Résoudre "Echec de la vérification de la position ou Position trop ancienne" Erreur dans la recherche d'activité pour le flux ZTNA

Table des matières

Problème

Après la vérification de la position d'accès réseau sans confiance, le problème se manifeste de deux façons selon la configuration de la stratégie :

- En présence d'une règle d'échec : Le trafic contourne l'application de la position et correspond à la règle « Pas de vérification de position ».
- Lorsque l'application stricte est activée : L'accès aux applications privées est refusé aux utilisateurs.

Environnement

- Cisco Secure Access — Flux d'accès réseau sans confiance
- Bureau Duo

Résolution

Collecte des diagnostics Duo Desktop : Activer la consignation du débogage et exécuter l'outil de support

Étape 1 : activation de la consignation du débogage (macOS et Windows)

1. Ouvrez l'application Duo Desktop.

2. Accédez à Préférences.

3. Cochez Activer les rapports de diagnostic détaillés.

Étape 2 - Reproduisez le problème

—

Étape 3 — Collecte du bundle DART - Collecte du bundle DART pour le client sécurisé

Étape 4 — Exécutez l'outil de support

Le script de l'outil de support est livré avec Duo Desktop 6.0.0+ et Duo Device Health 2.26.1+ pour macOS et Windows.

Il collecte les fichiers nécessaires, les débarrasse des informations sensibles et crée un fichier ZIP prêt à envoyer.

Emplacements des scripts

Fenêtres

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

- Intégrité des périphériques Duo : `C:\Program Fichiers (x86)\Duo Device Health\DeviceHealth-Support.ps1`

macOS

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

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

Remarque : Les chemins diffèrent entre les versions plus anciennes de Duo Device Health et les versions plus récentes de Duo Desktop — utilisez la paire qui correspond à votre installation.

Éléments collectés par l'outil d'assistance

Fenêtres

1. Crée un code postal pour stocker les informations collectées.

2. Exécute `Invoke-WebRequest` pour tester la connectivité à Duo.

3. Captures : paramètres du proxy système ; version du système d'exploitation, build et bit ; État de BitLocker ; fuseau horaire ; Journaux d'événements d'application associés à Duo.

4. Copies `...\AppData\Local\DuoDesktop\Logs` (ou `...\DuoDeviceHealth\Logs`) dans le fichier ZIP.

5. Exporte les clés de registre Duo de `HKLM:\SOFTWARE\Duo` et `HKCU\SOFTWARE\Duo Device Health` vers `system_info.txt`.

6. Copie les certificats associés à la carte de bouclage (`127.0.0.1`).

7. (Facultatif) Exporte les journaux des événements système.

8. Enregistre le code postal sur le bureau de l'utilisateur connecté, par exemple, `C:\Users\user_name\Desktop\Duo_Desktop_Support_2022-06-21-02-04-44.zip` (ou `DHA_Support_...zip`).

MacOS

1. Crée un code postal pour stocker les informations collectées.

2. Exécute `curl` pour tester la connectivité à Duo.

3. Captures : paramètres du proxy système ; `install.log` ; `system.log` ; Journaux d'incidents liés au duo ; OS et version du noyau.

4. Copie `/Users/user_name/Library/Logs/Duo Desktop/*.log` (ou `Duo Device Health`) dans le fichier

ZIP.

5. Copie les certificats associés à la carte de bouclage (`127.0.0.1`).

6. (Facultatif) Exporte tous les journaux utilisateur et de noyau.

7. Enregistre le code postal sur le Bureau de l'utilisateur connecté, par exemple, `/Users/user_name/Desktop/duo_desktop_support_2022-06-21-16-27-59.zip` (ou `DHA_Support_...zip`).

Options de ligne de commande

Windows (PowerShell)

Option | Description

| `-journaux des événements` | Exporte les journaux système. Options: `système` |

| `-jours` | Nombre de jours d'exportation des journaux d'événements de sécurité |

| `-utilisateur` | Spécifie l'utilisateur à partir duquel collecter les journaux (nécessaire lorsque vous exécutez en tant qu'administrateur sous un nom d'utilisateur différent) |

| `Obtenir de l'aide` | applet de commande intégrée ; l'appeler avant le script, par exemple, `Get-Help .\DuoDesktop-Support.ps1` |

macOS (Terminal)

`-a` | Exporte tous les journaux de panique des utilisateurs et du noyau.

`-h` | Affiche un message d'aide.

—

Procédure de bout en bout

Windows (exemple : exporter les journaux des événements système des 2 derniers jours)

1. Ouvrez une session PowerShell administrative sur le point de terminaison où Duo Desktop est

installé.

2. Activer la journalisation du débogage (Partie 1).

3. Reproduisez le numéro Duo.

4. Exécutez le script :

- Bureau Duo :

« powershell

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

«

- Intégrité des périphériques Duo :

« powershell

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

«

> Si vous voyez "L'exécution des scripts est désactivée sur ce système" : ajustez la stratégie d'exécution PowerShell pour autoriser l'exécution du script, puis réexécutez la commande.

MacOS (exemple : exporter tous les journaux paniques de l'utilisateur et du noyau)

1. Ouvrez une session Terminal sur le terminal sur lequel Duo Desktop est installé.

2. Activer la journalisation du débogage (Partie 1).

3. Reproduisez le numéro Duo.

4. Exécutez le script :

- Bureau Duo :

«bash

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

«

- Intégrité des périphériques Duo :

«bash

/Applications/Duo\ Équipement\ Intégrité.app/Contents/Resources/device_health_support.sh -a

«

—

Envoyez-les au TAC Cisco -

1 `Dossier` Dart et `Duo_Desktop_Support sur votre bureau vers le centre d'assistance technique Cisco.`

`2 Délais pour une tentative ayant échoué`

`3 Contrôles de position appliqués dans le profil de position.`

Motif

Un ou plusieurs contrôles de position (version du système d'exploitation, état AV, cryptage de disque, jonction de domaine, état du pare-feu) n'ont pas atteint le seuil défini dans la stratégie d'accès au réseau Zero Trust.

Autres informations utiles

- Configuration de la consignation du débogage Duo Desktop
- Outil d'assistance Duo Desktop
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.