Konfigurieren des Cisco ISE 3.0-Admin-Portals und der CLI mit IPv6

Inhalt

[Einleitung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Konfigurieren](#)
[Netzwerkdiagramm](#)
[Überprüfung](#)
[Fehlerbehebung](#)

Einleitung

Dieses Dokument beschreibt das Verfahren zur Konfiguration der Cisco Identity Services Engine (ISE) mit IPv6 für das Admin-Portal und die CLI.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Identity Services Engine (ISE)
- IPv6

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- ISE Version 3.0 Patch 4.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

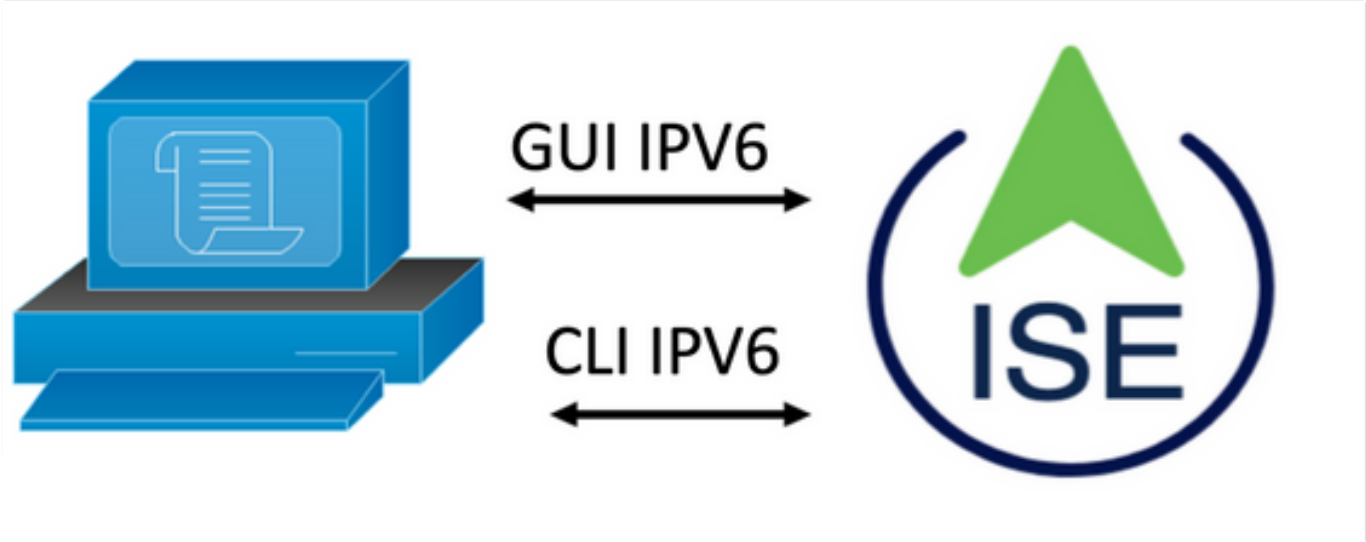
In den meisten Fällen kann die Cisco Identity Services Engine mit einer IPv4-Adresse konfiguriert werden, um die ISE über die Benutzeroberfläche (GUI) und die CLI zu verwalten. Die Anmeldung beim Admin-Portal erfolgt über eine IPv6-Adresse, ab ISE Version 2.6 über eine IPv6-Adresse. Beim Einrichtungsassistenten und über die CLI kann eine IPv6-Adresse für Eth0 (Schnittstelle)

konfiguriert werden. Bei konfigurierter IPv6-Adresse wird empfohlen, eine IPv4-Adresse (zusätzlich zur IPv6-Adresse) für die Cisco ISE-Knotenkommunikation zu konfigurieren. Daher ist ein Dual-Stack (Kombination von IPv4 und IPv6) erforderlich.
Secure Socket Shell (SSH) kann mit IPv6-Adressen konfiguriert werden. Die Cisco ISE unterstützt mehrere IPv6-Adressen auf jeder Schnittstelle, und diese IPv6-Adressen können über die CLI konfiguriert und verwaltet werden.

Konfigurieren

Netzwerkdiagramm

Das Bild zeigt ein Beispiel für ein Netzwerkdiagramm.



ISE-Konfiguration

Anmerkung: Standardmäßig ist die IPv6-Adressoption in allen ISE-Schnittstellen aktiviert. Es empfiehlt sich, diese Option zu deaktivieren, wenn sie nicht verwendet werden soll. Geben Sie ggf. **no ipv6 address autoconfig** und/oder **no ipv6 enable ein**. Mit dem Befehl **show run** können Sie überprüfen, für welche Schnittstellen ipv6 aktiviert ist.

Anmerkung: Die Konfiguration geht davon aus, dass die Cisco ISE bereits mit IPv4-Adressierung konfiguriert ist.

ems-ise-mnt001/admin# Terminal konfigurieren

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

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

% Durch Ändern der IP-Adresse können ise Services neu starten

Fahren Sie mit der Änderung der IP-Adresse fort? J/N [N]:**Y**

Anmerkung: Durch das Hinzufügen oder Ändern der IP-Adressierung auf einer Schnittstelle werden die Dienste neu gestartet.

Schritt 2: Führen Sie nach dem Neustart der Dienste den Befehl show application status ise (Anwendungsstatus anzeigen) aus, um zu überprüfen, ob die Dienste ausgeführt werden:

ems-ise-mnt001/admin# **Anwendungsstatus anzeigen**

ISE-PROZESSNAMEN - PROZESS-ID

—

Datenbank-Listener mit 1252

Datenbankserver mit 74 PROZESSEN

Anwendungsserver mit 1134

Profiler-Datenbank mit 6897

ISE-Indexmodul mit 14121

AD-Anschluss läuft 17184

M&T-Sitzungsdatenbank mit 6681

M&T Log-Prozessor mit 11337

Dienst der Zertifizierungsstelle, ausgeführt 17044

EST-Dienst mit 10559

SXP-Moduldienst deaktiviert

Docker-Daemon läuft 3579

TC-NAC-Service deaktiviert

pxGrid Infrastructure Service mit 9712

pxGrid Publisher Subscriber Service mit 9791

pxGrid Connection Manager mit 9761

pxGrid-Controller mit 9821

PassiveID-WMI-Dienst deaktiviert

PassiveID Syslog-Dienst deaktiviert

PassiveID-API-Dienst deaktiviert

PassiveID Agent-Dienst deaktiviert

PassiveID-Endpoint-Dienst deaktiviert

PassiveID SPAN-Dienst deaktiviert

DHCP-Server (dhcpd) deaktiviert

DNS-Server (Name) deaktiviert

ISE Messaging Service mit 4260

ISE API Gateway-Datenbankservice mit 5805

ISE API Gateway Service mit 8973

Segmentierungsrichtliniendienst deaktiviert

REST-Auth-Dienst deaktiviert

SSE Connector deaktiviert

Schritt 3: Geben Sie den Befehl **show run** aus, um IPv6 zu validieren, wurde auf Eth0 (Schnittstelle) konfiguriert:

ems-ise-mnt001/admin# show run

Konfiguration wird generiert...

!

hostname ems-ise-mnt001

!

ip domain-name ise.com

!

IPv6 aktivieren

!

interface GigabitEthernet 0

ip address 10.52.13.175 255.255.255.0

IPv6-Adresse 2001:420:404a:133::66/64

IPv6-Adresse Autoconfig

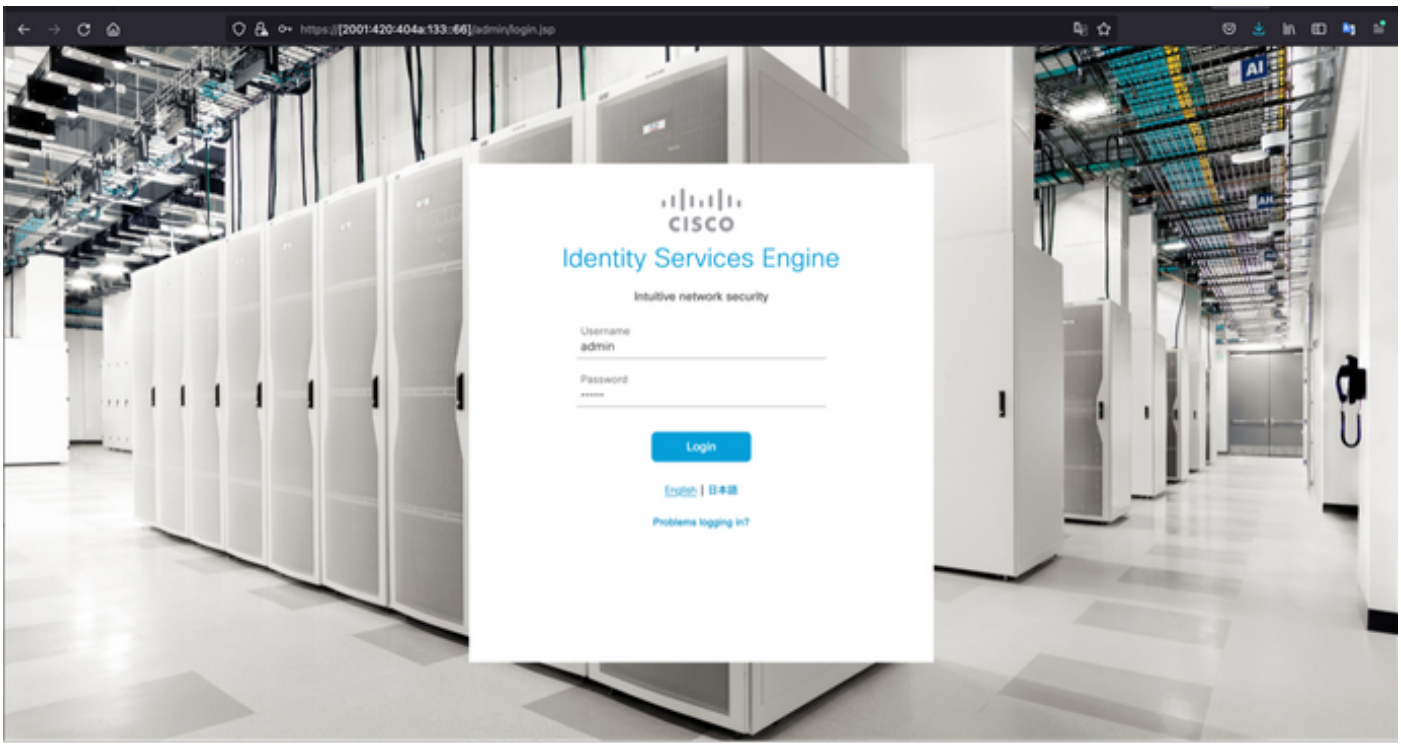
IPv6 aktivieren

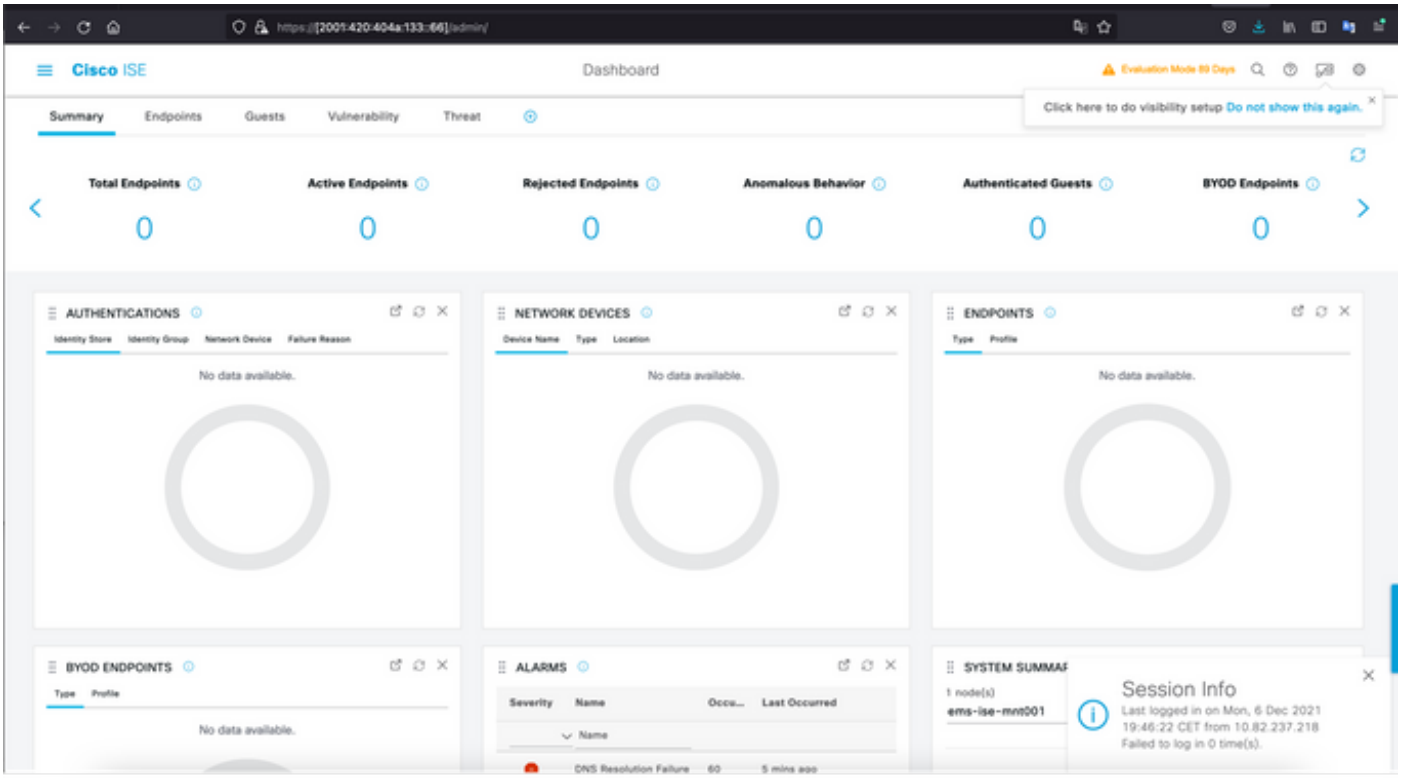
!

Überprüfung

Cisco ISE-Benutzeroberfläche

Schritt 1: Öffnen Sie einen neuen Fensterbrowser, und geben Sie https://[2001:420:404a:133::66] ein. Beachten Sie, dass die IPv6-Adresse in Klammern stehen muss.

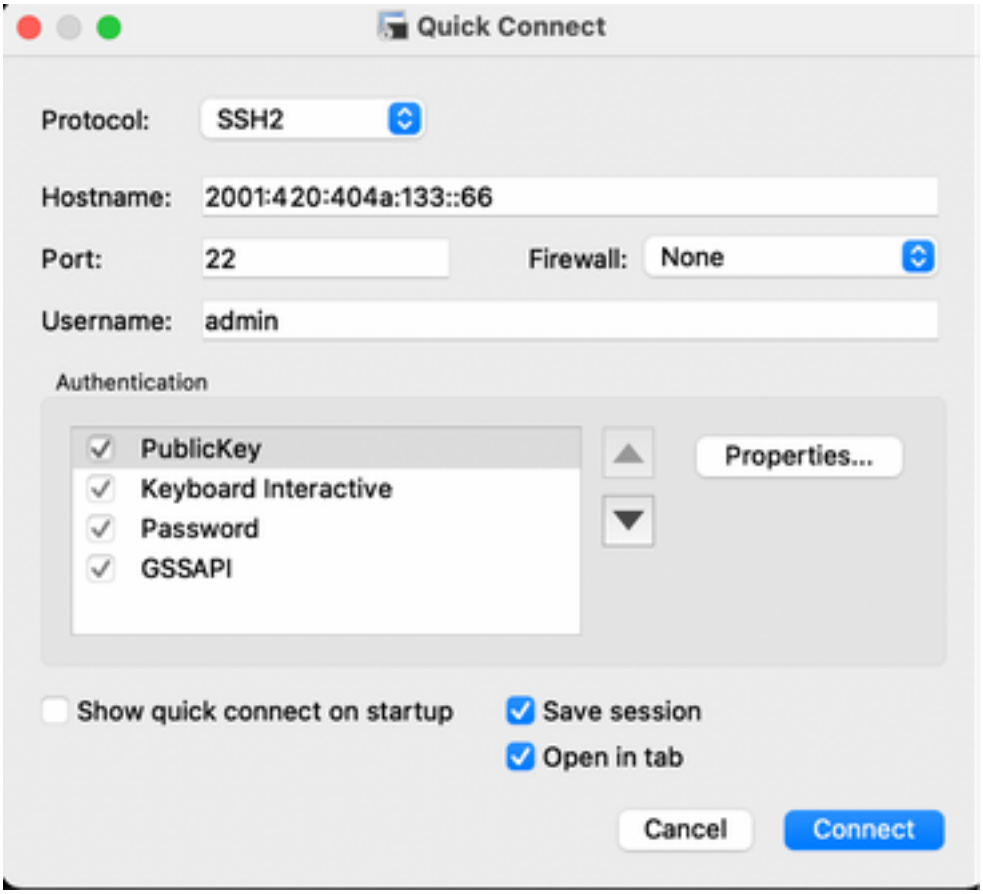


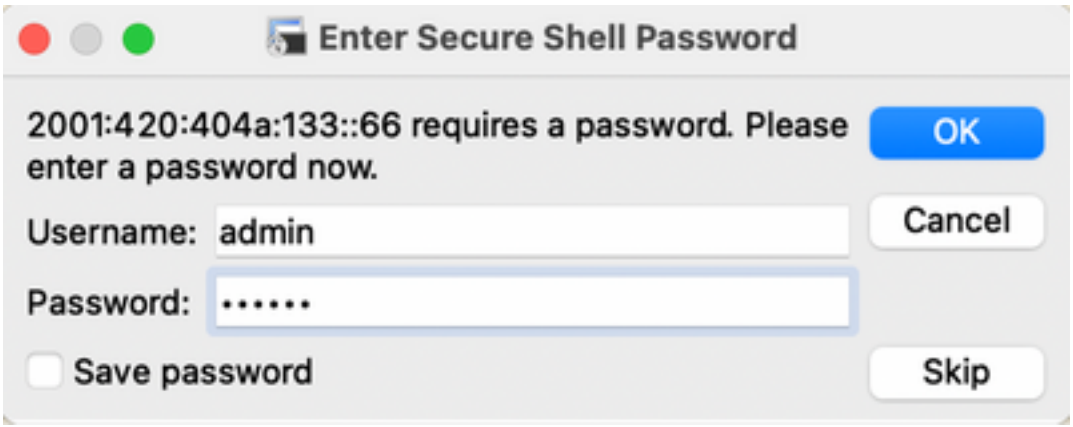


Cisco ISE SSH

Anmerkung: In diesem Beispiel wird Secure CRT verwendet.

Schritt 1: Öffnen Sie eine neue SSH-Sitzung, und geben Sie die IPv6-Adresse gefolgt von Benutzername und Kennwort für den Administrator ein.





Schritt 2: Geben Sie den Befehl show interface gigabitEthernet 0 ein, um die auf Eth0 (Schnittstelle) konfigurierte IPv6-Adresse zu validieren:

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

GigabitEthernet 0

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

inet 10.52.13.175 Netzmaske 255.255.255.0 Broadcast 10.52.13.255

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

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

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

RX-Pakete 17683390 Byte 15013193200 (13,9 GiB)

RX-Fehler 0 verworfen 7611 überschreitet 0 Frame 0

TX-Pakete 16604234 Byte 2712406084 (2,5 GiB)

TX errors 0 drop 0 overläufe 0 Carrier 0 Kollisionen 0

Schritt 3: Geben Sie den Befehl show users ein, um die IPv6-Quelladresse zu validieren.

ems-ise-mnt001/admin# show users

BENUTZERNAME ROLE HOST TTY LOGIN DATETITIME

Administrator, 10.82.237.218 Punkt/0 Mo. Dez. 6 19:47:38 2021

Admin **2001:420:c0c4:1005::589** pts/2 Mo. Dez. 6 20:09:04 20

Fehlerbehebung

In diesem Abschnitt finden Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

Kommunikationsvalidierung mit Ping für IPv6-Adressen unter MacOS

Schritt 1: Öffnen Sie ein Terminal, und verwenden Sie den Befehl **ping6 <IPv6-Adresse>,** um die Kommunikationsantwort von der ISE zu überprüfen.

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

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

16 Byte ab 2001:420:404a:133::66, icmp_seq=0 hlim=51 time=229,774 ms

16 Byte von 2001:420:404a:133::66, icmp_seq=1 hlim=51 time=231,262 ms

16 Byte von 2001:420:404a:133::66, icmp_seq=2 hlim=51 time=230,545 ms

16 Byte von 2001:420:404a:133::66, icmp_seq=3 hlim=51 time=320,207 ms

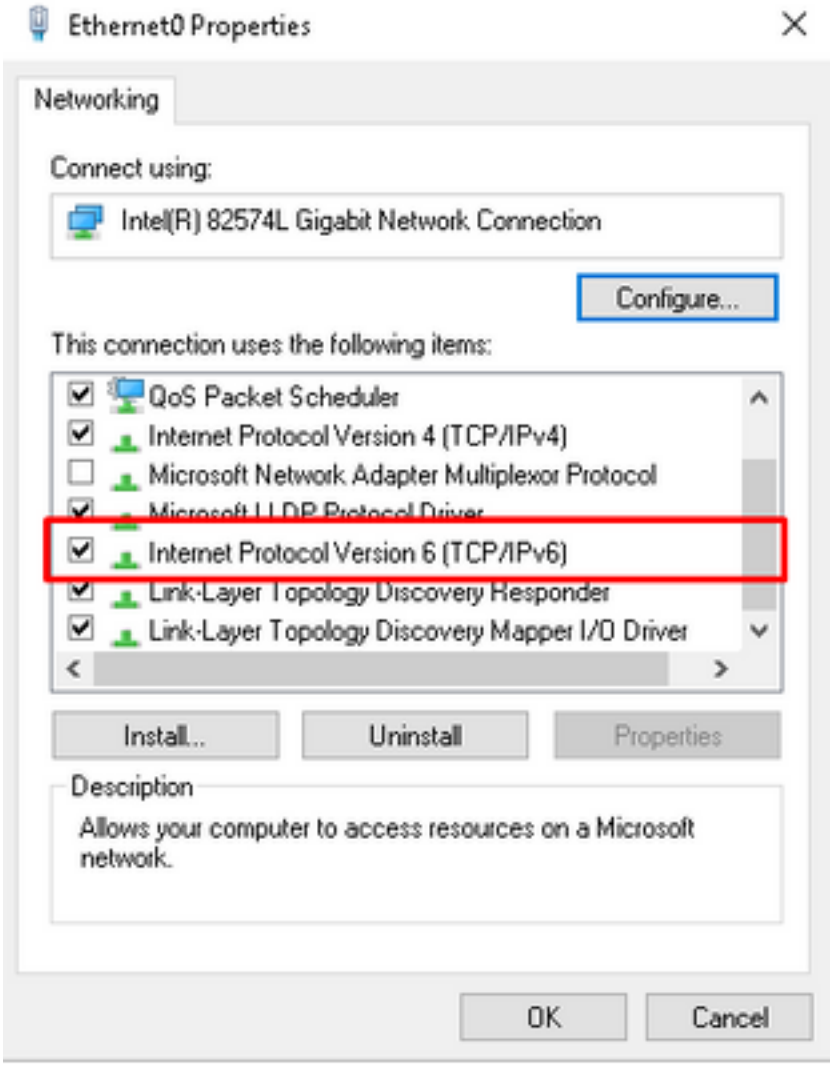
16 Byte ab 2001:420:404a:133::66, icmp_seq=4 hlim=51 time=236.246

Kommunikationsvalidierung mit Ping für IPv6-Adressen unter Windows

Damit der Befehl "IPv6 ping" funktioniert, muss IPv6 in der Netzwerkkonfiguration aktiviert werden.

Schritt 1: Wählen Sie Start > Einstellungen > Systemsteuerung > Netzwerk und Internet > Netzwerk- und Freigabecenter > Adaptereinstellungen ändern aus.

Schritt 2: Wenn Internet Protocol Version 6 (TCP/IPv6) aktiviert ist, aktivieren Sie das Kontrollkästchen, falls diese Option deaktiviert ist.



Schritt 3: Öffnen Sie ein Terminal, und verwenden Sie den Befehl **ping <IPv6-Adresse> oder ping -6 <ise_node_fqdn>,** um die Kommunikationsantwort von der ISE zu überprüfen.

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

Kommunikationsvalidierung mit Ping für IPv6-Adresse unter Ping IPv6 in Linux (Ubuntu, Debian, Mint, CentOS, RHEL).

Schritt 1: Öffnen Sie ein Terminal, und verwenden Sie den Befehl **ping <IPv6-Adresse> oder ping -6 <ise_node_fqdn>,** um die Kommunikationsantwort von der ISE zu überprüfen.

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

Kommunikationsvalidierung mit Ping für IPv6-Adresse unter Ping IPv6 in Cisco (IOS)

Anmerkung: Cisco stellt den Befehl ping im exec-Modus bereit, um die Verbindung zu den IPv6-Zielen zu überprüfen. Für den Ping-Befehl sind der IPv6-Parameter und die IPv6-Adresse des Ziels erforderlich.

Schritt 1: Melden Sie sich im exec-Modus beim Cisco IOS-Gerät an, und geben Sie den Befehl **ping IPv6 <IPv6-Adresse>** aus, um die Kommunikationsantwort von der ISE zu überprüfen.

 # ping IPv6 2001:420:404a:133:66

Anmerkung: Darüber hinaus können Sie auch Kapital aus der ISE nehmen, um den IPv6-Datenverkehr zu validieren.

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