セキュアアクセスローミングデバイス情報の収集と更新動作

内容

問題

Cisco Secure Access(CSA)ローミングデバイス情報の動作と仕様に関する説明要求。

この調査では、CSAが管理ポータルのManagement Portal > Resources > Roaming Devicesで エンドポイントデバイス情報を収集および表示する方法を理解することに重点が置かれていました 。具体的には次のとおりです。

- CSAがWindows、macOS、およびCisco iOSオペレーティングシステムからローミングデバイス情報を抽出するエンドポイント属性
- エンドポイントでホスト名またはOSバージョンが変更されたときにデバイス情報が自動的に更新されるかどうか
- エンドポイントとCSAクラウド間のローミングデバイス情報の同期の頻度とタイミング
- 属性の変更時にCSAがデバイスIDを決定する方法（同一デバイス決定ロジック）

CSA管理ポータルに表示される観察されるデバイス情報は、オペレーティングシステムによって異なります。

WindowsおよびmacOS

- ホスト名
- オリジナルホスト名
- オペレーティング システム
- シリアル番号

Cisco IOS

- デバイス名（シリアル番号）
- シリアル番号
- OSバージョン

環境

- Cisco Secure Access(CSA)管理ポータル
- セキュアアクセスクライアント（旧称：AnyConnect/Secure Client）
- エンドポイントオペレーティングシステム：Windows、macOS、Cisco iOS
- CSAクラウドインフラストラクチャ

解決方法

次の項で説明する内容は、CSAローミングデバイス情報の動作に関するものです。

オペレーティングシステムによるデバイス属性の収集

WindowsおよびmacOS

Secure Accessクライアントは、OSが提供する標準のデバイスプロパティからデバイス属性を収集します。

- Hostname:OSに設定されている現在のデバイス名
- 元のホスト名：初期登録時または最初のクライアント接続時に取得されたデバイス名

- オペレーティングシステム：OSのタイプとバージョン情報
- シリアル番号：OSから取得できるハードウェア識別情報

Cisco IOS

Appleプラットフォームの制限により、利用可能な情報は、Cisco iOSがアプリケーションにアクセスを許可するものに制限されています。

- デバイス名：Cisco iOSで定義された名前（シリアル番号で表示可能）
- シリアル番号：Cisco iOSによってアプリケーションに許可されるデバイス識別情報（ハードウェアアクセスは直接行われませんが、Apple認定の識別情報）
- OSバージョン：Cisco iOSシステムバージョン情報（Cisco iOS xx.x.xなど）

デスクトップオペレーティングシステムで使用できるホストレベルの属性は、プラットフォームの制約により、Cisco iOSではアクセスできません。

デバイス情報の更新動作

エンドポイントの変更（ホスト名の変更またはOSバージョンの更新）が発生すると、CSAは新しいデバイスレコードを作成するのではなく、既存のローミングデバイスエントリを自動的に更新します。更新は、クライアントが次にCSAクラウドと通信するときに発生し、エンドポイントの変更時には直ちに発生しません。Original Hostnameフィールドは、初期登録の識別参照として保持され、ホスト名が変更されても変更されません。

同期のタイミングとトリガー

デバイス情報の送信と更新は、次のイベントの間に行われます。

- セキュアアクセスクライアントの起動
- ユーザーのサインイン
- CSAサービスの接続または再接続

- 定期的なクラウドの同期

定期的な同期の詳細

自動同期は、再起動または再接続イベントが発生しない場合に、約20 ~ 30分ごとに実行されます。この間隔は固定ではありませんが、クラウド負荷の集中を防ぐために、クライアントごとのジッターがわずかにある内部同期ウィンドウを使用します。タイミングは、完全に固定されているわけでも、完全にランダムなものでもありません。

デバイス情報を即時に更新するには、クライアントの再起動または再接続が最も信頼性の高いトリガーとなります。

同じデバイスの判別ロジック

CSAは、デバイスIDの判別に単一のIDを使用しません。同一デバイスの判別では、これらのオペレーティングシステムの組み合わせを使用します。

WindowsおよびmacOS

- Secure Accessクライアントによって取得される複数の安定したOS提供デバイスID
- クライアントの初期登録時にCSAクラウドによって発行および維持されるCSAクラウドマネージド内部デバイスID

Cisco IOS

- Secure Accessクライアントで使用可能なCisco iOS許可デバイスID
- CSAクラウドマネージド内部デバイスID

管理ポータルに表示されるシリアル番号は、識別プロセスの要素の1つですが、デバイスIDの判別に単独で使用されるわけではありません。この複合アプローチにより、ホスト名やOSのバージョ

ンなどの個々の属性が変更された場合でも、CSAは同じデバイスを認識できます。

特記事項

- ローミングデバイス情報は、管理および可視性の目的で提供され、MDMソリューションのような詳細なエンドポイント制御や適用の目的では提供されません。
- 表示される属性と粒度は、OS側の制限または製品のアップデートにより、将来の製品リリースで変更される可能性があります。
- ここで説明する動作は、不具合ではなく、期待される製品の機能を表しています。

原因

これは、根本原因分析を必要とする技術的な問題ではなく、製品仕様と動作の明確化の要求でした。この問い合わせは、適切なシステム管理および計画の目的で、CSAデバイスの識別および情報同期メカニズムを理解する必要から発生しました。

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。