ZTNAフローのアクティビティ検索の"；ポスチャチェック失敗またはポスチャが古すぎる"；エラーの解決

内容

問題

Zero Trust Network Access（Zネットワークアクセス）ポスチャチェックを実行すると、ポリシー設定に応じて次の2つの方法で問題が発生します。

- フェールオープンルールが存在する場合：トラフィックはポスチャ強制をバイパスし、「ポスチャチェックなし」ルールと一致します。
- 厳密な適用が有効な場合：ユーザーはプライベートアプリケーションへのアクセスを拒否されます。

環境

- Cisco Secure Access：ゼロトラストネットワークアクセスのフロー
- Duoデスクトップ

解決方法

Duo Desktop診断の収集：デバッグログを有効にしてサポートツールを実行

###手順1：デバッグロギングの有効化（macOSおよびWindows）

1. Duo Desktopアプリを開きます。

2. Preferencesに移動します。

3. Enable detailed diagnostic reportsにチェックマークを入れます。

ステップ2：問題の再現

—

##ステップ3:DARTバンドルの収集 – セキュアクライアントのDARTバンドルの収集

##ステップ4：サポートツールを実行します。

サポートツールスクリプトには、macOSおよびWindows用のDuo Desktop 6.0.0+およびDuo Device Health 2.26.1+が付属しています。

必要なファイルを収集し、機密情報をスクラビング処理し、すぐに送信できるZIPを作成します。

###スクリプトロケーション

Windows

- Duoデスクトップ： `C:\Program Files (x86)\Duo Desktop\DuoDesktop-Support.ps1`

- Duoデバイスの正常性： `C:\Program Files (x86)\Duo Device Health\DeviceHealth-Support.ps1`

MacOS

- Duoデスクトップ： `/Applications/Duo Desktop.app/Contents/Resources/duo_desktop_support.sh`

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

注：古いDuo Device Healthリリースと新しいDuo Desktopリリースではパスが異なるため、ご使用のインストールに合ったペアを使用してください。

###サポートツールが収集するもの

Windows

1. 収集した情報を格納するZIPを作成します。

2. `Invoke-WebRequest`を実行して、Duoへの接続をテストします。

3. キャプチャ：システムプロキシ設定、OSバージョン、ビルド、およびビット、BitLockerの状態、タイムゾーン、Duo関連アプリケーションのイベントログ。

4. `..\AppData\Local\DuoDesktop\Logs`（または`...\DuoDeviceHealth\Logs`）をZIPにコピーします。

5. `HKLM:\SOFTWARE\Duo`および`HKCU\SOFTWARE\Duo Device Health`から`system_info.txt`にDuoレジストリキーをエクスポートします。

6. ループバックアダプタに関連付けられている証明書をコピーします(`127.0.0.1`)。

7.（任意）システムイベントログをエクスポートします。

8. C:\Users\user_name\Desktop\Duo_Desktop_Support_2022-06-21-02-04-44.zip（または`DHA_Support_...zip`）など、サインインしているユーザのデスクトップにZIPを保存します。

MacOS

1. 収集した情報を格納するZIPを作成します。

2. `curl`を実行して、Duoへの接続をテストします。

3. キャプチャ：システムプロキシ設定、`install.log`、`system.log`、Duo関連クラッシュログ、OSおよびカーネルバージョン。

4. `/Users/user_name/Library/Logs/Duo Desktop/*.log`（または`Duo Device Health`）をZIPにコピーします。

5. ループバックアダプタに関連付けられている証明書をコピーします(`127.0.0.1`)。

6.（任意）すべてのユーザログとカーネルログをエクスポートします。

7. /Users/user_name/Desktop/duo_desktop_support_2022-06-21-16-27-59.zip（または

DHA_Support_...zip ）など、サインインしているユーザのデスクトップにZIPを保存します。

###コマンドラインオプション

Windows (PowerShell)

オプション|説明

| -eventlogs |システムログをエクスポートします。オプション：system |

| -days |エクスポートするセキュリティイベントログの日数|

| -user |ログの収集元となるユーザを指定します（adminとして別のユーザ名で実行する場合に必要）|

| Get-Help |組み込みコマンドレット。スクリプトの前に呼び出します。たとえば、Get-Help .\DuoDesktop-Support.ps1 |

macOS（ターミナル）

-a |ユーザーおよびカーネルのパニック・ログをすべてエクスポートします。

-h |ヘルプメッセージを表示します。

—

##エンドツーエンドの手順

Windows（例：過去2日間のシステムイベントログのエクスポート）

1. Duo Desktopがインストールされているエンドポイントで、管理PowerShellセッションを開きます。

2. debug loggingを有効にします（パート1）。

3. Duoの問題を再現します。

4. スクリプトを実行します。

- Duoデスクトップ：

```powershell

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

"

- Duoデバイスのヘルス：

```powershell

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

"

> 「Running scripts is disabled on this system」が表示された場合：PowerShell 実行ポリシーを調整してスクリプトが実行できるようにしてから、コマンドを再実行してください。

### MacOS（例：すべてのユーザおよびカーネルパニックログをエクスポートする）

1. Duo Desktopがインストールされているエンドポイントでターミナルセッションを開きます。

2. debug loggingを有効にします（パート1）。

3. Duoの問題を再現します。

4. スクリプトを実行します。

- Duoデスクトップ：

“`bash

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

"

- Duoデバイスのヘルス：

“`bash

/Applications/Duo\ Device\ Health.app/Contents/Resources/device_health_support.sh -a

"

—

##これらをCisco TACに送信します。

デスクトップ上の1 DartおよびDuo_Desktop_Supportフォルダからcisco TACへ。

2失敗した試行のタイムフレーム

3ポスチャプロファイルにポスチャチェックが適用されます。

# 原因

1つ以上のポスチャチェック（OSバージョン、AVステータス、ディスク暗号化、ドメイン参加、ファイアウォール状態）が、Zero Trust Networkアクセスポリシーで定義されているしきい値を満たしませんでした。

# 関連コンテンツ

- Duo Desktopデバッグログの設定
- Duoデスクトップサポートツール
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。