Resolver "Falha na verificação de postura ou Postura muito antiga" Erro na pesquisa de atividade para o fluxo ZTNA

Contents

Problema

Após a verificação da aplicação da postura de acesso à rede com confiança zero, o problema se manifesta de duas maneiras, dependendo da configuração da política:

- Quando existe uma regra fail-open: O tráfego ignora a aplicação de postura e corresponde à regra "Sem verificações de postura".
- Quando a aplicação estrita estiver habilitada: Os usuários têm acesso negado a aplicativos privados.

Ambiente

- Cisco Secure Access — Fluxo de acesso à rede com confiança zero
- Desktop Duo

Resolução

Coletando diagnósticos de desktop do Duo: Ative o registro de depuração e execute a ferramenta de suporte

Etapa 1 - Ativar o registro de depuração (macOS e Windows)

1. Abra o aplicativo Duo Desktop.

2. Navegue até Preferências.

3. Marque Ativar relatórios de diagnóstico detalhados.

Etapa 2 - Reproduzir o problema

—

Etapa 3 — Coletar o pacote DART - Coletar o pacote DART para cliente seguro

Etapa 4 — Executar a ferramenta de suporte

O script da ferramenta de suporte é fornecido com o Duo Desktop 6.0.0+ e o Duo Device Health 2.26.1+ para MacOS e Windows.

Ele coleta os arquivos necessários, limpa-os de informações confidenciais e cria um ZIP pronto para enviar.

Localizações dos scripts

Windows

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

- Integridade do dispositivo Duo: `C:\Program Arquivos (x86)\Integridade do Dispositivo Duo\DeviceHealth-Support.ps1`

MacOS

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

- Integridade do dispositivo Duo: `/Applications/Duo Integridade do Dispositivo.app/Contents/Resources/device_health_support.sh`

Note: Os caminhos diferem entre as versões mais antigas do Duo Device Health e as versões mais novas do Duo Desktop — use o par que corresponde à sua instalação.

O que a ferramenta de suporte coleta

Windows

1. Cria um ZIP para armazenar as informações coletadas.

2. Executa `Invoke-WebRequest` para testar a conectividade ao Duo.

3. Capturas: configurações de proxy do sistema; Versão, compilação e bit do SO; Status do BitLocker; fuso horário; Registros de eventos do aplicativo relacionados ao Duo.

4. Cópias `...\AppData\Local\DuoDesktop\Logs` (ou `...\DuoDeviceHealth\Logs`) no ZIP.

5. Exporta chaves de registro Duo de `HKLM:\SOFTWARE\Duo` e `HKCU\SOFTWARE\Duo Device Health` para `system_info.txt`.

6. Copia certificados associados ao adaptador de loopback `127.0.0.1`).

7. (Opcional) Exporta logs de Eventos do Sistema.

8. Salva o ZIP no Desktop do usuário conectado, por exemplo, `C:\Users\user_name\Desktop\Duo_Desktop_Support_2022-06-21-02-04-44.zip` (ou `DHA_Support_...zip`).

MacOS

1. Cria um ZIP para armazenar as informações coletadas.

2. Executa `curl` para testar a conectividade com o Duo.

3. Capturas: configurações de proxy do sistema; `install.log`; `system.log`; Registros de colisão relacionados com o Duo; SO e versão kernel.

4. Copia `/Users/user_name/Library/Logs/Duo Desktop/*.log` (ou `Duo Device Health`) no ZIP.

5. Copia os certificados associados ao adaptador de loopback `127.0.0.1`).

6. (Opcional) Exporta todos os logs de usuário e de kernel.

7. Salva o ZIP no Desktop do usuário conectado, por exemplo, `/Users/user_name/Desktop/duo_desktop_support_2022-06-21-16-27-59.zip` (ou `DHA_Support_...zip`).

Opções da linha de comando

Windows (PowerShell)

Opção | Descrição

| `-logs de eventos` | Exporta logs do sistema. Opções: `sistema` |

| `-dias` | Número de dias de registros de eventos de segurança para exportar |

| `- usuário` | Especifica de qual usuário coletar logs (necessário ao executar como administrador com um nome de usuário diferente) |

| `Obter ajuda` | Cmdlet integrado; chame-o antes do script, por exemplo, `Get-Help .\DuoDesktop-Support.ps1` |

macOS (Terminal)

`-a` | Exporta todos os logs de pane do Kernel e do usuário.

`-h` | Exibe uma mensagem de ajuda.

—

Procedimento End-to-End

Windows (exemplo: exportar logs de eventos do sistema dos últimos 2 dias)

1. Abra uma sessão administrativa do PowerShell no endpoint onde o Duo Desktop está instalado.

2. Ativar o registro de depuração (Parte 1).

3. Reproduza o problema Duo.

4. Execute o script:

- Desktop Duo:

```powershell

& 'C:\Program de eventos (x86)\Duo Desktop\DuoDesktop-Support.ps1' -eventlogs system -dias 2

"
```

- Integridade do dispositivo Duo:

```powershell

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

"
```

> Se você vir "A execução de scripts está desativada neste sistema": ajuste a política de execução do PowerShell para permitir que o script seja executado e execute o comando novamente.

MacOS (exemplo: exportar todos os logs de pane de usuário e kernel)

1. Abra uma sessão do Terminal no endpoint onde o Duo Desktop está instalado.

2. Ativar o registro de depuração (Parte 1).

3. Reproduza o problema Duo.

4. Execute o script:

- Desktop Duo:

"bash

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

"

- Integridade do dispositivo Duo:

"bash

/Aplicativos/Duo\ Integridade do dispositivo\.app/Contents/Resources/device_health_support.sh -a

"

—

Enviar para o TAC da Cisco -

1 Pasta Dart e `Duo_Desktop_Support em sua área de trabalho para o Cisco TAC.`

`2 Intervalos de tempo para uma tentativa com falha`

`3 Verificações de postura aplicadas no perfil de postura.`

Causa

Uma ou mais verificações de postura (versão do SO, status do AV, criptografia de disco, ingresso no domínio, estado do firewall) não atenderam ao limite definido na política de acesso de Rede com Confiança Zero.

Conteúdo relacionado

- Configuração de registro de depuração do desktop Duo

- Ferramenta de suporte Duo para desktop
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.