排除ISE 3.3錯誤"SNS 37xx服務無法初始化"

目錄

簡介

本文檔描述了ISE 3.3及更高版本的可信平台模組(TPM)的重要性。

前提條件

您必須具備思科身份服務引擎(ISE)的基本知識。

背景資訊

可信平台模組(TPM)是一種電腦晶片（微控制器），可以安全儲存用於驗證平台（伺服器）的工件。

這些對象可以包括密碼、證書或加密金鑰。TPM還可用於儲存有助於確保平台保持可信度的平台度量。

身份驗證（確保平台可以證明其聲稱的身份）和證明（有助於證明平台值得信賴且未被攻破的流程）是確保所有環境中更安全計算的必要步驟。機箱防盜開關會通知任何未經授權的機械裝置訪問伺服器。

從3.3及更高版本開始，TPM模組需要初始化ISE服務。

ISE TPM框架包含兩個服務，即金鑰管理器、TPM管理器。

金鑰管理器
KeyManager子系統是處理金鑰的主要元件，是一個節點中的金鑰。這包括生成金鑰、密封/加密金鑰、解密/解密金鑰、提供對金鑰的訪問等等。
金鑰管理器會保留其正在處理的所有機密的名稱引用。金鑰/金鑰從不由key manager儲存在磁碟上。在進程載入程式期間，通過TPM管理器從TPM中檢索秘密並將秘密保留在進程記憶體中。

TPM管理器

TPM管理器完全負責初始化TPM、密封/解封或加密/解密機密以及安全儲存機密。TPM管理器決不會將任何金鑰/金鑰以明文形式儲存在磁碟上。在需要將金鑰/金鑰儲存在盤上的情況下，金鑰/金鑰用TPM中的金鑰加密，並以加密形式儲存。TPM管理器將與資訊（如名稱、日期、使用者）相關的金鑰/機密儲存在本地檔案中。

所需元件

本文件中的資訊是以下列軟體和硬體版本為依據

- 思科身分識別服務引擎3.3
- SNS 3715裝置

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

症狀（錯誤消息）

在37xx機箱上成功安裝ISE 3.3，初始網路配置後服務未初始化。

在我們安裝3.3 FCS時，在新的SNS 37xx中可以發現此問題；在3.3從任何其他版本升級時或在安裝3.3 FCS的補丁過程中可以發現此問題

根本原因

在SNS中必須啟用TPM模組，因為3.3版本（及更高版本）會驗證TPM模組。如果禁用TPM，則不會初始化TPM，這將導致無法初始化服務。

需要的日誌

在CLI上，

遇到此類問題時，您擁有SSH訪問許可權以便從CLI收集支援捆綁包。

所需的準確日誌為ade/ADE.log。

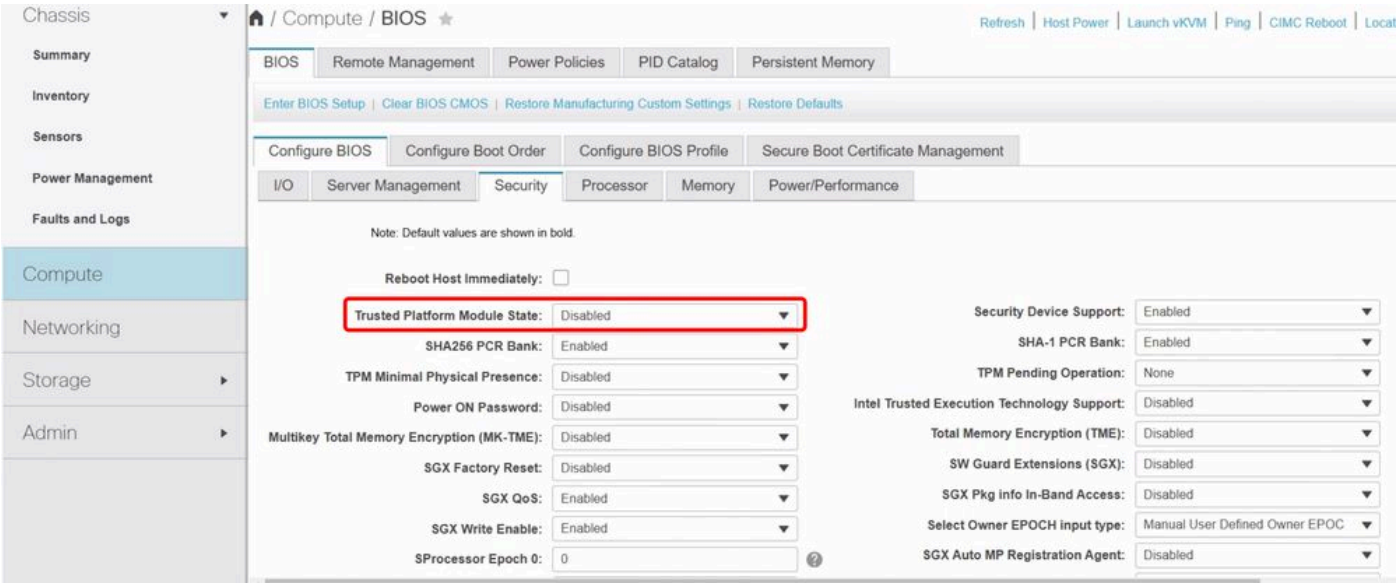
show logging system ade/ADE.log

日誌分析

案例研究1

根本原因："TPM模組未啟用。"

在CIMC計算>BIOS>配置BIOS>安全>受信任的平台模組狀態 — 已禁用



TPM已禁用

大多數服務沒有運行。

admin#show application status ise

ISE進程名稱狀態進程ID

資料庫監聽程式運行379643

運行175個進程的資料庫伺服器

應用程式伺服器未運行

Profiler資料庫未運行

ISE索引引擎未運行

AD聯結器未運行

M&T會話資料庫未運行

M&T日誌處理器未運行

證書頒發機構服務未運行

EST服務未運行

SXP引擎服務已禁用

TC-NAC服務已禁用

已禁用PassiveID WMI服務

PassiveID系統日誌服務已禁用

已禁用PassiveID API服務

已禁用PassiveID代理服務

已禁用PassiveID終結點服務

已禁用PassiveID SPAN服務

已禁用DHCP伺服器(dhcpd)

已禁用DNS伺服器（已命名）

ISE消息服務未運行

ISE API網關資料庫服務未運行

ISE API網關服務未運行

ISE pxGrid直接服務未運行

已禁用分段策略服務

REST身份驗證服務已禁用

已禁用SSE聯結器

Hermes（pxGrid雲代理）已禁用

McTrust（Meraki同步服務）已禁用

ISE節點匯出器未運行

ISE Prometheus服務未運行

ISE Grafana服務未運行

ISE MNT日誌分析彈性搜尋未運行

ISE Logstash服務未運行

ISE Kibana服務未運行

ISE本地IPSec服務未運行

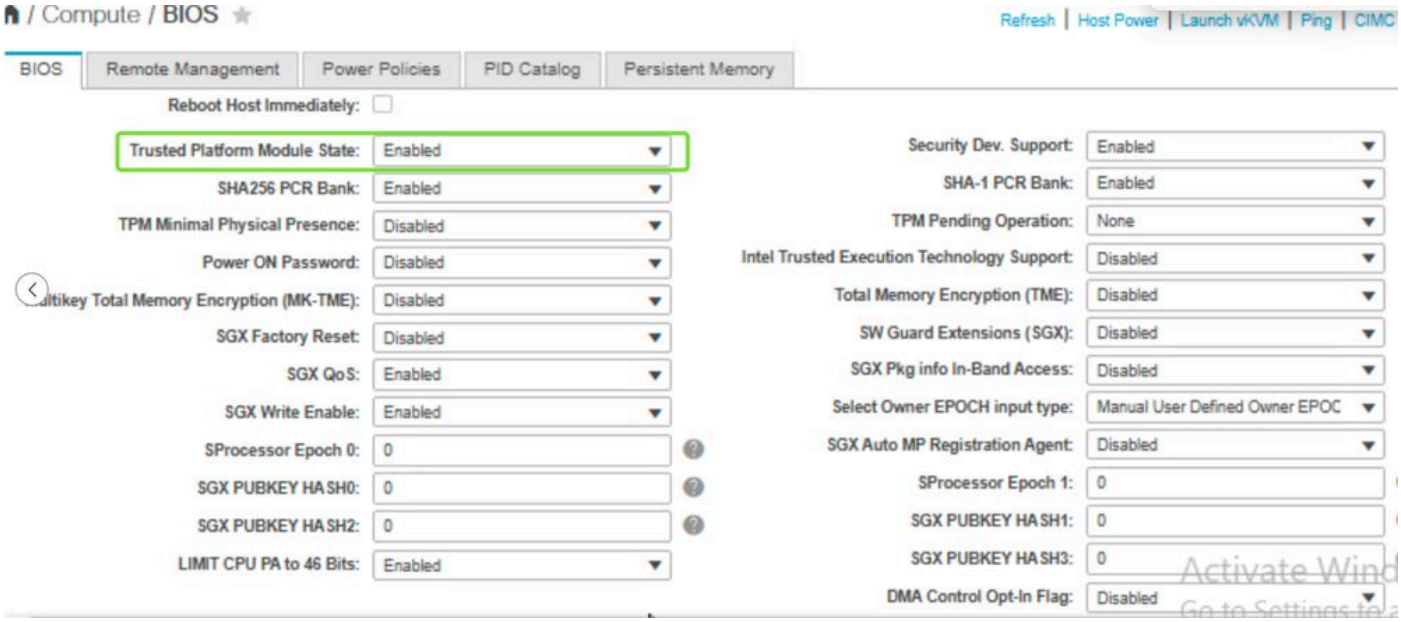
MFC探查器未運行

如果發現TPM2ManagerServer未初始化且響應代碼為400，請啟用TPM服務並重新映像該節點。

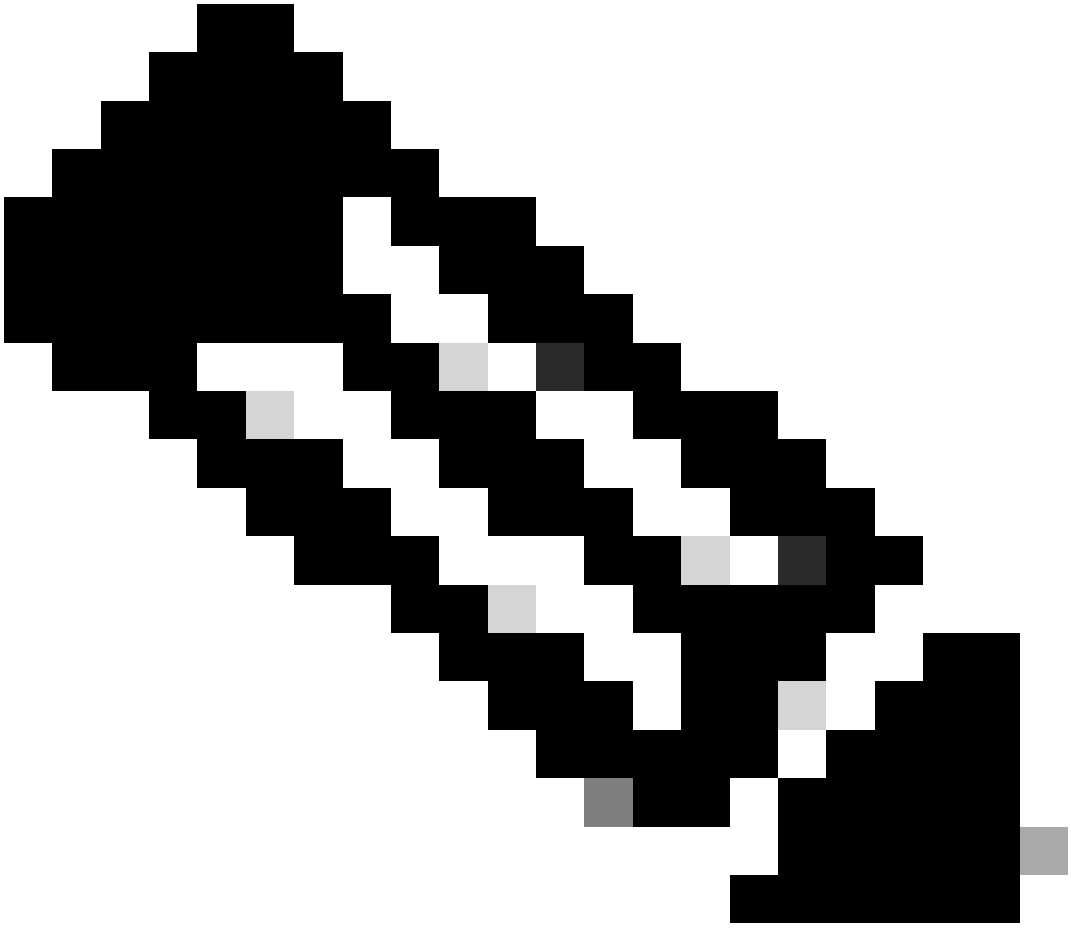
ADE.log:

2025-01-06T08:37:01.164816+00:00 lhrhblise journal[1411]: | 2025-01-06 08:37:01,164 |資訊 | 1411 | MainThread | tpm2_manager_server.py:133 | api:已呼叫運行狀況 |
2025-01-06T08:37:01.166050+00:00 lhrhblise journal[1411]: | 2025-01-06 08:37:01,166 |錯誤 | 1411 | MainThread | utils.py:26 | TPM2ManagerServer未初始化 |
2025-01-06T08:37:01.166179+00:00 lhrhblise journal[1411]: | 2025-01-06 08:37:01,166 |資訊 | 1411 | MainThread | web_log.py:206 | [2025年1月6日：08:37:01 +0000] "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液晶 | 2025-01-06 08:37:21,670 |資訊 | 372321 | MainThread | key_manager_server.py:87 | 正在初始化KeyManagerServer服務，請稍候，這可能需要一些時間 |
2025-01-06T08:37:21.672808+00:00液晶 | 2025-01-06 08:37:21,672 |錯誤 | 372321 | MainThread | key_manager_server.py:116 | 無法初始化KeyManagerServer服務：TPM2ManagerServer未初始化 |

解決方案：啟用TPM模組並執行節點的重新映像。



TPM已啟用



附註：請注意，如果您調整硬體TPM設定或執行任何更改，ISE將顯示意外行為。在這種情況下，您需要重新映像。

案例研究2

根本原因：由於TPM快取，TPM驗證失敗。

儘管BIOS中啟用了TPM設定，但我們在ADE.log中看到鎖定問題

ADE.log:

2024-09-12T16:01:58.063806+05:30 GRP-ACH-ISE-PAN日誌[1404]: | 2024-09-12 16:01:58,063 |資訊 | 1404 | MainThread | tpm2_manager_server.py:133 | api:已呼叫運行狀況 |

2024-09-12T16:01:58.063933+05:30 GRP-ACH-ISE-PAN日誌[1404]: | 2024-09-12 16:01:58,063 |資訊 | 1404 | MainThread | web_log.py:206 | [2024年9月12日 : 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日誌[1404]: | 2024-09-12 16:01:58,064 |資訊 | 1404 | MainThread | tpm2_manager_server.py:184 | api:已呼叫init |

2024-09-12T16:01:58.068413+05:30 GRP-ACH-ISE-PAN日誌[1404]: | 2024-09-12 16:01:58,068 |資訊 | 1404 | MainThread | tpm2_proxy.py:79 | Running命令：tpm2_clear |

2024-09-12T16:01:58.075085+05:30 GRP-ACH-ISE-PAN日誌[1404]: | 2024-09-12 16:01:58,074 |錯誤 | 1404 | MainThread | tpm2_proxy.py:85 | 無法運行tpm2_clear，原因是：tpm：警告(2.0):由於TPM處於DA鎖定模式，此時不允許對受DA保護的對象進行授權 |

2024-09-12T16:01:58.075194+05:30 GRP-ACH-ISE-PAN日誌[1404]: | 2024-09-12 16:01:58,075 |錯誤 | 1404 | MainThread | tpm2_manager_server.py:249 |錯誤：tpm：警告(2.0):由於TPM處於DA鎖定模式，此時不允許對受DA保護的對象進行授權 |

在安裝過程中，我們觀察到了KVM控制檯上的錯誤。

正在提取ISE資料庫內容……

正在啟動ISE資料庫進程……

執行緒「min」 com.cisco.cpm.exceptions中出現異常。TPMException:TPM指令碼執行失敗，返回代碼為非零。)

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

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

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

java.lang.IllegalArgumentException:空鍵

在javax.crypto.spec。SecretKeySpec.<init>(SecretKeySpec。Java:96)，網址為 com.cisco.cpm.auth.encryptor.crypt.Crypt.<init>(Crypt.java:73)

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

在com.cisco.cpm.auth.encryptor。PassudHelper.ma輸入(PassalHelper.java:46)

隨後可能會出現資料庫啟動操作：

錯誤日誌：

##

錯誤：資料庫啟動失敗！

這可能是由於網路介面配置不正確或裝置或VM上缺少資源所致。請解決問題並運行此CLI以重新填充資料庫：

'應用程式重置配置ise'

##########

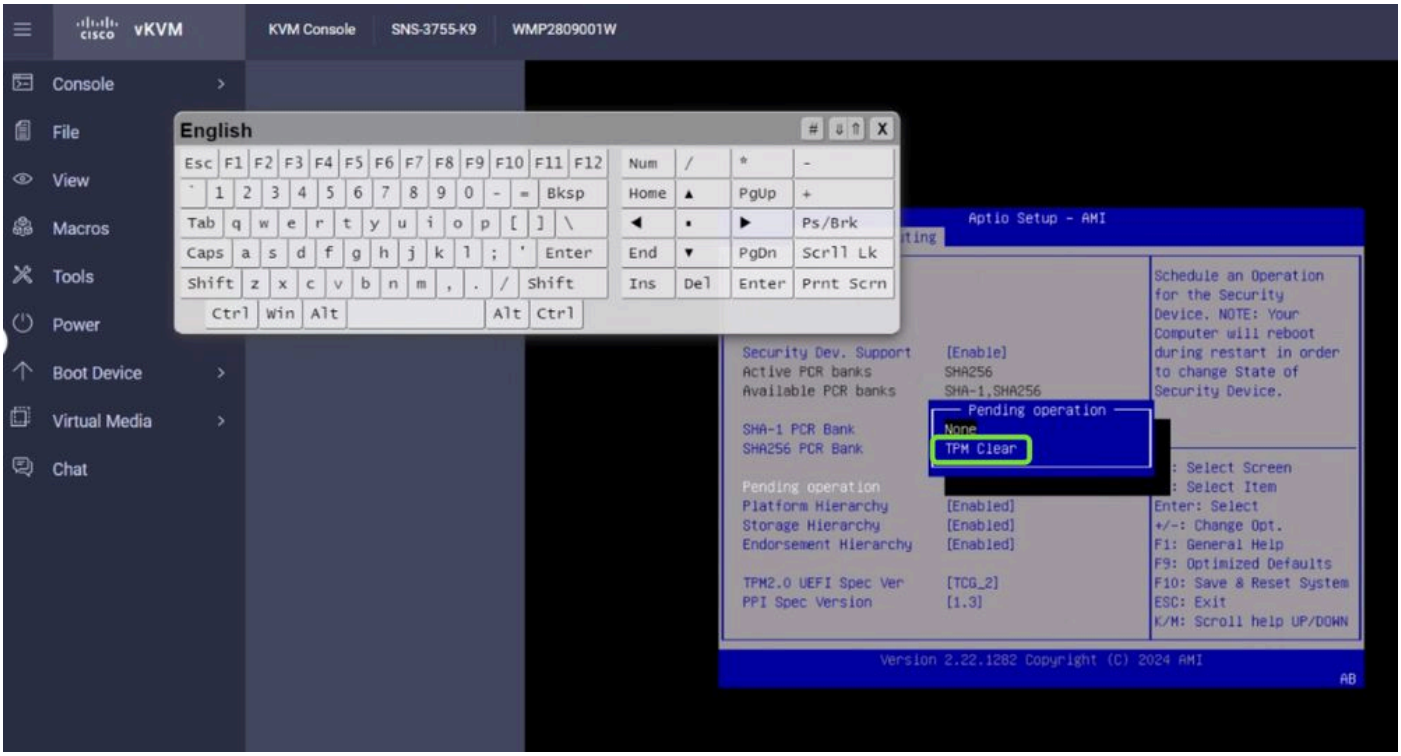
解決方案：如果您發現TPM模組被鎖定，則重置TPM快取可幫助您。

操作步驟：

啟動vKVM，伺服器必須重新啟動

出現Cisco徽標時

- 按F2（這是BIOS選單）
- TPM清除
- 電源重啟



關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。