解析"；狀態檢查失敗或狀態太舊"ZTNA流的活動搜尋出錯

目錄

問題

實施零信任網路訪問狀態檢查後，根據策略配置，問題以兩種方式顯示：

- 存在失效開放規則時：流量繞過狀態實施並匹配「無狀態檢查」規則。
- 啟用嚴格執行時：拒絕使用者訪問專用應用程式。

環境

- 思科安全訪問 — 零信任網路訪問流
- Duo台式機

解析

收集Duo Desktop Diagnostics:啟用調試日誌記錄並運行支援工具

###步驟1 — 啟用調試日誌記錄（macOS和Windows）

1.開啟Duo Desktop應用程式。

2.定位至首選項。

3.選中啟用詳細的診斷報告。

第2步 — 重現問題

—

##步驟3 — 收集Dart套件 — 收集安全客戶端的DART套件

##步驟4 — 運行支援工具

支援工具指令碼隨附用於macOS和Windows的Duo Desktop 6.0.0+和Duo Device Health 2.26.1+。

它收集必要的檔案，清除其中的敏感資訊，並建立可傳送的ZIP。

###指令碼位置

Windows

- Duo案頭：`C:\Program檔案(x86)\Duo Desktop\DuoDesktop-Support.ps1`

- Duo Device Health:`C:\Program檔案(x86)\Duo Device Health\DeviceHealth-Support.ps1`

macOS

- Duo案頭：`/Applications/Duo Desktop.app/Contents/Resources/duo_desktop_support.sh`

- Duo Device Health:`/Applications/Duo Device Health.app/Contents/Resources/device_health_support.sh`

附註：較舊的Duo Device Health版本和較新的Duo Desktop版本之間的路徑不同 — 請使用與您的安裝相匹配的對。

###支援工具收集的內容

Windows

1.建立ZIP以儲存收集的資訊。

2.運行Invoke-WebRequest以測試與Duo的連線。

3.捕獲：系統代理設定；OS版本、內部版本和位；BitLocker狀態；時區；Duo相關應用事件日誌。

4.副本……\AppData\Local\DuoDesktop\Logs(或...\DuoDeviceHealth\Logs)插入ZIP中。

5.將Duo登錄檔項從HKLM:\SOFTWARE\Duo和HKCU\SOFTWARE\Duo Device Health匯出到system_info.txt。

6.複製與環回介面卡127.0.0.1)關聯的證書。

7.（可選）導出系統事件日誌。

8.將ZIP儲存到登入使用者的案頭，例如C:\Users\user_name\Desktop\Duo_Desktop_Support_2022-06-21-02-04-44.zip(或DHA_Support_..zip)。

MacOS

1.建立ZIP以儲存收集的資訊。

2.運行curl以測試與Duo的連線。

3.捕獲：系統代理設定；install.log;system.log;Duo相關故障日誌；作業系統和核心版本。

4.將/Users/user_name/Library/Logs/Duo Desktop/*.log(或Duo Device Health)複製到ZIP中。

5.複製與環回介面卡127.0.0.1)關聯的證書。

6.（可選）導出所有使用者和核心日誌。

7.將ZIP儲存到登入使用者的案頭，例如/Users/user_name/Desktop/duo_desktop_support_2022-06-21-16-27-59.zip(或DHA_Support_..zip)。

###命令列選項

Windows(PowerShell)

選項 |說明

| -eventlogs |匯出系統日誌。Options:系統 |

| – 天 |要匯出的安全事件日誌的天數 |

| -user |指定從哪個使用者收集日誌（當以其他使用者名稱的管理員身份運行時，需要） |

| Get-Help |內建cmdlet;在指令碼前呼叫它，例如Get-Help .\DuoDesktop-Support.ps1 |

macOS（終端）

-a |匯出所有使用者和核心宕機日誌。

-h |顯示幫助消息。

—

##端到端流程

Windows(示例：匯出過去2天的系統事件日誌)

1.在安裝Duo Desktop的終端上開啟管理PowerShell會話。

2. 啟用調試日誌記錄（第1部分）。

3.重現Duo問題。

4.運行指令碼:

- Duo案頭：

```powershell

& 'C:\Program Files(x86)\Duo Desktop\DuoDesktop-Support.ps1' -eventlogs system — 第2天

'"

- Duo Device Health:
```

```powershell

& 'C:\Program Files(x86)\Duo Device Health\DeviceHealth-Support.ps1' -eventlogs system — 第2天

'''

>如果看到「在此系統上禁用運行指令碼」：調整PowerShell執行策略以允許指令碼運行，然後重新運行命令。

### MacOS(示例：匯出所有使用者和核心宕機日誌)

1.在安裝Duo Desktop的終端上開啟Terminal會話。

2. 啟用調試日誌記錄（第1部分）。

3.重現Duo問題。

4.運行指令碼:

- Duo案頭：

'''bash

/Applications/Duo\ Desktop.app/Contents/Resources/duo_desktop_support.sh -a

'''

- Duo Device Health:

'''bash

/Applications/Duo\ Device\ Health.app/Contents/Resources/device_health_support.sh -a

'''

—
```

##將這些產品提交至Cisco TAC -

將案頭上的Dart和Duo_Desktop_Support資料夾傳送到Cisco TAC。

失敗嘗試的2個時間段

在狀態配置檔案中實施3個狀態檢查。

原因

一個或多個狀態檢查（OS版本、AV狀態、磁碟加密、域加入、防火牆狀態）未滿足在零信任網路訪問策略中定義的閾值。

相關內容

- Duo Desktop調試日誌記錄配置
- Duo案頭支援工具
- 思科技術支援與下載

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）。