Troubleshooting de ISE 3.3 Error "Los servicios SNS 37xx no se inicializan"

Contenido

Introducción

Este documento describe la importancia de Trusted Platform Module (TPM) para ISE 3.3 y versiones posteriores.

Requisitos previos

Debe contar con los conocimientos básicos de Cisco Identity Service Engine (ISE).

Antecedentes

Un Módulo de plataforma segura (TPM) es un chip de equipo (microcontrolador) que puede almacenar de forma segura artefactos utilizados para autenticar la plataforma (servidor).

Estos artefactos pueden incluir contraseñas, certificados o claves de cifrado. Un TPM también se puede usar para almacenar mediciones de plataforma que ayudan a garantizar que la plataforma siga siendo confiable.

La autenticación (garantizar que la plataforma pueda demostrar que es lo que afirma ser) y la autenticación (un proceso que ayuda a demostrar que una plataforma es fiable y que no se ha infringido) son pasos necesarios para garantizar una informática más segura en todos los entornos. Un switch de intrusión en el chasis notifica cualquier acceso mecánico no autorizado al servidor.

A partir de la versión 3.3, se requiere el módulo TPM para inicializar los servicios ISE.

La estructura de ISE TPM consta de dos servicios: Key Manager y TPM Manager.

Administrador de claves

El subsistema KeyManager es el componente principal que gestiona los secretos y las claves de un nodo. Esto implica generar claves, sellar/cifrar claves, dessellar/descifrar claves, proporcionar acceso a claves, etc.
El administrador de claves mantiene una referencia, por nombre, de todos los secretos que está manejando. El administrador de claves nunca almacena los secretos o claves en el disco. Durante el proceso, los secretos de bootstrap se recuperan de TPM a través del Administrador de TPM y los secretos permanecen en la memoria del proceso.

Administrador de TPM

El administrador de TPM es el único responsable de inicializar TPM, sellar/dessellar o cifrar/descifrar secretos y proteger el almacenamiento de secretos. El administrador de TPM nunca almacena ningún secreto o clave en el disco. En caso de que sea necesario almacenar clave/secreto en el disco, la clave/secreto se cifra con clave del TPM y se almacena en el formulario cifrado. El administrador de TPM guarda las claves y los secretos relacionados con la información (como el nombre, la fecha o el usuario) en un archivo local.

Componentes necesarios

La información que contiene este documento se basa en estas versiones de software y hardware

- Cisco Identity Service Engine 3.3
- dispositivo SNS 3715

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Síntomas (mensajes de error)

La instalación de ISE 3.3 en un dispositivo 37xx se ha realizado correctamente y los servicios no se están inicializando tras la configuración de red inicial.

El problema se puede observar en el nuevo SNS 37xx cuando instalamos 3.3 FCS o se puede observar durante la actualización 3.3 desde cualquier otra versión o durante la instalación de parches de 3.3 FCS

Causa raíz

El módulo TPM debe estar habilitado en SNS, ya que la versión 3.3 (y posterior) valida el módulo TPM. Si está deshabilitado, TPM no se inicializa, lo que provoca un error al inicializar los servicios.

Registros necesarios

Desde CLI,

Con este tipo de problemas, tiene acceso SSH para recopilar el paquete de soporte de CLI.

El registro exacto necesario es ade/ADE.log.

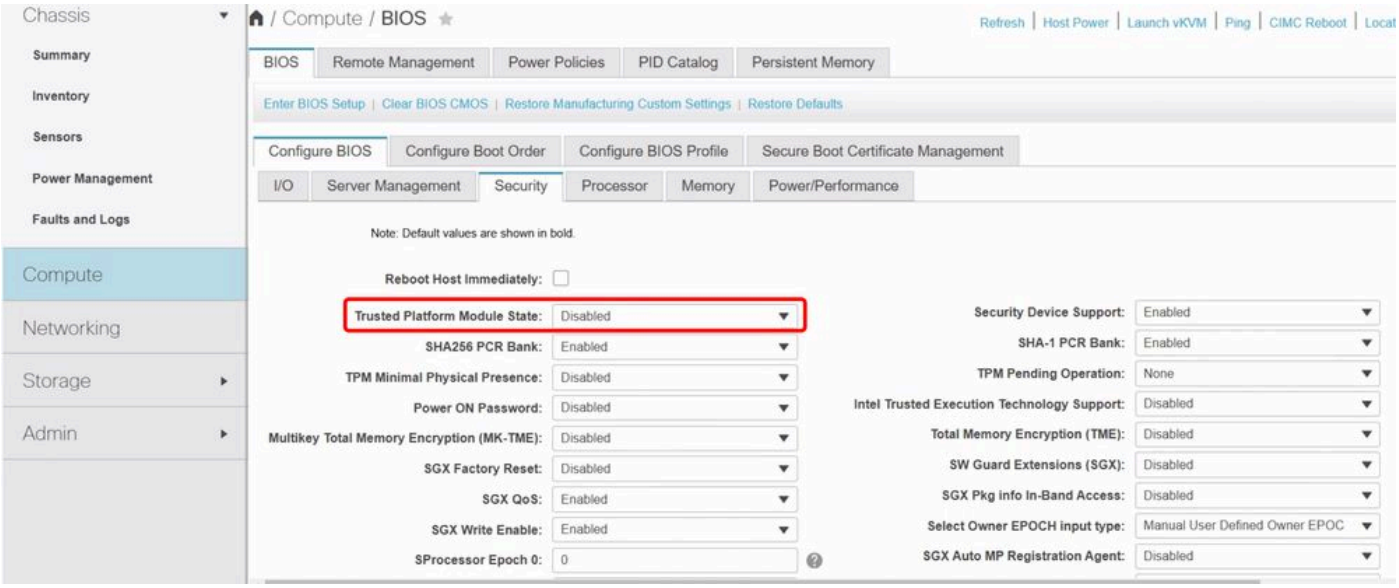
show logging system ade/ADE.log

Análisis de registro

Caso Práctico 1

Causa raíz: "El módulo TPM no está habilitado."

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



TPM está deshabilitado

La mayoría de los servicios no se están ejecutando.

admin#show application status ise

ID DE PROCESO DE ESTADO DE NOMBRE DE PROCESO ISE

Database Listener que ejecuta 379643

Servidor de base de datos con 175 PROCESOS

Servidor de aplicaciones no en ejecución

La base de datos del analizador no se está ejecutando

El motor de indexación de ISE no se está ejecutando

Conector AD no en ejecución

La base de datos de sesión de M&T no se está ejecutando

El procesador de registro de M&T no funciona

El Servicio de autoridad certificadora no se está ejecutando

El servicio EST no se está ejecutando

Servicio de motor SXP deshabilitado

Servicio TC-NAC deshabilitado

Servicio WMI de PassiveID deshabilitado

Servicio Syslog PassiveID deshabilitado

Servicio API PassiveID deshabilitado

Servicio de agente de PassiveID deshabilitado

PassiveID Endpoint Service deshabilitado

Servicio SPAN de PassiveID deshabilitado

Servidor DHCP (dhcpd) deshabilitado

Servidor DNS (con nombre) deshabilitado

El servicio de mensajería ISE no se está ejecutando

El servicio de base de datos ISE API Gateway no se está ejecutando

El servicio ISE API Gateway no se está ejecutando

El servicio ISE pxGrid Direct no se está ejecutando

Servicio de políticas de segmentación deshabilitado

Servicio de autenticación REST deshabilitado

Conector SSE deshabilitado

Hermes (pxGrid Cloud Agent) deshabilitado

McTrust (servicio Meraki Sync) desactivado

Exportador de nodo de ISE sin ejecución

El servicio ISE Prometheus no se está ejecutando

El servicio ISE Grafana no se está ejecutando

ISE MNT LogAnalytics Elasticsearch no se está ejecutando

El servicio ISE Logstash no se está ejecutando

El servicio ISE Kibana no se está ejecutando

El servicio IPSec nativo de ISE no se está ejecutando

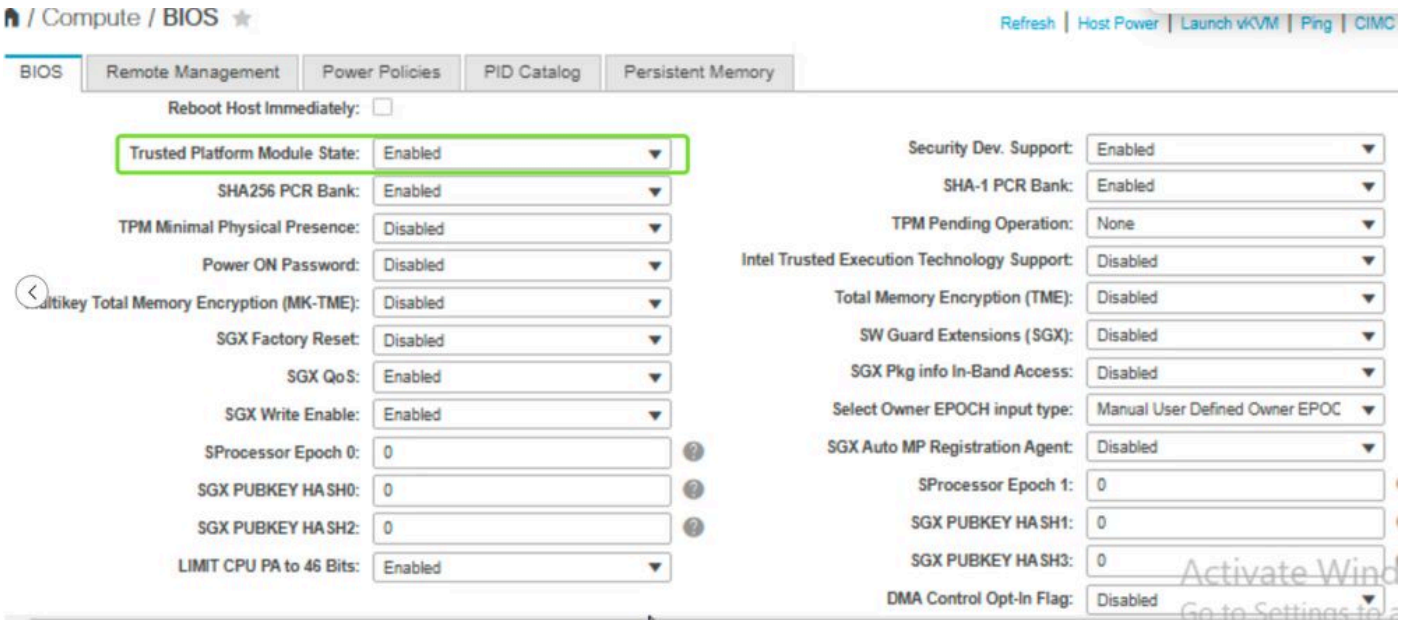
El analizador de MFC no se está ejecutando

Si observa que TPM2ManagerServer no está inicializado y responde al código 400, habilite el servicio TPM y vuelva a crear una imagen del nodo.

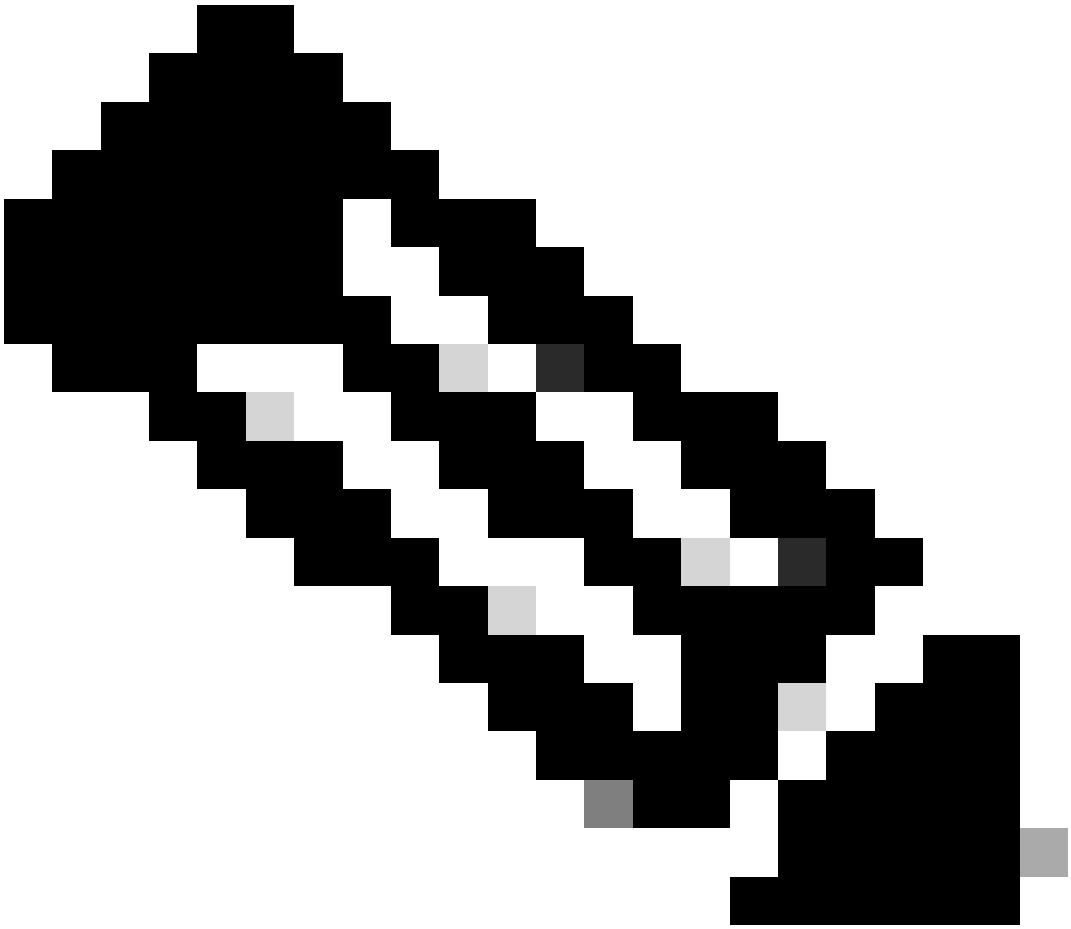
ADE.log:

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: estado llamado |
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 no se ha inicializado |
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 | Espere mientras inicializamos el servicio KeyManagerServer; puede tardar un poco |
2025-01-06T08:37:21.672808+00:00 lhrhblise | 2025-01-06 08:37:21,672 | ERROR | 372321 | MainThread | key_manager_server.py:116 | No se pudo inicializar el servicio KeyManagerServer: TPM2ManagerServer no se ha inicializado |

Solución: se habilitó el módulo TPM y se volvió a crear la imagen del nodo.



TPM está habilitado



Nota: Tenga en cuenta que si ajusta la configuración de TPM de hardware o realiza cambios, ISE muestra un comportamiento inesperado. En ese caso, debe hacer una recreación de la imagen.

Caso Práctico 2

Causa raíz: Error de validación de TPM debido a la caché de TPM.

Aunque la configuración de TPM está habilitada en BIOS, hay problemas de bloqueo en 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: estado llamado |

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 | Comando en ejecución: 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 | No se pudo ejecutar tpm2_clear Causado por: tpm:warn(2): no se permiten las autorizaciones para los objetos sujetos a la protección de DA en este momento porque TPM está en modo de bloqueo de DA |

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): no se permiten las autorizaciones para los objetos sujetos a la protección de DA en este momento porque TPM está en modo de bloqueo de DA |

Durante el proceso de instalación, observamos los errores en la consola KVM.

Extrayendo el contenido de la base de datos de ISE...

Iniciando procesos de base de datos de ISE...

Excepción en el subproceso "min" com.cisco.cpm.exception. Excepción de TPME: Error al ejecutar la secuencia de comandos de TPM con código de retorno distinto de cero.)

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

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

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

java.lang.IllegalArgumentException: Tecla vacía

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

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

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

Seguido de un cebado de base de datos podría aparecer:

Registros de errores:

##

ERROR: ERROR DE CEBADO DE BASE DE DATOS.

Esto puede deberse a una configuración incorrecta de la interfaz de red o a la falta de recursos en el dispositivo o la máquina virtual. Solucione el problema y ejecute esta CLI para volver a preparar la base de datos:

'application reset-config ise'

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

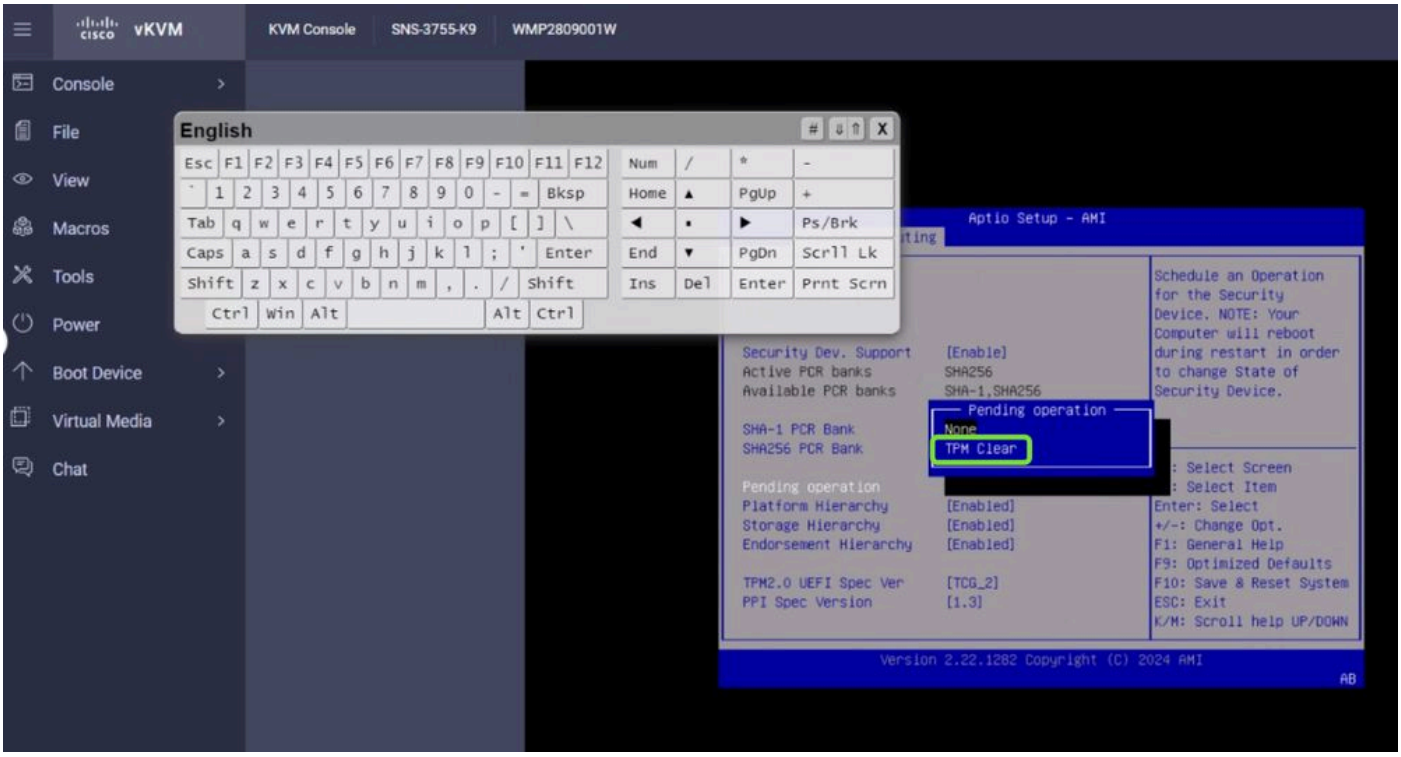
Solución: si observa que el módulo TPM está bloqueado, el restablecimiento de la caché de TPM le ayudará.

Pasos a seguir:

Inicie vKVM y el servidor debe reiniciarse

Cuando aparece el logotipo de Cisco

- Presione F2 (este es el menú BIOS)
- Borrar TPM
- Ciclo de alimentación



Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).