SysPrepゴールデンイメージを使用したセキュアアクセス展開での重複したZTNAデバイスIDの解決

内容

お問い合わせ内容

SysPrepゴールデンイメージから展開された複数のWindows物理マシンが同一のZTNAデバイスID、特に複数のエンドポイントで同一のztnaDeviceIdを生成しています。この重複により、次のような重大な問題が発生します。

- 同じZTNAデバイスIDを持つデバイスの再登録の繰り返し
- 再登録プロセスごとに公開キーを上書きする
- 最近登録されたデバイスを除くすべてのマシンでポスチャチェックが失敗する
- 影響を受けるエンドポイントのセキュアアクセスによるアクセスの失敗

確認された動作は、フリート内の複数のマシンが同じZTNAデバイスIDを共有し、それぞれの登録で前のマシンの公開キーが上書きされる場合に発生します。登録する最新のマシンを除くすべてのマシンがポスチャチェックの送信に失敗し、Secure Accessインフラストラクチャを介したアクセス拒否が発生します。

複数のホスト名とユーザIDのペアが同じZTNAデバイスIDにリンクされていることが確認され、導入全体で重複の問題の範囲が示されました。

環境

- Cisco Secure Access（ZTNA実装）
- Windows物理マシン（仮想マシンではない）

- SysPrepゴールデンイメージの導入方法
- イメージ展開用のWindows ADK（評価および展開キット）ツール
- イメージキャプチャ用のESD(Electronic Software Delivery)ファイル形式
- 必須ソフトウェアインストールを含む標準化されたOS強化プロセス
- 標準のローカル管理者およびゲストアカウントの設定

解決策

解決プロセスには、包括的なログ分析と、詳細な調査による根本原因の特定が含まれていました。

根本原因の特定と解決

調査の結果、ゴールデンイメージの導入時にSysPrepプロセスが一意のデバイスIDを正しく生成していなかったことが判明しました。

分析の対象：

Windowsレジストリキーの検査。具体的には次のとおりです。

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion
```

以下を使用して、ユーザのセキュリティID情報を収集します。

```
whoami /user
```

導入時にデバイス固有のIDが適切に再生成され、複数の物理マシン間でZTNAデバイスIDの重複が防止されるようにするために、SysPrepプロセスを修正する必要がありました。

- dartcli.exe -nu コマンドを実行してUDIDを更新すると、「

HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Cisco\Cisco Secure Client\DeviceDetails」レジストリパスの下のNounceの値が変更されます。

- C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollmentsからJSONファイルを削除し、ZTAサービスを再起動すると、ユーザの登録が解除されます。ユーザを手動で登録する必要があります。これにより、他の影響を受けずに新しいJSONファイルが生成されます。
- すべてのエンドポイントでUDIDを更新しても、どのサーバでも値が検証/評価されない限り、影響はありません。

1. 管理者としてコマンドプロンプトを起動し、「%ProgramFiles(x86)%\Cisco\Cisco Secure Client\DART」ディレクトリに移動します。

2. dartcli.exe -uを実行し、現在のUDIDの値を確認します。

3. dartcli.exe -nuコマンドを実行します。このコマンドは、UDIDを更新します。

4. 手順2のコマンドを繰り返して、新しい値を確認します。

5. C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollmentsディレクトリからJSONファイルを削除します。

6. VPNおよびZTAサービスを再起動します。この時点で、ZTAは未登録状態である必要があります。

7. ユーザーが手動でZTAを登録できるようにする

9. JSONファイル内の新しいztnaDeviceIdの値を確認します。

監視と検証

一意のZTNAデバイスIDの生成を保証するための是正措置を実施した後：

- 複数のマシンで登録プロセスを監視
- 各マシンが一意のZTNAデバイスIDを生成したことを確認
- すべての登録済みデバイスでポスチャチェック機能が正常に実行されたことを確認
- 登録時に公開キーの上書きが発生しなくなったことを検証

原因

根本原因は、SysPrepゴールデンイメージ展開プロセスがZTNA登録用の一意のデバイス識別子を正しく生成していないために特定されました。同じSysPrepゴールデンイメージから複数のWindows物理マシンを展開した場合、ZTNAデバイスIDの生成に使用される特定のデバイス固有の識別子は、展開されたすべてのマシンで同じままです。

SysPrepプロセスは、OS設定とソフトウェア導入の標準化には有効ですが、Cisco Secure Clientが一意のZTNAデバイスIDを作成するために使用する特定のIDを再生成するように設定されていませんでした。その結果、同じゴールデンイメージから導入されたすべてのマシンが同じZTNAデバイス識別パラメータを継承することになり、セキュアアクセスインフラストラクチャで登録の競合や認証の失敗が発生します。

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。