Fehler bei der auf Endpunkt-SvD-Zertifikaten basierenden automatischen Registrierung mit SHA1-Hashing-Inkompatibilität

Inhalt

Problem

Die Endpunkt-DLP-Registrierung schlägt während der zertifikatbasierten automatischen Registrierung mit wiederholten Initialisierungsfehlern fehl. Der Registrierungsprozess kann nicht mithilfe des Client-Identitätszertifikats authentifiziert werden, was zu kontinuierlichen Wiederholungsversuchen führt.

Die folgenden Fehlermeldungen werden in den Registrierungsprotokollen beobachtet:

```
[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 enrollme
```

Zusätzliche Authentifizierungsfehler auf TLS-Ebene werden mit der Fehlermeldung dokumentiert: "TLS-Warnung empfangen: schwerwiegendes/ungültiges Zertifikat."

Umwelt

- Technologie: Solution Support (SSPT - Vertrag erforderlich)
- Untertechnologie: Sicherer Zugriff - Einheitliche Richtlinien (Internetrichtlinien, private Richtlinien, DLP-Richtlinien, RBI, Sicherheitsprofile)
- Software-Version: ALLE
- Authentifizierungsmethode: Zertifikatbasierte automatische Registrierung
- Zertifikatspeicher: Clientzertifikate für den Benutzerspeicher
- Hashing-Algorithmus für Zertifikate: SHA1 (veraltet)

Auflösung

Die Auflösung beinhaltet das Regenerieren des Identitätszertifikats mit einem unterstützten Hashing-Algorithmus sowie das Sicherstellen der korrekten Installation und Konfiguration des Zertifikats.

Schritt 1: Identitätszertifikat mit unterstütztem Hashing-Algorithmus neu generieren

Generieren Sie das Identitätszertifikat, und stellen Sie es erneut mithilfe von SHA256- oder SHA-3-Hashing statt des veralteten SHA1-Algorithmus aus. Das Zertifikat muss mit den folgenden Spezifikationen erstellt werden:

- Hash-Algorithmus: SHA256 oder SHA-3 (SHA1 wird nicht unterstützt)
- Format: PKCS#12 (PFX)-Format
- Pflichtfeld: SAN-Feld mit RFC822-Name wie für die Registrierung angegeben

Phase 2: Installieren des aktualisierten Zertifikats im richtigen Zertifikatspeicher

Installieren Sie das neu generierte Zertifikat am entsprechenden Speicherort im Zertifikatspeicher:

- Speicherort des Zertifikatspeichers: Benutzer-/Computerpersonal > Zertifikatspeicher
- Zertifikatformat: PKCS#12 (PFX)

Schritt 3: Neustart des Endpunkts, um die Authentifizierung erneut auszulösen

Starten Sie nach der Installation des aktualisierten Zertifikats das Endgerätesystem neu, um den Authentifizierungsprozess erneut auszulösen, und ermöglichen Sie dem Registrierungsmechanismus, das neue Zertifikat zu erkennen.

Schritt 4: Authentifizierung von Nicht-Firmennetzwerken testen

Um SSL-Inspektions- oder Entschlüsselungsstörungen durch Edge-Firewalls auszuschließen, testen Sie den Authentifizierungsprozess in einer Umgebung außerhalb des Unternehmens. Auf diese Weise können potenzielle Probleme bei der Zertifikatsüberprüfung auf Netzwerkebene identifiziert werden, die den Registrierungsprozess beeinträchtigen könnten.

Schritt 5: Endpunkt-SvD-Registrierung wiederholen

Wenn Sie den Zertifikataustausch und den Systemneustart abgeschlossen haben, versuchen Sie erneut, den Endpunkt-SvD-Registrierungsprozess durchzuführen. Überwachen Sie die Registrierungsprotokolle, um die erfolgreiche Authentifizierung und den erfolgreichen Abschluss der Registrierung zu überprüfen.

Ursache

Der Registrierungsfehler wird durch die Verwendung des SHA1-Hash-Algorithmus in den Client-Identitätszertifikaten verursacht. SHA1 ist ein veralteter kryptografischer Hashing-Algorithmus, der von den Anforderungen der Registrierungsrichtlinie nicht mehr unterstützt wird. Das Registrierungssystem erfordert speziell, dass Zertifikate mit modernen, sicheren Algorithmen wie SHA256 oder SHA-3 gehasht werden, um aktuelle Sicherheitsstandards und die Einhaltung von Richtlinien zu erfüllen.

Wenn das Clientzertifikat beim Registrierungsprozess anhand der Registrierungsauswahlrichtlinie validiert wird, werden Zertifikate zurückgewiesen, die den veralteten SHA1-Hashing-Algorithmus verwenden. Das Ergebnis ist die Fehlermeldung "Keines der Clientzertifikate des Benutzerspeichers 1 stimmt mit der Registrierungsauswahlrichtlinie überein" und ein anschließender Initialisierungsfehler.

Verwandte Inhalte

- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.