Troubleshoot ISE 3.3 Error "SNS 37xx services fail to initialize"

Contents

Introduction

Pre-Requisites

- Background Information
- Components Required

Symptoms (Error Messages)

Root cause

Logs Needed

Log analysis

Introduction

This document describes the importance of **Trusted Platform Module (TPM)** for ISE 3.3 and later versions.

Pre-Requisites

You must have the basic knowledge of the Cisco Identity Service Engine (ISE).

Background Information

A Trusted Platform Module (TPM) is a computer chip (microcontroller) that can securely store artifacts used to authenticate the platform (server).

These artifacts can include passwords, certificates, or encryption keys. A TPM can also be used to store platform measurements that help ensure that the platform remains trustworthy.

Authentication (ensuring that the platform can prove that it is what it claims to be) and attestation (a process helping to prove that a platform is trustworthy and has not been breached) are necessary steps to ensure safer computing in all environments. A chassis intrusion switch gives a notification of any unauthorized mechanical access into the server.

From 3.3 and above, TPM module is required to initialize the ISE services.

ISE TPM Framework consists of two services namely Key Manager, TPM Manager.

Key Manager
KeyManager subsystem is the main component handling the secrets, keys in a node. This involves generating keys, sealing/encrypting keys, unsealing/decrypting keys, providing access to keys and so on. The key manager maintains a reference, by name, of all the secrets it is handling. The secrets/keys are never stored on the disk by key manager. During process bootstrap secrets are retrieved from TPM via TPM Manager and the secrets remain in the process memory.

TPM Manager

The TPM manager is solely responsible for initialising TPM, seal/unseal or encrypt/decrypt of secrets, and secure storage of secrets. TPM manager never stores any secret/key in clear on the disk. In case needed to store key/secret on the disk the key/secret is encrypted with key from the TPM and stored in the encrypted form. TPM manager keeps keys/secrets related to information (such as name, date, user) in a local file.

Components Required

The information in this document is based on these software and hardware versions

- Cisco Identity service Engine 3.3
- SNS 3715 appliance

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Symptoms (Error Messages)

Installation of ISE 3.3 on a 37xx box is successful and services are not getting initialized after initial network configuration.

The issue can be observed in new SNS 37xx when we install 3.3 FCS or it could be observed during 3.3 upgrade from any other version or during patch installation of 3.3 FCS

Root cause

TPM module must be enabled in SNS as 3.3 version (and later) validates the TPM module. If it is disabled, TPM is not initialized which results in failure to initialize services.

Logs Needed

From CLI,

With these kind of issues, you have SSH access to collect support bundle from CLI.

The exact log needed is ade/ADE.log.

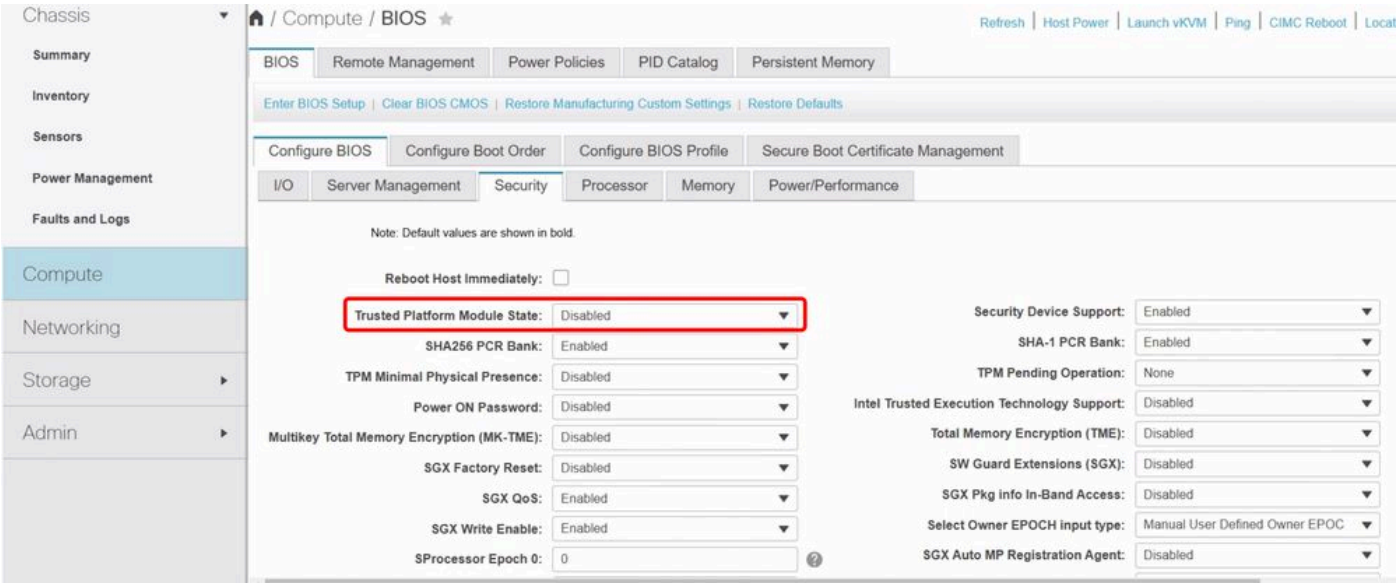
show logging system ade/ADE.log

Log analysis

Case Study 1

Root Cause: "TPM module is not enabled."

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



TPM is disabled

Most of the services are not running.

admin#show application status ise

ISE PROCESS NAME STATE PROCESS ID

Database Listener running 379643

Database Server running 175 PROCESSES

Application Server not running

Profiler Database not running

ISE Indexing Engine not running

AD Connector not running

M&T Session Database not running

M&T Log Processor not running

Certificate Authority Service not running

EST Service not running

SXP Engine Service disabled

TC-NAC Service disabled

PassiveID WMI Service disabled

PassiveID Syslog Service disabled

PassiveID API Service disabled

PassiveID Agent Service disabled

PassiveID Endpoint Service disabled

PassiveID SPAN Service disabled

DHCP Server (dhcpd) disabled

DNS Server (named) disabled

ISE Messaging Service not running

ISE API Gateway Database Service not running

ISE API Gateway Service not running

ISE pxGrid Direct Service not running

Segmentation Policy Service disabled

REST Auth Service disabled

SSE Connector disabled

Hermes (pxGrid Cloud Agent) disabled

McTrust (Meraki Sync Service) disabled

ISE Node Exporter not running

ISE Prometheus Service not running

ISE Grafana Service not running

ISE MNT LogAnalytics Elasticsearch not running

ISE Logstash Service not running

ISE Kibana Service not running

ISE Native IPSec Service not running

MFC Profiler not running

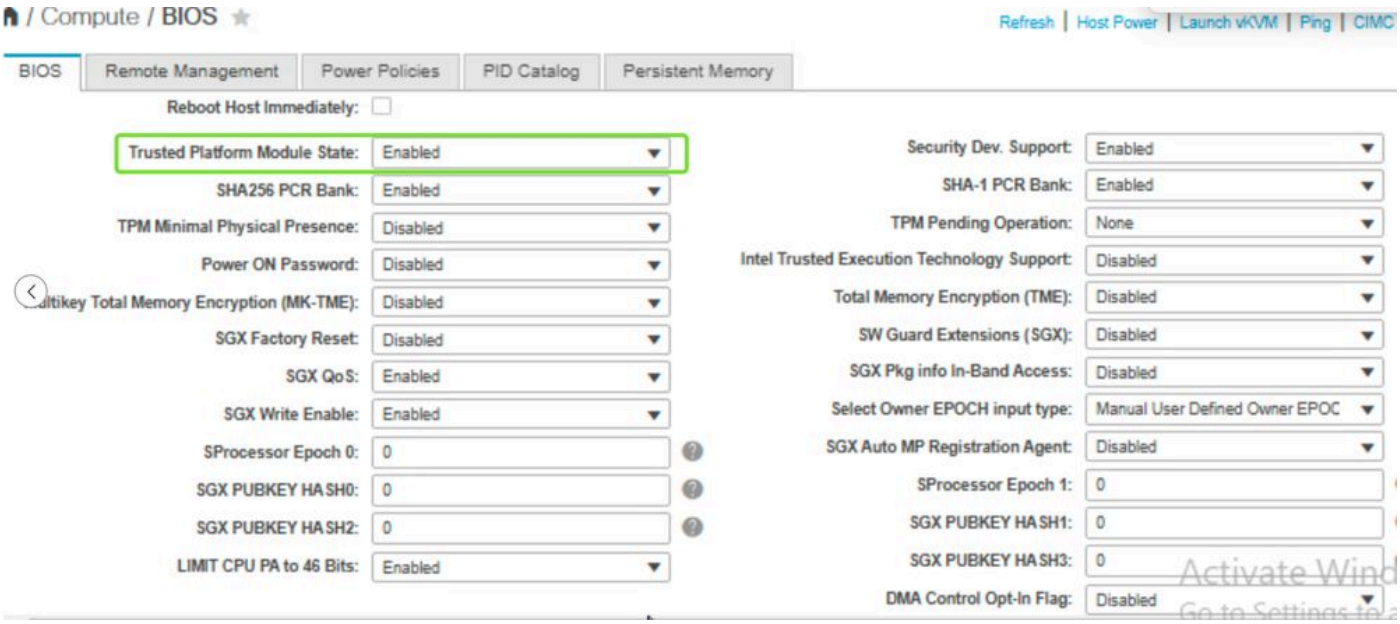
If you observe that TPM2ManagerServer is not initialized and response code 400, enable the TPM service and re-image the node.

ADE.log:

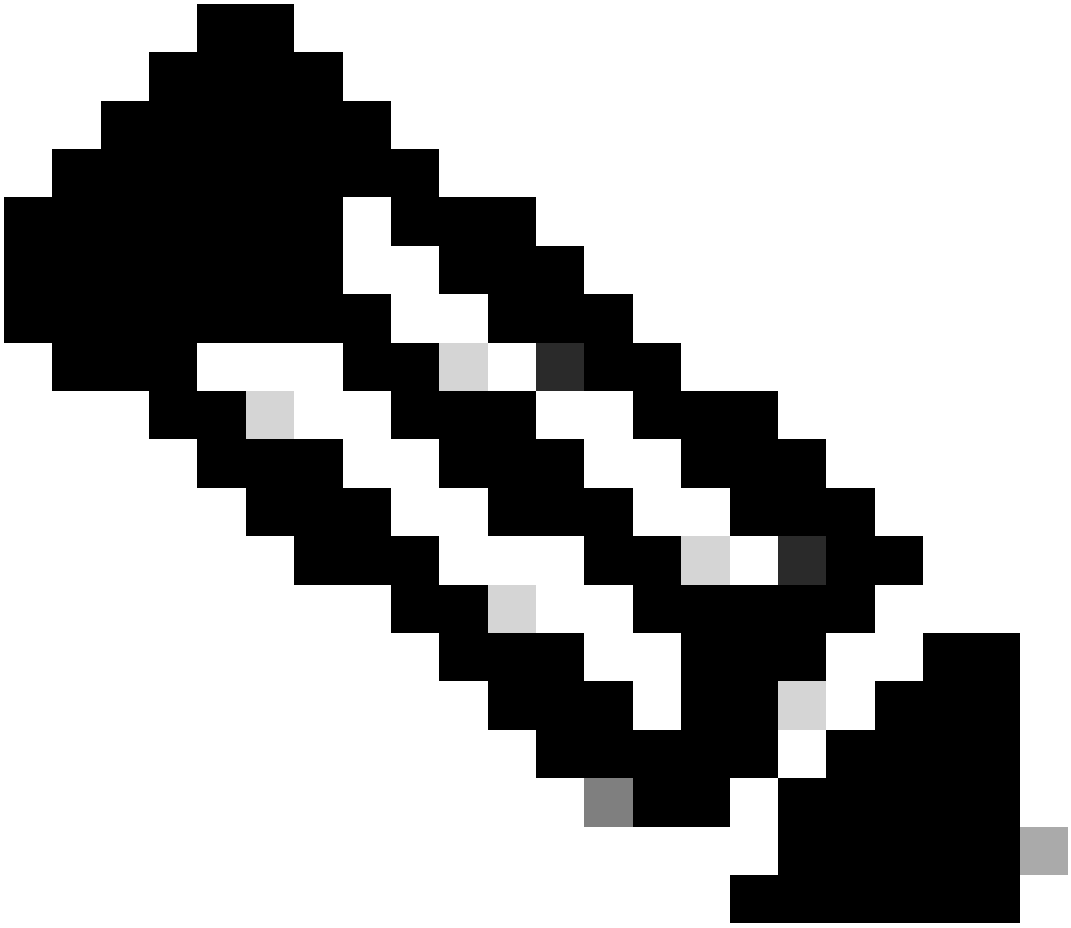
2025-01-06T08:37:01.164816+00:00 lhrhblise journal[1411]: | 2025-01-06 08:37:01,164 | INFO | 1411 | MainThread | tpm2_manager_server.py:133 | api: health called |
2025-01-06T08:37:01.166050+00:00 lhrhblise journal[1411]: | 2025-01-06 08:37:01,166 | ERROR | 1411 | MainThread | utils.py:26 | **TPM2ManagerServer is not initialized |**
2025-01-06T08:37:01.166179+00:00 lhrhblise journal[1411]: | 2025-01-06 08:37:01,166 | INFO | 1411 | MainThread | web_log.py:206 | [06/Jan/2025:08:37:01 +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 lhrhblise | 2025-01-06 08:37:21,670 | INFO | 372321 | MainThread | key_manager_server.py:87 | **Please wait while we initialize KeyManagerServer service, this might take a while |**
2025-01-06T08:37:21.672808+00:00 lhrhblise | 2025-01-06 08:37:21,672 | ERROR | 372321 | MainThread | key_manager_server.py:116 | **Could not initialize KeyManagerServer service: TPM2ManagerServer is not initialized |**

Solution: Enabled TPM module and perform re-image of the node.



TPM is enabled



Note: Be aware that if you adjust the hardware TPM settings or perform any changes, the ISE shows unexpected behavior. In that case you need to do a reimage.

Case Study 2

Root Cause: TPM validation failed due to TPM cache.

Though TPM settings enabled in BIOS, we are seeing lockout issues 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 | MainThread | tpm2_manager_server.py:133 | api: health called |

2024-09-12T16:01:58.063933+05:30 GRP-ACH-ISE-PAN journal[1404]: | 2024-09-12 16:01:58,063 | INFO | 1404 | MainThread | web_log.py:206 | [12/Sep/2024:10:31:58 +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 journal[1404]: | 2024-09-12 16:01:58,064 | INFO | 1404 | MainThread | tpm2_manager_server.py:184 | api: init called |

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

2024-09-12T16:01:58.075085+05:30 GRP-ACH-ISE-PAN journal[1404]: | 2024-09-12 16:01:58,074 | ERROR | 1404 | MainThread | tpm2_proxy.py:85 | **Could not run tpm2_clear** Caused By: tpm:warn(2.0): authorizations for objects subject to DA protection are not allowed at this time because the **TPM is in DA lockout mode** |

2024-09-12T16:01:58.075194+05:30 GRP-ACH-ISE-PAN journal[1404]: | 2024-09-12 16:01:58,075 | ERROR | 1404 | MainThread | tpm2_manager_server.py:249 | ERROR: tpm:warn(2.0): authorizations for objects subject to DA protection are not allowed at this time because the **TPM is in DA lockout mode** |

During the process of installation, we observed the errors on KVM console.

Extracting ISE database content...

Starting ISE database processes...

Exception in thread "min" com.cisco.cpm.exceptions. **TPMException: TPM script execution failed with non-zero return code.**)

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

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

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

java.lang.IllegalArgumentException: Empty key

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

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

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

Followed by database priming might appear:

Error Logs:

##

ERROR: DATABASE PRIMING FAILED!

This could be the result of incorrect network interface configuration, or lack of resources on the appliance or VM. Please fix the issue and run this CLI to re-prime database:

'application reset-config ise'

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

Solution: If you observe TPM module is locked out then resetting TPM cache helps.

Steps to do:

Launch vKVM, and the server must be rebooted

When Cisco logo appears

- Press F2 (this is BIOS menu)
- TPM Clear
- Power cycle

