Dépannage de l'erreur ISE 3.3 " ; Les services SNS 37xx ne parviennent pas à initialiser " ;

Table des matières

Introduction

Ce document décrit l'importance du module de plateforme sécurisée (TPM) pour ISE 3.3 et les versions ultérieures.

Conditions préalables

Vous devez posséder les connaissances de base de Cisco Identity Service Engine (ISE).

Informations générales

Un module TPM (Trusted Platform Module) est une puce informatique (microcontrôleur) qui peut stocker en toute sécurité les artefacts utilisés pour authentifier la plate-forme (serveur).

Ces artefacts peuvent inclure des mots de passe, des certificats ou des clés de chiffrement. Un TPM peut également être utilisé pour stocker les mesures de la plate-forme afin de garantir que celle-ci reste fiable.

L'authentification (pour s'assurer que la plate-forme peut prouver qu'elle est ce qu'elle prétend être) et l'attestation (un processus permettant de prouver qu'une plate-forme est fiable et n'a pas été violée) sont des étapes nécessaires pour garantir un traitement informatique plus sûr dans tous les environnements. Un commutateur anti-intrusion dans le châssis signale tout accès mécanique non autorisé au serveur.

À partir de la version 3.3, le module TPM est requis pour initialiser les services ISE.

L'infrastructure ISE TPM se compose de deux services, à savoir Key Manager et TPM Manager.

Gestionnaire de clés

Le sous-système KeyManager est le composant principal qui gère les secrets, les clés dans un noeud. Cela implique la génération de clés, le scellement/cryptage de clés, le déscellement/décryptage de clés, la fourniture d'un accès aux clés, etc.
Le gestionnaire de clés conserve une référence, par nom, de tous les secrets qu'il traite. Les secrets/clés ne sont jamais stockés sur le disque par le gestionnaire de clés. Pendant l'amorçage du processus, les secrets sont récupérés du module de plateforme sécurisée via le gestionnaire de module de plateforme sécurisée et les secrets restent dans la mémoire du processus.

Gestionnaire TPM

Le gestionnaire du module de plateforme sécurisée est seul responsable de l'initialisation du module de plateforme sécurisée, du scellement/déscellement ou du chiffrement/déchiffrement des secrets, ainsi que du stockage sécurisé des secrets. Le gestionnaire de module de plateforme sécurisée ne stocke jamais aucun secret/clé en clair sur le disque. Dans le cas où il est nécessaire de stocker la clé/le secret sur le disque, la clé/le secret est chiffré avec la clé du module de plateforme sécurisée et stocké sous la forme chiffrée. Le gestionnaire de module de plateforme sécurisée conserve dans un fichier local les clés/secrets relatifs aux informations (telles que le nom, la date, l'utilisateur).

Composants requis

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes

- Cisco Identity Service Engine 3.3
- Appliance SNS 3715

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Symptômes (messages d'erreur)

L'installation d'ISE 3.3 sur un boîtier 37xx a réussi et les services ne sont pas initialisés après la configuration initiale du réseau.

Le problème peut être observé dans le nouveau SNS 37xx lorsque nous installons 3.3 FCS ou il pourrait être observé pendant la mise à niveau 3.3 à partir de toute autre version ou pendant l'installation de correctif de 3.3 FCS

Cause première

Le module TPM doit être activé dans SNS car la version 3.3 (et ultérieure) valide le module TPM. Si elle est désactivée, le module de plateforme sécurisée n'est pas initialisé, ce qui entraîne l'échec de l'initialisation des services.

Journaux requis

Depuis CLI,

Avec ce genre de problèmes, vous avez un accès SSH pour collecter le bundle d'assistance à partir de l'interface de ligne de commande.

Le journal exact requis est ade/ADE.log.

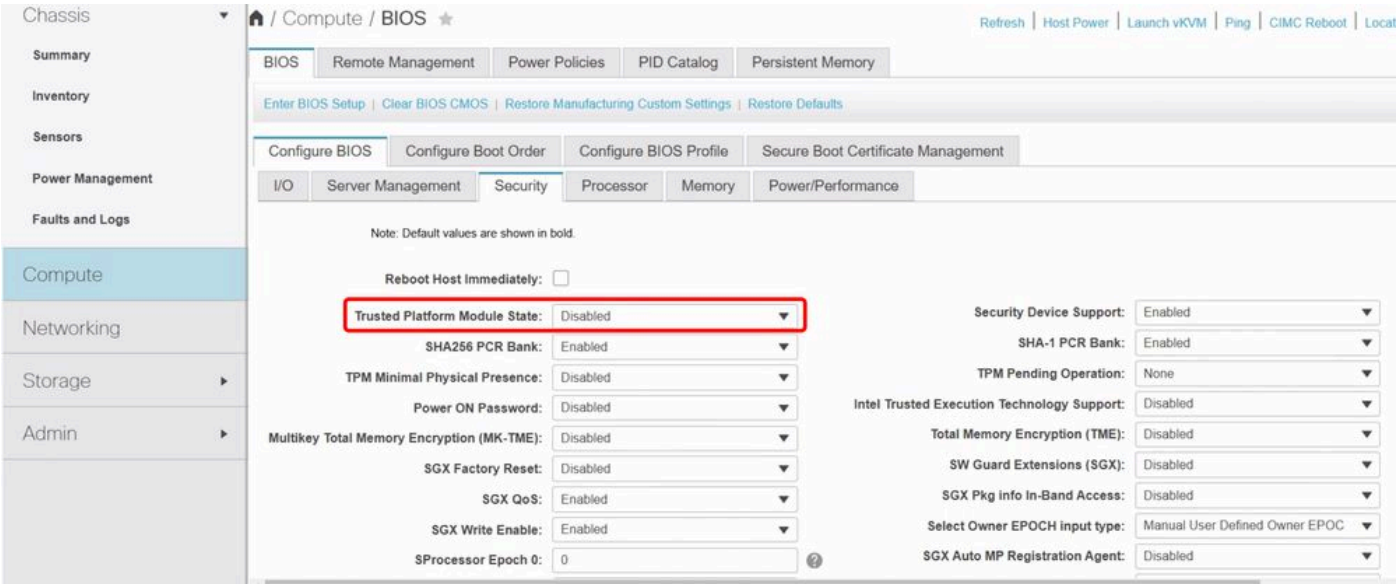
show logging system ade/ADE.log

Analyse du journal

Étude de cas 1

Cause première : "Le module TPM n'est pas activé."

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



Le TPM est désactivé

La plupart des services ne sont pas en cours d'exécution.

admin#show application status ise

NOM DU PROCESSUS ISE ÉTAT ID DU PROCESSUS

Écouteur de base de données exécutant 379643

Serveur de base de données exécutant 175 PROCESSUS

Serveur d'applications inactif

Base de données Profiler non exécutée

Moteur d'indexation ISE inactif

Connecteur AD inactif

Base de données de session M&T non exécutée

M&T Log Processor non exécuté

Service d'autorité de certification non actif

Service EST non exécuté

Service du moteur SXP désactivé

TC-NAC Service désactivé

Service WMI PassiveID désactivé

Service Syslog PassiveID désactivé

Service d'API PassiveID désactivé

Service d'agent PassiveID désactivé

Service de point de terminaison PassiveID désactivé

Service SPAN PassiveID désactivé

Serveur DHCP (dhcpd) désactivé

Serveur DNS (nommé) désactivé

Service de messagerie ISE inactif

Service de base de données de passerelle API ISE non exécuté

Service de passerelle d'API ISE non exécuté

Service direct ISE pxGrid non exécuté

Service de stratégie de segmentation désactivé

Service d'authentification REST désactivé

Connecteur SSE désactivé

Hermes (pxGrid Cloud Agent) désactivé

McTrust (Service de synchronisation Meraki) désactivé

Exportateur de noeud ISE non exécuté

Le service Prometheus ISE ne fonctionne pas

Service ISE Grafana non exécuté

ISE MNT LogAnalytics Elasticsearch non exécuté

Le service ISE Logstash ne fonctionne pas

Le service ISE Kibana ne fonctionne pas

Service IPSec natif ISE non exécuté

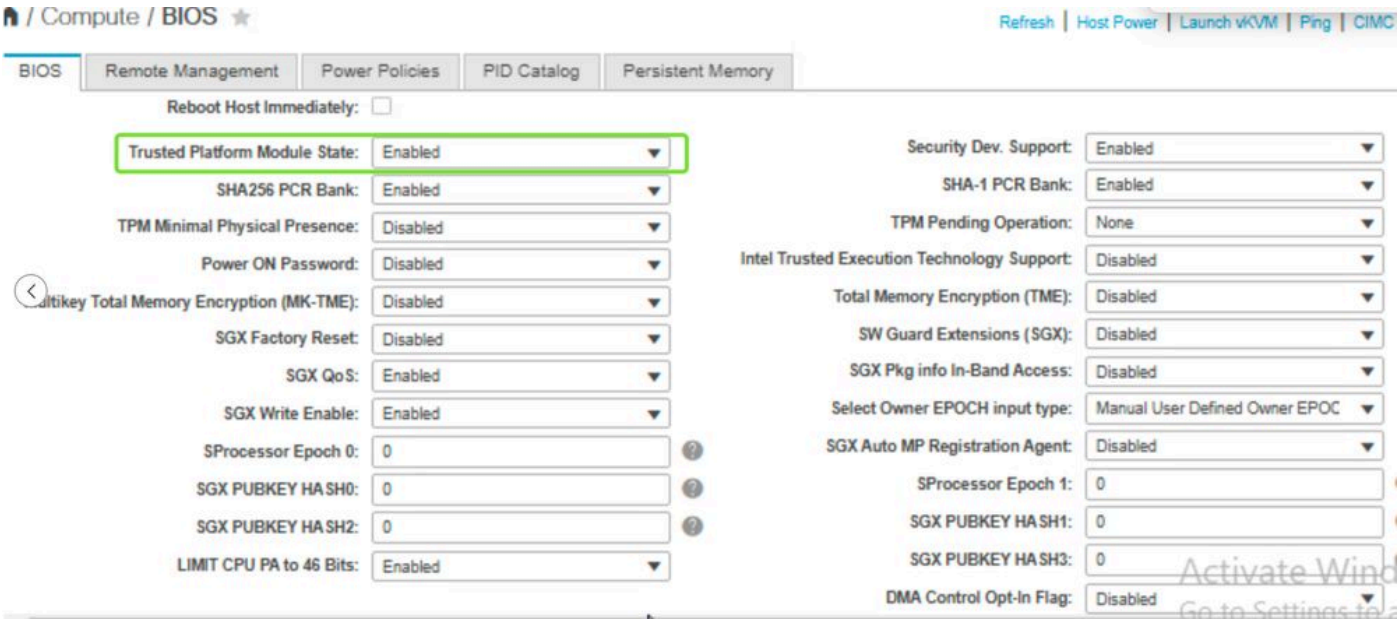
MFC Profiler non exécuté

Si vous constatez que TPM2ManagerServer n'est pas initialisé et que le code de réponse est 400, activez le service TPM et réinstallez le noeud.

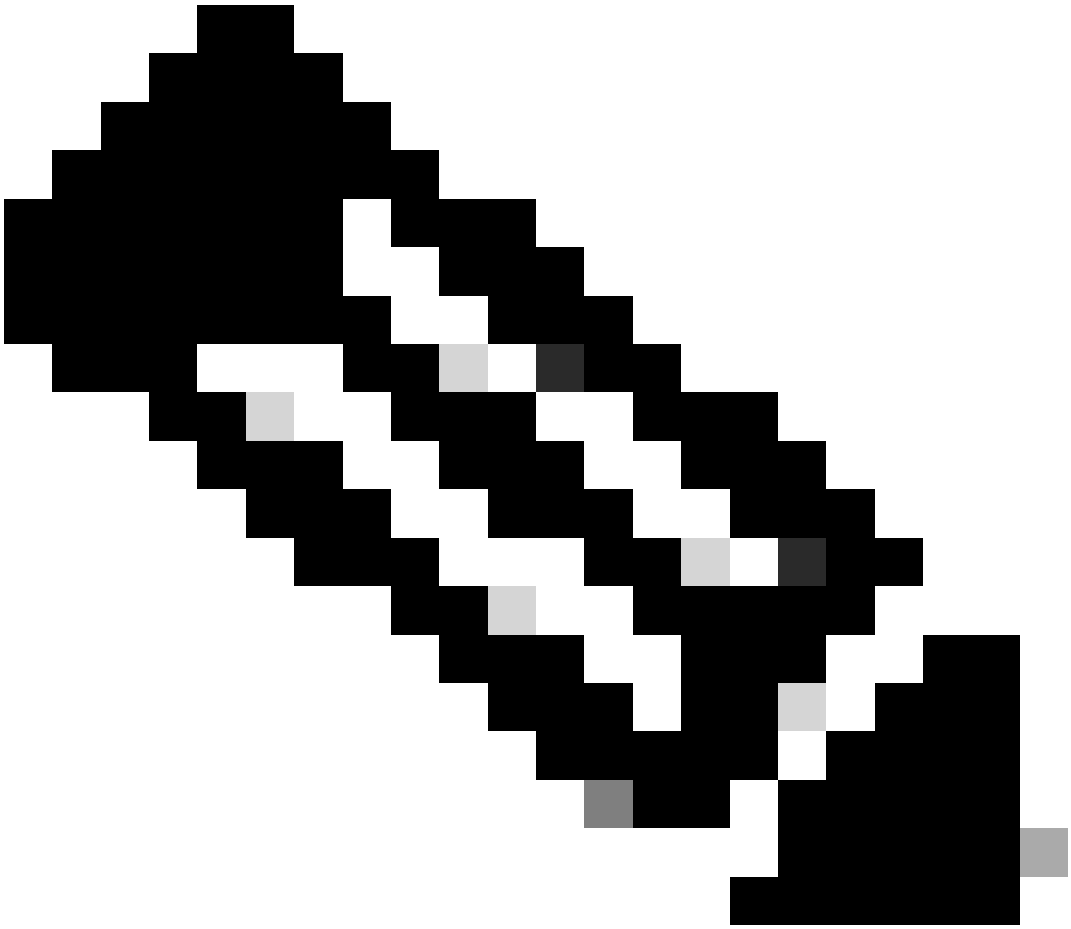
ADE.log :

2025-01-06T08:37:01.164816+00:00 lhrhblise journal[1411] : | 06/01/2025 08:37:01,164 | INFOS 1 411 | | MainThread | tpm2_manager_server.py:133 | api : appelé santé |
2025-01-06T08:37:01.166050+00:00 lhrhblise journal[1411] : | 06/01/2025 08:37:01,166 | ERREUR 1 411 | | MainThread | utils.py:26 | TPM2ManagerServer n'est pas initialisé |
2025-01-06T08:37:01.166179+00:00 lhrhblise journal[1411] : | 06/01/2025 08:37:01,166 | INFOS 1 411 | | MainThread | journal_web.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 | 06/01/2025 08:37:21 670 | INFOS | 372321 | MainThread | key_manager_server.py : 87 | Veuillez patienter pendant l'initialisation du service KeyManagerServer. Cette opération peut prendre un certain temps |
2025-01-06T08:37:21.672808+00:00 lhrhblise | 06/01/2025 08:37:21 672 | ERREUR | 372321 | MainThread | key_manager_server.py : 116 | Impossible d'initialiser le service KeyManagerServer : TPM2ManagerServer n'est pas initialisé |

Solution : activation du module de plateforme sécurisée et réinitialisation du noeud.



Le TPM est activé



Remarque : Sachez que si vous ajustez les paramètres du module de plateforme sécurisée matériel ou effectuez des modifications, l'ISE affiche un comportement inattendu. Dans ce cas, vous devez effectuer une nouvelle image.

Étude de cas 2

Cause première : Échec de la validation du TPM en raison du cache du TPM.

Bien que les paramètres du module de plateforme sécurisée soient activés dans le BIOS, des problèmes de verrouillage apparaissent dans ADE.log

ADE.log :

2024-09-12T16:01:58.063806+05:30 GRP-ACH-ISE-PAN journal[1404] : | 12-09-2024 16:01:58 063 | INFOS 1 404 | | MainThread | tpm2_manager_server.py:133 | api : appelé santé |

2024-09-12T16:01:58.063933+05:30 GRP-ACH-ISE-PAN journal[1404] : | 12-09-2024 16:01:58 063 | INFOS 1 404 | | MainThread | journal_web.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] : | 12-09-2024 16:01:58 064 | INFOS 1 404 | | MainThread | tpm2_manager_server.py:184 | api : init called |

2024-09-12T16:01:58.068413+05:30 GRP-ACH-ISE-PAN journal[1404] : | 12-09-2024 16:01:58 068 | INFOS 1 404 | | MainThread | tpm2_proxy.py:79 | Commande en cours : tpm2_clear |

2024-09-12T16:01:58.075085+05:30 GRP-ACH-ISE-PAN journal[1404] : | 12-09-2024 16:01:58 074 | ERREUR 1 404 | | MainThread | tpm2_proxy.py:85 | Impossible d'exécuter tpm2_clear Causé par : tpm:warn(2.0): les autorisations pour les objets soumis à la protection DA ne sont pas autorisées pour le moment car le TPM est en mode de verrouillage DA |

2024-09-12T16:01:58.075194+05:30 GRP-ACH-ISE-PAN journal[1404] : | 12-09-2024 16:01:58,075 | ERREUR 1 404 | | MainThread | tpm2_manager_server.py : 249 | ERREUR : tpm:warn(2.0): les autorisations pour les objets soumis à la protection DA ne sont pas autorisées pour le moment car le TPM est en mode de verrouillage DA |

Au cours du processus d'installation, nous avons observé les erreurs sur la console KVM.

Extraction du contenu de la base de données ISE...

Démarrage des processus de base de données ISE...

Exception dans le thread « min » com.cisco.cpm.exceptions. TPMException : L'exécution du script TPM a échoué avec un code de retour différent de zéro.)

à l'adresse com.cisco.cpm.auth.encryptor.crypt.TPPUL11.getResult(TPMUtil.java:53

sur com.cisco.cpm.auth.encryptor.crypt.TPMUL11.encrypt(TPER11.java:38) sur

com.cisco.cpm.auth.encryptor.crypt.KEKGenerator.return key (KEKGenerator.java:36)

à l'adresse com.cisco.cpm.auth.encryptor.crypt.KEKGenerator.main(KEKGenerator.java:77)

java.lang.IllegalArgumentException : Touche vide

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

à l'adresse com.cisco.cpm.auth.encryptor.crypt.DefaultCryptEncryptor encrypt(DefaultCryptEncryptar.java:81)

sur com.cisco.cpm.auth.encryptor. PassudHelper.ma Entrant (PassalHelper.java : 46)

L'amorçage de base de données peut apparaître :

Journaux des erreurs :

##

ERREUR : ÉCHEC DE L'AMORÇAGE DE BASE DE DONNÉES

Cela peut être dû à une configuration incorrecte de l'interface réseau ou à un manque de ressources sur l'appliance ou la machine virtuelle. Corrigez le problème et exécutez cette interface de ligne de commande pour réinitialiser la base de données :

'application reset-config ise'

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

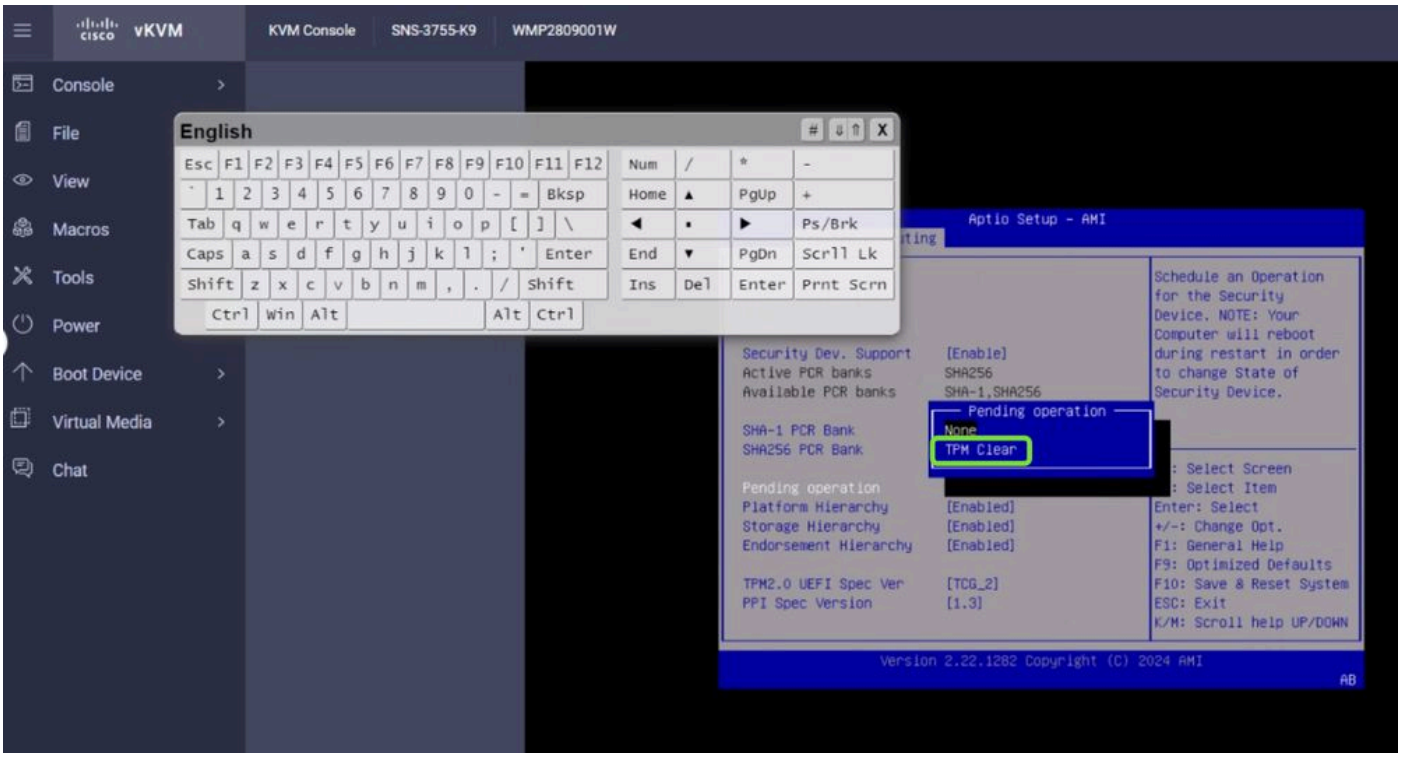
Solution : si vous constatez que le module TPM est verrouillé, la réinitialisation du cache TPM vous aide.

Étapes à suivre :

Lancez vKVM et le serveur doit être redémarré

Lorsque le logo Cisco apparaît

- Appuyez sur F2 (menu BIOS)
- TPM Clear
- Cycle d'alimentation


vKVM
KVM Console
SNS-3755-K9
WMP2809001W
Console
File
View
Macros
Tools
Power
Boot Device
Virtual Media
Chat
English
Aptio Setup - AMI
Security Dev. Support [Enable]
Active PCR banks SHA256
Available PCR banks SHA-1,SHA256
SHA-1 PCR Bank
SHA256 PCR Bank
Pending operation
None
TPM Clear
Pending operation
Platform Hierarchy [Enabled]
Storage Hierarchy [Enabled]
Endorsement Hierarchy [Enabled]
TPM2.0 UEFI Spec Ver [TCG_2]
PPI Spec Version [1.3]
Schedule an Operation for the Security Device. NOTE: Your Computer will reboot during restart in order to change State of Security Device.
Enter: Select
+/-: Change Opt.
F1: General Help
F9: Optimized Defaults
F10: Save & Reset System
ESC: Exit
K/M: Scroll help UP/DOWN
Version 2.22.1282 Copyright (C) 2024 AMI

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.