Op DLP-certificaat gebaseerde fout bij automatische inschrijving voor eindpunt met SHA1-hashing-incompatibiliteit

Inhoud

uitgeven

Endpoint DLP-inschrijving mislukt tijdens op certificaten gebaseerde automatische inschrijving met herhaalde initialisatiefouten. Het inschrijvingsproces kan niet worden geverifieerd met behulp van het clientidentiteitscertificaat, wat resulteert in continue pogingen om het opnieuw te proberen.

De volgende foutmeldingen worden waargenomen in de inschrijvingslogboeken:

```
[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 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
```

Aanvullende verificatiefouten op TLS-niveau worden gedocumenteerd met de foutmelding: "TLS-waarschuwing ontvangen: fataal / slecht certificaat."

milieu

- Technologie: oplossingsondersteuning (SSPT - contract vereist)
- Subtechnologie: Veilige toegang - Uniform beleid (internetbeleid, privébeleid, DLP-beleid, RBI, beveiligingsprofielen)
- Softwareversie: ALLE
- Authenticatiemethode: automatische inschrijving op basis van certificaten
- Certificaatarchief: clientcertificaten voor gebruikersopslag
- Certificaat-hashing-algoritme: SHA1 (verouderd)

resolutie

De oplossing omvat het regenereren van het identiteitscertificaat met een ondersteund hashing-algoritme en het garanderen van de juiste installatie en configuratie van het certificaat.

Stap 1: Identiteitscertificaat regenereren met ondersteund hashing-algoritme

Genereer en geef het identiteitscertificaat opnieuw uit met behulp van SHA256 of SHA-3 hashing in plaats van het afgekeurde SHA1-algoritme. Het certificaat moet worden gemaakt met de volgende specificaties:

- Hashing-algoritme: SHA256 of SHA-3 (SHA1 wordt niet ondersteund)
- Indeling: PKCS#12 (PFX)-indeling
- Vereist veld: SAN-veld met RFC822-naam zoals opgegeven voor inschrijving

Stap 2: Installeer bijgewerkt certificaat in de juiste certificaatopslag

Installeer het nieuw gegenereerde certificaat op de juiste locatie voor de certificaatopslag:

- Locatie certificaatarchief: gebruiker/machine > persoonlijke certificaatopslag
- Certificaatformaat: PKCS#12 (PFX)

Stap 3: Eindpunt opnieuw opstarten om verificatie opnieuw te activeren

Nadat u het bijgewerkte certificaat hebt geïnstalleerd, start u het eindpuntsysteem opnieuw op om het verificatieproces opnieuw te starten en het inschrijvingsmechanisme in staat te stellen het nieuwe certificaat te detecteren.

Stap 4: Verificatie testen via een niet-zakelijk netwerk

Om SSL-inspectie of decoderingsinterferentie door edge-firewalls uit te sluiten, test u het verificatieproces vanuit een niet-zakelijke netwerkomgeving. Dit helpt potentiële certificaatinspectieproblemen op netwerkniveau te isoleren die het inschrijvingsproces kunnen verstoren.

Stap 5: DLP-inschrijving voor eindpunt opnieuw proberen

Nadat u het vervangen van het certificaat en het opnieuw opstarten van het systeem hebt voltooid, probeert u het DLP-inschrijvingsproces voor Endpoint opnieuw. Controleer de inschrijvingslogboeken om na te gaan of de verificatie en de inschrijving zijn voltooid.

Oorzaak

De inschrijvingsfout wordt veroorzaakt door het gebruik van SHA1-hashing-algoritme in de cliëntidentiteitscertificaten. SHA1 is een verouderd cryptografisch hashing-algoritme dat niet langer wordt ondersteund door de vereisten van het inschrijvingsbeleid. Het inschrijvingssysteem vereist specifiek dat certificaten worden gehasht met moderne, veilige algoritmen zoals SHA256 of SHA-3 om te voldoen aan de huidige beveiligingsnormen en beleidsnaleving.

Wanneer het inschrijvingsproces het clientcertificaat valideert op basis van het inschrijvingskeuzebeleid, worden certificaten die gebruikmaken van het afgekeurde SHA1-hashingalgoritme afgewezen, wat resulteert in de foutmelding "Geen van de clientcertificaten van 1 gebruikerswinkel komt overeen met het inschrijvingskeuzebeleid" en de daaropvolgende initialisatiefout.

Verwante inhoud

- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.