Resolver "Error de comprobación de estado o Condición demasiado antigua" Error en la búsqueda de actividad para el flujo ZTNA

Contenido

Problema

Después de la verificación de la postura de acceso a la red de confianza cero, el problema se manifiesta de dos maneras dependiendo de la configuración de la política:

- Cuando existe una regla de fallo-apertura: El tráfico omite la aplicación de estado y coincide con la regla "Sin comprobaciones de estado".
- Cuando se habilita la aplicación estricta: A los usuarios se les deniega el acceso a aplicaciones privadas.

Entorno

- Cisco Secure Access: Flujo de acceso a la red sin confianza
- Escritorio Duo

Resolución

Recopilación de Duo Desktop Diagnostics: Habilitar el registro de depuración y ejecutar la herramienta de soporte

Paso 1 - Habilitar registro de depuración (macOS y Windows)

1. Abra la aplicación Duo Desktop.

2. Acceda a Preferencias.

3. Active Activar informes de diagnóstico detallados.

Paso 2 - Reproducción del problema

—

Paso 3: Recopile el paquete DART - Recopile el paquete DART para Secure Client

Paso 4 — Ejecutar la herramienta de soporte

La secuencia de comandos Support Tool se suministra con Duo Desktop 6.0.0+ y Duo Device Health 2.26.1+ para macOS y Windows.

Recopila los archivos necesarios, los borra de información confidencial y crea un ZIP listo para enviar.

Ubicaciones del script

Windows:

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

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

macOS

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

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

Nota: Las trayectorias difieren entre las versiones anteriores de Duo Device Health y las

---

versiones más recientes de Duo Desktop: utilice el par que coincida con su instalación.

Información que recopila la herramienta de asistencia

Windows:

1. Crea un ZIP para guardar la información recopilada.

2. Ejecuta `Invoke-WebRequest` para probar la conectividad a Duo.

3. Capturas: configuración de proxy del sistema; versión del sistema operativo, compilación y bit; estado de BitLocker; zona horaria; Registros de eventos de aplicación relacionados con Duo.

4. Copias `...\AppData\Local\DuoDesktop\Logs` (o `...\DuoDeviceHealth\Logs`) en el ZIP.

5. Exporta claves de registro Duo desde `HKLM:\SOFTWARE\Duo` y `HKCU\SOFTWARE\Duo Device Health` a `system_info.txt`.

6. Copia los certificados asociados con el adaptador de loopback `127.0.0.1`).

7. (Opcional) Exporta registros de sucesos del sistema.

8. Guarda el archivo ZIP en el escritorio del usuario que ha iniciado sesión, por ejemplo, `C:\Users\user_name\Desktop\Duo_Desktop_Support_2022-06-21-02-04-44.zip` (o `DHA_Support_...zip`).

MacOS

1. Crea un ZIP para guardar la información recopilada.

2. Ejecuta `rizo` para probar la conectividad a Duo.

3. Capturas: configuración de proxy del sistema; `install.log`; `system.log`; registros de colisión relacionados con el dúo; Versión del sistema operativo y del núcleo.

4. Copia `/Users/user_name/Library/Logs/Duo Desktop/*.log` (o `Duo Device Health`) en el ZIP.

5. Copia los certificados asociados con el adaptador de loopback `127.0.0.1`).

6. (Opcional) Exporta todos los registros de usuario y de núcleo.

7. Guarda el archivo ZIP en el escritorio del usuario que ha iniciado sesión, por ejemplo, `/Users/user_name/Desktop/duo_desktop_support_2022-06-21-16-27-59.zip` (o `DHA_Support_...zip`).

Opciones de la línea de comandos

Windows (PowerShell)

Opción | Descripción

| `-eventlogs` | Exporta registros del sistema. Opciones: `system` |

| `-días` | Número de días de registros de eventos de seguridad para exportar |

| `-user` | Especifica de qué usuario se deben recopilar los registros (necesario cuando se ejecuta como administrador con un nombre de usuario diferente) |

| `Get-Help` | cmdlet integrado; llámelo antes del script, por ejemplo, `Get-Help .\DuoDesktop-Support.ps1` |

macOS (Terminal)

`-a` | Exporta todos los registros de pánico de usuario y núcleo.

`-h` | Muestra un mensaje de ayuda.

—

Procedimiento de extremo a extremo

Windows (ejemplo: exportar registros de eventos del sistema de los últimos 2 días)

1. Abra una sesión administrativa de PowerShell en el terminal donde Duo Desktop está instalado.

2. Habilite el registro de depuración (Parte 1).

3. Reproduzca la cuestión del Duo.

4. Ejecute el script:

- Sobremesa Duo:

"PowerShell

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

"

- Duo Device Health:

"PowerShell

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

"

> Si ve "La ejecución de scripts está deshabilitada en este sistema": ajuste la directiva de ejecución de PowerShell para permitir que se ejecute el script y, a continuación, vuelva a ejecutar el comando.

MacOS (ejemplo: exportar todos los registros de pánico de usuario y núcleo)

1. Abra una sesión Terminal en el terminal donde Duo Desktop está instalado.

2. Habilite el registro de depuración (Parte 1).

3. Reproduzca la cuestión del Duo.

4. Ejecute el script:

- Sobremesa Duo:

"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

"

—

Envíe estos datos al TAC de Cisco:

1 `Carpeta` Dart y `Duo_Desktop_Support de su escritorio al TAC de Cisco.`

`2 Plazos para un intento fallido`

`3 Comprobaciones de posición aplicadas en Perfil de posición.`

Causa

Una o más comprobaciones de estado (versión del sistema operativo, estado de AV, cifrado de disco, unión a dominio, estado de firewall) no cumplieron el umbral definido en la directiva de acceso a la red de confianza cero.

Contenido relacionado

- Configuración de registro de depuración de escritorio Duo
- Duo Desktop Support Tool
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).