Risolvi "Controllo postura non riuscito o postura troppo vecchia" Errore nella ricerca attività per il flusso ZTNA

Sommario

Problema

Dopo aver applicato la verifica della postura di accesso alla rete con attendibilità zero, il problema si manifesta in due modi a seconda della configurazione dei criteri:

- Quando esiste una regola di apertura degli errori: Il traffico ignora l'applicazione della postura e corrisponde alla regola "Nessun controllo postura".
- Quando è abilitata l'applicazione rigorosa: Agli utenti viene negato l'accesso alle applicazioni private.

Ambiente

- Cisco Secure Access - Flusso di accesso alla rete senza trust
- Duo Desktop

Risoluzione

Raccolta di Duo Desktop Diagnostics: Abilita registrazione debug ed esegui lo strumento di supporto

Passaggio 1 - Abilitazione della registrazione di debug (macOS e Windows)

1. Aprire l'app Duo Desktop.

2. Passare a Preferenze.

3. Selezionare Abilita rapporti diagnostici dettagliati.

Fase 2 - Riprodurre il problema

—

Passaggio 3 — Raccolta del pacchetto Dart - Raccolta del pacchetto DART per Secure Client

Passaggio 4 - Esecuzione dello strumento di supporto

Lo script dello strumento di supporto viene fornito con Duo Desktop 6.0.0+ e Duo Device Health 2.26.1+ per macOS e Windows.

Raccoglie i file necessari, li pulisce di informazioni riservate e crea un file ZIP pronto per l'invio.

Posizioni script

Windows

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

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

macOS

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

- Stato dispositivo Duo: `/Applications/Duo Stato del dispositivo.app/Contents/Resources/device_health_support.sh`

Nota: I percorsi differiscono tra le versioni precedenti di Duo e le nuove versioni di Duo Desktop. Utilizzare la coppia corrispondente all'installazione in uso.

Informazioni raccolte dallo strumento di supporto

Windows

1. Crea un file ZIP in cui memorizzare le informazioni raccolte.

2. Esegue `Invoke-WebRequest` per verificare la connettività a Duo.

3. Acquisizioni: impostazioni proxy di sistema; versione, build e bit del sistema operativo; stato BitLocker; fuso orario; Registri eventi applicazione correlati a Duo.

4. Copie `...\AppData\Local\DuoDesktop\Logs` (o `...\DuoDeviceHealth\Logs`) in ZIP.

5. Esporta le chiavi del Registro di sistema Duo da `HKLM:\SOFTWARE\Duo` e `HKCU\SOFTWARE\Duo Device Health` in `system_info.txt`.

6. Copia i certificati associati all'adattatore loopback `127.0.0.1`).

7. (Facoltativo) Esporta i registri eventi di sistema.

8. Salva lo ZIP sul desktop dell'utente connesso, ad esempio `C:\Users\user_name\Desktop\Duo_Desktop_Support_2022-06-21-02-04-44.zip` (o `DHA_Support_...zip`)

MacOS

1. Crea un file ZIP in cui memorizzare le informazioni raccolte.

2. Esegue l'`arricciatura` per verificare la connettività a Duo.

3. Acquisizioni: impostazioni proxy di sistema; `install.log`; `registro.sistema`; registri di arresto anomalo relativi a Duo; Versione sistema operativo e kernel.

4. Copia `/Users/nome_utente/Libreria/Logs/Duo Desktop/*.log` (o `Duo Device Health`) nello ZIP.

5. Copia i certificati associati all'adattatore loopback `127.0.0.1`).

6. (Facoltativo) Esporta tutti i registri utente e kernel.

7. Salva lo ZIP sul desktop dell'utente connesso, ad esempio `/Users/user_name/Desktop/duo_desktop_support_2022-06-21-16-27-59.zip` (o `DHA_Support_...zip`)

Opzioni della riga di comando

Windows (PowerShell)

Opzione | Descrizione

| `-eventlog` | Esporta i registri di sistema. Options: `sistema` |

| `-giorni` | Numero di giorni di log eventi di sicurezza da esportare |

| `-utente` | Specifica l'utente da cui raccogliere i log (necessario quando l'utente viene eseguito come amministratore con un nome utente diverso) |

| `Guida` | Cmdlet predefinito; chiamarlo prima dello script, ad esempio `Get-Help .\DuoDesktop-Support.ps1` |

macOS (terminale)

`-a` | Esporta tutti i registri di utenti e kernel non autorizzati.

`-h` | Visualizza un messaggio della Guida.

—

Procedura end-to-end

Finestre (esempio: esporta registri eventi di sistema degli ultimi 2 giorni)

1. Aprire una sessione amministrativa di PowerShell sull'endpoint in cui è installato Duo Desktop.

2. Abilitare la registrazione del debug (parte 1).

3. Riprodurre il problema relativo al Duo.

4. Eseguire lo script:

- Duo Desktop:

"powershell

& 'C:\Program (x86)\Duo Desktop\DuoDesktop-Support.ps1' -sistema eventlogs -giorni 2

"

- Stato dispositivo Duo:

"powershell

& 'C:\Program (x86)\Duo Device Health\DeviceHealth-Support.ps1' -sistema eventlogs -giorni 2

"

> Se viene visualizzato il messaggio "Running scripts is disabled on this system": modificare i criteri di esecuzione di PowerShell per consentire l'esecuzione dello script, quindi eseguire nuovamente il comando.

MacOS (esempio: Esporta tutti i registri utente e kernel (ansiosi)

1. Aprire una sessione terminale sull'endpoint in cui è installato Duo Desktop.

2. Abilitare la registrazione del debug (parte 1).

3. Riprodurre il problema relativo al Duo.

4. Eseguire lo script:

- Duo Desktop:

"bash

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

"

- Stato dispositivo Duo:

"bash

/Applications/Duo\ Dispositivo\ Integrità.app/Contents/Resources/device_health_support.sh -a

"

—

Invia i messaggi a Cisco TAC -

1 Cartella Dart e `Duo_Desktop_Support sul desktop in Cisco TAC.`

`2 intervalli di tempo per un tentativo non riuscito`

`3 Controlli di postura applicati nel profilo di postura.`

Causa

Una o più verifiche della postura (versione del sistema operativo, stato AV, crittografia del disco, aggiunta al dominio, stato del firewall) non hanno raggiunto la soglia definita nel criterio di accesso alla rete con attendibilità totale.

Contenuto correlato

- Duo Desktop - Configurazione registrazione debug
- Duo Desktop Support Tool
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).