终端DLP基于证书的自动注册失败与SHA1散列不兼容

目录

问题

基于证书的自动注册期间终端DLP注册失败，并出现重复的初始化错误。注册过程无法使用客户端身份证书进行身份验证，从而导致连续重试尝试。

注册日志中观察到以下错误消息：

```
[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
```

其他TLS级别的身份验证失败记录有以下错误消息："已收到TLS警报：致命的/错误的证书。"

环境

- 技术：解决方案支持（SSPT — 需要合同）
- 子技术：安全访问 — 统一策略（互联网策略、私有策略、DLP策略、RBI、安全配置文件）
- 软件版本:全部

- 认证方法:基于证书的自动注册
- 证书存储：用户存储客户端证书
- 证书散列算法：SHA1（已弃用）

分辨率

解决方案涉及使用支持的散列算法重新生成身份证书，并确保正确的证书安装和配置。

步骤 1：使用支持的散列算法重新生成身份证书

使用SHA256或SHA-3散列（而不是弃用的SHA1算法）生成并重新颁发身份证书。必须使用以下规范创建证书：

- 散列算法：SHA256或SHA-3（不支持SHA1）
- Format:PKCS#12(PFX)格式
- 必填字段:SAN字段，其名称为注册指定的RFC822

步骤 2：在正确的证书存储中安装更新的证书

在适当的证书存储位置安装新生成的证书：

- 证书存储位置：User/Machine Personal > Certificates store
- 证书格式：PKCS#12(PFX)

步骤 3：重新启动终端以重新触发身份验证

安装更新后的证书后，重新启动终端系统以重新触发身份验证过程，并允许注册机制检测新证书。

步骤 4：测试来自非公司网络的身份验证

要排除边缘防火墙的SSL检查或解密干扰，请从非公司网络环境测试身份验证过程。这有助于隔离可能干扰注册过程的潜在网络级证书检查问题。

步骤 5：重试终端DLP注册

完成证书替换和系统重新启动后，再次尝试终端DLP注册过程。监控注册日志以验证身份验证成功和注册完成。

原因

注册失败是由于在客户端身份证书中使用SHA1散列算法导致的。SHA1是已被弃用的加密散列算法，不再受注册策略要求支持。注册系统特别要求证书使用现代、安全的算法（如SHA256或SHA-3）进行散列处理，以满足当前安全标准和策略合规性。

当注册进程根据注册选择策略验证客户端证书时，它会拒绝使用已弃用的SHA1散列算法的证书，从而导致“1个用户存储客户端证书都不匹配注册选择策略”错误消息和后续初始化失败。

相关内容

- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。