

ISE 3.3 트러블슈팅 오류 "SNS 37xx 서비스 초기화 실패"

목차

[소개](#)

[전제 조건](#)

[배경 정보](#)

[필수 구성 요소](#)

[증상\(오류 메시지\)](#)

[근본 원인](#)

[필요한 로그](#)

[로그 분석](#)

소개

이 문서에서는 ISE 3.3 이상 버전용 TPM(Trusted Platform Module)의 중요성에 대해 설명합니다.

전제 조건

Cisco ISE(Identity Service Engine)에 대한 기본 지식이 있어야 합니다.

배경 정보

TPM(Trusted Platform Module)은 플랫폼(서버)을 인증하는 데 사용되는 아티팩트를 안전하게 저장할 수 있는 컴퓨터 칩(마이크로컨트롤러)입니다.

이러한 아티팩트에는 비밀번호, 인증서 또는 암호화 키가 포함될 수 있습니다. TPM은 플랫폼의 신뢰성을 유지하는 데 도움이 되는 플랫폼 측정값을 저장하는 데에도 사용할 수 있습니다.

모든 환경에서 보다 안전한 컴퓨팅을 구현하려면 인증(플랫폼이 신뢰할 수 있고 보안 침해를 당하지 않았음을 입증하는 프로세스) 및 증명(플랫폼이 신뢰할 수 있고 보안 침해를 당하지 않았음을 입증하는 데 도움이 됨)이 필요합니다. 새시 침입 스위치는 서버에 대한 무단 기계적 액세스에 대한 알림을 제공합니다.

3.3 이상에서는 ISE 서비스를 초기화하기 위해 TPM 모듈이 필요합니다.

ISE TPM 프레임워크는 두 가지 서비스, 즉 Key Manager, TPM Manager로 구성됩니다.

키 관리자

KeyManager 하위 시스템은 노드의 키인 비밀을 처리하는 기본 구성 요소입니다. 여기에는 키 생성, 키 봉인/암호화, 키 봉인/해독 해제, 키에 대한 액세스 제공 등이 포함됩니다.

키 관리자는 처리 중인 모든 비밀에 대한 참조를 이름별로 유지 관리합니다. 암호/키는 키 관리자에

의해 디스크에 저장되지 않습니다. 프로세스 중에 부트스트랩 비밀은 TPM 관리자를 통해 TPM에서 검색되며 비밀은 프로세스 메모리에 남아 있습니다.

TPM 관리자

TPM 관리자는 TPM 초기화, 비밀 봉인/봉인 해제 또는 암호화/암호 해독, 비밀 저장 보안을 전담합니다. TPM 관리자는 디스크에 비밀/키를 지우지 않습니다. 디스크에 키/암호를 저장해야 하는 경우 키/암호는 TPM의 키로 암호화되어 암호화된 형식으로 저장됩니다. TPM 관리자는 이름, 날짜, 사용자 등의 정보와 관련된 키/암호를 로컬 파일에 보관합니다.

필수 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Identity Service Engine 3.3
- SNS 3715 어플라이언스

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

증상(오류 메시지)

37xx 상자에 ISE 3.3을 성공적으로 설치했으며 초기 네트워크 컨피그레이션 후 서비스가 초기화되지 않습니다.

이 문제는 3.3 FCS를 설치할 때 새로운 SNS 37xx에서 관찰될 수 있으며, 다른 버전에서 3.3 업그레이드를 하는 동안이나 3.3 FCS의 패치를 설치하는 동안 관찰될 수 있습니다

근본 원인

3.3 버전 이상이 TPM 모듈을 검증하므로 SNS에서 TPM 모듈을 활성화해야 합니다. 비활성화된 경우 TPM이 초기화되지 않으므로 서비스를 초기화하지 못합니다.

필요한 로그

CLI에서,

이러한 종류의 문제로 인해 CLI에서 지원 번들을 수집할 수 있는 SSH 액세스 권한이 있습니다.

정확한 로그는 ade/ADE.log입니다.

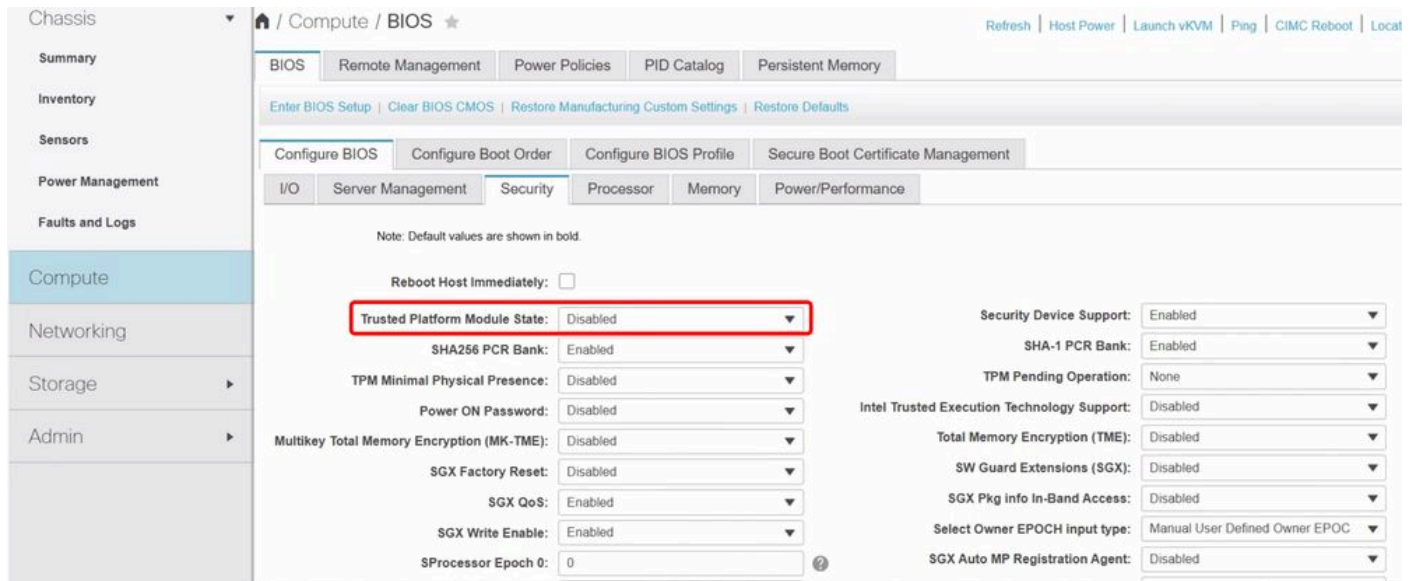
show logging system ade/ADE.log

로그 분석

사례 연구 1

근본 원인: "TPM 모듈이 활성화되지 않았습니다."

CIMC Compute(CIMC 컴퓨팅)>BIOS > Configure BIOS(BIOS 구성) > Security(보안) > Trusted Platform Module State-Disabled(신뢰할 수 있는 플랫폼 모듈 상태 비활성화됨)에서



TPM이 비활성화되었습니다.

대부분의 서비스가 실행되고 있지 않습니다.

admin#show application status ise

ISE 프로세스 이름 상태 프로세스 ID

데이터베이스 리스너에서 379643 실행

175개 프로세스를 실행하는 데이터베이스 서버

응용 프로그램 서버가 실행되고 있지 않습니다.

프로파일러 데이터베이스가 실행되고 있지 않습니다.

ISE 인덱싱 엔진이 실행되고 있지 않음

AD 커넥터가 실행되고 있지 않습니다.

M&T 세션 데이터베이스가 실행되고 있지 않음

M&T 로그 프로세서가 실행되고 있지 않음

인증 기관 서비스가 실행되고 있지 않습니다.

EST 서비스가 실행되고 있지 않음

SXP 엔진 서비스 사용 안 함

TC-NAC 서비스 사용 안 함

PassiveID WMI 서비스를 사용할 수 없습니다.

PassiveID Syslog 서비스 사용 안 함

PassiveID API 서비스 사용 안 함

PassiveID 에이전트 서비스 사용 안 함

PassiveID 엔드포인트 서비스 사용 안 함

PassiveID SPAN 서비스 사용 안 함

DHCP 서버(dhcpd) 사용 안 함

DNS 서버(명명된) 사용 안 함

ISE 메시징 서비스가 실행되고 있지 않음

ISE API 게이트웨이 데이터베이스 서비스가 실행되고 있지 않습니다.

ISE API 게이트웨이 서비스가 실행되고 있지 않음

ISE pxGrid Direct 서비스가 실행되고 있지 않음

세그먼테이션 정책 서비스 사용 안 함

REST 인증 서비스 사용 안 함

SSE 커넥터 사용 안 함

Hermes(pxGrid Cloud Agent) 비활성화

McTrust(Meraki 동기화 서비스) 사용 안 함

ISE 노드 익스포터가 실행되지 않음

ISE Prometheus 서비스가 실행되고 있지 않음

ISE Grafana 서비스가 실행되고 있지 않음

ISE MNT LogAnalytics Elasticsearch가 실행되지 않음

ISE Logstash 서비스가 실행되고 있지 않음

ISE Kibana Service가 실행되지 않음

ISE 네이티브 IPSec 서비스가 실행되고 있지 않음

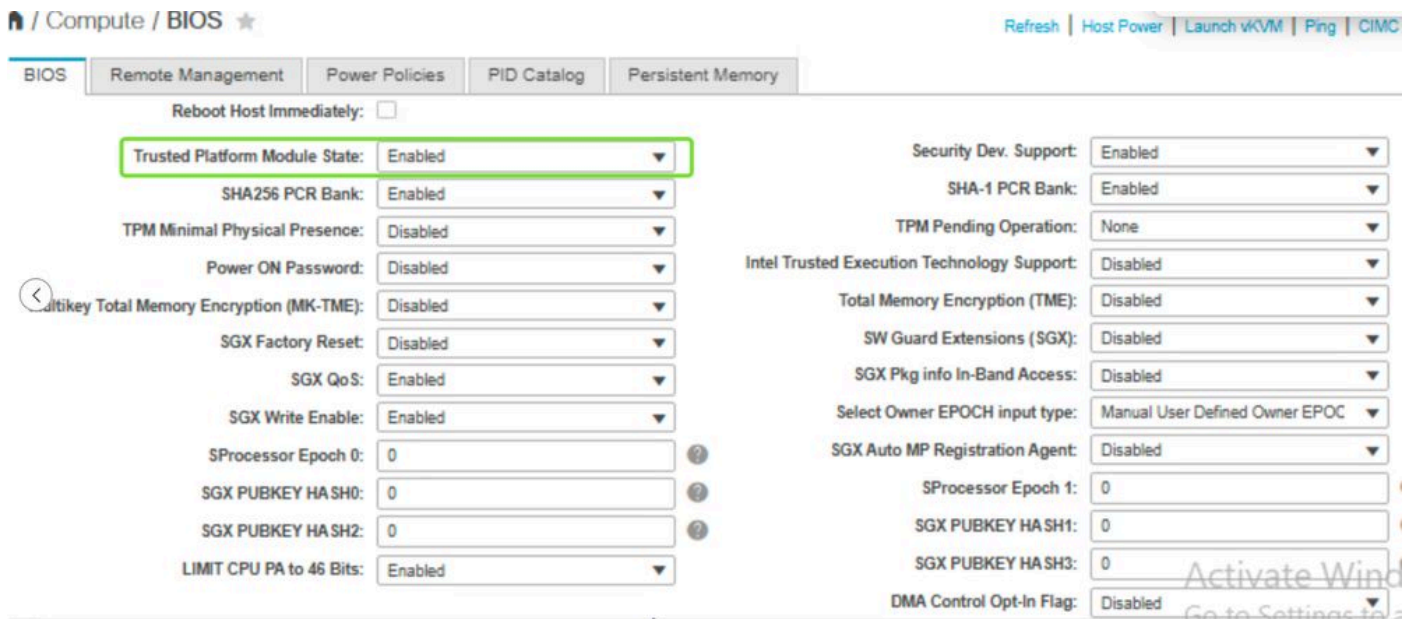
MFC 프로파일러가 실행되고 있지 않음

TPM2ManagerServer가 초기화되지 않았으며 응답 코드 400이 표시되면 TPM 서비스를 활성화하고 노드를 다시 이미징합니다.

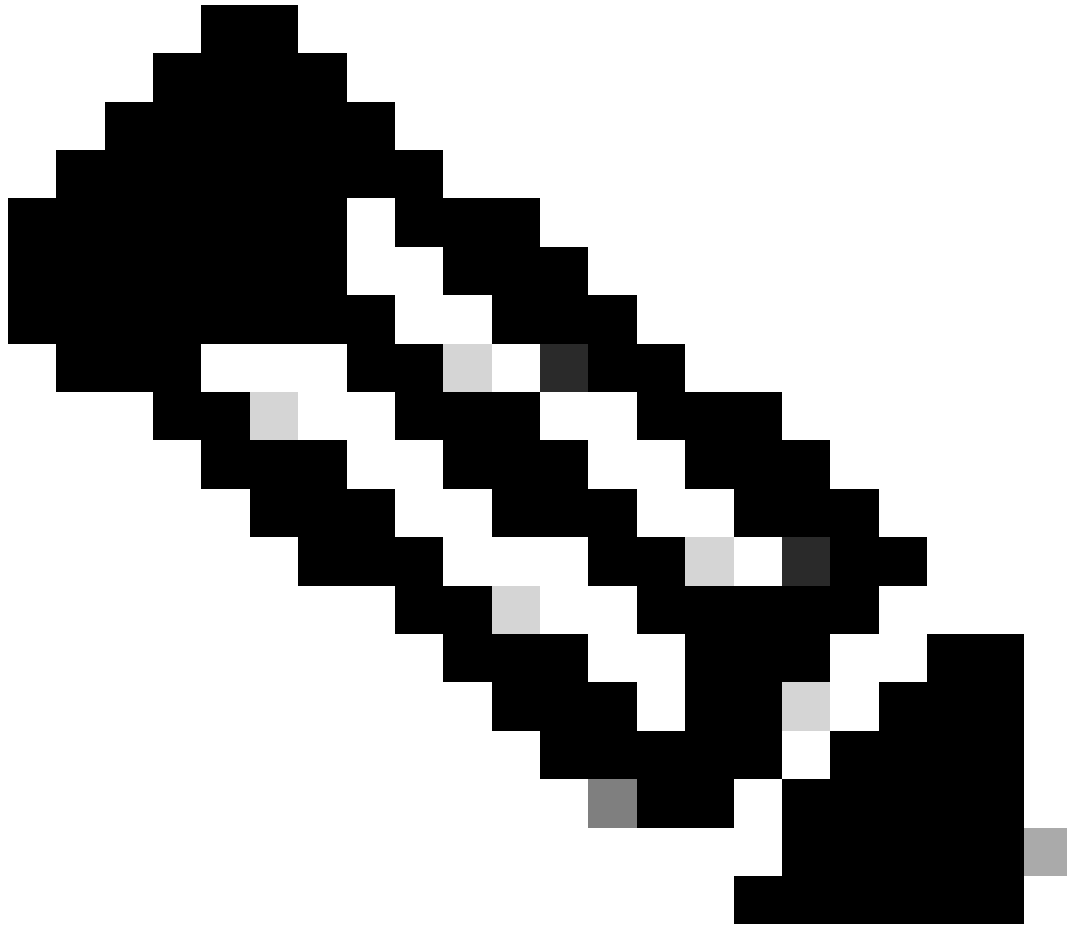
ADE.log:

2025-01-06T08:37:01.164816+00:00 Ihrhblise 저널[1411]: | 2025-01-06 08:37:01,164 | 정보 | 1411 | MainThread | tpm2_manager_server.py:133 | api: 상태 호출 |
2025-01-06T08:37:01.166050+00:00 Ihrhblise 저널[1411]: | 2025-01-06 08:37:01,166 | 오류 | 1411 | MainThread | utils.py:26 | TPM2ManagerServer가 초기화되지 않았습니다. |
2025-01-06T08:37:01.166179+00:00 Ihrhblise 저널[1411]: | 2025-01-06 08:37:01,166 | 정보 | 1411 | MainThread | web_log.py:206 | [06/Jan/2025:08:37:01 +000] "POST /api/system/v1/tpm2-manager/unseal HTTP/1.1" 400 215 "-" "python-requests/2.20.0" |
2025-01-06T08:37:21.670490+00:00 소매 | 2025-01-06 08:37:21,670 | 정보 | 372321 | MainThread | key_manager_server.py:87 | KeyManagerServer 서비스를 초기화하는 동안 잠시 기다려 주십시오. 이 작업은 시간이 걸릴 수 있습니다 |
2025-01-06T08:37:21.672808+00:00 소매 | 2025-01-06 08:37:21,672 | 오류 | 372321 | MainThread | key_manager_server.py:116 | KeyManagerServer 서비스를 초기화할 수 없습니다. TPM2ManagerServer가 초기화되지 않았습니다. |

해결 방법: TPM 모듈을 활성화하고 노드 이미지 재작성을 수행합니다.



TPM이 활성화되었습니다.



참고: 하드웨어 TPM 설정을 조정하거나 변경을 수행하는 경우 ISE에서 여기치 않은 동작이 표시됩니다. 그런 경우에는 이미지를 다시 작성해야 합니다.

사례 연구 2

근본 원인: TPM 캐시로 인해 TPM 유효성 검사에 실패했습니다.

BIOS에서 TPM 설정을 활성화했지만 ADE.log에서 잠금 문제가 발생합니다.

ADE.log:

2024-09-12T16:01:58.063806+05:30 GRP-ACH-ISE-PAN 저널[1404]: | 2024-09-12 16:01:58,063 |
정보 | 1404 | MainThread | tpm2_manager_server.py:133 | api: 상태 호출 |

2024-09-12T16:01:58.063933+05:30 GRP-ACH-ISE-PAN 저널[1404]: | 2024-09-12 16:01:58,063 |
정보 | 1404 | MainThread | web_log.py:206 | [12/Sep/2024:10:31:58 +000] "GET
/api/system/v1/tpm2-manager/health HTTP/1.1" 200 158 "-" "python-requests/2.20.0" |

2024-09-12T16:01:58.064968+05:30 GRP-ACH-ISE-PAN 저널[1404]: | 2024-09-12 16:01:58,064 | 정보 | 1404 | MainThread | tpm2_manager_server.py:184 | api: init 호출됨 |

2024-09-12T16:01:58.068413+05:30 GRP-ACH-ISE-PAN 저널[1404]: | 2024-09-12 16:01:58,068 | 정보 | 1404 | MainThread | tpm2_proxy.py:79 | 명령 실행: tpm2_지우기 |

2024-09-12T16:01:58.075085+05:30 GRP-ACH-ISE-PAN 저널[1404]: | 2024-09-12 16:01:58,074 | 오류 | 1404 | MainThread | tpm2_proxy.py:85 | 다음으로 인해 tpm2_clear를 실행할 수 없음: tpm:warn(2.0): TPM이 DA 잠금 모드에 있으므로 DA 보호 대상 개체에 대한 권한 부여가 현재 허용되지 않습니다 |

2024-09-12T16:01:58.075194+05:30 GRP-ACH-ISE-PAN 저널[1404]: | 2024-09-12 16:01:58,075 | 오류 | 1404 | MainThread | tpm2_manager_server.py:249 | 오류: tpm:warn(2.0): TPM이 DA 잠금 모드에 있으므로 DA 보호 대상 개체에 대한 권한 부여가 현재 허용되지 않습니다 |

설치 과정에서 KVM 콘솔에서 오류를 확인했습니다.

ISE 데이터베이스 콘텐츠를 추출하는 중...

ISE 데이터베이스 프로세스를 시작하는 중...

스레드 "min" com.cisco.cpm.exceptions에 예외가 있습니다. TPMException: 0이 아닌 반환 코드 때문에 TPM 스크립트를 실행하지 못했습니다.)

at com.cisco.cpm.auth.encryptor.crypt.TPPUL11.getResult(TPMUtil.java:53

com.cisco.cpm.auth.encryptor.crypt.TPMUL11.encrypt(TPER11.java:38),
com.cisco.cpm.auth.encryptor.crypt.KEKGenerator.returnkey(KEKGenerator.java:36)

com.cisco.cpm.auth.encryptor.crypt.KEKGenerator.main(KEKGenerator.java:77)에서

java.lang.IllegalArgumentException: 빈 키

javax.crypto.spec에 있습니다. SecretKeySpec.<init>(SecretKeySpec.
Java:96)(com.cisco.cpm.auth.encryptor.crypt.Crypt.<init>(Crypt.java:73))

com.cisco.cpm.auth.encryptor.crypt.DefaultCryptEncryptor 암호화(DefaultCryptEncryptor.java:81)

com.cisco.cpm.auth.encryptor에 있습니다. [PassudHelper.ma](#) 입력(PasssalHelper.java:46)

데이터베이스 초기화 다음에 다음이 나타날 수 있습니다.

오류 로그:

#####

오류: 데이터베이스 초기화 실패!

이는 잘못된 네트워크 인터페이스 컨피그레이션 또는 어플라이언스 또는 VM의 리소스 부족으로 인해 발생할 수 있습니다. 문제를 해결하고 이 CLI를 실행하여 데이터베이스를 다시 초기화하십시오.

'애플리케이션 재설정-구성 ise'

#####

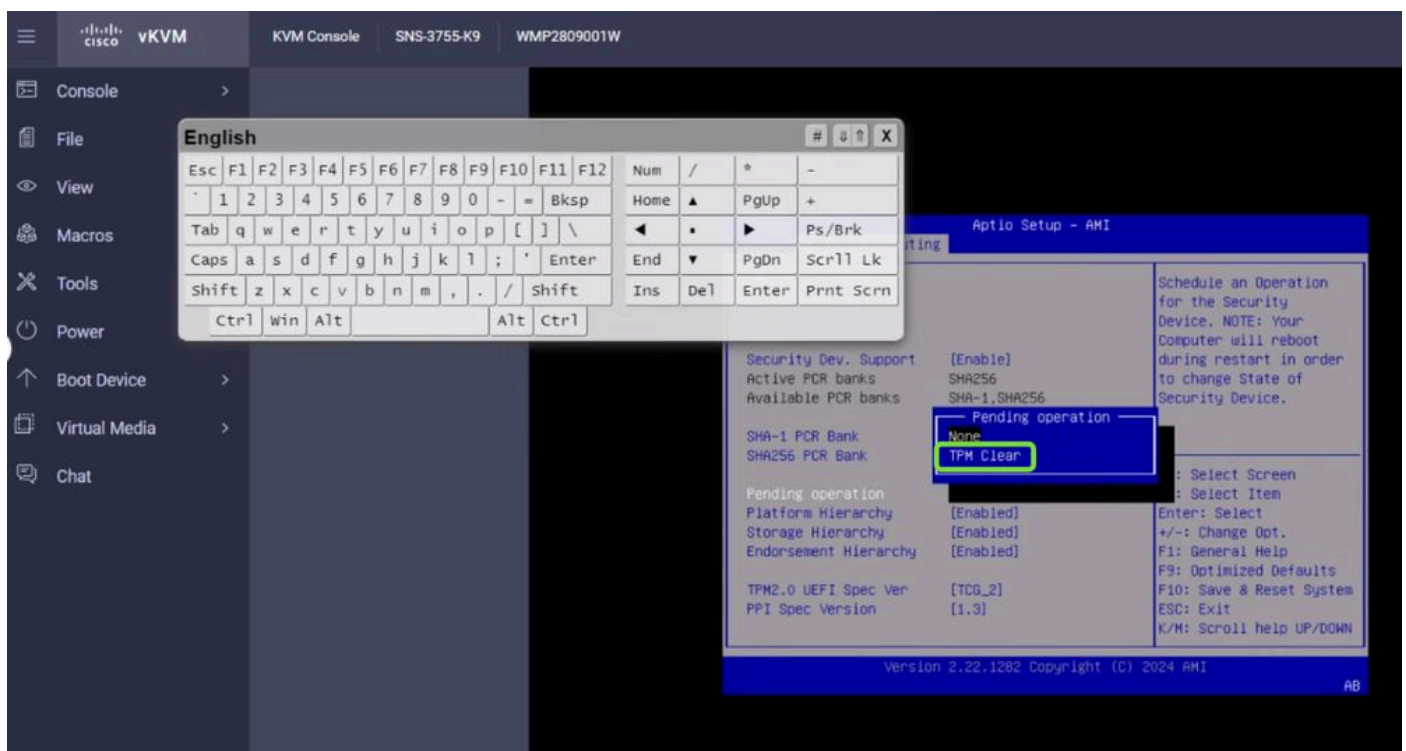
해결 방법: TPM 모듈이 잠겨 있는 경우 TPM 캐시를 재설정하면 도움이 됩니다.

수행할 단계:

vKVM을 실행하면 서버를 재부팅해야 합니다.

Cisco 로고가 나타나면

- F2 키를 누릅니다(BIOS 메뉴).
- TPM 지우기
- 전원 주기



이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.