

Errore di registrazione automatica basata su certificato DLP endpoint con incompatibilità di hashing SHA1

Sommario

Problema

La registrazione DLP dell'endpoint non riesce durante la registrazione automatica basata su certificati con errori di inizializzazione ripetuti. Il processo di registrazione non è in grado di eseguire l'autenticazione utilizzando il certificato di identità del client. Verranno eseguiti tentativi continui.

Nei log di registrazione vengono rilevati i messaggi di errore seguenti:

```
[2026-02-05 13:24:58.154989] [info] [AutoEnrollMonitor.cpp:633] Auto-enrollment attempt #5 with enrollme
[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 certific
[2026-02-05 13:24:58.407289] [info] [SSEZtnaEnroller.cpp:2237] Notifying enrollment completion with res
[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
```

Ulteriori errori di autenticazione a livello TLS sono documentati con il seguente messaggio di errore: "Ricevuto avviso TLS: certificato non valido o irreversibile."

Ambiente

- Tecnologia: Supporto per la soluzione (SSPT - contratto obbligatorio)
- Sottotecnologia: Accesso sicuro - Criteri unificati (Criteri Internet, Criteri privati, Criteri di prevenzione della perdita dei dati, RBI, Profili di sicurezza)
- Versione del software: TUTTO
- Metodo di autenticazione: Iscrizione automatica basata su certificati
- Archivio certificati: Certificati client dell'archivio utenti
- Algoritmo di hash certificato: SHA1 (deprecato)

Risoluzione

La risoluzione implica la rigenerazione del certificato di identità con un algoritmo hash supportato e la verifica della corretta installazione e configurazione del certificato.

Passaggio 1: Rigenera certificato di identità con algoritmo hash supportato

Generare e rimettere il certificato di identità utilizzando l'hashing SHA256 o SHA-3 anziché l'algoritmo SHA1 deprecato. Il certificato deve essere creato con le seguenti specifiche:

- Algoritmo di hash: SHA256 o SHA-3 (SHA1 non è supportato)
- Formato: Formato PKCS#12 (PFX)
- Campo obbligatorio: Campo SAN con il nome RFC822 specificato per la registrazione

Passaggio 2: Installa il certificato aggiornato nell'archivio certificati corretto

Installare il certificato appena generato nel percorso dell'archivio certificati appropriato:

- Percorso archivio certificati: Utente/computer Personale > Archivio certificati
- Formato certificato: PKCS#12 (PFX)

Passaggio 3: Riavvia endpoint per riattivare l'autenticazione

Dopo aver installato il certificato aggiornato, riavviare il sistema dell'endpoint per riavviare il

processo di autenticazione e consentire al meccanismo di registrazione di rilevare il nuovo certificato.

Passaggio 4: Test di autenticazione da una rete non aziendale

Per escludere l'interferenza dell'ispezione SSL o della decrittografia da parte dei firewall periferici, verificare il processo di autenticazione da un ambiente di rete non aziendale. In questo modo è possibile isolare potenziali problemi di controllo dei certificati a livello di rete che potrebbero interferire con il processo di registrazione.

Passaggio 5: Riprova registrazione DLP endpoint

Dopo aver completato la sostituzione del certificato e il riavvio del sistema, ritentare il processo di registrazione DLP endpoint. Monitorare i registri di registrazione per verificare la riuscita dell'autenticazione e il completamento della registrazione.

Causa

L'errore di registrazione è causato dall'utilizzo dell'algoritmo hash SHA1 nei certificati di identità del client. SHA1 è un algoritmo hash di crittografia deprecato non più supportato dai requisiti dei criteri di registrazione. Il sistema di registrazione richiede in modo specifico l'hashing dei certificati con algoritmi moderni e sicuri, ad esempio SHA256 o SHA-3, per soddisfare gli standard di sicurezza correnti e la conformità ai criteri.

Quando il processo di registrazione convalida il certificato client in base al criterio di scelta della registrazione, rifiuta i certificati che utilizzano l'algoritmo hash SHA1 deprecato, generando il messaggio di errore "Nessuno dei certificati client di archiviazione utente corrisponde al criterio di scelta della registrazione" e il successivo errore di inizializzazione.

Contenuto correlato

- [Supporto tecnico Cisco e download](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).