為Secure Access支援團隊排除故障並收集基本資訊

目錄

簡介

必要條件

- 需求
- 採用元件

背景資訊

查詢安全訪問組織ID

思科安全使用者端診斷和報告工具(DART)

啟用ZTNA和SWG模組的調試日誌

- 啟用ZTNA的調試日誌
- 啟用SWG的調試日誌
- 啟用DUO的調試日誌

收集ZTNA和SWG、DNS模組的KDF日誌(Windows)

- 必要條件

HTTP封存(HAR)擷取

封包擷取

策略調試輸出

常見命令排除站點到站點隧道故障

常見命令資源聯結器故障排除

將結果上傳到思科支援服務請求

相關資訊

簡介

本檔案介紹與思科安全存取支援團隊合作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
- 通過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

處理Cisco Secure Access時，您可能會遇到需要聯絡思科支援團隊，或者希望對問題進行基本調查並嘗試檢視日誌並忽略問題的問題。本文介紹如何收集與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，一旦您登入到Secure Access Dashboard，就可以在URL中找到。

查詢組織ID的步驟：

1.登入sse.cisco.com
2.如果有多家組織，請切換至正確的組織。
3.組織ID可以在以下模式的URL中找到：https://dashboard.sse.cisco.com/org/{7_digit_org_id}/概述

思科安全使用者端診斷和報告工具(DART)

Cisco Secure Client Diagnostic and Reporting Tool(DART)是隨Secure Client軟體包安裝的工具，可幫助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
— 其他安全客戶端載入項或外掛日誌，安裝在

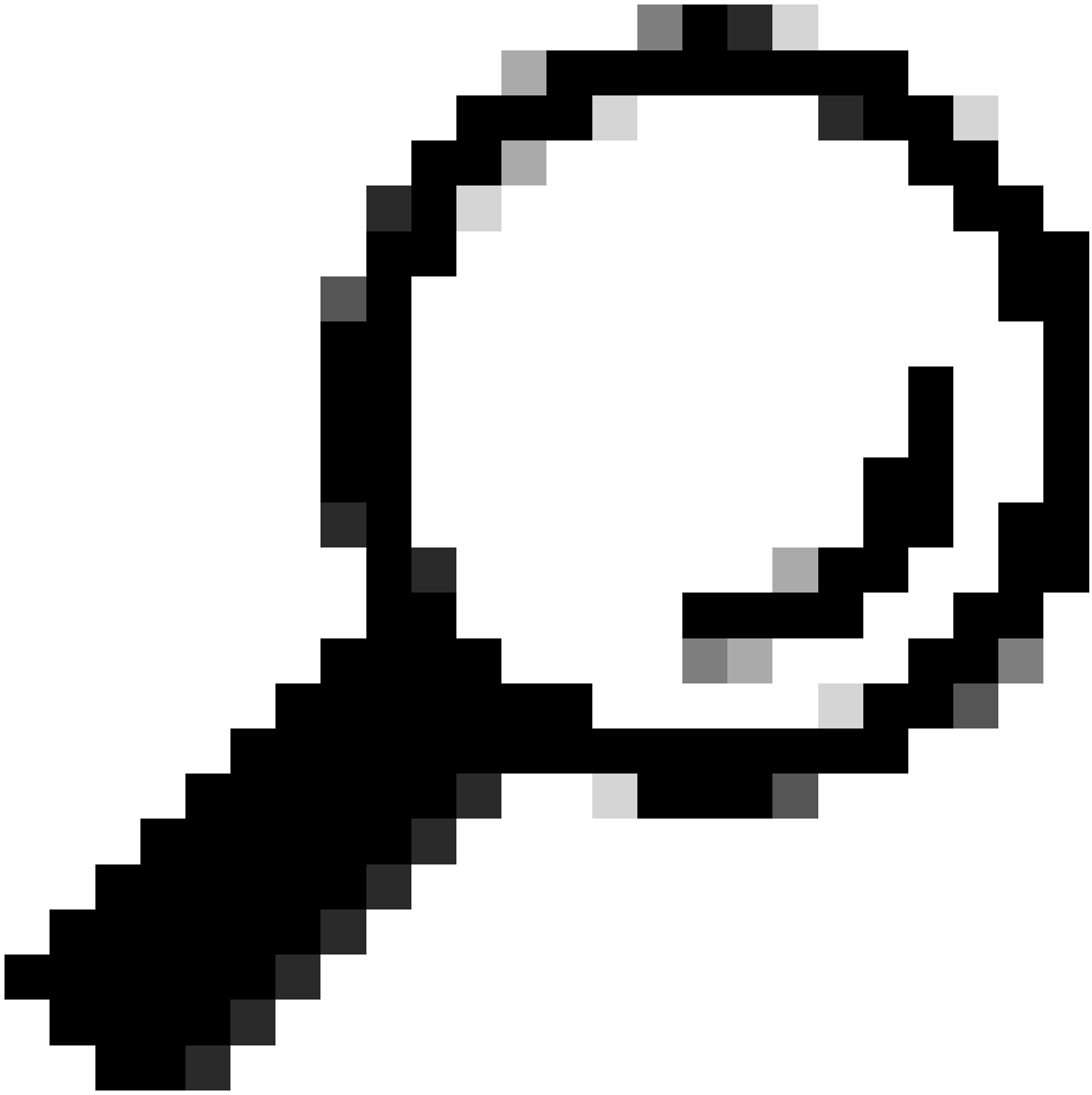
收集DART的說明：

步驟1.啟動DART。

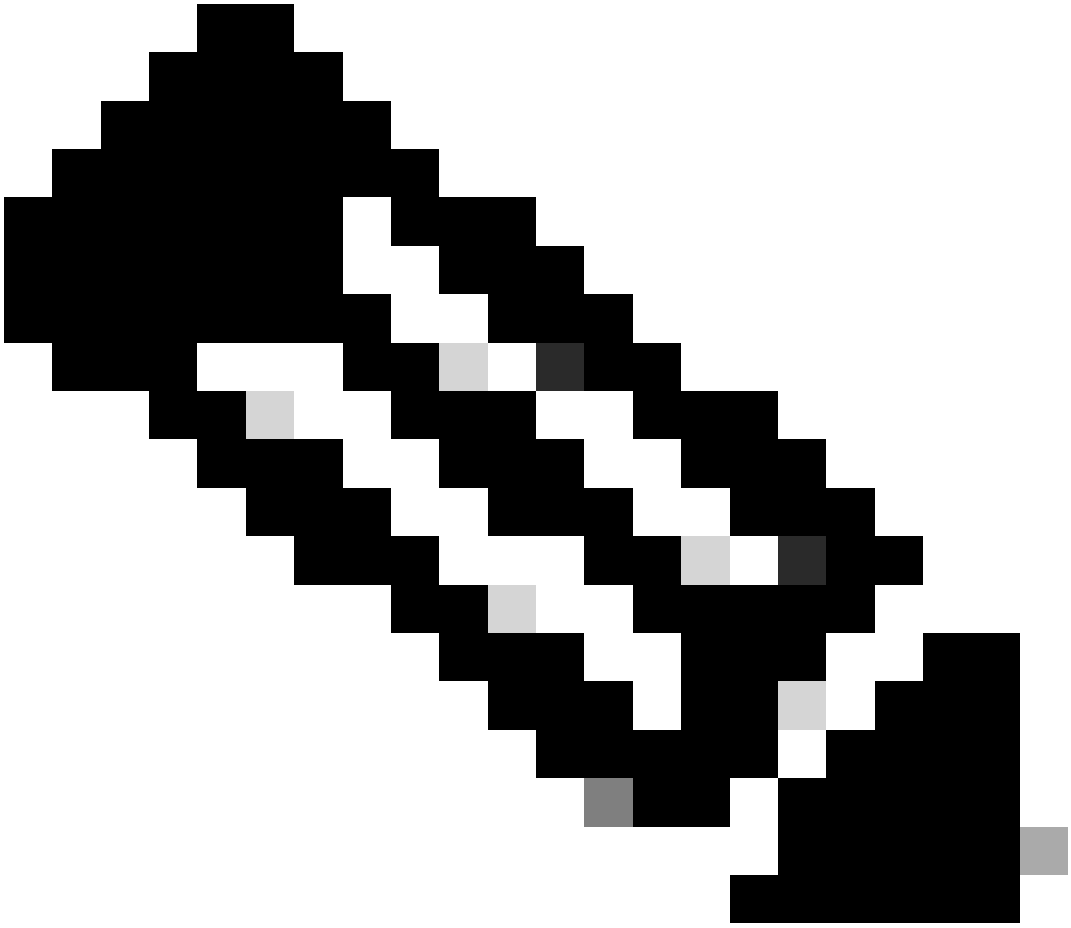
1.對於Windows電腦，啟動Cisco Secure Client。
2.對於Linux電腦，請選**Applications > Internet > Cisco DART**擇/opt/cisco/anyconnect/dart/dartui。
3.對於Mac電腦，請選擇Applications > Cisco > Cisco DART。

步驟2.單擊Statistics頁籤，然後點選Details。

步驟3.選擇Default或Custom Bundle Creation。



提示：套件組合的預設名稱為DARTBundle.zip，且已儲存到本機案頭。



附註：如果您選擇「預設」，DART將開始建立捆綁包。如果選擇自定義，則繼續嚮導提示以指定日誌、首選項檔案、診斷資訊以及任何其他自定義設定

啟用ZTNA和SWG模組的調試日誌

在某些情況下，支援團隊需要啟用跟蹤或調試級別日誌才能確定更複雜的問題。

完成本節中提供的步驟以啟用每個模組的調試。

啟用ZTNA的調試日誌

步驟1.建立名為logconfig.json的json檔案

步驟2.在檔案中輸入此文字

```
{ "global": "DBG_TRACE" }
```

步驟3.根據作業系統將檔案放入正確的目錄

- Windows:C:\ProgramData\Cisco\Cisco安全客戶端\ZTA
- MacOS:/opt/cisco/secureclient/zta

步驟4.重新啟動ZTNA模組或Cisco安全客戶端，使日誌生效。

啟用SWG的調試日誌

步驟1.建立名為SWGConfigOverride.json的json檔案

步驟2.在檔案中輸入此文字

```
{"logLevel": "1"}□
```

步驟3.根據作業系統將檔案放入正確的目錄

- Windows: C:\ProgramData\Cisco\Cisco安全Client\Umbrella\SWG\
- MacOS:/opt/cisco/secureclient/umbrella/swg

步驟4.重新啟動SWG模組或Cisco Secure Client以使日誌生效。

啟用DUO的調試日誌

啟用DUO KDF日誌（狀態故障排除、註冊問題）

```
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Duo\Duo Device Health” /v verbose_logging_enabled /d 1 /f
```

禁用DUO KDF日誌

```
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Duo\Duo Device Health” /v verbose_logging_enabled /d 0 /f
```

收集ZTNA和SWG、DNS模組的KDF日誌(Windows)

在某些情況下，支援團隊需要收集kdf日誌以識別更複雜的問題。

完成本節中提供的步驟以配置和收集kdf日誌。

必要條件

需要安裝DebugView才能正確收集日誌。可以使用此源安裝的軟體：https://learn.microsoft.com/en-us/sysinternals/downloads/debugview

啟用DNS登錄檔項

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\acsock" /v DebugFlags /d 0x20801FF /t reg
```

啟用SWG登錄檔項

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\acsock" /v DebugFlags /d 0x70C01FF /t reg
```

啟用ZTNA登錄檔項

```
"%ProgramFiles(x86)%\Cisco\Cisco Secure Client\acsocktool.exe" -sdf 0x40018EF52
```

禁用所有標誌

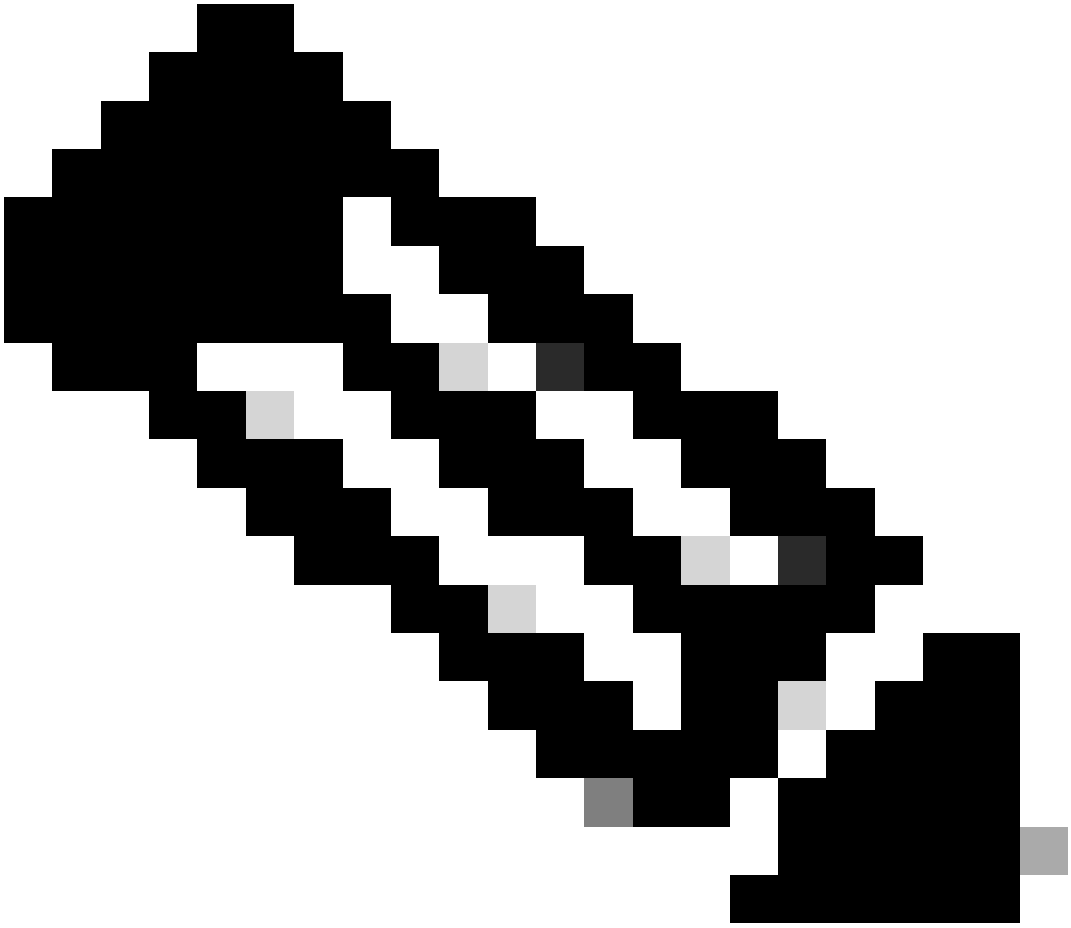
```
"%ProgramFiles(x86)%\Cisco\Cisco Secure Client\acsocktool.exe" -cdf
```

HTTP封存(HAR)擷取

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.有關錯誤消息、請求詳細資訊和報頭的內部資訊。
3.計時和延遲資訊
4.有關基於瀏覽器的請求的其他雜項資訊。

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



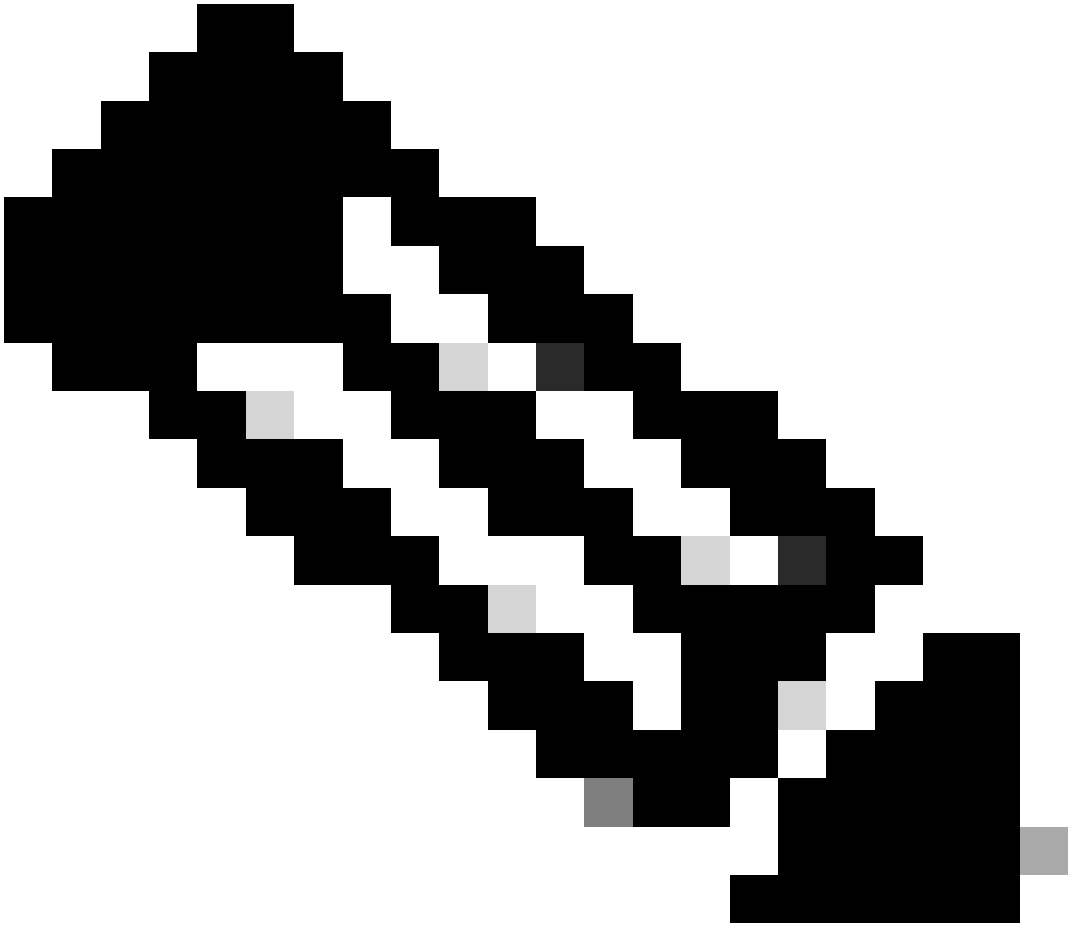
附註：您需要刷新瀏覽器會話才能收集正確的資料

封包擷取

在檢測到效能問題、資料包丟失或網路總中斷的情況下，資料包捕獲非常有用。收集捕獲的最常見工具是和wireshark**tcpdump**。或收集裝置本身中pcap檔案格式的內建功能，如思科防火牆或路由器。

要收集終端上有用的資料包捕獲，請確保包括：

1.環回介面，用於捕獲通過安全客戶端外掛傳送的流量。
2.資料包路徑中涉及的所有其他介面。
3.應用最低限度的篩選條件，或根本沒有篩選條件，以確保收集到所有資料。



附註：在網路裝置上收集捕獲時，請確保根據流量的源和目標進行過濾，並將捕獲限製為僅相關的埠和服務，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Secure Access保護時通過使用者瀏覽器傳送的診斷輸出。其中包括有關部署的關鍵資訊。

1.組織標識
2.部署型別
3.連線的代理
4.公有IP地址和私有IP地址
5.與流量來源相關的其他資訊。

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

如果您的瀏覽器中出現證書錯誤消息，請確保您信任安全訪問根證書。

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)

常見命令排除站點到站點隧道故障

<#root>

 # Tunnel Establishment

```
asa>show crypto ikev1 sa
asa>show crypto ikev2 sa
asa>show crypto ipsec sa
asa>show crypto session
```

#BGP Troubleshooting

```
asa>show running-config router bgp
asa>show bgp summary
asa>show ip bgp neighbors
```

#Routes Advertisements

```
asa>show bgp ipv4 unicast neighbors <sse-dc-ip> advertised-routes
asa>show bgp ipv4 unicast neighbors <sse-dc-ip> received-routes
asa>show bgp ipv4 unicast neighbors <sse-dc-ip> routes
```

#Debug BGP events

```
asa>debug ip bgp
asa>debug ip bgp events
asa>debug ip bgp updates
asa>debug ip routing
```

#Disable Debugs

```
asa>undebug all
```

常見命令資源聯結器故障排除

提供的清單提供了資源聯結器的綜合檢視，以及安全訪問支援團隊的重要故障排除詳細資訊

<#root>

#DNS and connectivity tests on the local IP address, gateway, Secure Access APIs

```
rc-cli> diagnostic
#Software version, VPN tunnel state, system health, sysctl settings, routes and iptables

rc-cli> techsupport
#Packet captures

rc-cli> tcpdump <host>
```

將結果上傳到思科支援服務請求

您可以透過以下步驟將檔案上傳到支援案件：

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，或按一下內部瀏覽本地電腦以上載檔案。

步驟5.添加說明並為所有檔案或單獨指定一個類別。

相關資訊

- 思科技術支援與下載
- Secure Access文檔和使用手冊
- 思科安全使用者端軟體下載

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）。