為安全訪問支援團隊排除故障並收集基本資訊

目錄

簡介

本文檔介紹使用Cisco安全訪問支援團隊時需要收集的基本資訊

必要條件

需求

思科建議您瞭解以下主題：

- Cisco Secure Access
- 思科安全使用者端
- 透過Wireshark和tcpdump捕獲資料包

採用元件

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

在使用Cisco Secure Access時，您可能會遇到需要聯絡思科支援團隊的問題，或者希望對問題執行基本調查並嘗試檢視日誌並忽略問題。本文繼續介紹如何收集與Secure Access相關的基本故障排除日誌。請注意，並非所有步驟都適用於每個場景。

查詢安全訪問組織ID

為了讓思科工程師找到您的帳戶，請提供您的組織ID，在您登入安全訪問控制台後，您可在URL中找到。

尋找組織ID的步驟：

1. 登入sse.cisco.com
2. 如果您有多個組織，請切換至正確的組織。
3. 組織ID可以在URL中找到，其模式為：https://dashboard.sse.cisco.com/org/{7_digit_org_id}/overview

Cisco Secure Client Diagnostic and Reporting Tool (DART)

Cisco Secure Client Diagnostic and Reporting Tool (DART)是隨Secure Client軟體套件安裝的工具，有助於收集有關使用者終端的重要資訊。

DART捆綁包收集的資訊示例：

- ZTNA日誌
- 安全客戶端日誌和配置檔案資訊
- 系統資訊
- 其他安裝在

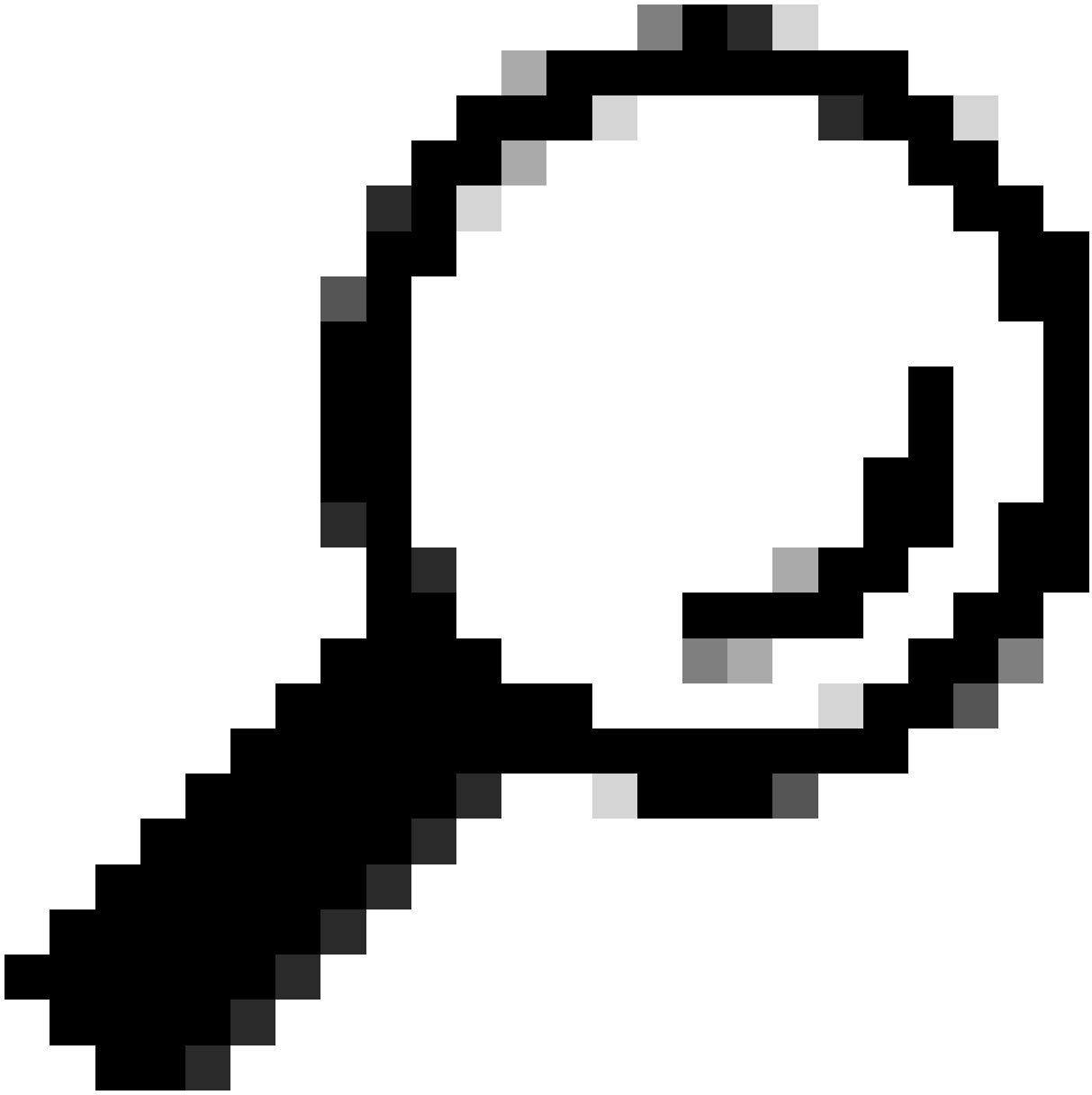
收集DART的說明：

步驟 1.啟動DART。

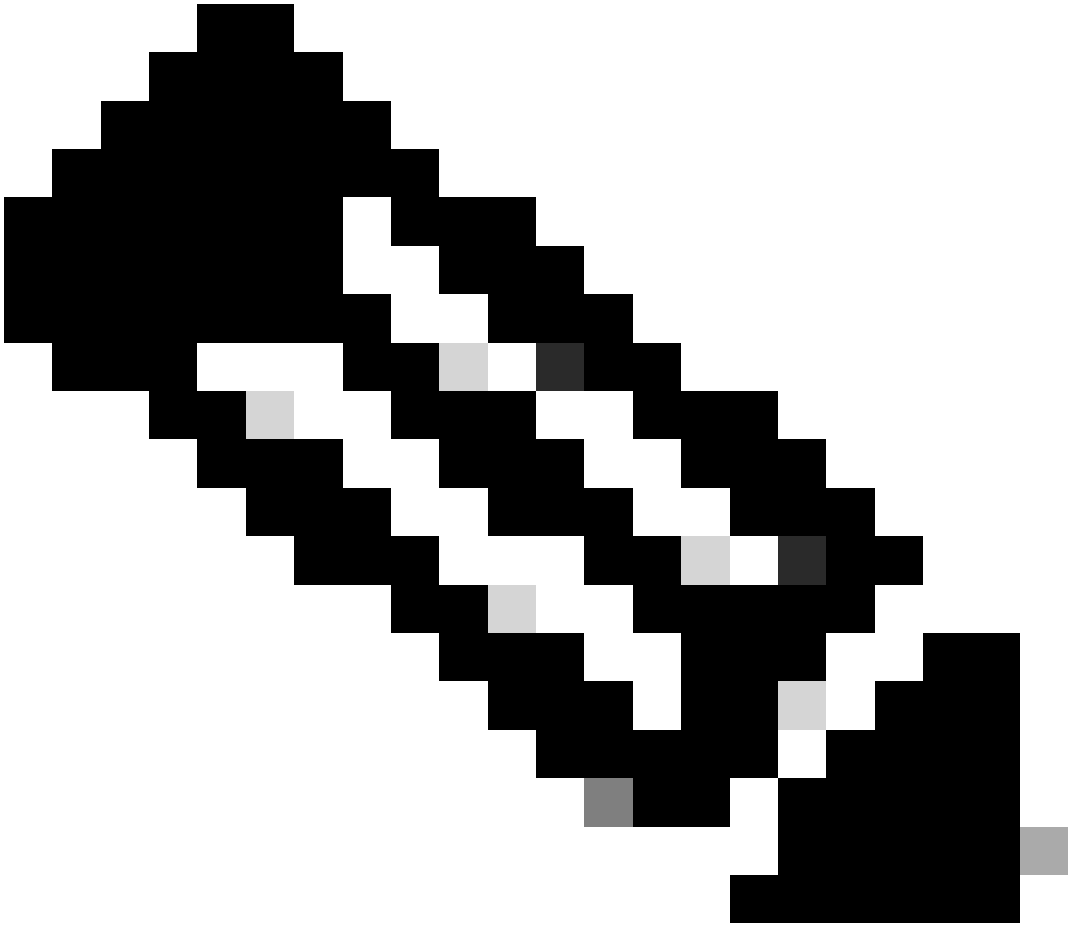
1. 對於Windows電腦，請啟動Cisco Secure Client。
2. 對於Linux電腦，請選擇 **Applications** > **Internet** > **Cisco DART**或/opt/cisco/anyconnect/dart/dartui。
3. 對於Mac電腦，請選擇Applications > Cisco > Cisco DART。

步驟 2.按一下統計資料頁簽，然後按一下詳細資訊。

步驟 3.選擇「預設」或「自訂束」建立。



提示：捆綁的預設名稱為DARTBundle.zip，並且已儲存到本地案頭。



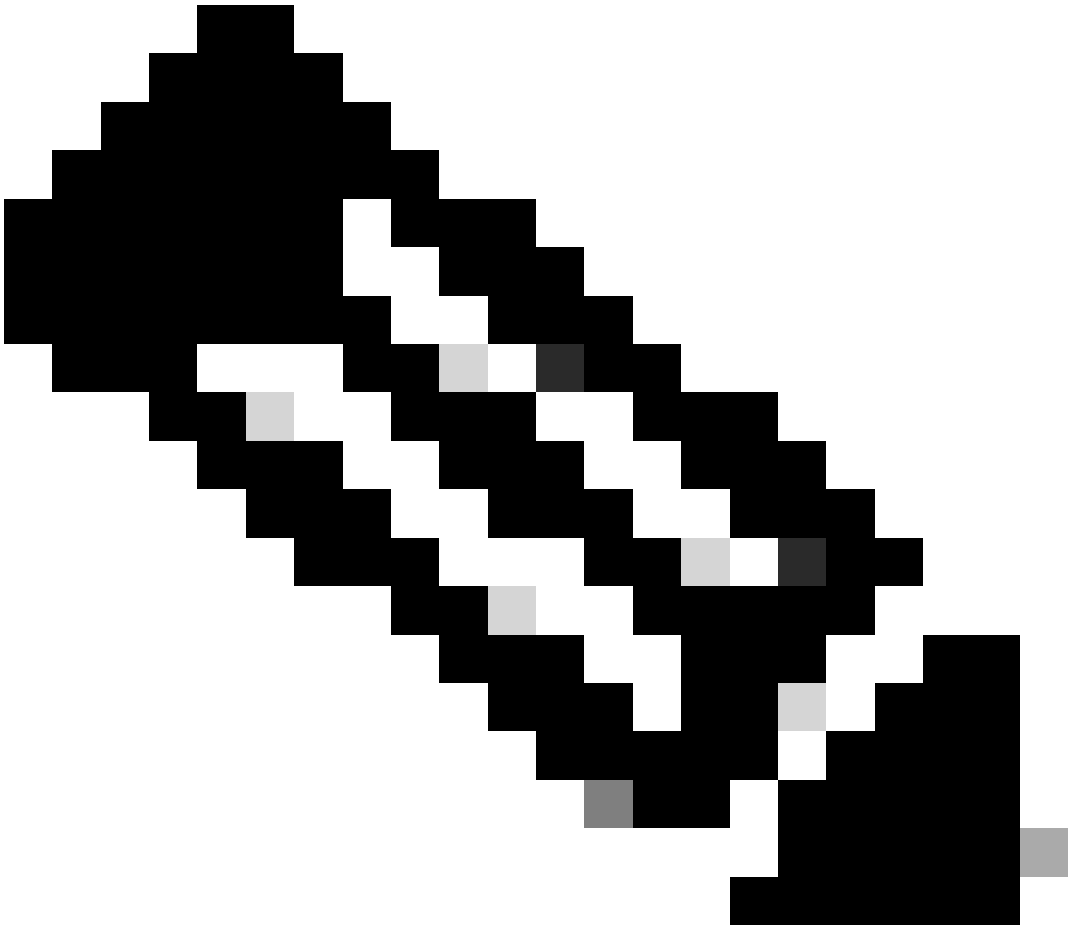
注意：如果選擇預設值，DART將開始建立捆綁包。如果您選擇「自訂」，請繼續精靈提示以指定記錄、偏好設定檔案、診斷資訊及任何其他自訂

HTTP查扣(HAR)擷取

您可以從不同的瀏覽器收集HAR。它提供多種資訊，包括：

1. HTTPS請求的解密版本。
2. 有關錯誤訊息、請求明細及表頭的內部資訊。
3. 計時和延遲資訊
4. 有關瀏覽器型請求的其它雜項資訊。

要收集HAR捕獲，請使用以下來源中介紹的步驟：https://toolbox.googleapps.com/apps/har_analyzer/



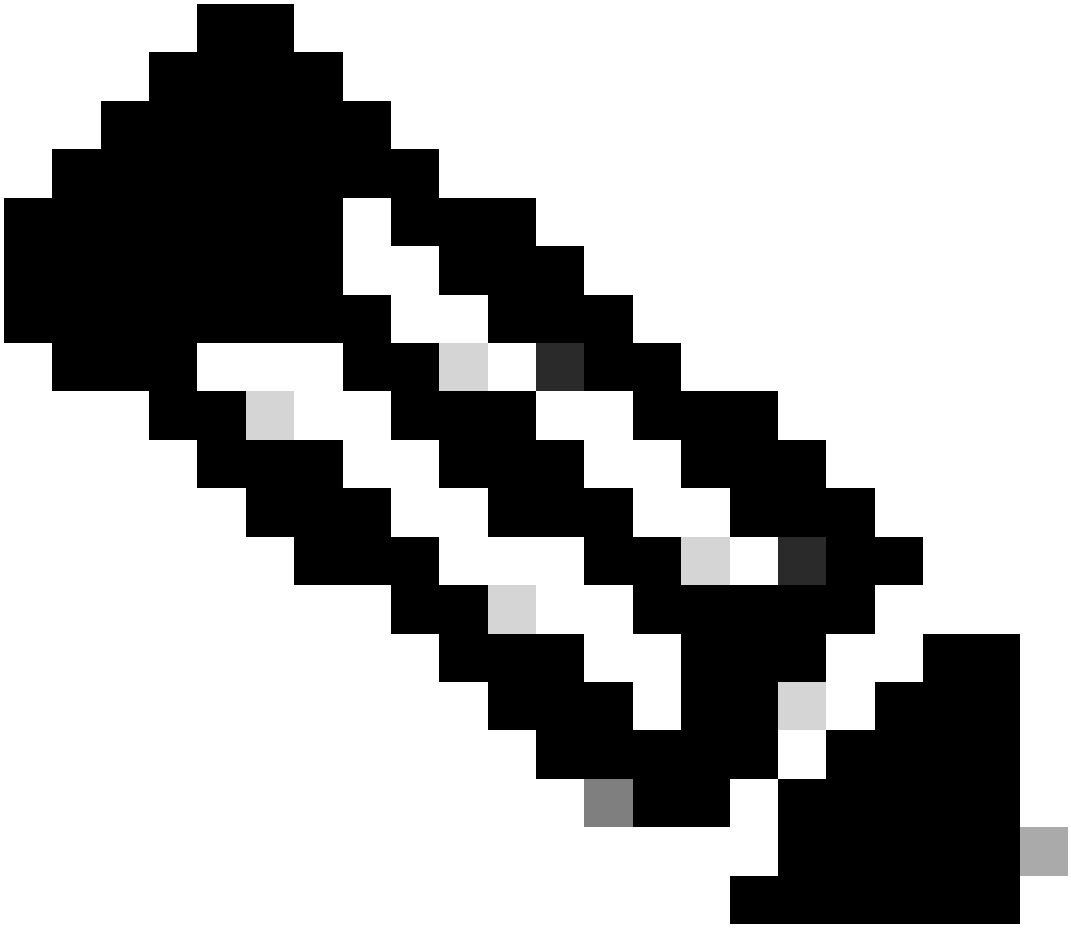
附註：您必須重新整理瀏覽器階段作業，才能收集正確的資料

封包擷取

在檢測到效能問題、資料包丟失或網路完全中斷的情況下，資料包捕獲非常有用。收集捕獲的最常用工具是wireshark和 **tcpdump**。或者內建在裝置內部收集pcap檔案格式的功能，如Cisco防火牆或路由器。

要收集終端上的有用資料包捕獲，請確保包括：

1. 環回介面，用於捕獲透過Secure Client外掛傳送的流量。
2. 資料包路徑中涉及的所有其他介面。
3. 套用最小的過濾條件，或完全不套用過濾條件，以確保已收集所有資料。



注意：在網路裝置上收集捕獲資訊時，請確保過濾流量的源和目標，並將捕獲資訊限制為僅限相關埠和服務，以避免此活動導致的任何效能。

策略調試輸出

策略調試輸出是在受到安全訪問保護時透過使用者瀏覽器傳送的診斷輸出。其中包括有關部署的重要資訊。

1.

組織辨識碼

2. 部署型別

3. 已連線的代理

4. 公有和私有IP地址

5. 與流量來源相關的其他資訊。

要運行策略測試結果，請從受保護的端點登入到此連結：https://policy.test.sse.cisco.com/

如果您的瀏覽器中出現證書錯誤消息，請確保您信任Secure Access Root證書。

要下載安全訪問根證書，請執行以下操作：

導航至Secure Access Dashboard > Secure > Settings > Certificate > (Internet Destinations tab)

將結果上傳到思科支援服務要求

您可以透過以下步驟將檔案上傳至支援案例：

步驟 1.登入SCM。

步驟 2.若要檢視及編輯案件，請按一下清單中的案件編號或案件標題。「案件摘要」頁面隨即開啟。

步驟 3.按一下Add Files以選擇檔案並並上傳至案件做為附件。系統顯示SCM檔案上傳程式工具。

步驟 4.在「選擇要上傳的檔案」對話方塊中，拖動要上傳的檔案，或按一下內部以瀏覽本地電腦以查詢要上傳的檔案。

步驟 5.新增說明並指定所有檔案或個別檔案的類別。

相關資訊

- **思科技術支援與下載**
- **Secure Access文檔和使用手冊**
- **Cisco Secure Client軟體下載**

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）。