

Probleemoplossing ISE 3.3 fout "SNS 37xx-services kunnen niet worden geïnitieerd"

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Achtergrondinformatie](#)

[Vereiste componenten](#)

[Symptomen \(foutmeldingen\)](#)

[Hoofdoorzaak](#)

[Behoeftte aan logs](#)

[Analyse van logboeken](#)

Inleiding

Dit document beschrijft het belang van Trusted Platform Module (TPM) voor ISE 3.3 en latere versies.

Voorwaarden

U moet de basiskennis van Cisco Identity Service Engine (ISE) hebben.

Achtergrondinformatie

Een Trusted Platform Module (TPM) is een computerchip (microcontroller) die veilig artefacten kan opslaan die gebruikt worden om het platform te authenticeren (server).

Deze artefacten kunnen wachtwoorden, certificaten of coderingssleutels bevatten. Een TPM kan ook worden gebruikt om platformmetingen op te slaan die helpen ervoor te zorgen dat het platform betrouwbaar blijft.

Verificatie (ervoor zorgen dat het platform kan bewijzen dat het is wat het beweert te zijn) en attestatie (een proces dat helpt om te bewijzen dat een platform betrouwbaar is en niet is geschonden) zijn noodzakelijke stappen om een veiliger computergebruik in alle omgevingen te waarborgen. Een chassisinbraakdetectiesysteem geeft een melding van ongeoorloofde switch toegang tot de server.

Vanaf 3.3 en hoger is TPM-module vereist om de ISE-diensten te initialiseren.

ISE TPM Framework bestaat uit twee diensten, namelijk Key Manager, TPM Manager.

Toetsenbeheer

KeyManager subsysteem is de belangrijkste component die de geheimen, sleutels in een knoop behandelen. Het gaat om het genereren van sleutels, het verzegelen/versleutelen van sleutels, het ontsluiten/decrypteren van sleutels, het verlenen van toegang tot sleutels enzovoort.

De key manager houdt bij naam een verwijzing bij van alle geheimen die hij behandelt. De geheimen/toetsen worden nooit op de disk opgeslagen door key manager. Tijdens proces bootstrap geheimen worden opgehaald van TPM via TPM Manager en de geheimen blijven in het procesgeheugen.

TPM Manager

De TPM-beheerder is als enige verantwoordelijk voor het initialiseren van TPM, verzegeling/ontzegeling of versleuteling/ontsleuteling van geheimen en het veilig opslaan van geheimen. TPM Manager slaat nooit een geheim/sleutel op in duidelijke vorm op de disk. Indien nodig om sleutel/geheim op de schijf op te slaan, wordt de sleutel/het geheim versleuteld met sleutel uit de TPM en opgeslagen in het versleutelde formulier. TPM Manager houdt sleutels/geheimen met betrekking tot informatie (zoals naam, datum, gebruiker) in een lokaal bestand.

Vereiste componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies

- Cisco Identity Service Engine 3.3
- SNS 3715 apparaat

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Symptomen (foutmeldingen)

De installatie van ISE 3.3 op een 37xx box is succesvol en de diensten worden niet geïnitieerd na eerste netwerkconfiguratie.

Het probleem kan worden waargenomen in nieuwe SNS 37xx wanneer we 3.3 FCS installeren of het kan worden waargenomen tijdens 3.3 upgrade van een andere versie of tijdens patchinstallatie van 3.3 FCS

Hoofdoorzaak

TPM module moet worden ingeschakeld in SNS als versie 3.3 (en later) de TPM module valideert. Als TPM uitgeschakeld is, wordt het niet geïnitieerd, wat resulteert in het niet initialiseren van de services.

Behoeft aan logs

Van CLI,

Met dit soort problemen hebt u SSH-toegang om ondersteuningsbundel van CLI te verzamelen.

Het exacte logbestand dat nodig is, is ade/ADE.log.

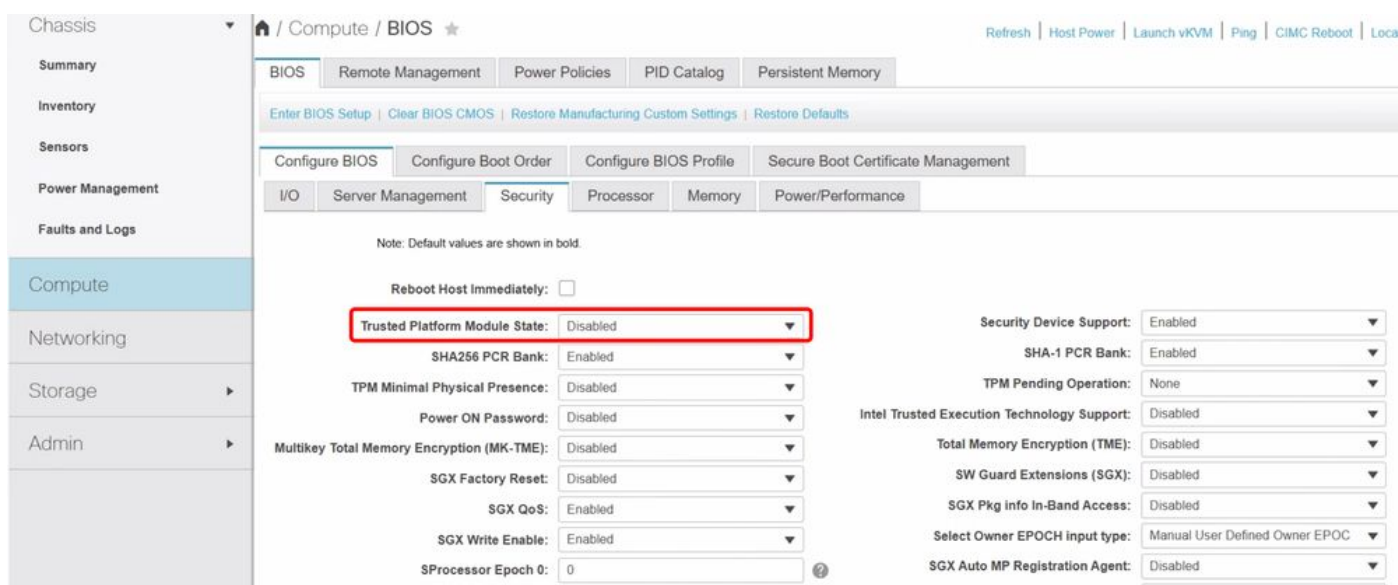
logboekstelsysteem tonen ade/ADE.log

Analyse van logboeken

Casestudy 1

Hoofdoorzaak: "TPM-module is niet ingeschakeld."

In CIMC computing>BIOS> Configure BIOS> Security> Trusted Platform Module - Statusuitgeschakeld



TPM is uitgeschakeld

De meeste services worden niet uitgevoerd.

admin#show-toepassingsstatus

ISE-PROCES NAAM STAAT PROCES-ID

379643 van Databaselozer

Databaseserver met 175 processen

Toepassingsserver niet actief

Profiler-database niet actief

ISE-indexeringsengine is niet actief

AD-connector niet actief

M&T Session Database is niet actief

M&T-logprocessor niet actief

Service van certificeringsinstantie niet actief

EST-service is niet actief

SXP Engine Service uitgeschakeld

TC-NAC-service uitgeschakeld

Passive-id WMI-service uitgeschakeld

Passive-id systeemservice uitgeschakeld

Passive-id API-service uitgeschakeld

Service voor passieve id Agent uitgeschakeld

PassiveID-endpointservice uitgeschakeld

Passive-ID SPAN-service uitgeschakeld

DHCP-server (dhcpd) uitgeschakeld

DNS-server (genaamd) uitgeschakeld

ISE-berichtenservice is niet actief

ISE API Gateway-databaseservice niet actief

ISE API Gateway-service niet actief

ISE PxGrid Direct Service niet actief

Segmenteringsbeleidsservice uitgeschakeld

REST-autorisatieservice uitgeschakeld

SSE-connector uitgeschakeld

Hermes (pxGrid Cloud Agent) uitgeschakeld

McTrust (Meraki Sync Service) uitgeschakeld

ISE-knoopexporteur niet actief

ISE-promethusservice niet actief

ISE Grafana Service niet actief

ISE MNT LogAnalytics Elasticsearch niet actief

ISE-logstaservice wordt niet uitgevoerd

ISE Kibana Service niet actief

ISE-native IPSec-service is niet actief

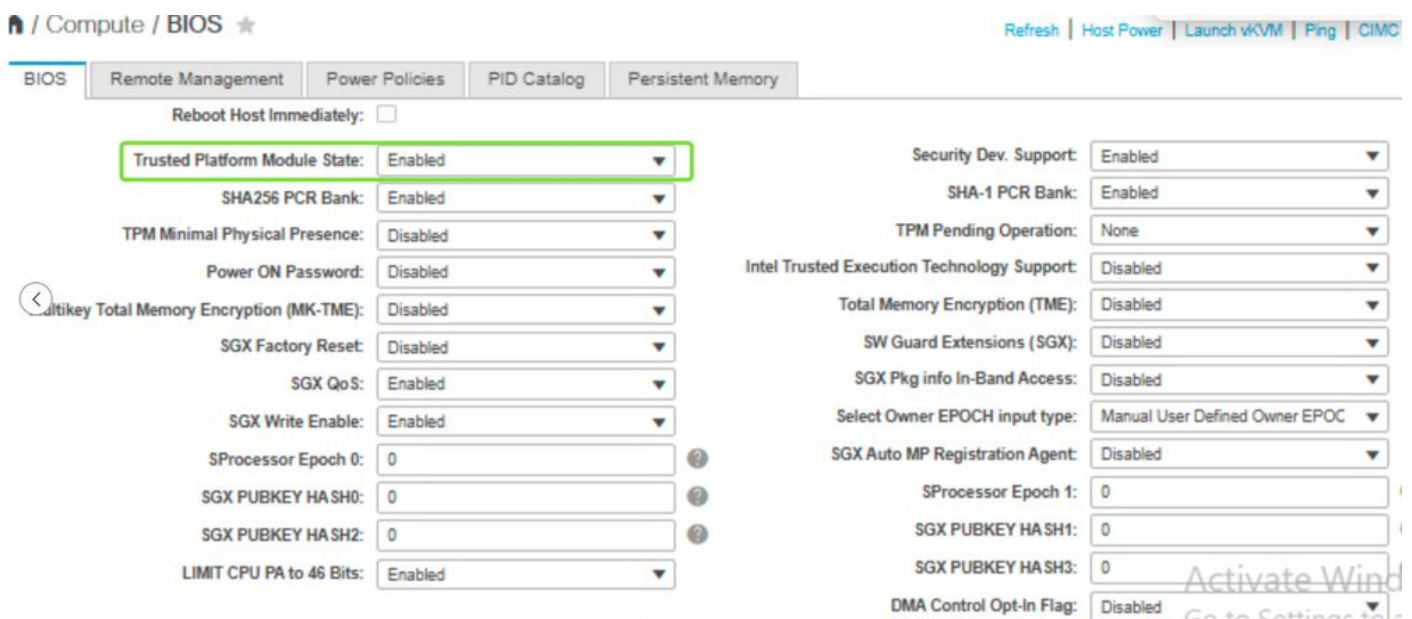
MFC-profiel niet actief

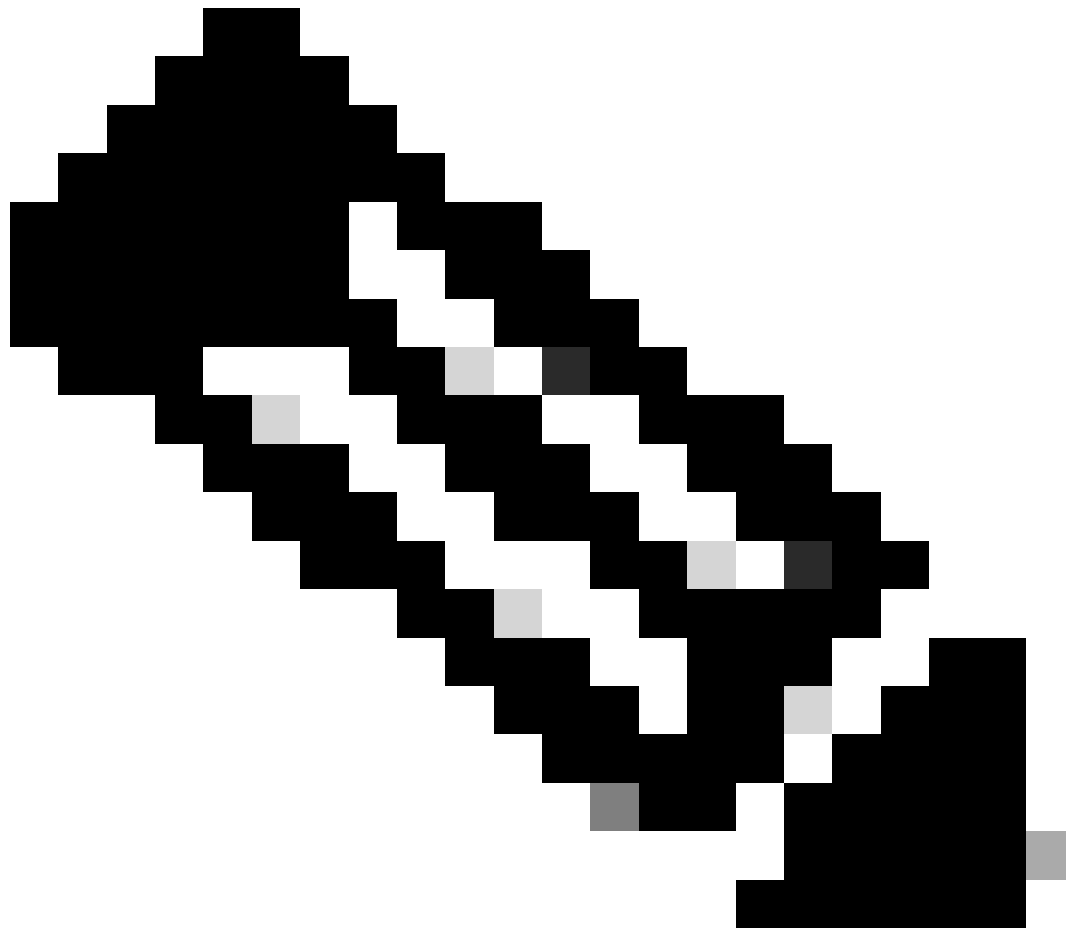
Als u merkt dat TPM2ManagerServer niet is geïnitieerd en responscode 400 gebruikt, schakelt u de TPM-service in en plaatst u het knooppunt opnieuw.

ADE.log:

2025-01-06T08:37:01.164816+00:00 lhblise journal[1411]: | 2025-01-06 08:37:01,164 | INFO | 1411 | MainThread | tpm2_manager_server.py:133 | API: gezondheid |
2025-01-06T08:37:01.166050+00:00 lhblise journal[1411]: | 2025-01-06 08:37:01,166 | FOUT | 1411 | MainThread | utils.py:26 | TPM2ManagerServer is niet geïnitieerd |
2025-01-06T08:37:01.166179+00:00 lhblise journal[1411]: | 2025-01-06 08:37:01,166 | INFO | 1411 | MainThread | web_log.py:2006 | [06/jan/2025:08:37:01 +0000] "POST /api/system/v1/tpm2-manager/unseal HTTP/1.1" 400 215 "-" "python-request/2.20.0" |
2025-01-06T08:37:21.670490+00:00 helder | 2025-01-06 08:37:21.670 | INFO | 372321 | MainThread | key_manager_server.py:87 | Gelieve te wachten terwijl wij de dienst van KeyManagerServer initialiseren, zou dit een tijdje kunnen vergen |
2025-01-06T08:37:21.672808+00:00 helder | 2025-01-06 08:37:21.672 | FOUT | 372321 | MainThread | key_manager_server.py:116 | Kan de KeyManagerServer-service niet initialiseren: TPM2Manager-server is niet geïnitieerd |

Oplossing: TPM-module ingeschakeld en opnieuw image van het knooppunt uitvoeren.





Opmerking: Houd er rekening mee dat als u de hardware-TPM-instellingen aanpast of wijzigingen uitvoert, de ISE onverwacht gedrag vertoont. In dat geval moet u een nieuwe afbeelding maken.

Casestudy 2

Hoofdoorzaak: TPM-validatie is mislukt vanwege TPM-cache.

Hoewel de TPM-instellingen in het BIOS zijn ingeschakeld, zien we uitschakelingsproblemen in ADE.log

ADE.log:

2024-09-12T16:01:58.063806+05:30 GRP-ACH-ISE-PAN-magazine[1404]: | 2024-09-12
16:01:58,063 | INFO | 1404 | MainThread | tpm2_manager_server.py:133 | API: gezondheid |

2024-09-12T16:01:58.063933+05:30 GRP-ACH-ISE-PAN-magazine[1404]: | 2024-09-12 16:01:58,063 | INFO | 1404 | MainThread | web_log.py:2006 | [12/sep/2024:10:31:58 +000] "GET /api/system/v1/tpm2-manager/health HTTP/1.1" 200 158 "-" "python-request/2.20.0" |

2024-09-12T16:01:58.064968+05:30 GRP-ACH-ISE-PAN-magazine[1404]: | 2024-09-12 16:01:58,064 | INFO | 1404 | MainThread | tpm2_manager_server.py:184 | API: bijgenaamd |

2024-09-12T16:01:58.068413+05:30 GRP-ACH-ISE-PAN-magazine[1404]: | 2024-09-12 16:01:58,068 | INFO | 1404 | MainThread | tpm2_proxy.py:79 | Operationele opdracht: tpm2_clear |

2024-09-12T16:01:58.075085+05:30 GRP-ACH-ISE-PAN-magazine[1404]: | 2024-09-12 16:01:58,074 | FOUT | 1404 | MainThread | tpm2_proxy.py:85 | Kan tpm2_clear niet uitvoeren, veroorzaakt door: toeren/ minuut:waarschuwen (2.0): autorisatie voor objecten die onderworpen zijn aan DA-bescherming is op dit moment niet toegestaan omdat de TPM in DA-lockout-modus staat |

2024-09-12T16:01:58.075194+05:30 GRP-ACH-ISE-PAN-magazine[1404]: | 2024-09-12 16:01:58,075 | FOUT | 1404 | MainThread | tpm2_manager_server.py:249 | FOUT: toeren/ minuut:waarschuwen (2.0): autorisatie voor objecten die onderworpen zijn aan DA-bescherming is op dit moment niet toegestaan omdat de TPM in DA-lockout-modus staat |

Tijdens het installatieproces hebben we de fouten op de KVM-console geobserveerd.

ISE-databaseinhoud extraheren...

ISE-databaseprocessen starten...

Uitzondering in thread "min" com.cisco.cpm.exclusion. TPME-uitzondering: TPM-scriptuitvoering is mislukt met niet-nul-retourcode.)

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

op com.cisco.cpm.auth.encryptor.crypt.TPMUL11.encrypt (TPER11.java:38) op com.cisco.cpm.auth.encryptor.crypt.KEKGenerator.return-key (KEKGenerator.java:36)

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

java.lang.IllegalArgumentException: Lege toets

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

op com.cisco.cpm.auth.encryptor.crypt.DefaultCryptEncryptor encrypt(DefaultCryptEncryptar.java:81)

op com.cisco.cpm.auth.encryptor. [PassudHelper.ma](#) in (PasssalHelper.java:46)

Gevolgd door database priming kan verschijnen:

Foutlogbestanden:

#####

FOUT: HET OPSTARTEN VAN DE DATABASE IS MISLUKT.

Dit kan het gevolg zijn van een onjuiste configuratie van de netwerkkinterface of een gebrek aan resources op het apparaat of de VM. Los het probleem op en voer deze CLI uit om de database te reprimeren:

'application reset-config-ise'

#####

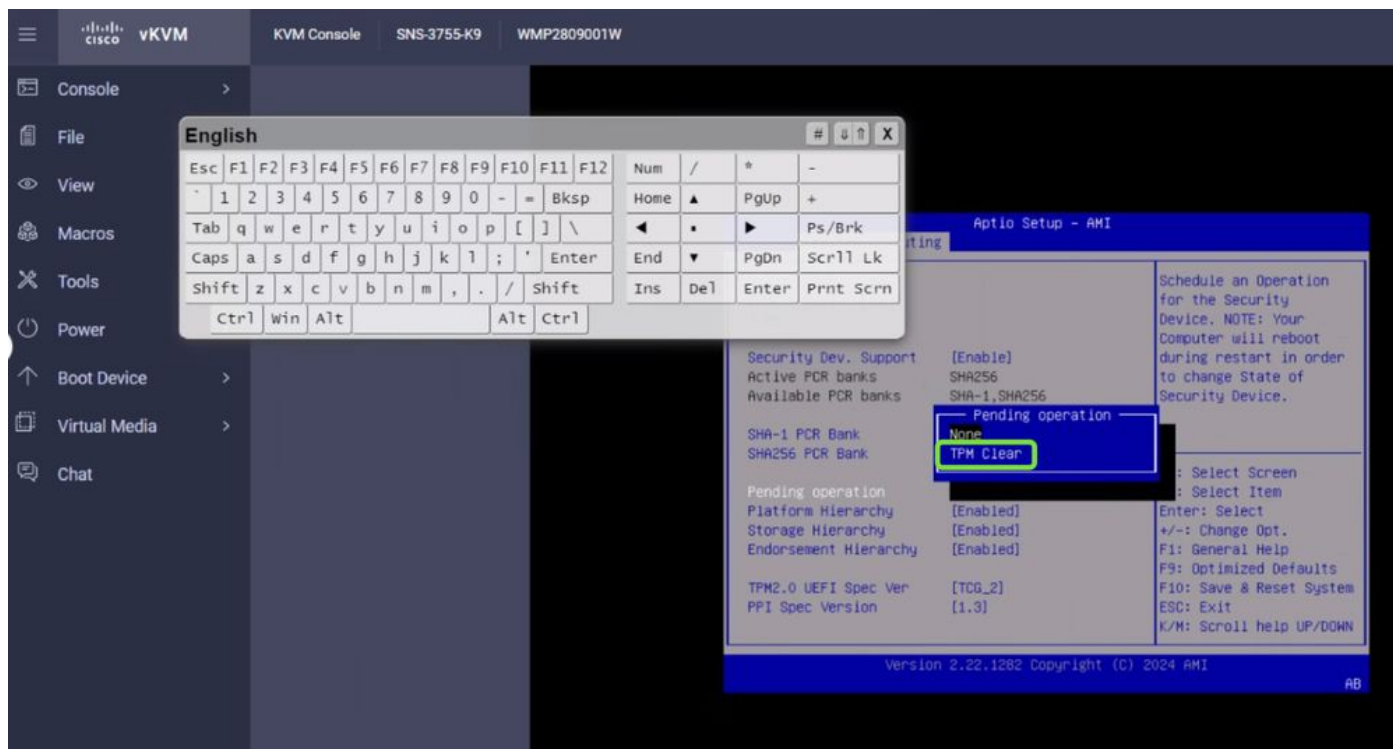
Oplossing: Als u ziet dat de TPM-module is vergrendeld, dan helpt het herstellen van de TPM-cache.

Te doen stappen:

Start vKVM en start de server opnieuw op

Wanneer het Cisco-logo verschijnt

- Druk op F2 (dit is het BIOS-menu)
- TPM Clear
- Stroomprogramma



Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.