解决"；状况检查失败或状况太旧(")ZTNA流的活动搜索出错

目录

问题

实施零信任网络访问状态检查后，根据策略配置，问题以两种方式显示：

- 当存在失效开放规则时：流量绕过状况实施并匹配“无状况检查”规则。
- 启用严格实施时：拒绝用户访问私有应用。

环境

- 思科安全访问 — 零信任网络访问流
- Duo桌面

分辨率

收集Duo Desktop Diagnostics:启用调试日志记录并运行支持工具

###步骤1 — 启用调试日志记录（macOS和Windows）

1.打开Duo Desktop应用。

2.定位至首选项。

3.选中启用详细诊断报告。

第2步 — 重现问题

—

##第3步 — 收集Dart套件 — 收集安全客户端的DART套件

##步骤4 — 运行支持工具

支持工具脚本随附用于macOS和Windows的Duo Desktop 6.0.0+和Duo Device Health 2.26.1+。

它会收集必要的文件，清除其中的敏感信息，并创建可立即发送的ZIP。

###脚本位置

Windows 窗口版本

- Duo桌面：`C:\Program文件(x86)\Duo Desktop\DuoDesktop-Support.ps1`

— 双设备运行状况：`C:\Program Files(x86)\Duo Device Health\DeviceHealth-Support.ps1`

macOS

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

— 双设备运行状况：`/Applications/Duo Device Health.app/Contents/Resources/device_health_support.sh`

注意：旧版Duo Device Health版本和新版Duo Desktop版本之间的路径不同 — 使用与您的安装匹配的对。

###支持工具收集的内容

Windows 窗口版本

1.创建ZIP以保存收集的信息。

2.运行Invoke-WebRequest以测试与Duo的连接。

3.捕获：系统代理设置；操作系统版本、内部版本和位；BitLocker状态；时区;Duo相关应用事件日志。

4.副本...(或.....\DuoDeviceHealth\Logs)插入ZIP中。

5.将Duo注册表项从HKLM:\SOFTWARE\Duo和HKCU\SOFTWARE\Duo Device Health导出到system_info.txt。

6.复制与环回适配器(127.0.0.1)关联的证书。

7.（可选）导出系统事件日志。

8.将ZIP保存到登录用户的桌面，例如C:\Users\user_name\Desktop\Duo_Desktop_Support_2022-06-21-02-04-44.zip(或DHA_Support_..zip)。

MacOS

1.创建ZIP以保存收集的信息。

2.运行curl以测试与Duo的连接。

3.捕获：系统代理设置；install.log;system.log;Duo相关的故障日志；操作系统和内核版本。

4.将/Users/user_name/Library/Logs/Duo Desktop/*.log（或Duo Device Health）复制到ZIP中。

5.复制与环回适配器(127.0.0.1)关联的证书。

6.（可选）导出所有用户和内核日志。

7.将ZIP保存到登录用户的桌面，例如/Users/user_name/Desktop/duo_desktop_support_2022-06-21-16-27-59.zip(或DHA_Support_..zip)。

###命令行选项

Windows(PowerShell)

选项 |说明

| -eventlogs |导出系统日志。选项:system |

| – 天 |要导出的安全事件日志的天数 |

| -user |指定从哪个用户收集日志（当以其他用户名的管理员身份运行时，需要） |

| Get-Help |内置cmdlet;在脚本之前调用它，例如Get-Help .\DuoDesktop-Support.ps1 |

macOS（终端）

-a |导出所有用户和内核死机日志。

-h |显示帮助消息。

—

##端到端流程

Windows(示例：导出过去2天的系统事件日志)

1.在安装Duo Desktop的终端上打开管理PowerShell会话。

2.启用调试日志记录（第1部分）。

3.重现Duo问题。

4.运行脚本:

- Duo桌面：

```powershell

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

'''

— 双设备运行状况：
```

```powershell

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

'''

>如果看到“在此系统上禁用运行脚本”：调整PowerShell执行策略以允许脚本运行，然后重新运行命令。

### MacOS(示例：导出所有用户和内核死机日志)

1.在安装了Duo Desktop的终端上打开Terminal会话。

2.启用调试日志记录（第1部分）。

3.重现Duo问题。

4.运行脚本:

- Duo桌面：

'''bash

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

'''

— 双设备运行状况：

'''bash

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

'''

—
```

##将这些信息提交给思科TAC -

1桌面上的Dart和Duo_Desktop_Support文件夹到Cisco TAC。

失败尝试的2个时间段

在状态配置文件中实施3个状态检查。

原因

一个或多个状态检查（操作系统版本、AV状态、磁盘加密、域加入、防火墙状态）未达到在零信任网络访问策略中定义的阈值。

相关内容

- Duo Desktop调试日志记录配置
- Duo桌面支持工具
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。