排除ISE 3.3错误"SNS 37xx服务无法初始化"

目录

简介

本文档介绍ISE 3.3及更高版本的可信平台模块(TPM)的重要性。

前提条件

您必须具备思科身份服务引擎(ISE)的基本知识。

背景信息

可信平台模块(TPM)是一种可以安全地存储用于验证平台（服务器）的信息的计算机芯片（微控制器）。

这些对象可以包括密码、证书或加密密钥。TPM还可用于存储平台度量，以帮助确保平台保持可信。

身份验证（确保平台可以证明它声称自己是真实的）和证明（有助于证明平台值得信赖且未被违反的过程）是确保所有环境中计算安全性的必要步骤。机箱入侵交换机发出任何未经授权的机械访问服务器的通知。

从3.3及更高版本开始，需要使用TPM模块初始化ISE服务。

ISE TPM框架包括两个服务，即密钥管理器、TPM管理器。

密钥管理器
KeyManager子系统是处理密钥的主要组件，是一个节点中的密钥。这包括生成密钥、加密/加密密钥、解密/解密密钥、提供密钥访问等等。
密钥管理器会保留其处理的所有机密的名称引用。密钥管理器绝不会将密钥/密钥存储在磁盘上。在进程期间，通过TPM管理器从TPM检索引导程序机密，并且机密保留在进程内存中。

TPM管理器

TPM管理器完全负责初始化TPM、密封/解封或加密/解密机密以及安全存储机密。TPM管理器绝不会在磁盘上以明文方式存储任何密钥/密钥。在需要将密钥/密钥存储在磁盘上时，密钥/密钥使用TPM中的密钥进行加密，并以加密形式存储。TPM管理器将与信息（例如名称、日期、用户）相关的密钥/机密保存在本地文件中。

所需组件

本文档中的信息基于以下软件和硬件版本

- 思科身份服务引擎3.3
- SNS 3715设备

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

症状（错误消息）

在37xx机箱上成功安装ISE 3.3，且初始网络配置后服务未初始化。

在新的SNS 37xx中，当我们安装3.3 FCS时，可以发现此问题；在任何其他版本的3.3升级期间，或者在3.3 FCS的补丁安装期间，可以发现此问题

根本原因

TPM模块必须在SNS中启用，因为3.3版本（及更高版本）会验证TPM模块。如果禁用，TPM未初始化，这将导致无法初始化服务。

所需的日志

在CLI中，

对于此类问题，您拥有SSH访问权限以从CLI收集支持捆绑包。

所需的确切日志为ade/ADE.log。

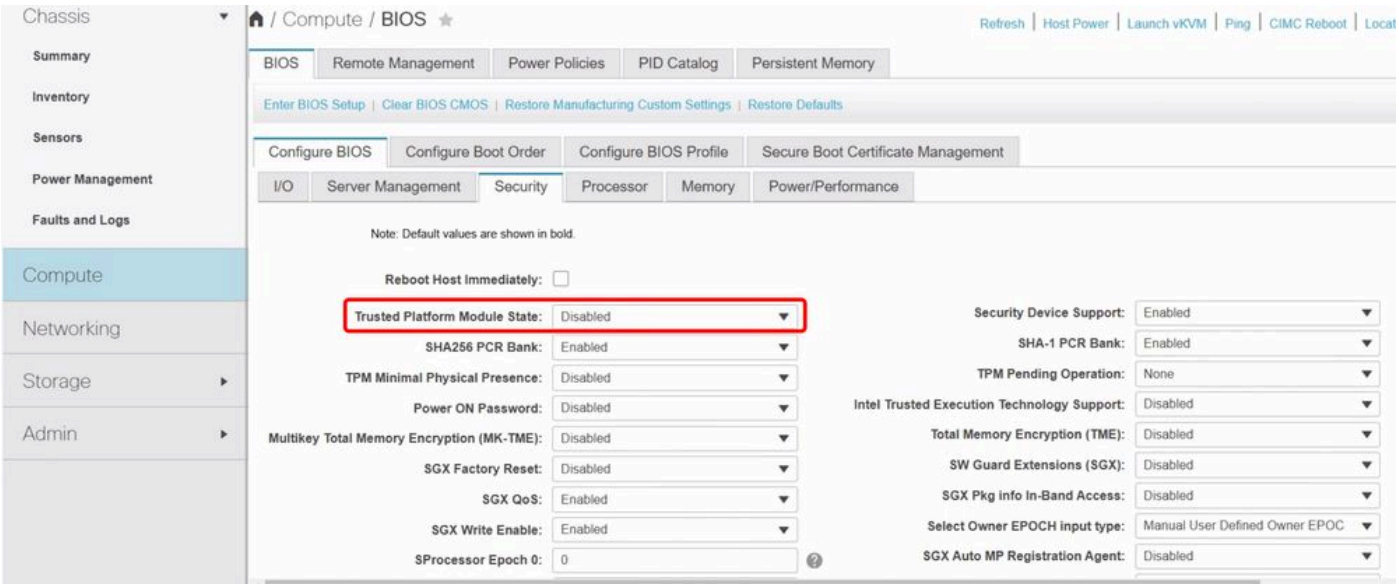
show logging system ade/ADE.log

日志分析

案例研究1

根本原因："未启用TPM模块。"

在CIMC Compute>BIOS> Configure BIOS> Security> Trusted Platform Module State-Disabled



TPM已禁用

大多数服务未运行。

admin#show application status ise

ISE进程名称状态进程ID

数据库监听程序运行379643

运行175个进程的数据库服务器

应用程序服务器未运行

Profiler数据库未运行

ISE索引引擎未运行

AD连接器未运行

M&T会话数据库未运行

M&T日志处理器未运行

证书颁发机构服务未运行

EST服务未运行

SXP引擎服务已禁用

TC-NAC服务已禁用

已禁用PassiveID WMI服务

PassiveID系统日志服务已禁用

已禁用PassiveID API服务

已禁用PassiveID代理服务

已禁用PassiveID终端服务

已禁用PassiveID SPAN服务

DHCP服务器(dhcpd)已禁用

已禁用DNS服务器（已命名）

ISE消息服务未运行

ISE API网关数据库服务未运行

ISE API网关服务未运行

ISE pxGrid直接服务未运行

已禁用分段策略服务

REST身份验证服务已禁用

SSE连接器已禁用

Hermes（pxGrid云代理）已禁用

McTrust（Meraki同步服务）已禁用

ISE节点导出器未运行

ISE Prometheus服务未运行

ISE Grafana服务未运行

ISE MNT日志分析弹性搜索未运行

ISE Logstash服务未运行

ISE Kibana服务未运行

ISE本地IPSec服务未运行

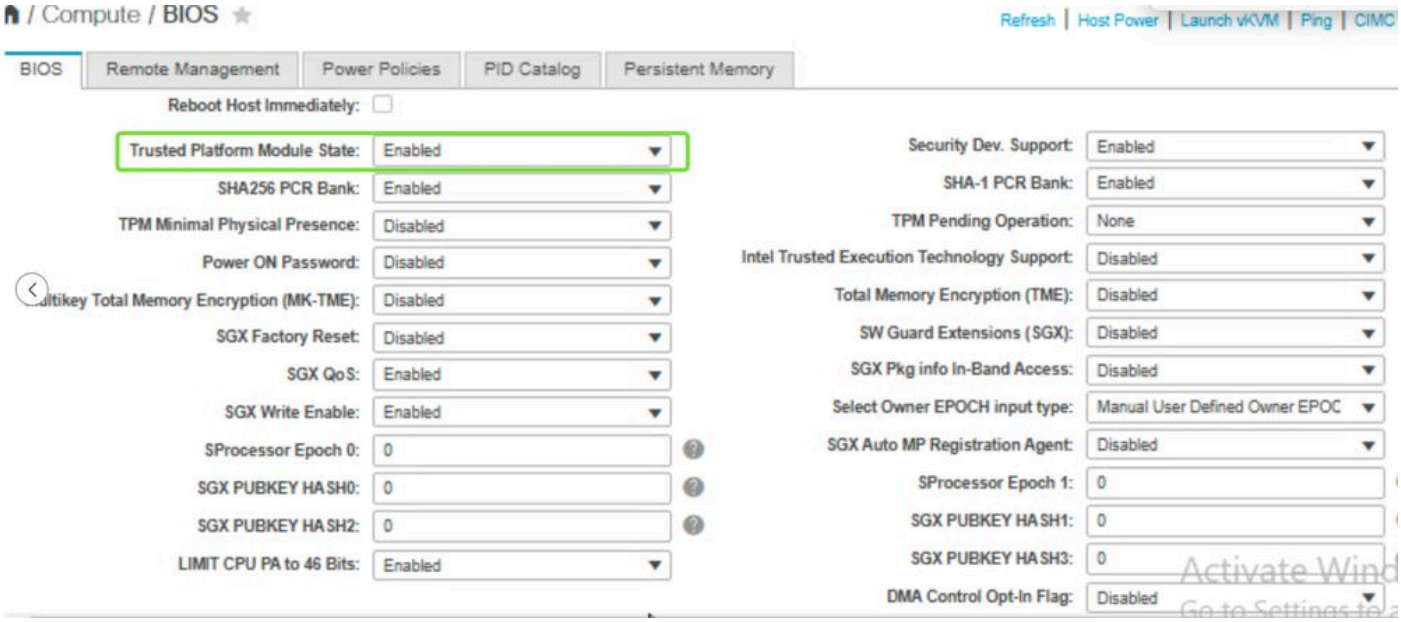
MFC分析器未运行

如果发现TPM2ManagerServer未初始化且响应代码为400，请启用TPM服务并重新映像节点。

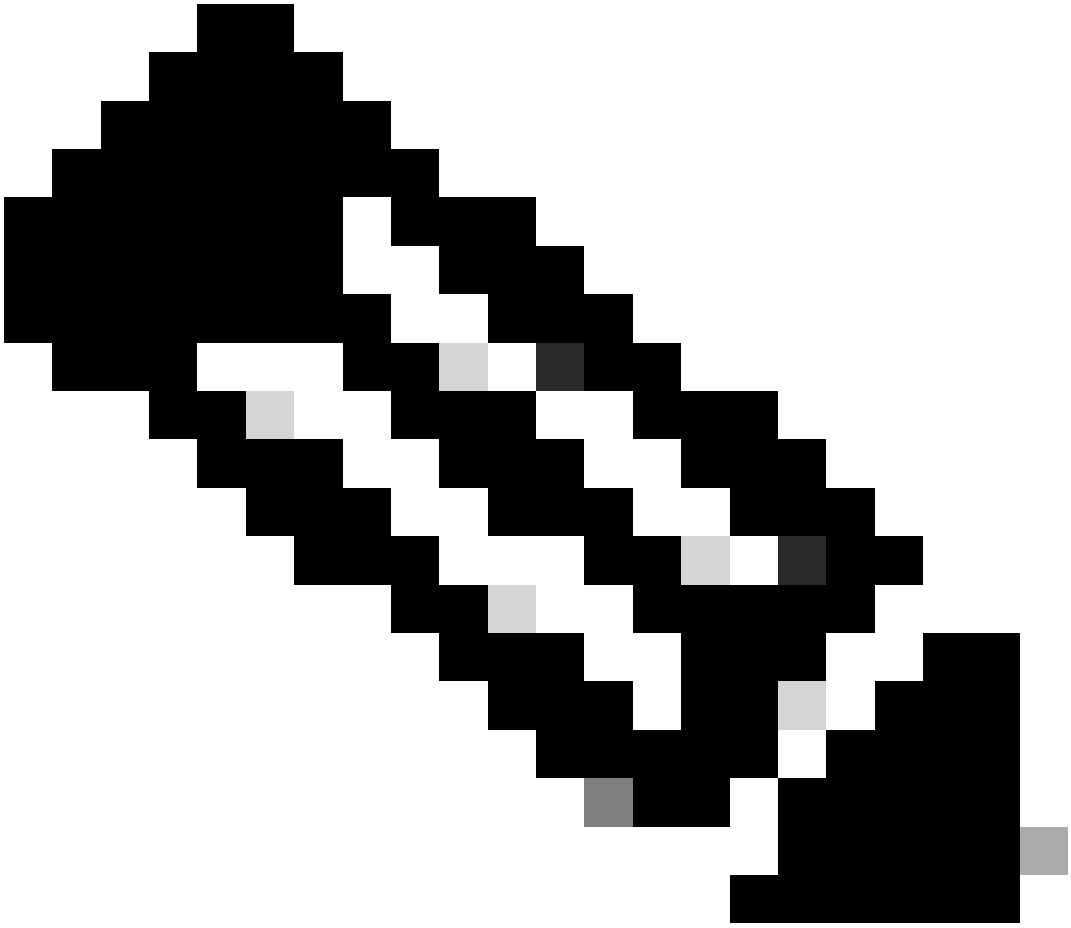
ADE.log:

2025-01-06T08:37:01.164816+00:00 Lhrhblise journal[1411]: | 2025-01-06 08:37:01,164 |信息 | 1411 | MainThread | tpm2_manager_server.py:133 | api:运行状况已调用 |
2025-01-06T08:37:01.166050+00:00 Lhrhblise journal[1411]: | 2025-01-06 08:37:01,166 |错误 | 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 |信息 | 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 |信息 | 372321 | MainThread | key_manager_server.py:87 | 正在初始化KeyManagerServer服务，请稍候，这可能需要一些时间 |
2025-01-06T08:37:21.672808+00:00液晶 | 2025-01-06 08:37:21,672 |错误 | 372321 | MainThread | key_manager_server.py:116 | 无法初始化KeyManagerServer服务：TPM2ManagerServer未初始化 |

解决方案：启用TPM模块并执行节点的重新映像。



TPM已启用



注意：请注意，如果您调整硬件TPM设置或执行任何更改，ISE将显示意外行为。在这种情况下，您需要重新映像。

案例研究2

根本原因：由于TPM缓存，TPM验证失败。

虽然BIOS中启用了TPM设置，但我们在ADE.log中看到锁定问题

ADE.log:

2024-09-12T16:01:58.063806+05:30 GRP-ACH-ISE-PAN日志[1404]: | 2024-09-12 16:01:58,063 |信息 | 1404 | MainThread | tpm2_manager_server.py:133 | api:运行状况已调用 |

2024-09-12T16:01:58.063933+05:30 GRP-ACH-ISE-PAN日志[1404]: | 2024-09-12 16:01:58,063 |信息 | 1404 | MainThread | web_log.py:206 | [2024年9月12日：10:31:58 +0000] "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日志[1404]: | 2024-09-12 16:01:58,064 |信息 | 1404 | MainThread | tpm2_manager_server.py:184 | api:init called |

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

2024-09-12T16:01:58.075085+05:30 GRP-ACH-ISE-PAN日志[1404]: | 2024-09-12 16:01:58,074 |错误 | 1404 | MainThread | tpm2_proxy.py:85 | 无法运行tpm2_clear，原因是：tpm：警告(2.0):由于TPM处于DA锁定模式，此时不允许对受DA保护的对象进行授权 |

2024-09-12T16:01:58.075194+05:30 GRP-ACH-ISE-PAN日志[1404]: | 2024-09-12 16:01:58,075 |错误 | 1404 | MainThread | tpm2_manager_server.py:249 |错误：tpm：警告(2.0):由于TPM处于DA锁定模式，此时不允许对受DA保护的对象进行授权 |

在安装过程中，我们观察到了KVM控制台上的错误。

正在提取ISE数据库内容……

正在启动ISE数据库进程……

线程“min” com.cisco.cpm.exceptions中存在异常。TPMException:TPM脚本执行失败，返回代码为非零。(E)

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

在com.cisco.cpm.auth.encryptor.crypt.TPMUL11.encrypt(TPER11.java:38)，网址为 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:空键

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

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

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

随后可能会显示数据库启动功能：

错误日志：

##

错误：数据库启动失败！

这可能是由于网络接口配置不正确或设备或VM上缺少资源导致的。请解决该问题并运行此CLI以重新初始化数据库：

'application reset-config ise'

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

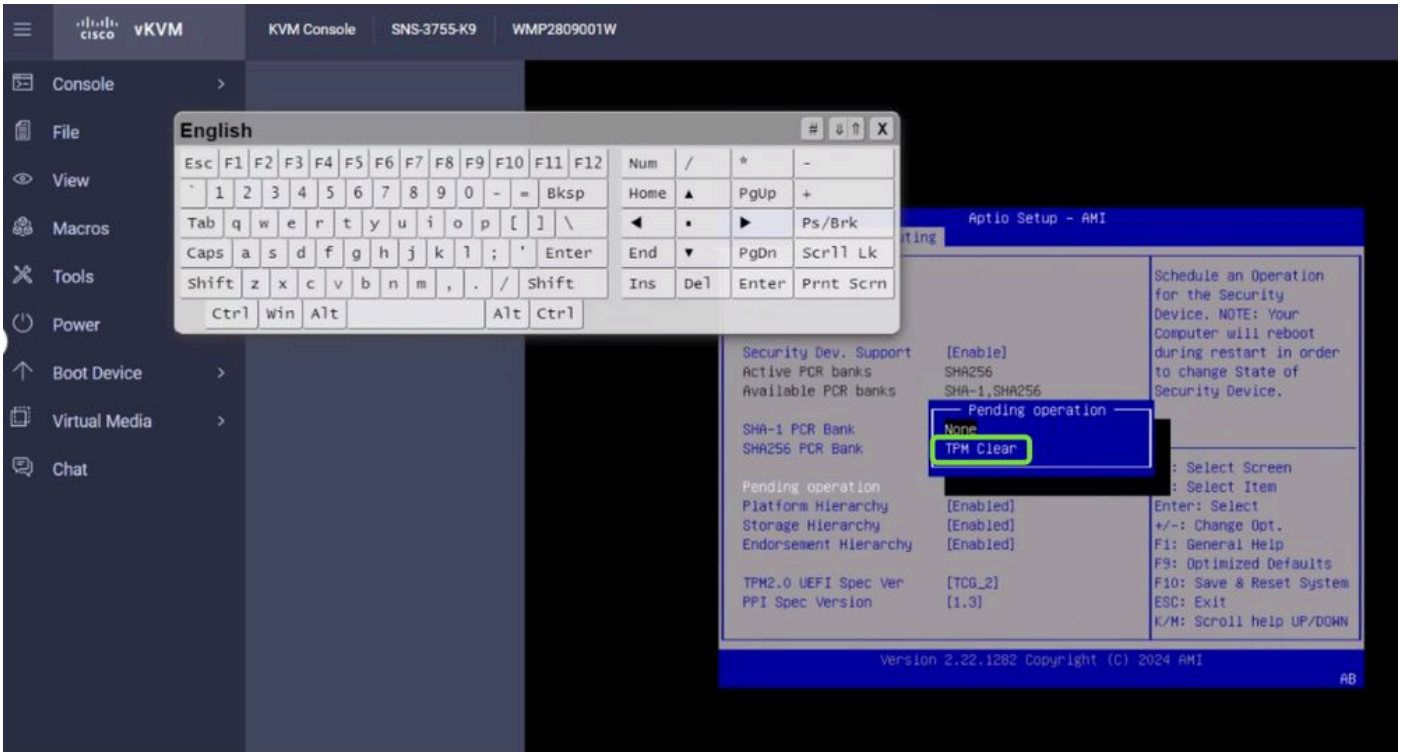
解决方案：如果观察TPM模块被锁定，则重置TPM缓存有帮助。

操作步骤：

启动vKVM，服务器必须重新启动

思科徽标出现时

- 按F2（这是BIOS菜单）
- TPM清除
- 重新通电



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）。