Troubleshooting de Erro do ISE 3.3 "Falha dos serviços SNS 37xx ao inicializar"

Contents

Introdução

Este documento descreve a importância do Trusted Platform Module (TPM) para o ISE 3.3 e versões posteriores.

Pré-requisitos

Você deve ter o conhecimento básico do Cisco Identity Service Engine (ISE).

Informações de Apoio

Um Trusted Platform Module (TPM) é um chip de computador (microcontrolador) que pode armazenar com segurança artefatos usados para autenticar a plataforma (servidor).

Esses artefatos podem incluir senhas, certificados ou chaves de criptografia. Um TPM também pode ser usado para armazenar medidas de plataforma que ajudam a garantir que a plataforma permaneça confiável.

Autenticação (garantir que a plataforma possa provar que é o que afirma ser) e atestado (um processo que ajuda a provar que uma plataforma é confiável e não foi violada) são etapas necessárias para garantir uma computação mais segura em todos os ambientes. Um switch de violação do chassi notifica qualquer acesso mecânico não autorizado ao servidor.

Do 3.3 e posterior, o módulo TPM é necessário para inicializar os serviços do ISE.

O ISE TPM Framework consiste em dois serviços denominados Gerenciador de chaves, Gerenciador de TPM.

Gerenciador de Chaves

O subsistema KeyManager é o componente principal que manipula os segredos, as chaves em um nó. Isso envolve a geração de chaves, chaves de vedação/criptografia, chaves de desselagem/descriptografia, acesso a chaves, etc.
O gerenciador de chaves mantém uma referência, por nome, de todos os segredos que está manipulando. Os segredos/chaves nunca são armazenados no disco pelo gerenciador de chaves. Durante o processo, segredos de bootstrap são recuperados do TPM através do Gerenciador do TPM e permanecem na memória do processo.

Gerenciador de TPM

O gerenciador do TPM é o único responsável por inicializar o TPM, lacrar/deslacrar ou criptografar/descriptografar segredos e armazenar segredos com segurança. O gerenciador do TPM nunca armazena nenhum segredo/chave em modo limpo no disco. Caso seja necessário armazenar a chave/segredo no disco, a chave/segredo é criptografada com a chave do TPM e armazenada na forma criptografada. O gerenciador do TPM mantém chaves/segredos relacionados às informações (como nome, data, usuário) em um arquivo local.

Componentes necessários

As informações neste documento são baseadas nestas versões de software e hardware

- Cisco Identity Service Engine 3.3
- Dispositivo SNS 3715

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Sintomas (mensagens de erro)

A instalação do ISE 3.3 em uma caixa 37xx foi bem-sucedida e os serviços não estão sendo inicializados após a configuração de rede inicial.

O problema pode ser observado no novo SNS 37xx quando instalamos o FCS 3.3 ou durante o upgrade 3.3 de qualquer outra versão ou durante a instalação do patch do FCS 3.3

Causa raiz

O módulo TPM deve ser habilitado no SNS, pois a versão 3.3 (e posterior) valida o módulo TPM. Se estiver desabilitado, o TPM não será inicializado, o que resultará em falha na inicialização dos serviços.

Logs necessários

Do CLI,

Com esse tipo de problema, você tem acesso SSH para coletar o pacote de suporte da CLI.

O registro exato necessário é ade/ADE.log.

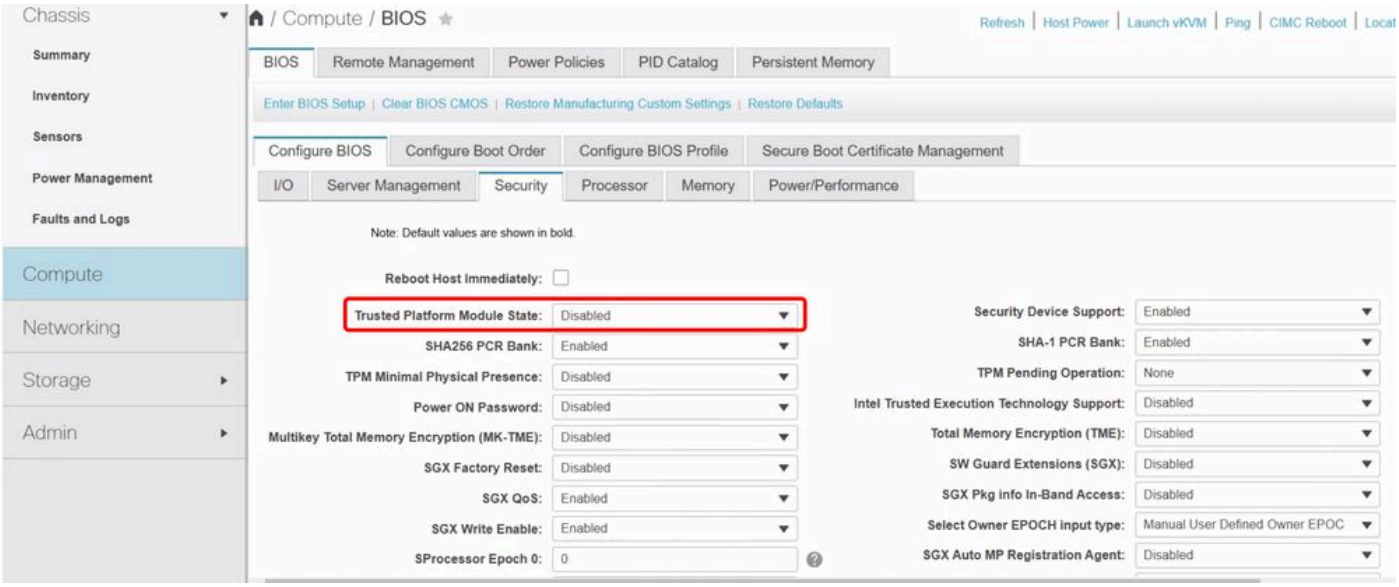
show logging system ade/ADE.log

Análise de log

Casos Práticos 1

Causa raiz: "O módulo TPM não está habilitado."

No CIMC Compute>BIOS> Configure BIOS> Security> Trusted Platform Module State-Disabled



TPM desabilitado

A maioria dos serviços não está em execução.

admin#show application status ise

ID DO PROCESSO DO ESTADO DO NOME DO PROCESSO DO ISE

Ouvinte de Banco de Dados executando 379643

Servidor de banco de dados executando 175 PROCESSES

O servidor de aplicativos não está em execução

O banco de dados do Profiler não está em execução

O mecanismo de indexação do ISE não está em execução

O Conector AD não está em execução

O banco de dados da sessão M&T não está em execução

Processador de Log M&T não está em execução

O Serviço da Autoridade de Certificação não está em execução

Serviço EST não está em execução

Serviço do Mecanismo SXP desabilitado

Serviço TC-NAC desabilitado

Serviço WMI PassiveID desabilitado

Serviço Syslog PassiveID desabilitado

Serviço de API PassiveID desabilitado

Serviço PassiveID Agent desabilitado

Serviço de Ponto de Extremidade PassiveID desabilitado

Serviço SPAN PassiveID desabilitado

Servidor DHCP (dhcpd) desabilitado

Servidor DNS (nomeado) desabilitado

O serviço de mensagens do ISE não está em execução

O Serviço de Banco de Dados do Gateway da API do ISE não está em execução

O Serviço de Gateway da API do ISE não está em execução

O serviço ISE pxGrid Direct não está em execução

Serviço de Política de Segmentação desabilitado

Serviço de autenticação REST desabilitado

Conector SSE desabilitado

Hermes (pxGrid Cloud Agent) desativado

McTrust (Meraki Sync Service) desabilitado

O ISE Node Exporter não está em execução

O ISE Prometheus Service não está em execução

O serviço ISE Grafana não está em execução

LogAnalytics do ISE MNT Pesquisa elástica não está em execução

O Serviço de LogStash do ISE não está em execução

O serviço ISE Kibana não está em execução

O serviço IPSec nativo do ISE não está em execução

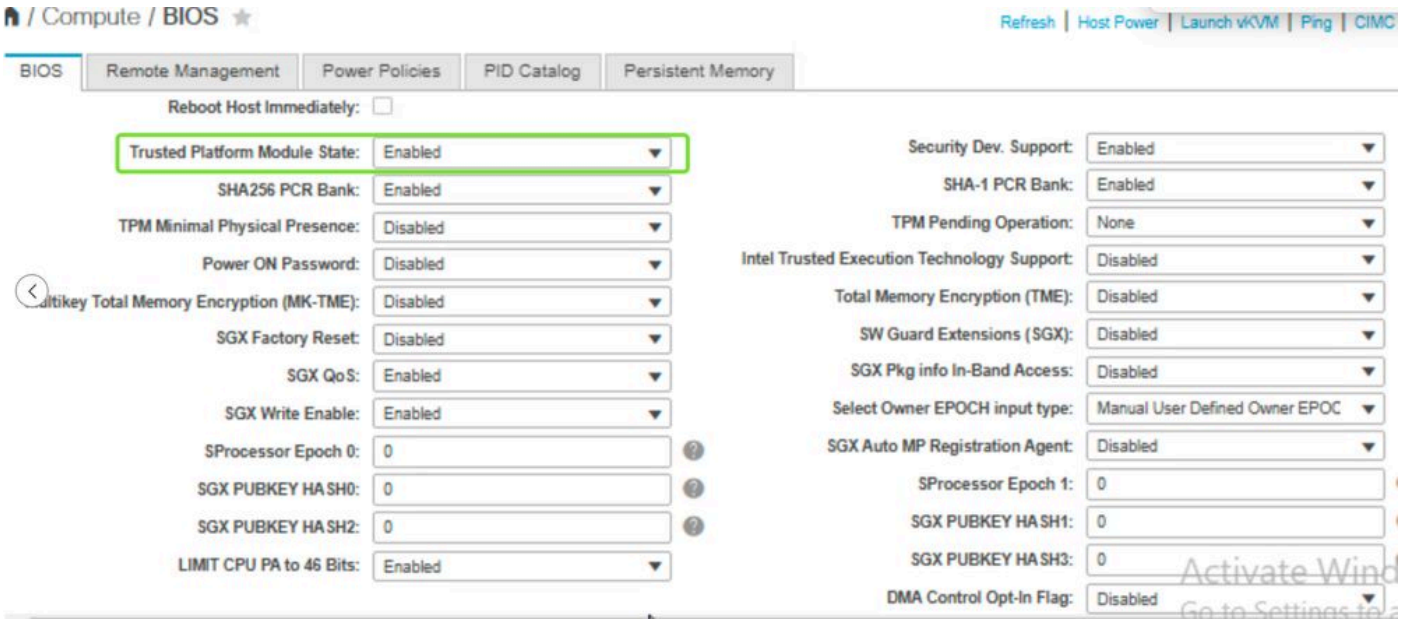
O MFC Profiler não está em execução

Se você observar que o TPM2ManagerServer não foi inicializado e o código de resposta 400, habilite o serviço TPM e recrie a imagem do nó.

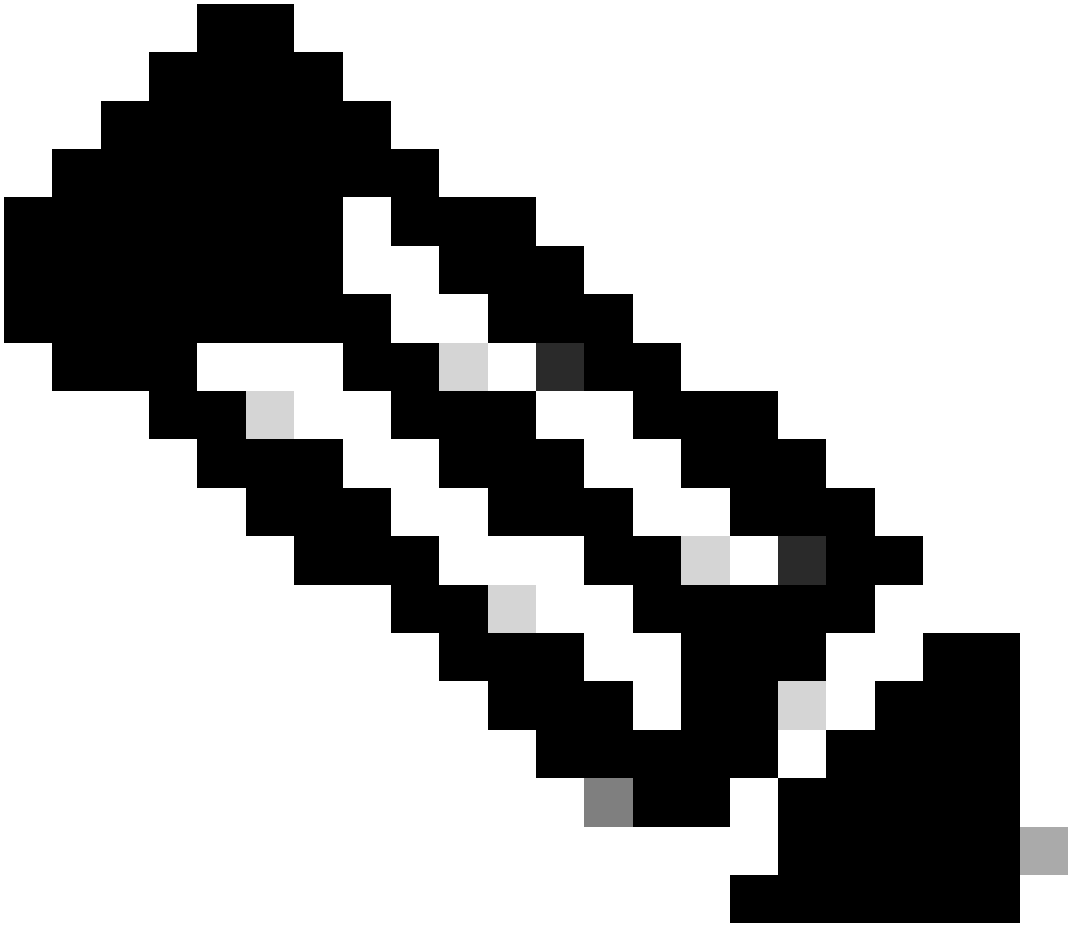
ADE.log:

2025-01-06T08:37:01.164816+00:00 lhrblise journal[1411]: | 2025-01-06 08:37:01,164 | INFORMAÇÕES | 1411 | ThreadPrincipal | tpm2_manager_server.py:133 | api: saúde chamada | 2025-01-06T08:37:01.166050+00:00 lhrblise journal[1411]: | 2025-01-06 08:37:01,166 | ERRO | 1411 | ThreadPrincipal | utils.py:26 | TPM2ManagerServer não inicializado | 2025-01-06T08:37:01.166179+00:00 lhrblise journal[1411]: | 2025-01-06 08:37:01,166 | INFORMAÇÕES | 1411 | ThreadPrincipal | 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 lhblise | 2025-01-06 08:37:21,670 | INFORMAÇÕES | 372321 | ThreadPrincipal | key_manager_server.py:87 | Aguarde enquanto inicializamos o serviço KeyManagerServer, isso pode demorar um pouco | 2025-01-06T08:37:21.672808+00:00 lhblise | 2025-01-06 08:37:21,672 | ERRO | 372321 | ThreadPrincipal | key_manager_server.py:116 | Não foi possível inicializar o serviço KeyManagerServer: TPM2ManagerServer não inicializado |

Solução: Módulo TPM habilitado e nova imagem do nó.



TPM habilitado



Note: Lembre-se de que, se você ajustar as configurações de TPM do hardware ou executar qualquer alteração, o ISE mostrará um comportamento inesperado. Nesse caso, você precisa fazer uma recriação.

Casos Práticos 2

Causa raiz: Falha na validação do TPM devido ao cache do TPM.

Embora as configurações de TPM estejam habilitadas no BIOS, estamos vendo problemas de bloqueio no 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 | INFORMAÇÕES | 1404 | ThreadPrincipal | tpm2_manager_server.py:133 | api: saúde chamada |

2024-09-12T16:01:58.063933+05:30 GRP-ACH-ISE-PAN journal[1404]: | 2024-09-12

16:01:58,063 | INFORMAÇÕES | 1404 | ThreadPrincipal | web_log.py:206 | [12/set/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 | INFORMAÇÕES | 1404 | ThreadPrincipal | tpm2_manager_server.py:184 | api: init chamado |

2024-09-12T16:01:58.068413+05:30 GRP-ACH-ISE-PAN journal[1404]: | 2024-09-12 16:01:58,068 | INFORMAÇÕES | 1404 | ThreadPrincipal | tpm2_proxy.py:79 | Executando comando: tpm2_clear |

2024-09-12T16:01:58.075085+05:30 GRP-ACH-ISE-PAN journal[1404]: | 2024-09-12 16:01:58,074 | ERRO | 1404 | ThreadPrincipal | tpm2_proxy.py:85 | Não foi possível executar tpm2_clear Causado por: tpm:warn(2.0): no momento, não são permitidas autorizações para objetos sujeitos à proteção do DA porque o TPM está no modo de bloqueio do DA |

2024-09-12T16:01:58.075194+05:30 GRP-ACH-ISE-PAN journal[1404]: | 2024-09-12 16:01:58,075 | ERRO | 1404 | ThreadPrincipal | tpm2_manager_server.py:249 | ERRO: tpm:warn(2.0): no momento, não são permitidas autorizações para objetos sujeitos à proteção do DA porque o TPM está no modo de bloqueio do DA |

Durante o processo de instalação, observamos os erros no console KVM.

Extraindo conteúdo do banco de dados do ISE...

Iniciando processos do banco de dados do ISE...

Exceção no segmento "min".com.cisco.cpm.exception. Exceção TPME: Falha na execução do script TPM com código de retorno diferente de zero.)

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

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

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

java.lang.IllegalArgumentException: Chave vazia

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

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

em com.cisco.cpm.auth.encryption. Entrada de PassudHelper.ma (PasssalHelper.java:46)

Seguido pelo priming do banco de dados pode aparecer:

Logs de erro:

##

ERRO: FALHA NA PRIMEIRA IMPLEMENTAÇÃO DO BANCO DE DADOS!

Isso pode ser o resultado de uma configuração incorreta da interface de rede ou da falta de recursos no dispositivo ou na VM. Corrija o problema e execute esta CLI para refazer o prime do banco de dados:

'application reset-config ise'

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

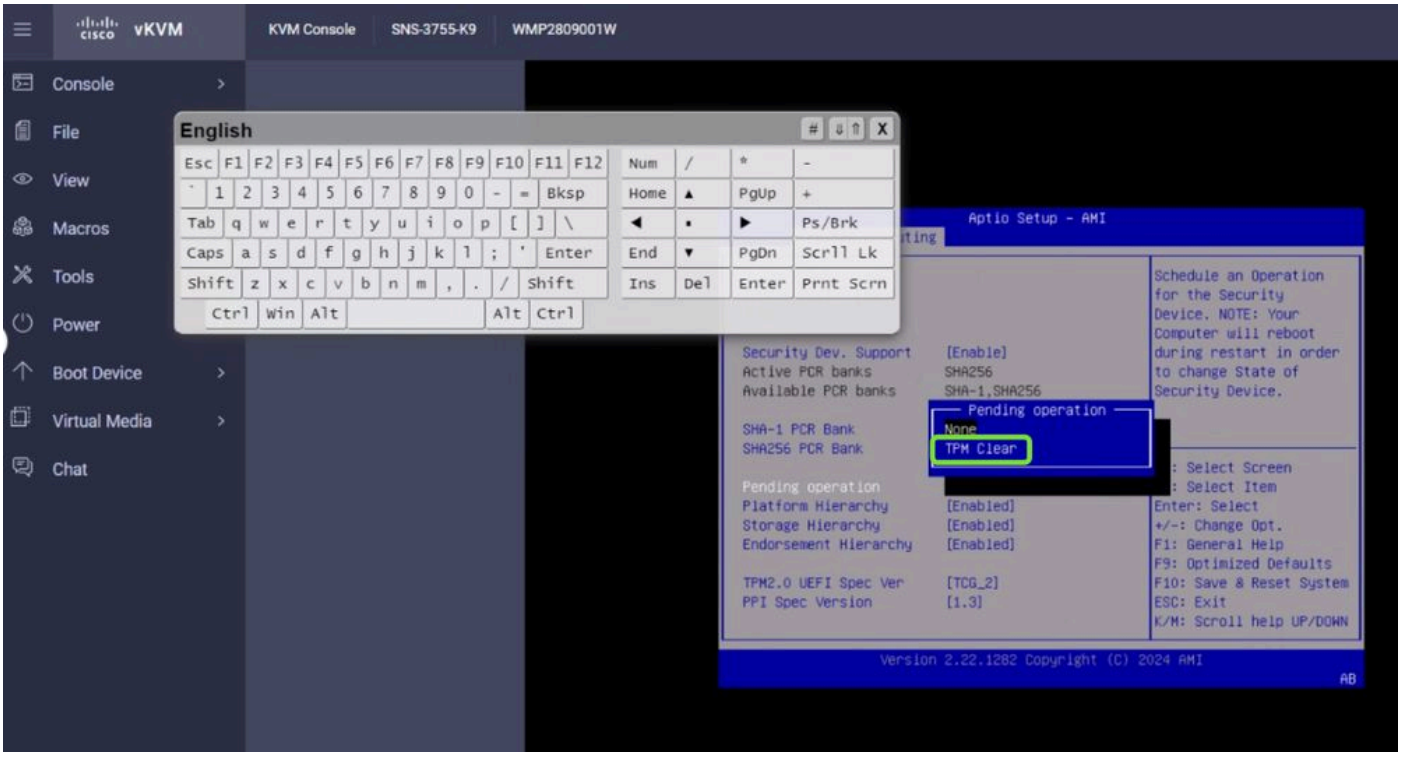
Solução: se você observar que o módulo TPM está bloqueado, a redefinição do cache do TPM ajudará.

Etapas a serem executadas:

Inicie o vKVM e o servidor deverá ser reinicializado

Quando o logotipo da Cisco aparece

- Pressione F2 (este é o menu do BIOS)
- Limpar TPM
- Ciclo de energia



Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.