Configurer le portail d'administration et l'interface de ligne de commande Cisco ISE 3.0 avec IPv6

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Components Used](#)
[Configuration](#)
[Diagramme du réseau](#)
[Vérification](#)
[Dépannage](#)

Introduction

Ce document décrit la procédure à suivre pour configurer Cisco Identity Services Engine (ISE) avec IPv6 pour le portail Admin et l'interface de ligne de commande.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Identity Services Engine (ISE)
- IPv6

Components Used

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

- Correctif ISE version 3.0 4.

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.

Informations générales

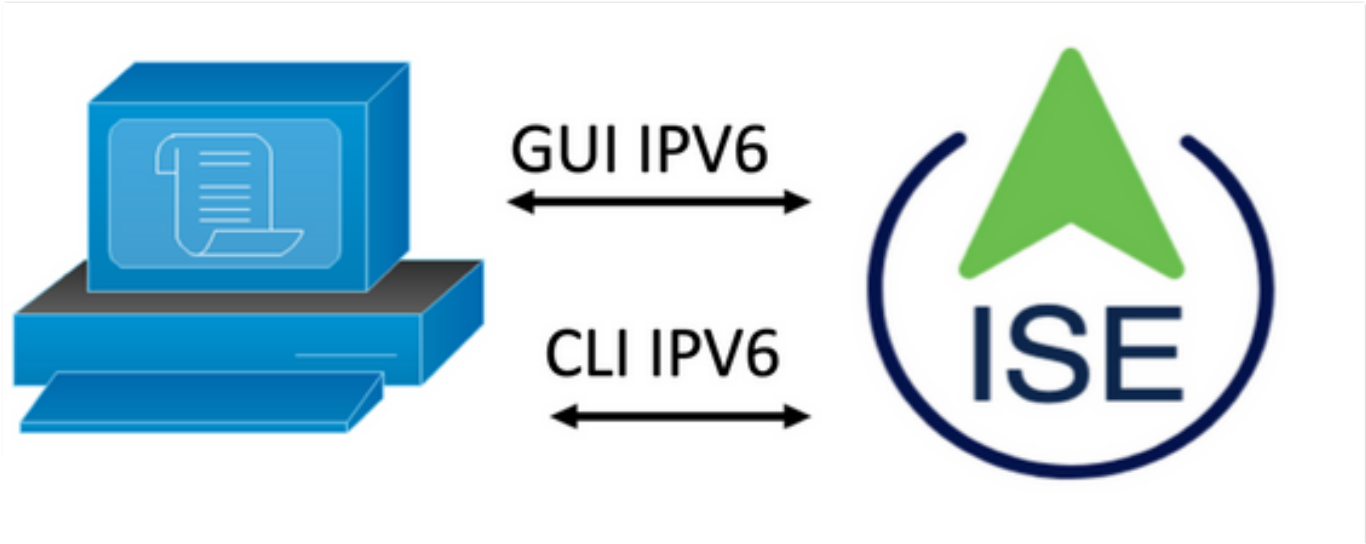
Dans la plupart des cas, Cisco Identity Services Engine peut être configuré avec une adresse Ipv4 pour gérer ISE via l'interface utilisateur (GUI) et l'interface de ligne de commande (CLI) pour se connecter au portail Admin. Cependant, depuis ISE version 2.6 et ultérieure, Cisco ISE peut être géré via une adresse IPv6 et configurer une adresse IPv6 sur Eth0 (interface) lors de l'assistant de configuration ainsi que via l'interface de ligne de commande. Lorsqu'une adresse IPv6 est

configurée, il est recommandé de configurer une adresse IPv4 (en plus de l'adresse IPv6) pour la communication de noeud Cisco ISE. Par conséquent, une double pile (combinaison d'IPv4 et d'IPv6) est requise.
Il est possible de configurer Secure Socket Shell (SSH) avec des adresses IPv6. Cisco ISE prend en charge plusieurs adresses IPv6 sur n'importe quelle interface et ces adresses IPv6 peuvent être configurées et gérées à l'aide de l'interface de ligne de commande.

Configuration

Diagramme du réseau

L'image fournit un exemple de schéma de réseau



Configuration ISE

Note: Par défaut, l'option ipv6 address est activée dans toutes les interfaces ISE. Il est recommandé de désactiver cette option si elle n'est pas prévue pour être utilisée, émettez la commande **no ipv6 address autoconfig** et/ou **no ipv6 enable** le cas échéant. Utilisez la commande **show run** pour valider les interfaces pour lesquelles ipv6 est activé.

Note: La configuration considère que cisco ISE est déjà configuré avec l'adressage IPv4.

ems-ise-mnt001/admin# Configurer le terminal

ems-ise-mnt001/admin(config)# int GigabitEthernet 0

ems-ise-mnt001/admin(config-GigabitEthernet)# ipv6 address **2001:420:404a:133::66**

% La modification de l'adresse IP peut entraîner le redémarrage des services ISE

Continuer avec la modification de l'adresse IP ? O/N [N] : **Y**

Note: L'ajout ou la modification de l'adressage IP sur une interface entraîne le redémarrage des services

Étape 2. Une fois les services redémarrés, exécutez la commande show application status ise

pour valider l'exécution des services :

ems-ise-mnt001/admin# **show application status ise**

ID DE PROCESSUS D'ÉTAT DE NOM DE PROCESSUS ISE

—

Écouteur de base de données exécuté 1252

Serveur de base de données exécutant 74 PROCESSUS

Serveur d'applications exécutant 1134

Base de données Profiler exécutant 6897

Moteur d'indexation ISE exécutant 14121

Connecteur AD exécutant 17184

Base de données de session M&T exécutant 6681

Processeur de journaux M&T 11337

Service d'autorité de certification exécuté 17044

Service EST exécuté 10559

Service moteur SXP désactivé

Démon Docker exécutant 3579

Service TC-NAC désactivé

pxGrid Infrastructure Service exécuté en 9712

service d'abonné pxGrid Publisher exécutant 9791

pxGrid Connection Manager exécutant 9761

contrôleur pxGrid exécutant 9821

Service WMI PassiveID désactivé

Service Syslog PassiveID désactivé

Service API PassiveID désactivé

Service 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 exécuté sur 4260

Service de base de données de passerelle d'API ISE exécutant 5805

Service de passerelle d'API ISE exécutant 8973

Service de stratégie de segmentation désactivé

Service d'authentification REST désactivé

Connecteur SSE désactivé

Étape 3. Émettez la commande **show run** pour valider IPv6 a été configurée sur Eth0 (interface) :

ems-ise-mnt001/admin# show run

Génération de la configuration...

!

nom d'hôte ems-ise-mnt001

!

ip domain-name ise.com

!

ipv6 enable

!

interface GigabitEthernet 0

ip address 10.52.13.175 255.255.255.0

ipv6 address 2001:420:404a:133::66/64

ipv6 address autoconfig

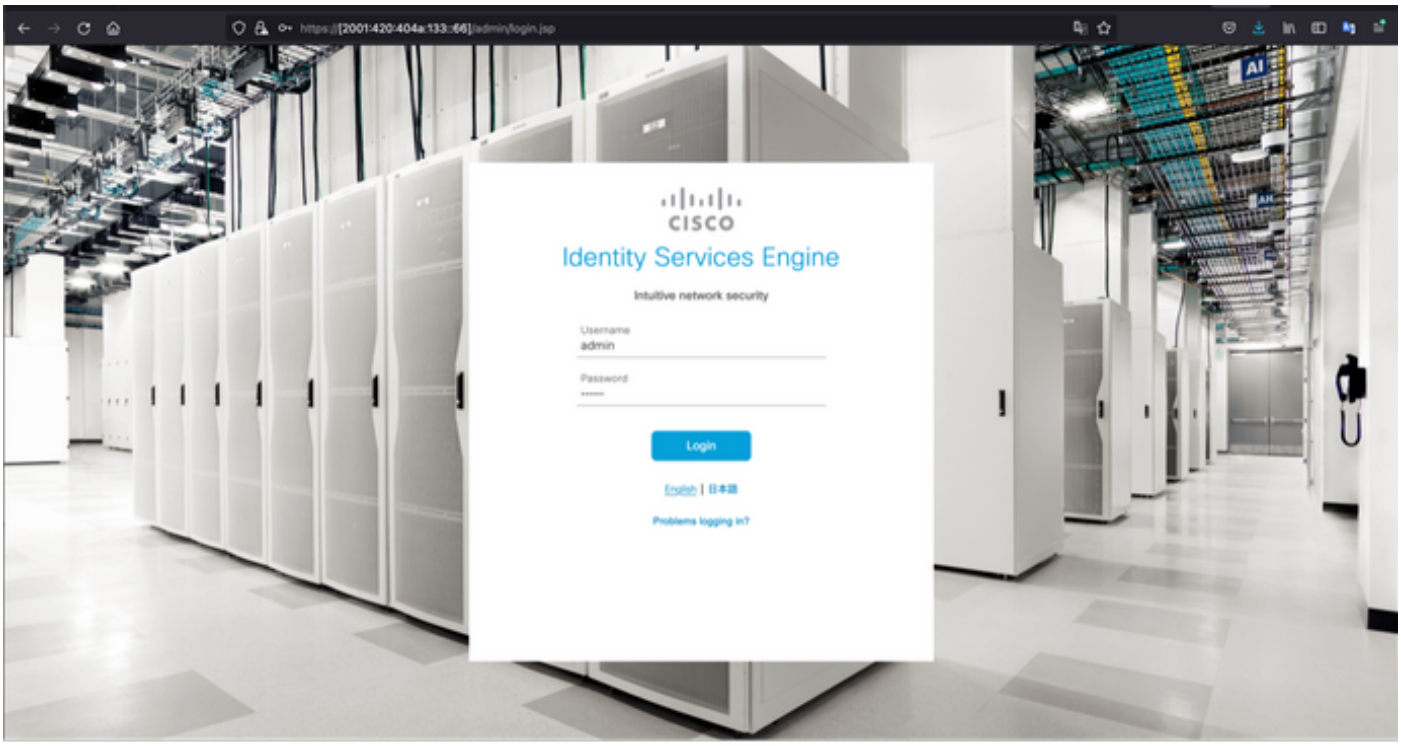
ipv6 enable

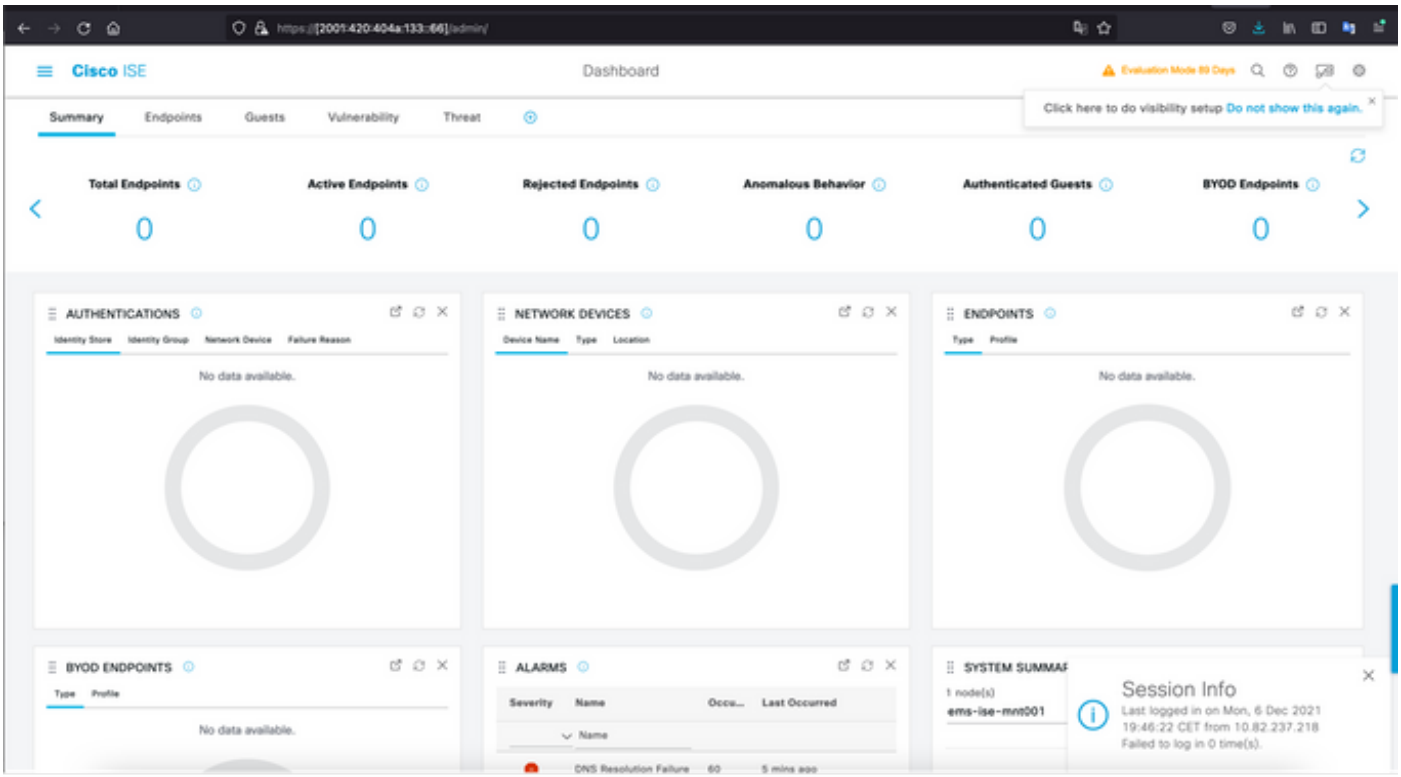
!

Vérification

Interface utilisateur de Cisco ISE

Étape 1. Ouvrez un nouveau navigateur de fenêtre et tapez https://[2001:420:404a:133::66]. Notez que l'adresse IPv6 doit être entre crochets.

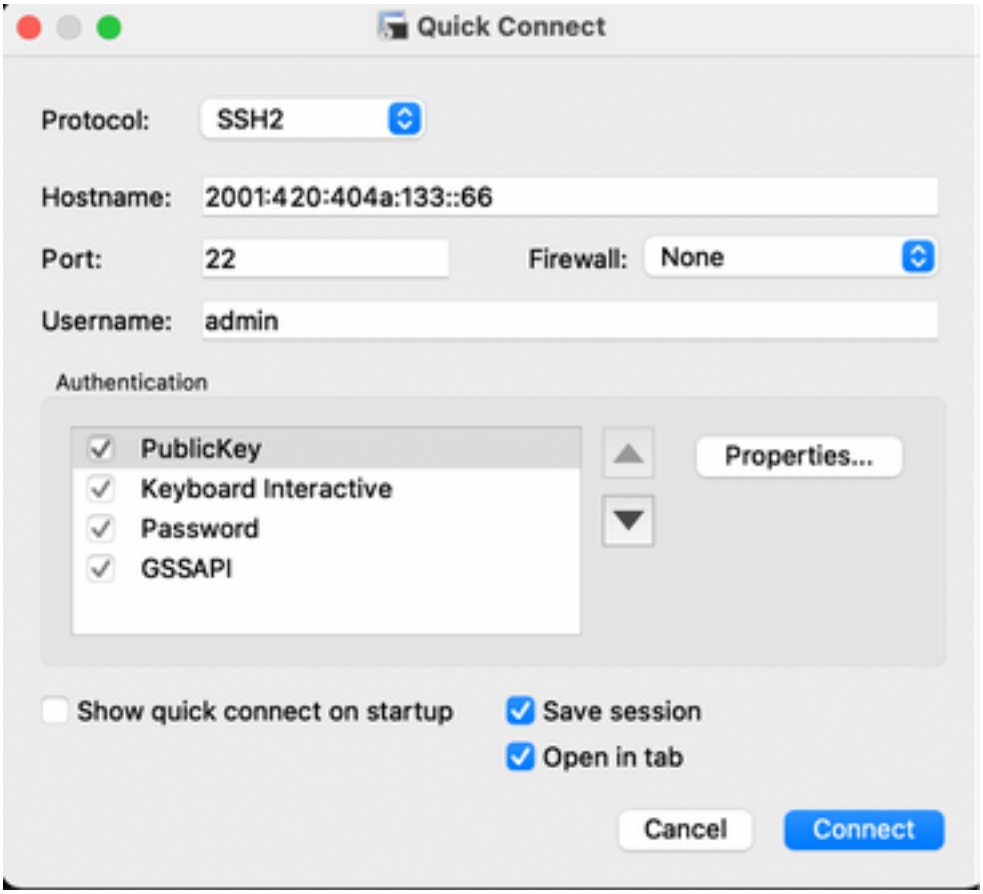


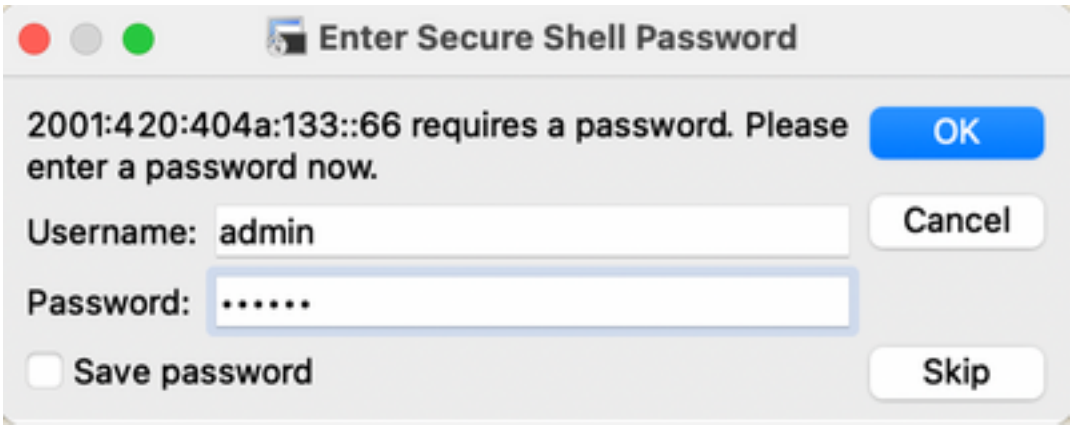


SSH Cisco ISE

Note: Secure CRT est utilisé dans cet exemple.

Étape 1. Ouvrez une nouvelle session SSH et tapez l'adresse IPv6 suivie du nom d'utilisateur et du mot de passe Admin.





Étape 2. Exécutez la commande **show interface gigabitEthernet 0** pour valider l'adresse IPv6 configurée sur Eth0 (interface) :

ems-ise-mnt001/admin# show interface gigabitEthernet 0

GigabitEthernet 0

flags=4163<UP, BROADCAST, RUNNING, MULTICAST> mtu 1500

inet 10.52.13.175 masque de réseau 255.255.255.0 diffusion 10.52.13.255

inet6 2001:420:404a:133:117:4cd6:4dfe:811 prefixlen 64 scopeid 0x0<global>

inet6 2001:420:404a:133::66 prefixlen 64 scopeid 0x0<global>

éther 00:50:56:89:74:4f txqueuelen 1000 (Ethernet)

Paquets RX 17683390 octets 15013193200 (13,9 GiB)

Erreurs RX 0 abandonnées 7611 dépasse 0 trame 0

Paquets TX 16604234 octets 2712406084 (2,5 GiB)

Erreurs TX 0 0 0 dépassements 0 collisions de porteuse 0

Étape 3. Exécutez la commande **show users** pour valider l'adresse IPv6 source.

ems-ise-mnt001/admin# show users

JOURNÉE DE CONNEXION DE L'HÔTE TTY DU RÔLE D'UTILISATEUR

admin Admin 10.82.237.218 pts/0 Lun 6 déc. 19:47:38 2021

admin Admin **2001:420:c0c4:1005::589** pts/2 Lun 6 déc 20:09:04 20

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Validation des communications avec l'utilisation de la commande ping pour l'adresse IPv6 sur MacOS

Étape 1. Ouvrez un terminal et utilisez la commande **ping6 <adresse IPv6>** pour valider la réponse de communication d'ISE

M-65PH :~ ecanogut$ ping6 2001:420:404a:133::66

PING6(56=40+8+8 octets) 2001:420:c0c4:1005::589 —> 2001:420:404a:133::66

16 octets à partir de 2001:420:404a:133::66, icmp_seq=0 hlim=51 time=229,774 ms

16 octets à partir de 2001:420:404a:133::66, icmp_seq=1 hlim=51 time=231,262 ms

16 octets à partir de 2001:420:404a:133::66, icmp_seq=2 hlim=51 time=230,545 ms

16 octets à partir de 2001:420:404a:133::66, icmp_seq=3 hlim=51 time=320.207 ms

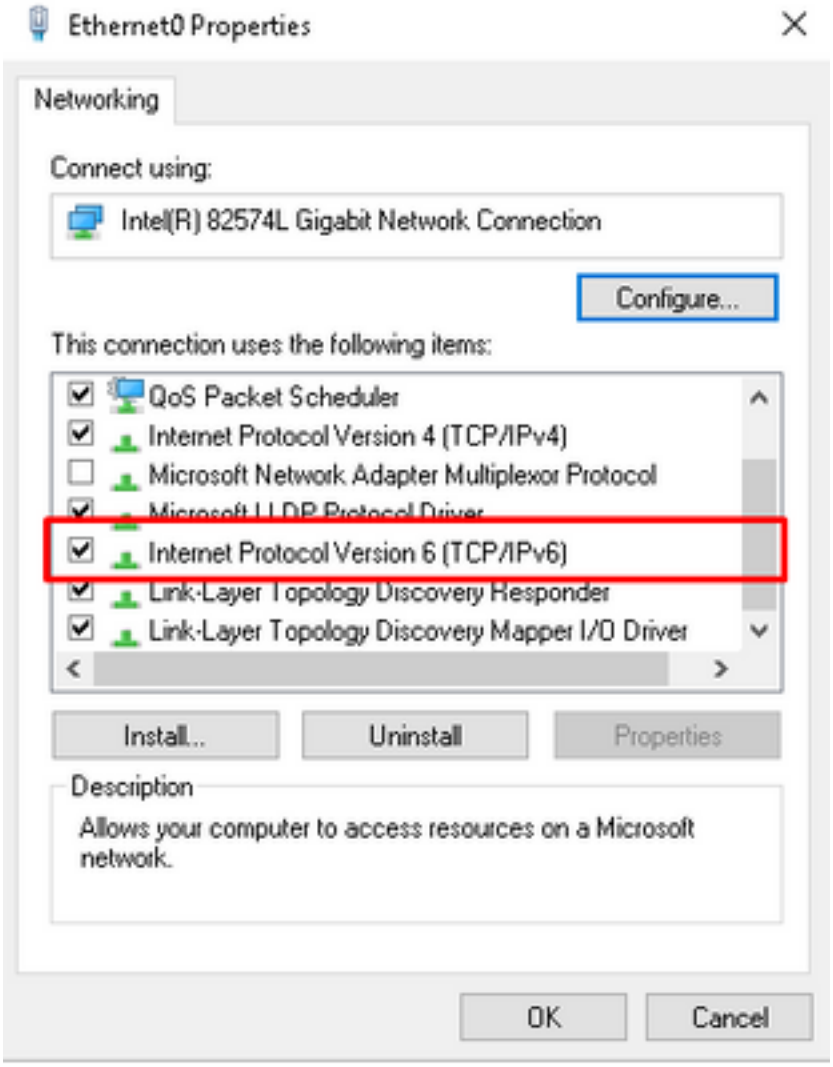
16 octets à partir de 2001:420:404a:133::66, icmp_seq=4 hlim=51 time=236.246

Validation des communications avec l'utilisation de la commande ping pour l'adresse IPv6 sous Windows

Pour que la commande ping IPv6 fonctionne, Ipv6 doit être activé sur la configuration réseau.

Étape 1. Sélectionnez Démarrer > Paramètres > Panneau de configuration > Réseau et Internet > Centre Réseau et partage > Modifier les paramètres de la carte.

Étape 2. La validation de la version 6 du protocole Internet (TCP/IPv6) est activée, cochez la case si cette option est désactivée.



Étape 3 : Ouvrez un terminal et utilisez la commande **ping <adresse IPv6> ou ping -6 <ise_node_fqdn>** pour valider la réponse de communication d'ISE

> ping 2001:420:404a:133::66

Validation de la communication avec l'utilisation de la commande ping pour l'adresse IPv6 sur Ping IPv6 sous Linux (Ubuntu, Debian, Mint, CentOS, RHEL).

Étape 1. Ouvrez un terminal et utilisez la commande **ping <adresse IPv6> ou ping -6 <ise_node_fqdn>** pour valider la réponse de communication d'ISE

ping $ 2001:420:404a:133::66

Validation de la communication avec l'utilisation de la commande ping pour l'adresse IPv6 sur Envoyez une requête ping à IPv6 dans Cisco (IOS)

Note: Cisco fournit la commande ping en mode exec afin de vérifier la connectivité aux cibles IPv6. La commande ping requiert le paramètre ipv6 et l'adresse IPv6 de la cible.

Étape 1. Connectez-vous au périphérique Cisco IOS en mode exec et exécutez la commande **ping Ipv6 <Adresse IPv6>** pour valider la réponse de communication de ISE

 # ping ipv6 2001:420:404a:133::66

Note: En outre, vous pouvez également prendre des paquets de ISE pour valider le trafic IPv6 de revenu

Référence supplémentaire : https://community.cisco.com/t5/security-documents/cisco-ise-identity-services-engine-ipv6-support/ta-p/4480704#toc-hId-1800166300

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.