使用恢複方法排除陷入隔離的安全端點故障

目錄

簡介

本文檔介紹使用從隔離模式安裝的安全終結點聯結器來恢復終結點的過程。

必要條件

需求

思科建議您瞭解以下主題：

- 安全終端聯結器
- 安全終端主控台
- 端點隔離功能

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 安全終結點控制檯版本v5.4.2021092321
- 安全終端Windows聯結器版本7.4.5.20701
- 安全終端Mac連線版本v1.21.0

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。

背景資訊

本文檔中介紹的過程在終端裝置處於此狀態且無法禁用隔離模式的情況下非常有用。

端點隔離功能可以阻止電腦上的網路活動（輸入和輸出），以防止資料洩露和惡意軟體傳播等威脅。其網址為：

- 支援7.0.5版及更高版本的Windows聯結器的64位版本
- 支援Mac聯結器1.21.0版及更高版本的Mac版本。

端點隔離會話不影響聯結器和思科雲之間的通訊。您的終端具有與會話前相同的保護級別和可視性。可以配置IP隔離允許地址清單，以避免在活動端點隔離會話處於活動狀態時聯結器阻塞有問題的IP地址。您可以在此處檢視有關端點隔離功能的更多詳細資訊。

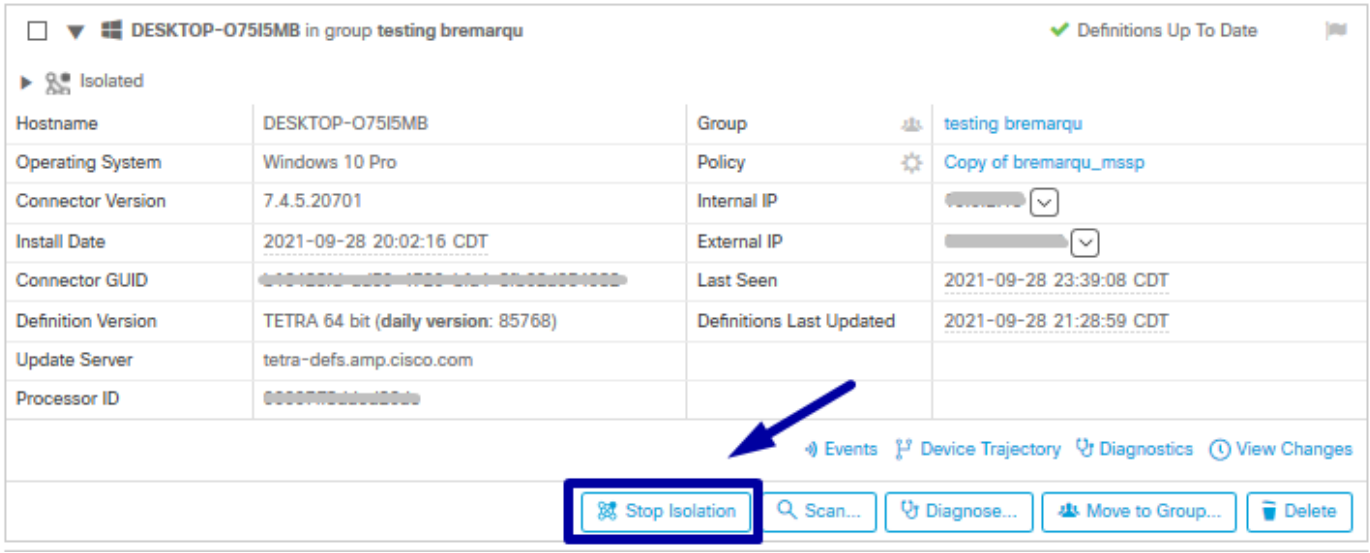
停止隔離

一旦要在電腦上停止終端隔離，請通過安全終端控制檯或命令列執行這些快速步驟。

從控制檯停止隔離會話

停止隔離作業階段，並將所有網路流量還原到端點。

步驟1.在控制檯中，導航到**管理>電腦**。
步驟2.找到要停止隔離的電腦，然後按一下以顯示詳細資訊。
步驟3.按一下「**Stop Isolation**」按鈕，如下圖所示。



步驟4.輸入有關停止終端上隔離功能的原因的任何註釋。

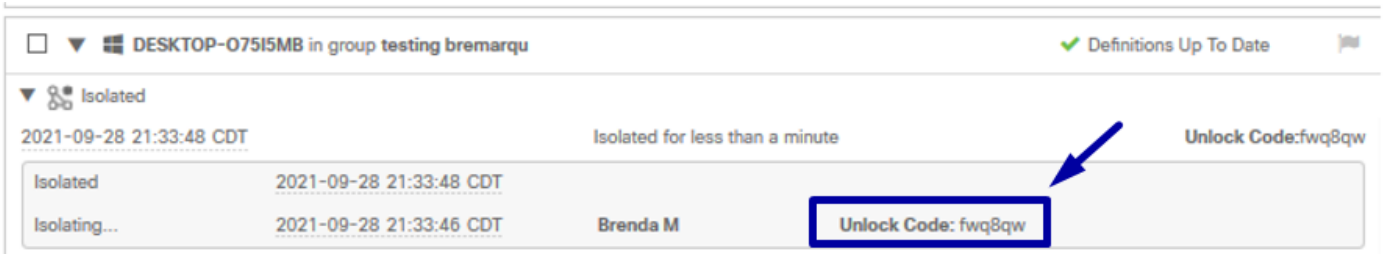
從命令列停止隔離會話

如果隔離端點斷開與思科雲的連線，並且您無法從控制檯停止隔離會話。在這些情況下，您可以使用解鎖代碼從命令列在本地停止會話。

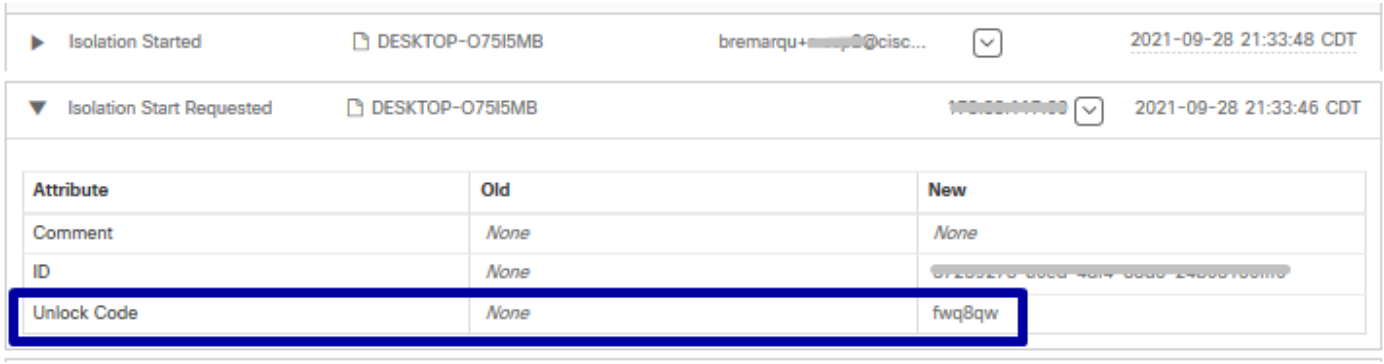
步驟1.在控制檯中，導航到**管理>電腦**。

步驟2.找到要停止隔離的電腦，然後按一下以顯示詳細資訊。

步驟3.請注意**Unlock Code**，如下圖所示。



步驟4.如果導覽至**Account > Audit Log**，則還可以找到**Unlock Code**，如下圖所示。



步驟5. 在隔離的電腦上，以管理員許可權開啟命令提示符。

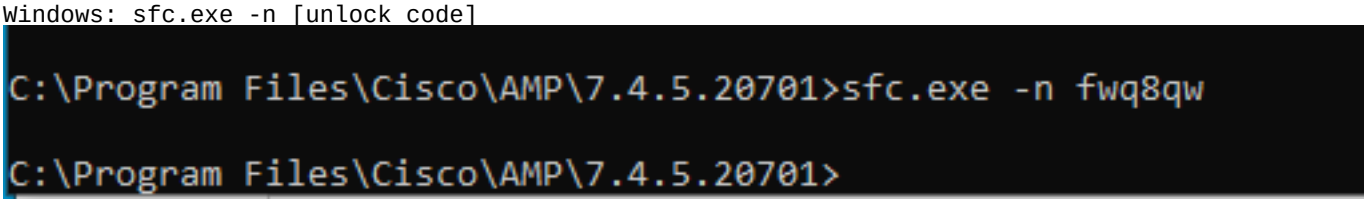
步驟6. 導航到安裝聯結器的目錄

Windows: C:\Program Files\Cisco\AMP\[版本號]

Mac:/opt/cisco/amp

步驟7.運行stop命令

```
Windows: sfc.exe -n [unlock code]
```




```
Mac: ampcli isolate stop [unlock code]
```

注意：如果解鎖代碼輸入錯誤5次，則必須在等待30分鐘後再嘗試再次解鎖。

復原疑難排解

如果已用盡所有途徑，但仍無法從安全終端控制檯或本地使用解鎖代碼恢復孤立的終端，則可以使用緊急恢複方法恢復孤立的終端。

Mac Recovery:

刪除隔離配置並重新啟動安全終結點服務

```
sudo rm /Library/Application\ Support/Cisco/Secure\ Endpoint/endpoint_isolation.xml
sudo launchctl unload /Library/LaunchDaemons/com.cisco.amp.daemon.plist
sudo launchctl load /Library/LaunchDaemons/com.cisco.amp.daemon.plist
```

Windows恢復：

從命令列恢復隔離方法

如果您的終端裝置以隔離方式停滯，且無法通過安全終端控制檯或解鎖代碼禁用隔離，請執行以下步驟。

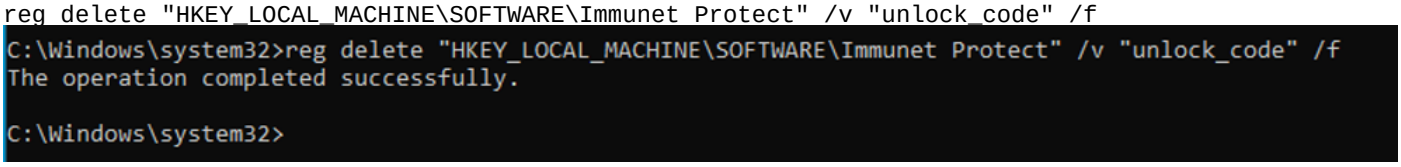
步驟1.通過聯結器使用者介面或Windows服務停止連線**器服務**。

步驟2.找到安全終結點聯結器服務並停止該服務。

步驟3.在隔離的電腦上，以管理員許可權開啟命令提示符。

步驟4.運行命令**reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\Immunet Protect" /v "unlock_code" /f**，如下圖所示。

```
reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\Immunet Protect" /v "unlock_code" /f
```

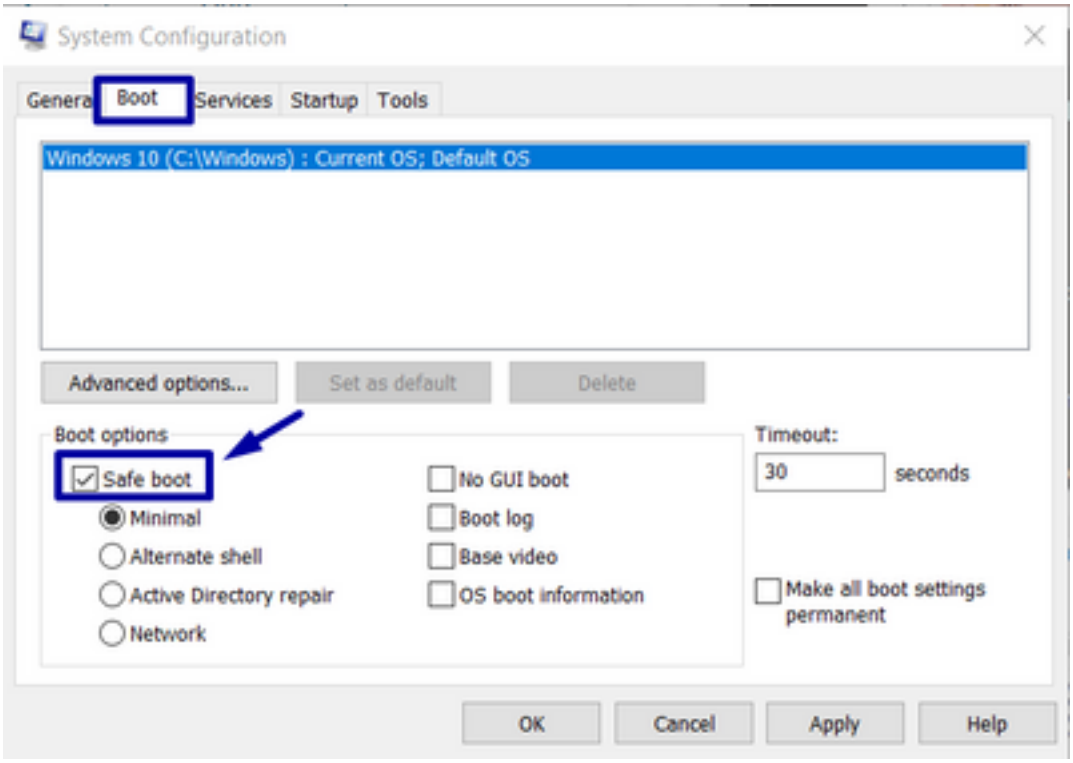


步驟5.消息**The operation completed successfully**表示操作已完成。（如果顯示另一條消息，如「錯誤：訪問被拒絕」，則需要在運行命令之前停止安全終結點聯結器服務）。

步驟6.啟動安全終結點聯結器服務。

> **提示**：如果無法從聯結器使用者介面或Windows服務停止安全終結點聯結器服務，可以執行安全啟動。

在隔離端點上，導覽至**System Configuration > Boot > Boot options**，然後選擇**Safe boot**，如下圖所示。

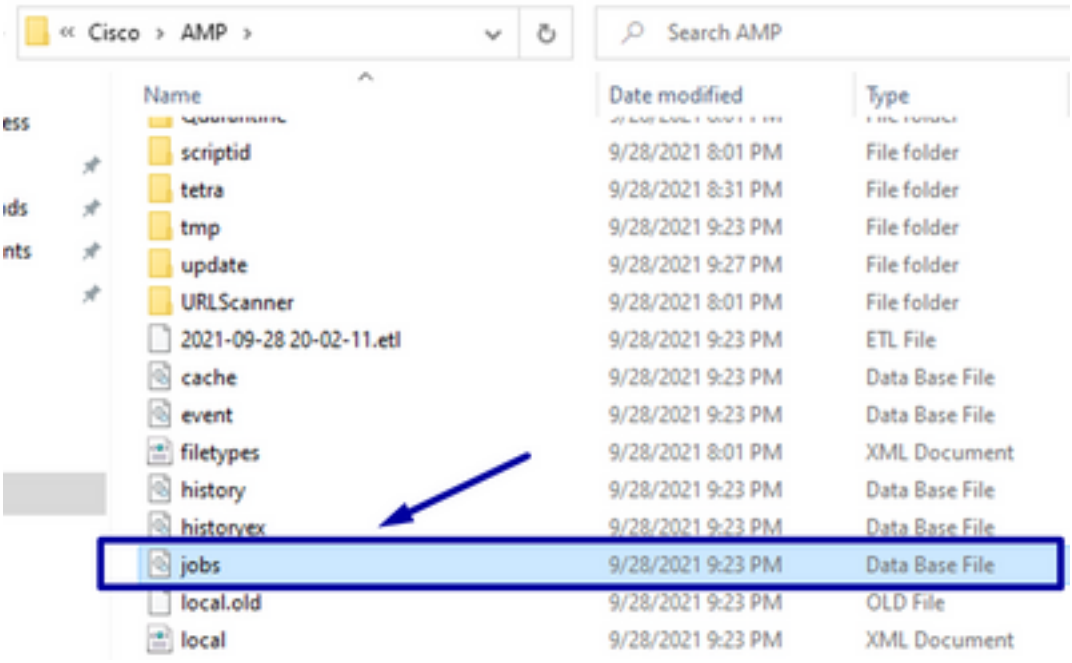


無命令列時的恢復隔離方法

如果您的終端裝置在隔離狀態下停滯，且無法通過安全終端控制檯或解鎖代碼禁用隔離，或者即使您無法使用命令列，請執行以下步驟：

步驟1.通過聯結器使用者介面或Windows服務停止連線**器服務**。

步驟2.導航到安裝聯結器的目錄(C:\Program Files\Cisco\AMP\)，然後刪除**jobs.db**檔案，如下圖所示。



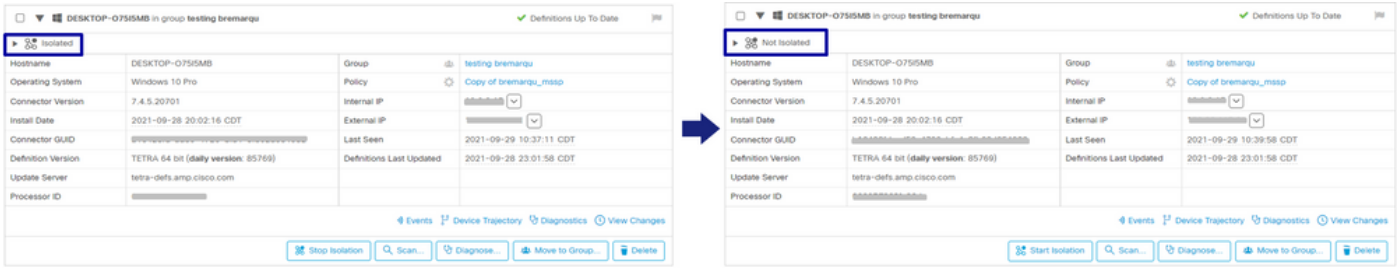
3.重新啟動電腦。

此外，如果在控制檯中看到Isolation事件，可以導航到**Error Details**以檢視錯誤代碼及其說明，如圖所示。

驗證

若要驗證端點已恢復隔離或不再隔離，您可以看到「安全端點聯結器」使用者介面將「隔離」狀態顯示為「Not Isolated」，如下圖所示。

在安全終端控制檯中，如果瀏覽**管理>電腦**，然後找到相關電腦，可以按一下以顯示詳細資訊。隔離狀態顯示**Not Isolated**，如下圖所示。



相關資訊

- [安全端點使用手冊]
- [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）。