Échec de l'inscription automatique basée sur les certificats DLP des terminaux avec incompatibilité de hachage SHA1

Table des matières

Problème

L'inscription DLP du point de terminaison échoue lors de l'inscription automatique basée sur les certificats avec des erreurs d'initialisation répétées. Le processus d'inscription ne peut pas s'authentifier à l'aide du certificat d'identité client, ce qui entraîne des tentatives continues.

Les messages d'erreur suivants sont observés dans les journaux d'inscription :

```
[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
```

Des échecs d'authentification supplémentaires au niveau TLS sont documentés avec le message d'erreur : "Alerte TLS reçue : fatal / mauvais certificat."

Environnement

- Technologie : Assistance pour les solutions (SSPT - contrat requis)
- Sous-technologie : Accès sécurisé - Stratégie unifiée (stratégies Internet, stratégies privées, stratégies DLP, RBI, profils de sécurité)
- Version du logiciel: TOUS
- Méthode d'authentification : Inscription automatique basée sur les certificats
- Magasin de certificats : Certificats client du magasin d'utilisateurs
- Algorithme de hachage de certificat : SHA1 (déconseillé)

Résolution

La résolution implique la régénération du certificat d'identité avec un algorithme de hachage pris en charge et la garantie d'une installation et d'une configuration correctes du certificat.

Étape 1: Régénération du certificat d'identité avec algorithme de hachage pris en charge

Générez et réémettez le certificat d'identité à l'aide du hachage SHA256 ou SHA-3 au lieu de l'algorithme SHA1 déconseillé. Le certificat doit être créé avec les spécifications suivantes :

- Algorithme de hachage : SHA256 ou SHA-3 (SHA1 non pris en charge)
- Format : Format PKCS#12 (PFX)
- Champ obligatoire : Champ SAN avec le nom RFC822 spécifié pour l'inscription

Étape 2: Installer le certificat mis à jour dans le magasin de certificats correct

Installez le certificat nouvellement généré à l'emplacement approprié du magasin de certificats :

- Emplacement du magasin de certificats : Utilisateur/Ordinateur personnel > Magasin de certificats
- Format du certificat : PKCS#12 (PFX)

Étape 3: Redémarrer le point de terminaison pour relancer l'authentification

Après avoir installé le certificat mis à jour, redémarrez le système d'extrémité pour relancer le processus d'authentification et permettre au mécanisme d'inscription de détecter le nouveau certificat.

Étape 4: Tester l'authentification à partir du réseau non professionnel

Pour exclure l'inspection SSL ou les interférences de déchiffrement par les pare-feu de périphérie, testez le processus d'authentification à partir d'un environnement réseau autre qu'une entreprise. Cela permet d'isoler les problèmes potentiels d'inspection de certificat au niveau du réseau qui pourraient interférer avec le processus d'inscription.

Étape 5: Réessayer l'inscription DLP des terminaux

Une fois le remplacement du certificat terminé et le redémarrage du système terminé, tentez à nouveau le processus d'inscription DLP du point d'extrémité. Surveillez les journaux d'inscription pour vérifier que l'authentification et l'inscription ont réussi.

Motif

L'échec de l'inscription est causé par l'utilisation de l'algorithme de hachage SHA1 dans les certificats d'identité du client. SHA1 est un algorithme de hachage cryptographique déconseillé qui n'est plus pris en charge par les exigences de la stratégie d'inscription. Le système d'inscription exige spécifiquement que les certificats soient hachés à l'aide d'algorithmes modernes et sécurisés tels que SHA256 ou SHA-3 pour répondre aux normes de sécurité et à la conformité aux politiques actuelles.

Lorsque le processus d'inscription valide le certificat client par rapport à la stratégie de choix d'inscription, il rejette les certificats qui utilisent l'algorithme de hachage SHA1 déconseillé, ce qui entraîne le message d'erreur « Aucun des 1 certificats client de magasin d'utilisateurs ne correspond à la stratégie de choix d'inscription » et l'échec d'initialisation suivant.

Autres informations utiles

- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.