

ZTNAクライアントエラー"Active Directory Integration not detected for this user device" on Entra-Joined Devices

内容

問題

ZTNA機能をテストするユーザで、Entraに参加しているデバイスでZTNAクライアントに「Active Directory Integration not detected for this user device」と表示される断続的なエラーが発生します。このエラーは一時的で、ユーザ間で一貫性がないため、ZTNAのアクセスチェック中に予期しないエラーが発生します。Entraに参加しているデバイスを使用しているユーザの一部では、このエラーが発生することはありませんが、このエラーが何度も発生するユーザもいます。エラーは一般に、ユーザの介入なしに一定の時間が経過すると消失します。

この問題は、Entra加入デバイスとオンプレミスAD加入デバイスに対して個別のアクセスルールが設定されているポスチャ評価プロセスに関連していると考えられます。これらのポスチャチェック中に、影響を受けるユーザにフラグが付けられたり、ZTNAリソースへのアクセスがブロックされたりして、Zero Trust Network Accessフレームワークを介した内部システムへの接続に影響が及ぶ可能性があります。

環境

- ・ ソリューションサポート (SSPT – 契約が必要)
- ・ セキュアなアクセス：ゼロトラストアクセス (ZTNA、ポスチャ、クライアントベース、登録、プライベートリソース)
- ・ Active Directoryドメインに参加しているオンプレミスのデバイスとEntraドメインに参加しているデバイスの両方を含む混在環境
- ・ EntraデバイスとオンプレミスADデバイスに対して個別のポスチャプロファイルを設定
- ・ デュアルアクセスポリシールール：「すべての内部リソース – Entraデバイス」および「すべての内部リソース – MacおよびオンプレミスDS」

- 組織全体のテストグループに複数のユーザ

解決方法

このActive Directory統合の断続的な検出の問題を解決するには、次の項で説明するトラブルシューティングと検証の手順に従ってください。

ステップ1: ZTNAクライアントのバージョンを更新します。

最新のZTNAクライアントバージョン5.1.16にアップグレードし、問題が継続してアップデートされたクライアントソフトウェアで発生するかどうかをテストします。

ステップ2：発生の詳細情報の収集

エラーが発生したら、次の情報を文書化します。

- エラーが発生した時刻の正確なタイムスタンプ
- 影響を受けるユーザ名とデバイスID
- 影響を受けるデバイスのオペレーティングシステムのバージョン
- エラー発生時のユーザの場所とネットワークコンテキスト
- 自動解決までのエラー持続期間

ステップ3：デバイス登録ステータスの確認

エラーが発生した際に、影響を受けるデバイスで次のコマンドを実行して、ドメイン登録のステータスを確認します。

```
dsregcmd /status
```

このコマンドの完全な出力をキャプチャして、デバイスのEntra ID登録ステータスを確認し、登録の不整合を特定します。

ステップ4：デバイスアカウント設定の文書化

Settings > Accounts > Access work or schoolの順に移動し、エラー発生時のアカウント設定のスクリーンショットをキャプチャして、ユーザインターフェイスの観点からデバイスドメインの参加ステータスを確認します。

ステップ5:DARTログとエラースクリーンショットを確認する

影響を受けるデバイスからのDART(Data Analysis and Reporting Tool)出力とエラースクリーンショットを収集して分析し、間欠的な検出エラーの原因である可能性がある、ポスチャ評価プロセスのパターンを特定します。

ステップ6：回避策の適用

この動作は、システムの起動中のタイミングの問題と一貫しているように見えます。システムの起動中には、Windowsが再起動後にEntra (Azure AD)の初期化を完全に完了する前に、ZTNAクライアントが初期ポスチャチェックを実行できます。これにより、デバイスが正しくEntra-joinedであっても、一時的に「Active Directory Integration not detected for this user device」というメッセージが表示される場合があります。

最初の簡単な回避策として、ZTNAエージェントがブート時に短い遅延で起動するように設定することをお勧めします。

ステップ

1.- Services (services.msc)を開きます。

2.- Cisco Secure Client - Zero Trust Access Agentを見つけます。

3.- Propertiesを右クリックします。

4.- Startup typeをAutomatic (Delayed Start)に設定します。

5.- Applyをクリックし、OKをクリックします。

6. – マシンを再起動し、ZTNAアクセスをテストします。

この起動の遅延（通常は60 ～ 120秒）により、ZTNAポスチャ評価が実行される前に、Entra参加状態、Azure AD PRT、およびWindows IDサービス(WAM)が完全に初期化されるまでの時間が確保されます。

原因

間欠的な「Active Directory Integration not detected」エラーは、Entraに参加しているデバイスのポスチャ評価プロセスの不一致に関連していると考えられます。この問題は、ZTNAクライアントポスチャアセスメントフレームワーク内でのデバイスドメイン検証チェック中のタイミングまたは同期の問題に起因している可能性があります。ドメイン認識の制限により、Entra加入デバイスとオンプレミスAD加入デバイスでは別々のポスチャプロファイルが必要になるため、評価プロセスでEntraドメインメンバーシップを適切に識別できないことが時々あり、その結果、一時的なエラー状態が発生します。

関連コンテンツ

- [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。