Error de inscripción automática basada en certificado DLP de terminal con incompatibilidad de hash SHA1

Contenido

Problema

La inscripción de DLP de terminal falla durante la inscripción automática basada en certificados con errores de inicialización repetidos. El proceso de inscripción no se puede autenticar mediante el certificado de identidad del cliente, lo que provoca continuos intentos de reintento.

Los siguientes mensajes de error se observan en los registros de inscripción:

```
[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
```

Los errores de autenticación adicionales de nivel TLS se documentan con el mensaje de error: "Alerta TLS recibida: certificado fatal / incorrecto".

Entorno

- Tecnología: Asistencia para soluciones (SSPT, contrato necesario)
- Subtecnología: Acceso seguro: política unificada (políticas de Internet, políticas privadas, políticas DLP, RBI, perfiles de seguridad)
- Versión del software: ALL
- método de autentificación: Inscripción automática basada en certificados
- Almacén de certificados: Certificados de cliente de almacenamiento de usuario
- Algoritmo de hash de certificado: SHA1 (obsoleto)

Resolución

La resolución implica la regeneración del certificado de identidad con un algoritmo de hash admitido y la garantía de la instalación y configuración correctas del certificado.

Paso 1: Regenere el certificado de identidad con un algoritmo de hash admitido

Genere y vuelva a emitir el certificado de identidad mediante hashing SHA256 o SHA-3 en lugar del algoritmo SHA1 desaprobado. El certificado debe crearse con las siguientes especificaciones:

- Algoritmo de hash: SHA256 o SHA-3 (SHA1 no es compatible)
- Formato: Formato PKCS#12 (PFX)
- Campo obligatorio: Campo SAN con el nombre RFC822 especificado para la inscripción

Paso 2: Instalar certificado actualizado en el almacén de certificados correcto

Instale el certificado recién generado en la ubicación de almacén de certificados apropiada:

- Ubicación del almacén de certificados: User/Machine Personal > Almacén de certificados
- Formato del certificado: PKCS#12 (PFX)

Paso 3: Reinicie el terminal para volver a activar la autenticación

Después de instalar el certificado actualizado, reinicie el sistema de punto final para volver a

activar el proceso de autenticación y permitir que el mecanismo de inscripción detecte el nuevo certificado.

Paso 4: Probar autenticación de red no corporativa

Para descartar la inspección SSL o la interferencia de descifrado por parte de los firewalls perimetrales, pruebe el proceso de autenticación desde un entorno de red no corporativo. Esto ayuda a aislar posibles problemas de inspección de certificados en el nivel de red que podrían interferir con el proceso de inscripción.

Paso 5: Reintentar inscripción de DLP de terminal

Después de completar la sustitución del certificado y el reinicio del sistema, intente de nuevo el proceso de inscripción de DLP para terminales. Supervise los registros de inscripción para verificar que la autenticación y la inscripción se han completado correctamente.

Causa

El error de inscripción se debe al uso del algoritmo hash SHA1 en los certificados de identidad del cliente. SHA1 es un algoritmo de hash criptográfico desaprobado que ya no es compatible con los requisitos de la directiva de inscripción. El sistema de inscripción requiere específicamente que los certificados se rompan con algoritmos modernos y seguros, como SHA256 o SHA-3, para cumplir con los estándares de seguridad actuales y el cumplimiento de las políticas.

Cuando el proceso de inscripción valida el certificado de cliente con la directiva de opciones de inscripción, rechaza los certificados que utilizan el algoritmo hash SHA1 desaprobado, lo que da como resultado el mensaje de error "Ninguno de los 1 certificados de cliente de almacén de usuarios coincide con la directiva de opciones de inscripción" y el error de inicialización subsiguiente.

Contenido relacionado

- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).