Auflösen von "Statusüberprüfung fehlgeschlagen oder Status zu alt" Fehler bei Aktivitätssuche für ZTNA-Fluss

Inhalt

Problem

Nach der Überprüfung des Status des Netzwerkzugriffs auf die Vertrauenswürdigkeit "Zero Trust" (keine Vertrauensstellung) zeigt sich das Problem je nach Richtlinienkonfiguration auf zwei Arten:

- Wenn eine Fail-Open-Regel vorhanden ist: Datenverkehr umgeht die Durchsetzung von Sicherheitsstatus und entspricht der Regel "Keine Statusüberprüfung".
- Wenn strikte Durchsetzung aktiviert ist: Benutzern wird der Zugriff auf private Anwendungen verweigert.

Umwelt

- Cisco Secure Access - kein Vertrauen in den Netzwerkzugriff
- Duo-Desktop

Auflösung

Erfassen der Duo Desktop-Diagnose: Debug-Protokollierung aktivieren und das Support-Tool ausführen

Schritt 1 - Debug-Protokollierung aktivieren (macOS und Windows)

1. Öffnen Sie die Duo Desktop-App.

2. Navigieren Sie zu Voreinstellungen.

3. Aktivieren Sie Detaillierte Diagnoseberichte aktivieren.

Schritt 2 - Reproduzieren des Problems

—

Schritt 3: Sammeln des DART-Pakets - Sammeln des DART-Pakets für einen sicheren Client

Schritt 4: Ausführen des Support-Tools

Das Support Tool-Skript wird mit Duo Desktop 6.0.0+ und Duo Device Health 2.26.1+ für MacOS und Windows ausgeliefert.

Es sammelt die erforderlichen Dateien, entfernt sie von vertraulichen Informationen und erstellt eine versandbereite ZIP.

Skriptspeicherorte

Windows

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

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

MacOS

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

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

Anmerkung: Die Pfade unterscheiden sich zwischen den älteren Duo Device Health-

---

Versionen und den neueren Duo Desktop-Versionen - verwenden Sie das Paar, das zu Ihrer Installation passt.

Was das Support-Tool sammelt

Windows

1. Erstellt eine ZIP-Adresse für die erfassten Daten.

2. Führt `Invoke-WebRequest aus`, um die Verbindung zu Duo zu testen.

3. Erfasst: System-Proxy-Einstellungen; Betriebssystemversion, Build und Bit; BitLocker-Status Zeitzone; Anwendungsprotokolle mit Duo-Bezug.

4. Kopien `..\AppData\Local\DuoDesktop\Logs` (oder `...\DuoDeviceHealth\Logs`) in die ZIP-Adresse übertragen.

5. Exportiert Duo Registrierungsschlüssel von `HKLM:\SOFTWARE\Duo` und `HKCU\SOFTWARE\Duo Device Health` nach `system_info.txt`.

6. Kopiert Zertifikate, die dem Loopback-Adapter (`127.0.0.1)` zugeordnet sind.

7. (Optional) Exportiert Systemereignisprotokolle.

8. Speichert die ZIP auf dem Desktop des angemeldeten Benutzers, z.B. `C:\Users\user_name\Desktop\Duo_Desktop_Support_2022-06-21-02-04-44.zip` (oder `DHA_Support_...zip`).

MacOS

1. Erstellt eine ZIP-Adresse für die erfassten Daten.

2. Führt `Curl` aus, um die Verbindung zu Duo zu testen.

3. Erfasst: System-Proxy-Einstellungen; `install.log`; `system.log`; Absturzprotokolle mit Duo-Bezug; Betriebssystem- und Kernelversion.

4. Kopiert /`Users/user_name/Library/Logs/Duo Desktop/*.log` (oder `Duo Device Health`) in die ZIP-Datei.

5. Kopiert Zertifikate, die dem Loopback-Adapter (`127.0.0.1`) zugeordnet sind.

6. (Optional) Exportiert alle Benutzer- und Kernel-Protokolle.

7. Speichert die ZIP auf dem Desktop des angemeldeten Benutzers, z.B. `/Users/user_name/Desktop/duo_desktop_support_2022-06-21-16-27-59.zip` (oder `DHA_Support_...zip`).

Befehlszeilenoptionen

Windows (PowerShell)

Option | Beschreibung

| `-Ereignisprotokolle` | Exportiert Systemprotokolle. Optionen: `System` |

| `-Tage` | Anzahl der Tage der zu exportierenden Sicherheitsereignisprotokolle |

| `-Benutzer` | Gibt an, von welchem Benutzer Protokolle gesammelt werden sollen (erforderlich, wenn die Funktion als Administrator unter einem anderen Benutzernamen ausgeführt wird). |

| `Get-Help` | Integriertes Cmdlet; vor dem Skript aufrufen, z. B. `Get-Help .\DuoDesktop-Support.ps1` |

macOS (Terminal)

`-a` | Exportiert alle Benutzer- und Kernel-Panic-Protokolle.

`-h` | Zeigt eine Hilfemeldung an.

—

End-to-End-Verfahren

Windows (Beispiel: Exportieren von Systemereignisprotokollen der letzten 2 Tage)

1. Öffnen Sie eine administrative PowerShell-Sitzung auf dem Endpunkt, auf dem Duo Desktop installiert ist.

2. Aktivieren Sie die Debug-Protokollierung (Teil 1).

3. Reproduzieren des Duo-Problems

4. Führen Sie das Skript aus:

- Duo Desktop:

```powershell

& 'C:\Program Dateien (x86)\Duo Desktop\DuoDesktop-Support.ps1' -Ereignisprotokollsystem -Tage 2

"

- Duo Device Health:

```powershell

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

"

> Wenn "Skripte auf diesem System ausführen ist deaktiviert": Passen Sie die PowerShell-Ausführungsrichtlinie so an, dass das Skript ausgeführt werden kann, und führen Sie dann den Befehl erneut aus.

### MacOS (Beispiel: alle Benutzer- und Kernel-Panic-Protokolle exportieren)

1. Öffnen Sie eine Terminal-Sitzung auf dem Endpunkt, auf dem Duo Desktop installiert ist.

2. Aktivieren Sie die Debug-Protokollierung (Teil 1).

3. Reproduzieren des Duo-Problems

4. Führen Sie das Skript aus:

- Duo Desktop:

"bash

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

"

- Duo Device Health:

"bash

/Anwendungen/Duo\ Gerätestatus.app/Contents/Resources/device_health_support.sh -a

"

—

## Diese beim Cisco TAC einreichen -

1 DART- und `Duo_Desktop_Support-Ordner auf Ihrem Desktop zum Cisco TAC.`

`2 Zeitrahmen für einen fehlgeschlagenen Versuch`

`3 Statusprüfungen im Statusprofil erzwungen.`

# Ursache

Eine oder mehrere Statusprüfungen (Betriebssystemversion, AV-Status, Festplattenverschlüsselung, Domänenbeitritt, Firewall-Status) erfüllten nicht den in der Richtlinie für den Netzwerkzugriff ohne Vertrauensstellung definierten Schwellenwert.

# Verwandte Inhalte

- Konfiguration der Duo Desktop-Debugprotokollierung

- Duo Desktop-Support-Tool
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.