Fehlerbehebung bei ISE 3.3 Fehler "SNS 37xx-Services konnte " nicht initialisieren

Inhalt

Einleitung

In diesem Dokument wird die Bedeutung des Trusted Platform Module (TPM) für ISE 3.3 und höher beschrieben.

Voraussetzungen

Sie müssen über die Grundkenntnisse der Cisco Identity Service Engine (ISE) verfügen.

Hintergrundinformationen

Ein Trusted Platform Module (TPM) ist ein Computerchip (Mikrocontroller), der Artefakte zur Authentifizierung der Plattform (Server) sicher speichern kann.

Diese Artefakte können Kennwörter, Zertifikate oder Verschlüsselungsschlüssel enthalten. Ein TPM kann auch verwendet werden, um Plattformmessungen zu speichern, die sicherstellen, dass die Plattform vertrauenswürdig bleibt.

Authentifizierung (d. h. die Gewährleistung, dass die Plattform nachweisen kann, dass sie dem entspricht, was sie vorgibt zu sein) und Zertifizierung (ein Prozess, der dabei hilft, nachzuweisen, dass eine Plattform vertrauenswürdig ist und nicht verletzt wurde) sind notwendige Schritte, um sicherere Datenverarbeitung in allen Umgebungen zu gewährleisten. Ein Switch für unbefugten Gehäusezugriff informiert Sie über jeden unbefugten mechanischen Zugriff auf den Server.

Ab Version 3.3 und höher ist das TPM-Modul zum Initialisieren der ISE-Services erforderlich.

Das ISE TPM-Framework besteht aus zwei Diensten: dem Key-Manager, dem TPM-Manager.

Schlüsselmanager

Das KeyManager-Subsystem ist die Hauptkomponente, die die Schlüssel in einem Knoten behandelt. Dazu gehören das Generieren von Schlüsseln, das Versiegeln/Verschlüsseln von Schlüsseln, das Entsiegeln/Entschlüsseln von Schlüsseln, das Bereitstellen von Zugriff auf Schlüssel usw.
Der Schlüssel-Manager verwaltet einen Verweis auf alle Geheimnisse, die er behandelt. Die Geheimnisse/Schlüssel werden vom Schlüsselmanager nie auf der Festplatte gespeichert. Während des Prozess-Bootstrap werden Geheimnisse von TPM über den TPM-Manager abgerufen, und die Geheimnisse bleiben im Prozessspeicher.

TPM-Manager

Der TPM-Manager ist allein für die Initialisierung des TPM, das Versiegeln/Entsiegeln oder das Verschlüsseln/Entschlüsseln von Geheimnissen sowie die sichere Speicherung von Geheimnissen verantwortlich. Der TPM-Manager speichert niemals einen geheimen Schlüssel auf der Festplatte. Falls erforderlich, um Schlüssel/Schlüssel auf der Festplatte zu speichern, wird der Schlüssel/Schlüssel mit dem Schlüssel des TPM verschlüsselt und in verschlüsselter Form gespeichert. Der TPM-Manager speichert Schlüssel/Schlüssel, die mit Informationen (wie Name, Datum, Benutzer) in einer lokalen Datei in Zusammenhang stehen.

Erforderliche Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen

- Cisco Identity Service Engine 3.3
- SNS 3715-Appliance

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Symptome (Fehlermeldungen)

Die Installation von ISE 3.3 auf einem Gerät der Serie 37xx war erfolgreich, und die Dienste werden nach der ersten Netzwerkkonfiguration nicht initialisiert.

Das Problem kann in der neuen SNS 37xx bei der Installation von 3.3 FCS festgestellt werden, oder es kann während der 3.3-Aktualisierung von einer anderen Version oder während der Patch-Installation von 3.3 FCS festgestellt werden

Ursache

Das TPM-Modul muss in SNS aktiviert werden, da das TPM-Modul in Version 3.3 (und höher) validiert wird. Wenn es deaktiviert ist, wird TPM nicht initialisiert, was dazu führt, dass die Dienste nicht initialisiert werden können.

Erforderliche Protokolle

Über die CLI:

Bei diesen Problemen haben Sie SSH-Zugriff, um das Support-Paket von der CLI zu erhalten.

Das genaue Protokoll ist ade/ADE.log.

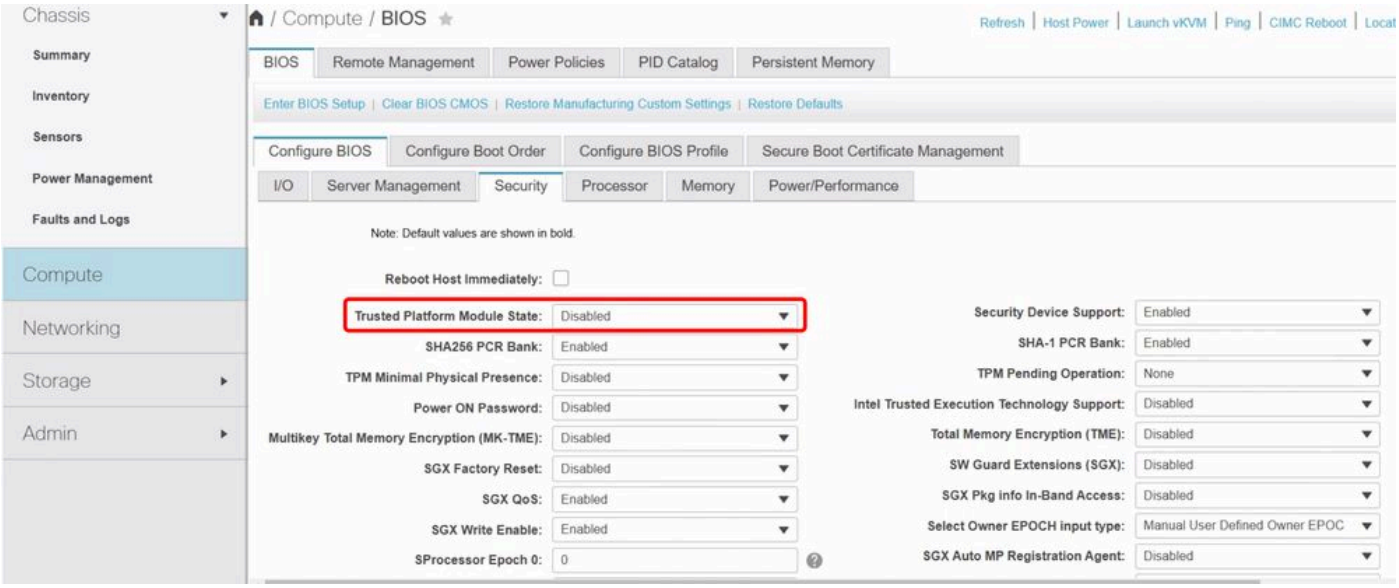
show logging system ade/ADE.log

Protokollanalyse

Anwenderbericht 1

Ursache: "Das TPM-Modul ist nicht aktiviert."

In CIMC Compute>BIOS> BIOS konfigurieren> Sicherheit> Vertrauenswürdiger Plattformmodul-Status deaktiviert



TPM ist deaktiviert.

Die meisten Dienste laufen nicht.

admin#show application status ise

ISE PROZESSNAME STATUS PROZESS-ID

Datenbank-Listener mit 379643

Datenbankserver mit 175 PROZESSEN

Anwendungsserver wird nicht ausgeführt

Profilerdatenbank wird nicht ausgeführt

ISE-Indexmodul wird nicht ausgeführt

AD-Connector wird nicht ausgeführt

M&T-Sitzungsdatenbank wird nicht ausgeführt

M&T-Protokollprozessor wird nicht ausgeführt

Der Zertifizierungsstellendienst wird nicht ausgeführt.

EST-Dienst wird nicht ausgeführt

SXP-Moduldienst deaktiviert

TC-NAC-Dienst deaktiviert

PassiveID WMI-Dienst deaktiviert

PassiveID-Syslog-Dienst deaktiviert

PassiveID API-Dienst deaktiviert

PassiveID-Agent-Dienst deaktiviert

PassiveID-Endpunktdienst deaktiviert

PassiveID SPAN-Dienst deaktiviert

DHCP-Server (DHCP) deaktiviert

DNS-Server (mit Namen) deaktiviert

ISE Messaging Service wird nicht ausgeführt

ISE API-Gateway-Datenbankdienst wird nicht ausgeführt

ISE-API-Gateway-Dienst wird nicht ausgeführt

ISE pxGrid Direct Service wird nicht ausgeführt

Segmentierungsrichtliniendienst deaktiviert

REST-Auth-Dienst deaktiviert

SSE-Connector deaktiviert

Hermes (pxGrid Cloud-Agent) deaktiviert

McTrust (Meraki-Synchronisierungsdienst) deaktiviert

ISE Node Exporter wird nicht ausgeführt

ISE-Prometheus-Dienst wird nicht ausgeführt

ISE Grafana-Dienst wird nicht ausgeführt

ISE MNT LogAnalytics Elastische Suche wird nicht ausgeführt

ISE-Protokolldienst wird nicht ausgeführt

ISE Kibana-Dienst wird nicht ausgeführt

ISE Nativer IPSec-Dienst wird nicht ausgeführt

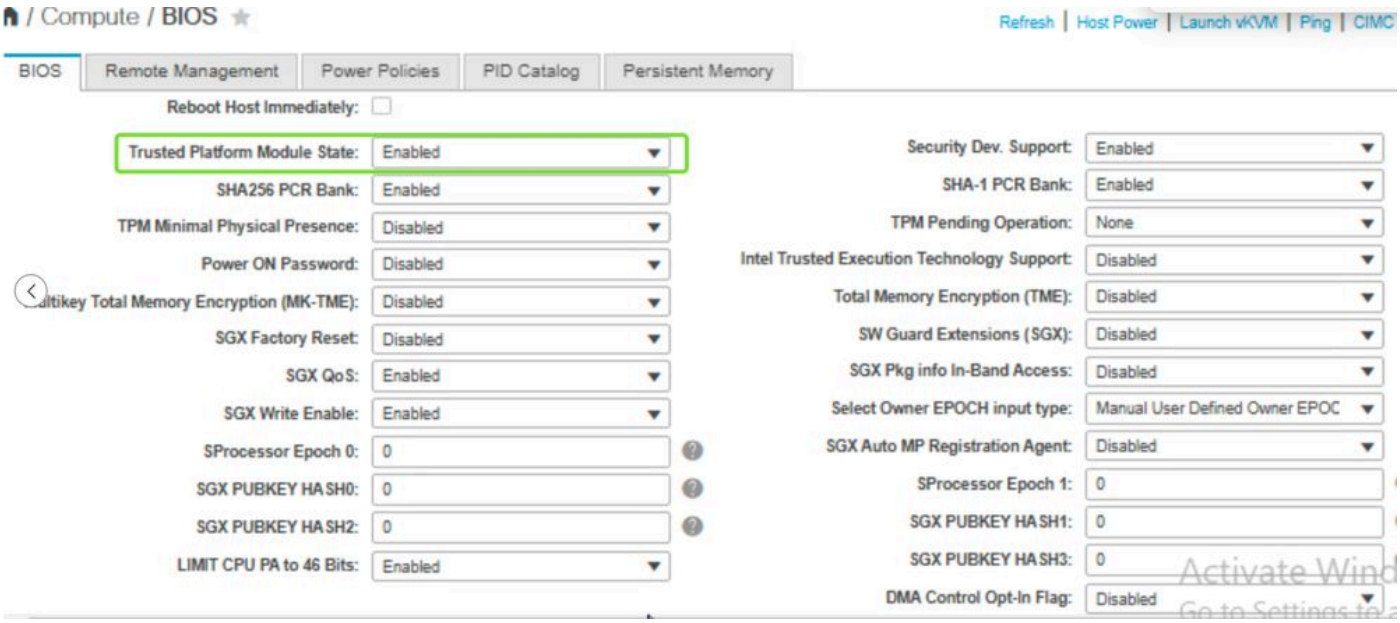
MFC Profiler wird nicht ausgeführt

Wenn Sie feststellen, dass der TPM2ManagerServer nicht initialisiert ist und Antwortcode 400 lautet, aktivieren Sie den TPM-Dienst, und erstellen Sie ein neues Image des Knotens.

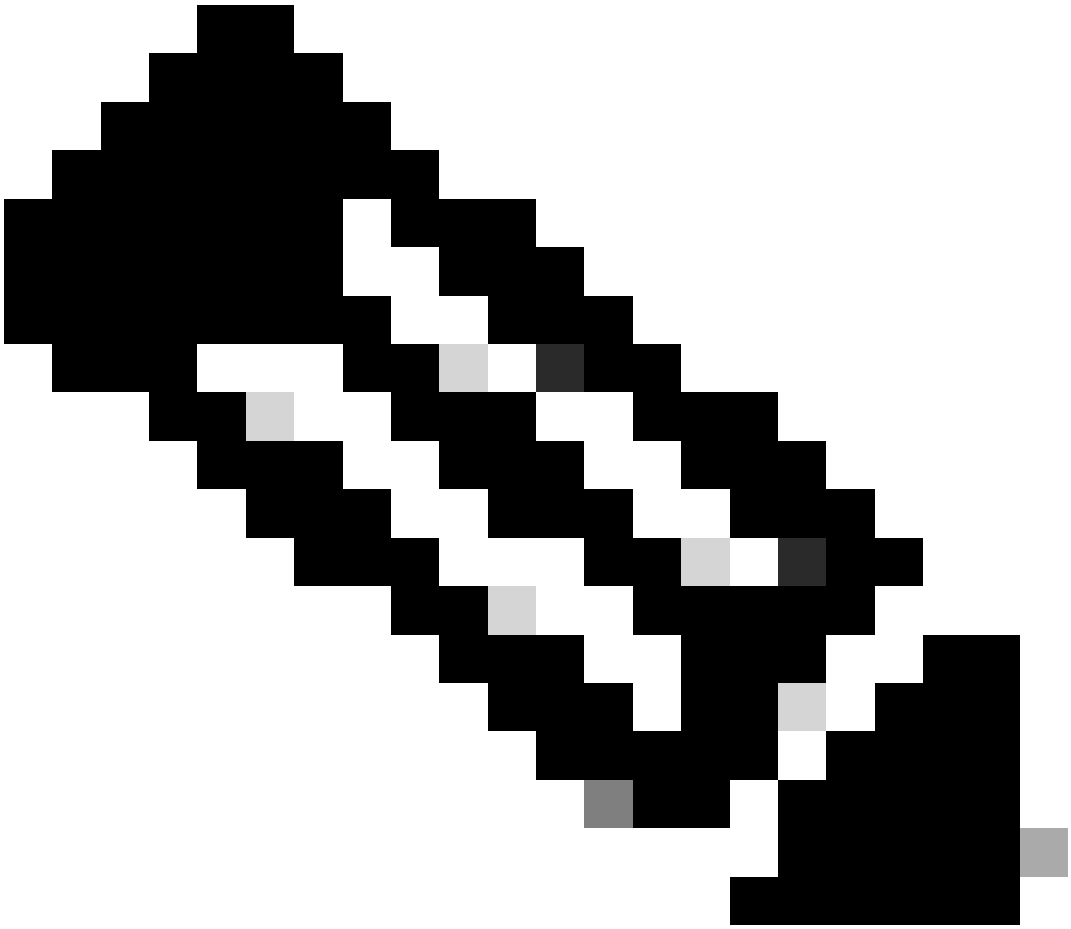
ADE.log:

2025-01-06T08:37:01.164816+00:00 Lhrhblise Journal[1411]: | 2025-01-06 08:37:01,164 | INFO | 1411 | Hauptthread | tpm2_manager_server.py:133 | API: Gesundheitsberuf |
2025-01-06T08:37:01.166050+00:00 Lhrhblise Journal[1411]: | 2025-01-06 08:37:01,166 | FEHLER | 1411 | Hauptthread | utils.py:26 | TPM2ManagerServer ist nicht initialisiert |
2025-01-06T08:37:01.166179+00:00 Lhrhblise Journal[1411]: | 2025-01-06 08:37:01,166 | INFO | 1411 | Hauptthread | web_log.py:206 | [06/Jan/2025:08:37:01 +0000] "POST /api/system/v1/tpm2-manager/unseal HTTP/1.1" 400 215 "-" "python-requirements/2.20.0" |
2025-01-06T08:37:21.670490+00:00 hrhblise | 2025-01-06 08:37:21,670 | INFO | 372321 | Hauptthread | key_manager_server.py:87 | Bitte warten Sie, während der KeyManagerServer-Dienst initialisiert wird. Dies kann einige Zeit in Anspruch nehmen. |
2025-01-06T08:37:21.672808+00:00 hrhblise | 2025-01-06 08:37:21,672 | FEHLER | 372321 | Hauptthread | key_manager_server.py:116 | KeyManagerServer-Dienst konnte nicht initialisiert werden: TPM2ManagerServer ist nicht initialisiert |

Lösung: TPM-Modul aktiviert und neues Image des Knotens durchgeführt.



TPM ist aktiviert



Anmerkung: Beachten Sie, dass die ISE unerwartetes Verhalten zeigt, wenn Sie die TPM-Einstellungen der Hardware anpassen oder Änderungen vornehmen. In diesem Fall müssen Sie ein neues Image erstellen.

Anwenderbericht 2

Ursache: TPM-Validierung aufgrund von TPM-Cache fehlgeschlagen.

Obwohl die TPM-Einstellungen im BIOS aktiviert sind, gibt es Sperrprobleme in ADE.log

ADE.log:

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

2024-09-12T16:01:58.063933+05:30 GRP-ACH-ISE-PAN journal[1404]: | 2024-09-12 16:01:58,063 | INFO | 1404 | Hauptthread | web_log.py:206 | [12/Sep/2024:10:31:58 +0000] "GET /api/system/v1/tpm2-manager/health HTTP/1.1" 200 158 "-" "python-requirements/2.20.0" |

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

2024-09-12T16:01:58.068413+05:30 GRP-ACH-ISE-PAN journal[1404]: | 2024-09-12 16:01:58,068 | INFO | 1404 | Hauptthread | tpm2_proxy.py:79 | Befehl wird ausgeführt: tpm2_clear |

2024-09-12T16:01:58.075085+05:30 GRP-ACH-ISE-PAN journal[1404]: | 2024-09-12 16:01:58,074 | FEHLER | 1404 | Hauptthread | tpm2_proxy.py:85 | tpm2_clear konnte nicht ausgeführt werden, verursacht durch: tpm:warn(2.0): Berechtigungen für Objekte, die dem DA-Schutz unterliegen, sind derzeit nicht zulässig, da sich das TPM im DA-Sperrmodus befindet. |

2024-09-12T16:01:58.075194+05:30 GRP-ACH-ISE-PAN journal[1404]: | 2024-09-12 16:01:58,075 | FEHLER | 1404 | Hauptthread | tpm2_manager_server.py:249 | FEHLER: tpm:warn(2.0): Berechtigungen für Objekte, die dem DA-Schutz unterliegen, sind derzeit nicht zulässig, da sich das TPM im DA-Sperrmodus befindet. |

Während der Installation wurden die Fehler auf der KVM-Konsole festgestellt.

Inhalt der ISE-Datenbank wird extrahiert...

ISE-Datenbankprozesse werden gestartet...

Ausnahme in Thread "min" com.cisco.cpm.exception. TPME-Ausnahme: Fehler bei der TPM-Skriptausführung mit Rückgabecode ungleich null.)

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

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

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

java.lang.IllegalArgumentException: Leerer Schlüssel

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

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

unter com.cisco.cpm.auth.encryptor. PassudHelper.ma In (PasssalHelper.java:46)

Danach kann die Datenbankprimierung angezeigt werden:

Fehlerprotokolle:

##########################

FEHLER: DATENBANKPRIMING FEHLGESCHLAGEN!

Dies kann die Folge einer falschen Konfiguration der Netzwerkschnittstelle oder eines Mangels an Ressourcen auf der Appliance oder VM sein. Beheben Sie das Problem, und führen Sie diese CLI aus, um die Datenbank erneut zu primieren:

'application reset-config ise'

##########################

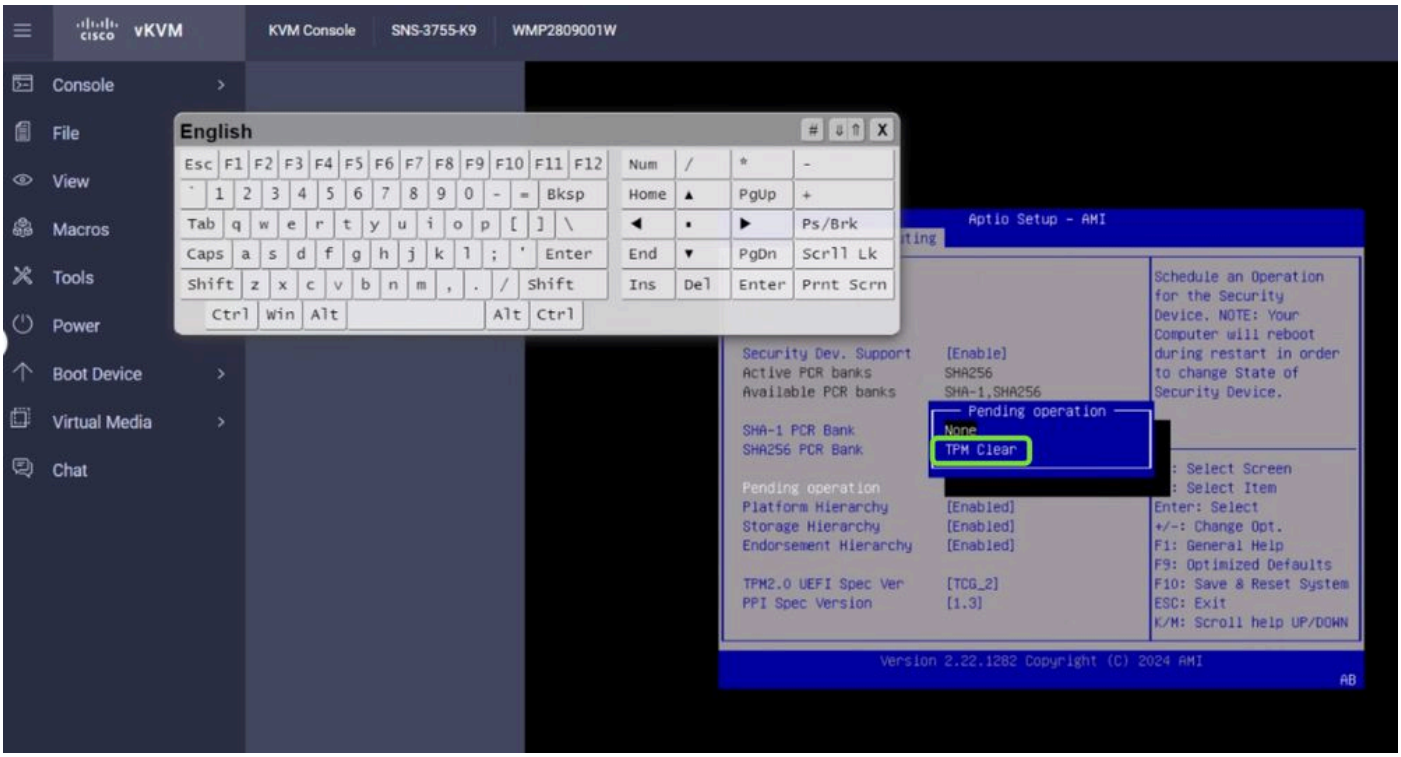
Lösung: Wenn Sie beobachten, dass das TPM-Modul gesperrt ist, hilft das Zurücksetzen des TPM-Caches.

Mögliche Schritte:

Starten Sie vKVM, und der Server muss neu gestartet werden

Wenn das Cisco Logo angezeigt wird

- F2 drücken (dies ist das BIOS-Menü)
- TPM - Löschen
- Power-Zyklus


vKVM
KVM Console
SNS-3755-K9
WMP2809001W
Console
File
View
Macros
Tools
Power
Boot Device
Virtual Media
Chat
English
Aptio Setup - AMI
Security Dev. Support [Enable]
Active PCR banks SHA256
Available PCR banks SHA-1,SHA256
SHA-1 PCR Bank
SHA256 PCR Bank
Pending operation
None
TPM Clear
Pending operation
Platform Hierarchy [Enabled]
Storage Hierarchy [Enabled]
Endorsement Hierarchy [Enabled]
TPM2.0 UEFI Spec Ver [TCG_2]
PPI Spec Version [1.3]
Schedule an Operation for the Security Device. NOTE: Your Computer will reboot during restart in order to change State of Security Device.
Enter: Select
+/-: Change Opt.
F1: General Help
F9: Optimized Defaults
F10: Save & Reset System
ESC: Exit
K/M: Scroll help UP/DOWN
Version 2.22.1282 Copyright (C) 2024 AMI

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.