恢復由安全終結點隔離的檔案

目錄

簡介

本文檔介紹如何從安全端點控制檯恢復由安全端點聯結器隔離的檔案。

必要條件

需求

思科建議您瞭解以下主題：

- 思科安全終端主控台

採用元件

本檔案中的資訊是根據以下軟體版本：

- 安全終端控制檯5.4.2025030619

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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

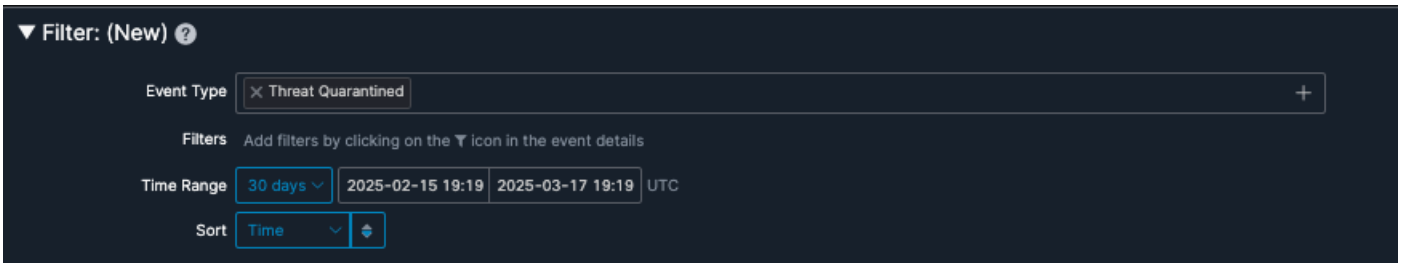
問題

當安全終結點(SE)聯結器隔離的檔案已知安全時，可以檢索該檔案以進行檔案分析、誤報提交或還原。管理員可以直接從安全終結點控制檯執行此操作。

解決方案

1.導航到SE控制檯上的Events頁。

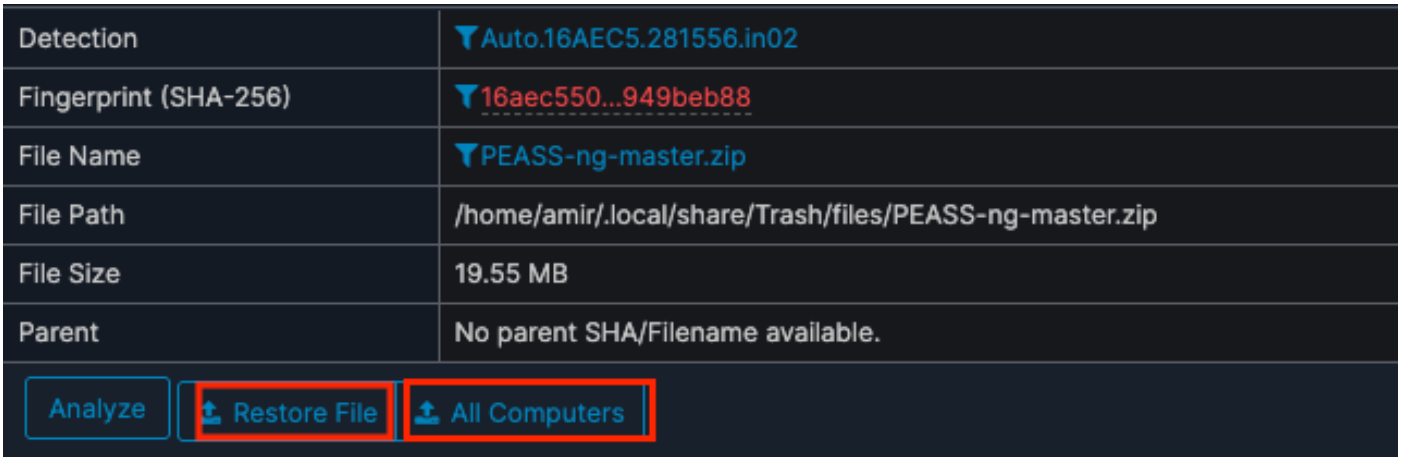
2.通過選擇過濾器Event Type = Threat Quarantined來過濾事件以顯示所有成功的隔離區。



威脅隔離事件型別

3.確定與需要還原的檔案相關聯的檢測事件。

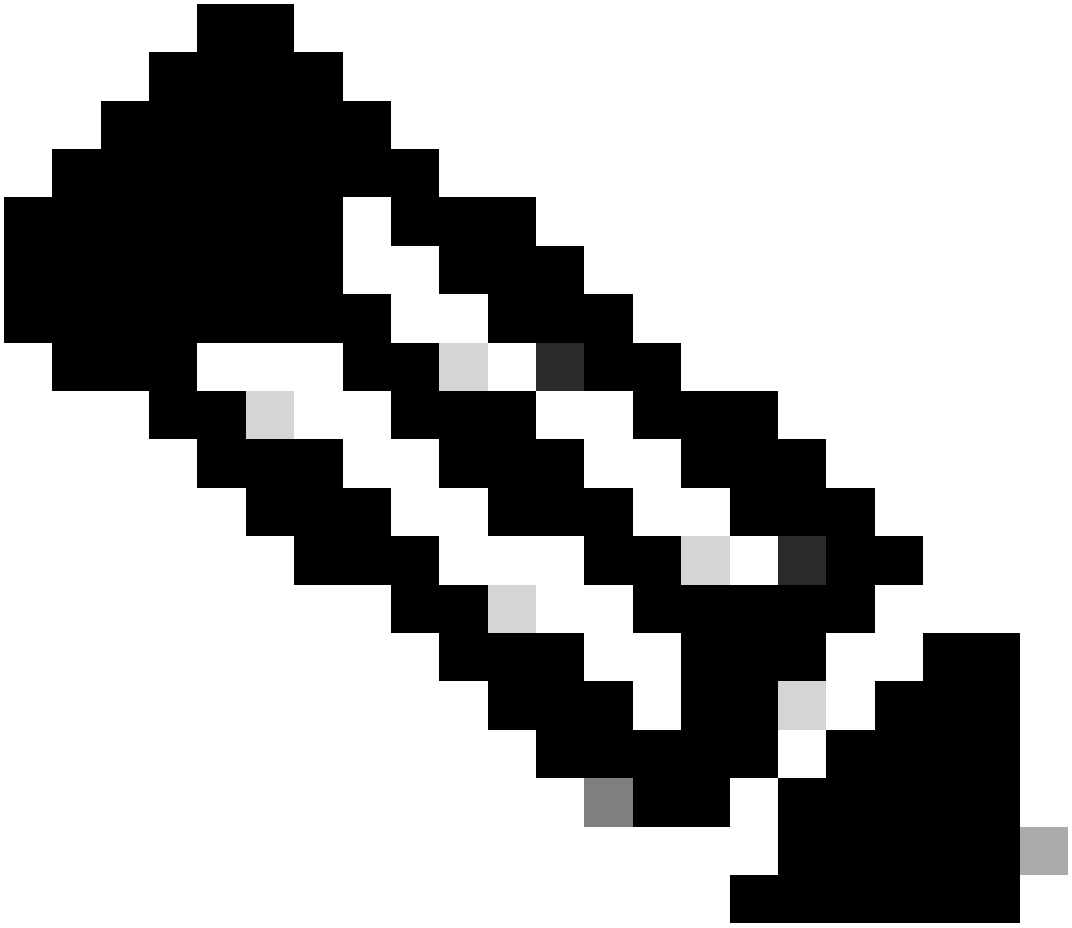
4.展開事件詳細資訊以訪問恢復檔案選項。選擇恢復檔案將恢復受影響電腦上的檔案。選擇All Computers可在檔案被隔離的所有電腦上恢復該檔案。



恢復檔案選項

5. 「波動訊號間隔」是聯結器呼叫總部以檢視是否有任何檔案由管理員恢復的頻率。一旦受影響的電腦聯機或發生下一個波動訊號間隔，就會恢復檔案。

6.如果檔案受信任，請將其新增到允許清單中，以防止再次隔離該檔案。



附註：檔案在隔離區中保留30天，或者在隔離資料夾達到100 MB時清除最舊的檔案。清除隔離的檔案後，無法再恢復這些檔案。

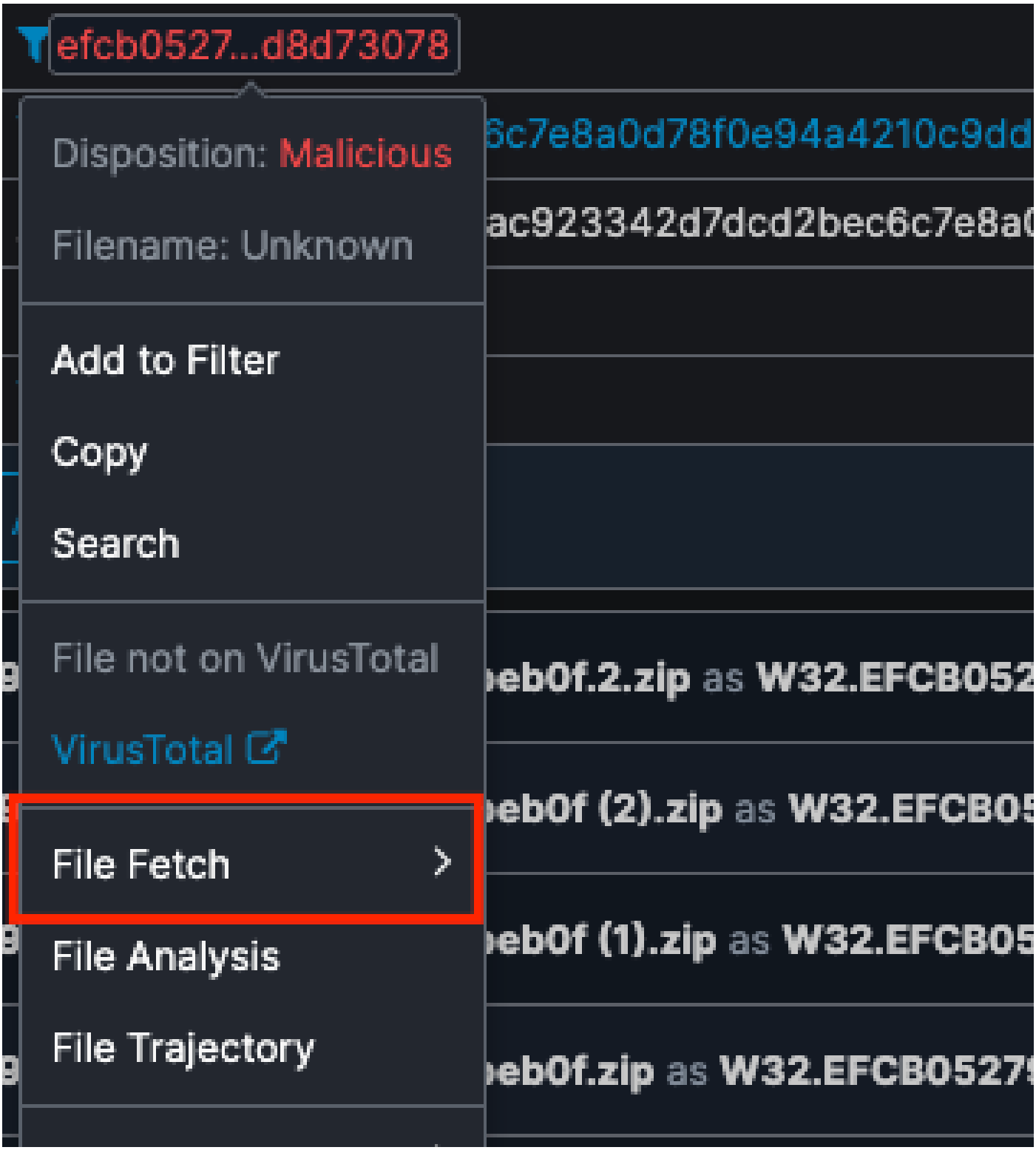
如果您只需下載隔離檔案以進行威脅分析或進行誤報提交而不將其還原到您的環境，可以使用檔案提取功能。下載隔離檔案的步驟：

1.導航到SE控制檯上的Events頁。

2.通過選擇過濾器Event Type = Threat Quarantined來過濾事件以顯示所有成功的隔離區。

3.確定與需要下載的檔案相關聯的檢測事件。

4.按一下隔離檔案的SHA-256值，顯示「檔案提取」選項。



檔案擷取

這提供了檔案回遷的狀態、啟動回遷的選項以及檢視檔案儲存庫中檔案的訪問許可權。

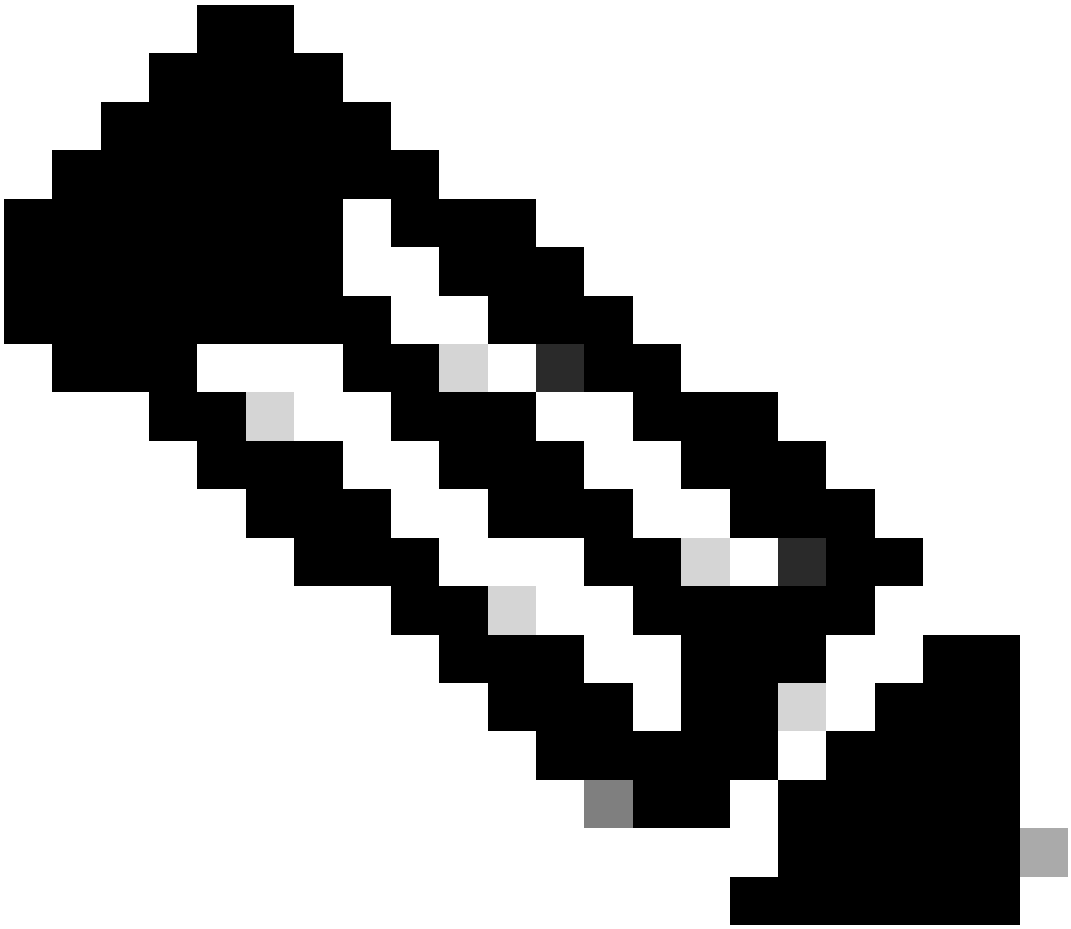
5.按一下獲取檔案，選擇要從中檢索檔案的電腦，然後按一下獲取進行確認。

6.一旦檔案上傳到檔案儲存庫，就會傳送電子郵件通知。

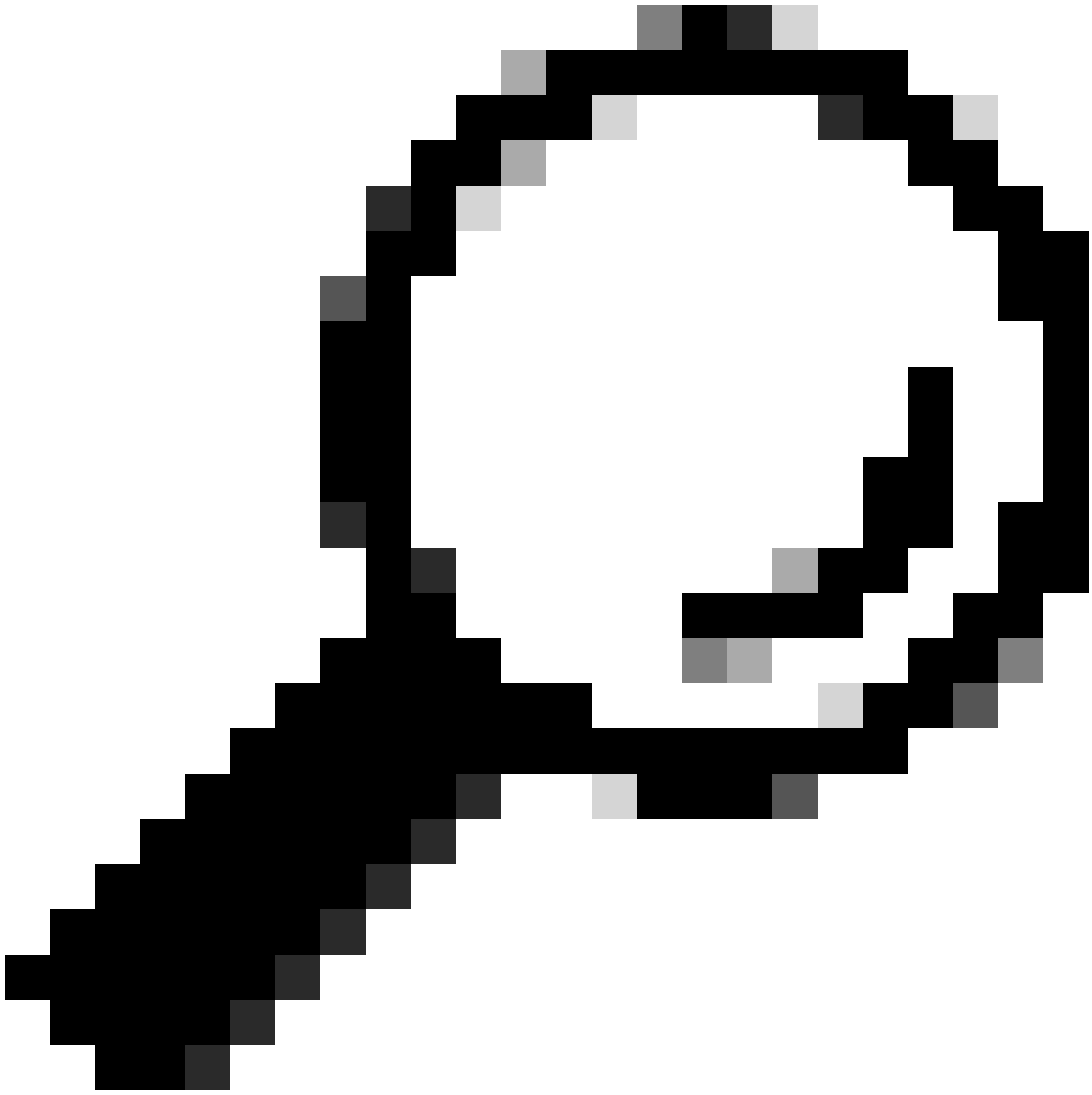
7.一旦檔案可用，您就可以在Analysis > File Repository中看到該檔案以及下載該檔案的選項。

下載檔案

從「檔案儲存庫」下載的所有檔案都將被壓縮並受密碼保護。



附註：要使檔案提取正常運行，必須根據您的雲區域允許網路流量到相應的檔案提取伺服器：歐洲:rff.eu.amp.cisco.com北美：rff.amp.cisco.com 亞太地區、日本及中國：rff.apjc.amp.cisco.com。此外，請確保為管理員帳戶啟用雙因素身份驗證(2FA)，因為成功啟動檔案提取請求需要該身份驗證。



提示：可以使用Event Type = Quarantined Restore Failed和Event Type = File Fetch Failed來篩選事件，以識別失敗並分別檢視還原和檔案提取操作的相應原因。

如果無法按照所列步驟恢復檔案，請與Cisco TAC聯絡，並提供位於C:\Program Files\Cisco\AMP\Quarantine目錄中的.qrt檔案。

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）。