SHA1ハッシュ非互換性でのエンドポイントDLP証明書ベースの自動登録の失敗

内容

お問い合わせ内容

初期化エラーが繰り返し発生し、証明書ベースの自動登録中にエンドポイントDLP登録が失敗する。登録プロセスでは、クライアントID証明書を使用して認証できないため、再試行が繰り返されます。

登録ログに次のエラーメッセージが記録されます。

```
[2026-02-05 13:24:58.154989] [info] [AutoEnrollMonitor.cpp:633] Auto-enrollment attempt #5 with enrollm
[2026-02-05 13:24:58.154989] [info] [SSEZtnaEnroller.cpp:185] Processing start event
[2026-02-05 13:24:58.155992] [info] [SSEZtnaEnroller.cpp:205] Starting Enrollment
[2026-02-05 13:24:58.398260] [error] [SSEZtnaEnroller.cpp:335] spIdentities count: 1
[2026-02-05 13:24:58.399259] [error] [SSEZtnaEnroller.cpp:355] None of the 1 user store client certifica
[2026-02-05 13:24:58.407289] [info] [SSEZtnaEnroller.cpp:2237] Notifying enrollment completion with resu
[2026-02-05 13:24:58.407289] [info] [SSEZtnaEnroller.cpp:2241]
Enrollment Stats
================
Authentication type           : certificate
Bootstrap                     : failure (0.251 sec)
----------------
Overall result                : failure (0.251 sec)
[2026-02-05 13:24:58.408287] [info] [AutoEnrollMonitor.cpp:214] Notified of enrollment state change to
[2026-02-05 13:24:58.408287] [info] [AutoEnrollMonitor.cpp:214] Notified of enrollment state change to
[2026-02-05 13:24:58.408287] [info] [AutoEnrollMonitor.cpp:615] Will retry the enrollment with enrollmen
```

その他のTLSレベルの認証の失敗については、「TLSアラートを受信しました：致命的/無効な証明書」というエラーメッセージで説明されています。

環境

- テクノロジー：ソリューションサポート（SSPT – 契約が必要）

- サブテクノロジー：セキュアなアクセス：ユニファイドポリシー（インターネットポリシー、プライベートポリシー、DLPポリシー、RBI、セキュリティプロファイル）
- ソフトウェアバージョン：すべて
- 認証方法：証明書ベースの自動登録
- 証明書ストア：ユーザーストアクライアント証明書
- 証明書ハッシュアルゴリズム： SHA1（非推奨）

解決策

この問題を解決するには、サポートされているハッシュアルゴリズムを使用してID証明書を再生成し、証明書のインストールと設定が適切に行われていることを確認する必要があります。

手順1：サポートされているハッシュアルゴリズムを使用してID証明書を再生成する

廃止されたSHA1アルゴリズムの代わりに、SHA256またはSHA-3ハッシュを使用してID証明書を生成し、再発行します。証明書は、次の仕様に従って作成する必要があります。

- ハッシュアルゴリズム：SHA256またはSHA-3（SHA1はサポートされません）
- 形式：PKCS#12(PFX)形式
- 必須フィールド：登録用に指定されたRFC822名のSANフィールド

手順2：更新された証明書を正しい証明書ストアにインストールする

新しく生成された証明書を適切な証明書ストアの場所にインストールします。

- 証明書ストアの場所：ユーザー/マシンの個人用>証明書ストア
- 証明書の形式：PKCS#12(PFX)

ステップ3：エンドポイントをリブートして認証を再トリガーする

更新された証明書をインストールした後、エンドポイントシステムを再起動して認証プロセスを

再トリガーし、登録メカニズムが新しい証明書を検出できるようにします。

ステップ4：社外ネットワークからの認証をテストする

エッジファイアウォールによるSSLインスペクションまたは復号化の干渉を排除するには、企業ネットワーク以外の環境から認証プロセスをテストします。これは、登録プロセスを妨げる可能性があるネットワークレベルの証明書検査の問題を特定するのに役立ちます。

ステップ5：エンドポイントDLP登録の再試行

証明書の交換とシステムのリブートが完了したら、エンドポイントDLP登録プロセスを再試行します。登録ログをモニタして、認証が成功し、登録が完了したことを確認します。

原因

クライアントID証明書でSHA1ハッシュアルゴリズムを使用すると、登録エラーが発生します。SHA1は廃止された暗号化ハッシュアルゴリズムであり、登録ポリシーの要件ではサポートされなくなりました。登録システムでは、現在のセキュリティ標準とポリシーコンプライアンスを満たすために、証明書をSHA256やSHA-3などの最新の安全なアルゴリズムでハッシュする必要があります。

登録プロセスが登録選択ポリシーに照らしてクライアント証明書を検証すると、廃止されたSHA1ハッシュアルゴリズムを使用する証明書が拒否され、「None of the 1 user store client certificate(s) match the enrollment choice policy」エラーメッセージが表示され、その後の初期化が失敗します。

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。