Falha no Registro Automático Baseado em Certificado DLP do Ponto de Extremidade com Incompatibilidade de Hash SHA1

Contents

Problema

O registro DLP do ponto final falha durante o registro automático baseado em certificado com erros de inicialização repetidos. O processo de registro não pode ser autenticado usando o certificado de identidade do cliente, resultando em tentativas contínuas de repetição.

As seguintes mensagens de erro são observadas nos logs de inscrição:

```
[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
```

Falhas adicionais de autenticação em nível de TLS são documentadas com a mensagem de erro: "Alerta TLS recebido: certificado fatal/inválido."

Ambiente

- Tecnologia: Suporte à solução (SSPT - contrato necessário)
- Subtecnologia: Acesso seguro - Política unificada (políticas da Internet, políticas privadas, políticas DLP, RBI, perfis de segurança)
- Versão de software: TODOS
- método de autenticação: Inscrição automática baseada em certificado
- Repositório de Certificados: Certificados de cliente de repositório de usuários
- Algoritmo de hash de certificado: SHA1 (preterido)

Resolução

A resolução envolve regenerar o certificado de identidade com um algoritmo de hash suportado e garantir a instalação e a configuração adequadas do certificado.

Passo 1: Regenerar Certificado de Identidade com Algoritmo de Hashing Suportado

Gere e emita novamente o certificado de identidade usando hash SHA256 ou SHA-3 em vez do algoritmo SHA1 preterido. O certificado deve ser criado com as seguintes especificações:

- Algoritmo de dispersão: SHA256 ou SHA-3 (SHA1 não é suportado)
- Formato: Formato PKCS#12 (PFX)
- Campo obrigatório: Campo SAN com Nome RFC822 conforme especificado para registro

Passo 2: Instalar Certificado Atualizado no Repositório de Certificados Correto

Instale o certificado recém-gerado no local de armazenamento de certificados apropriado:

- Local do repositório de certificados: Usuário/Computador Pessoal > repositório de certificados
- Formato do certificado: PKCS#12 (PFX)

Passo 3: Reinicializar Ponto de Extremidade para Redisparar a Autenticação

Após instalar o certificado atualizado, reinicialize o sistema de ponto final para disparar novamente o processo de autenticação e permitir que o mecanismo de registro detecte o novo certificado.

Passo 4: Testar autenticação de rede não corporativa

Para descartar a interferência de inspeção ou descriptografia de SSL por firewalls de borda, teste o processo de autenticação a partir de um ambiente de rede não corporativo. Isso ajuda a isolar possíveis problemas de inspeção de certificado em nível de rede que possam interferir no processo de inscrição.

Passo 5: Tentar Registro DLP do Ponto de Extremidade Novamente

Após concluir a substituição de certificado e a reinicialização do sistema, tente o processo de registro de DLP do endpoint novamente. Monitore os logs de registro para verificar a autenticação bem-sucedida e a conclusão do registro.

Causa

A falha de registro é causada pelo uso do algoritmo de hash SHA1 nos certificados de identidade do cliente. SHA1 é um algoritmo de hash criptográfico preterido que não é mais suportado pelos requisitos da política de registro. O sistema de registro exige especificamente que os certificados sejam misturados com algoritmos modernos e seguros, como SHA256 ou SHA-3, para atender aos padrões de segurança atuais e à conformidade com a política.

Quando o processo de registro valida o certificado do cliente em relação à política de escolha de registro, ele rejeita certificados que usam o algoritmo de hash SHA1 preterido, resultando na mensagem de erro "Nenhum dos 1 certificados de cliente do repositório de usuários corresponde à política de escolha de registro" e na falha de inicialização subsequente.

Conteúdo relacionado

- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.