濾事件並將其儲存在記錄器上的記憶體中，如圖1所示。

SNMP饋送是一種可選的ICM功能，允許您通過SNMP相容介面(TCP/IP)接收事件饋送。 使用SNMP源時，可以將其配置為將SNMP陷阱傳送到所需的管理客戶端。

圖1 - CSFS饋送



問題

根據設計，在雙工環境中重新啟動一個記錄器後，或者如果一個記錄器跳出，則可能會生成過期的SNMP陷阱並在配置的SNMP管理站中顯示。 當CSFS進程作為記錄器的一部分啟動時，它收到要報告給遠端客戶端的事件（警報）（通過SNMP、系統日誌或遠端監視服務[RMS]），並將該事件的副本儲存到記憶體中，稱為基本記錄。在雙工、容錯的環境中，當一端的CSFS進程關閉並重新啟動時，它從另一端接收所有未處理的基礎記錄，並將它們轉發給管理客戶端。

解決方案

本節介紹可用於防止報告過期SNMP資訊的可能方法。解決方案1顯示如何從記錄器中清除過期的SNMP資訊，解決方案2顯示如何從管理客戶端抑制或過濾過期的SNMP資訊。

解決方案1

清除基本記錄。為此，請同時停止兩端的記錄器，然後重新啟動它們。此程式會清除來自CSFS進程的所有過期SNMP陷阱。

注意：此過程應在維護時段或低路由影響時間內完成。

1. 停止記錄器B。
2. 停止記錄器A。
3. 啟動記錄器A。
4. 啟動記錄器B。

解決方案2

另一個解決方案是讓客戶的管理客戶端過濾器警報早於某個持續時間（例如，一週）。SNMP服務傳送到客戶的第二方應用程式（如HP OpenView）的每個陷阱都包含實際事件發生的時間戳。然後，客戶可以將其第三方應用程式配置為忽略具有早於特定天數或周的時間戳的警報。必須注意的是，思科聯絡中心技術支援中心(TAC)不協助配置客戶選擇用來管理這些事件/陷阱的特定第三方應用程式。

相關資訊

- Cisco Unified Intelligent Contact Management Enterprise支援文檔
- 技術支援與文件 - Cisco Systems