

Configuración del portal de administración y la CLI de Cisco ISE 3.0 con IPv6

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Verificación](#)

[Troubleshoot](#)

Introducción

Este documento describe el procedimiento para configurar Cisco Identity Services Engine (ISE) con IPv6 para Admin Portal y CLI.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Identity Services Engine (ISE)
- IPv6

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- ISE versión 3.0 Parche 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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

En la mayoría de los casos, Cisco Identity Services Engine se puede configurar con una dirección Ipv4 para administrar ISE a través de la interfaz de usuario (GUI) y el inicio de sesión de CLI en el Portal de administración; sin embargo, desde la versión 2.6 de ISE y posterior, Cisco ISE se puede administrar a través de una dirección IPv6 y configurar una dirección IPv6 en Eth0 (interfaz) cuando se configura el asistente de configuración y a través de CLI. Cuando se

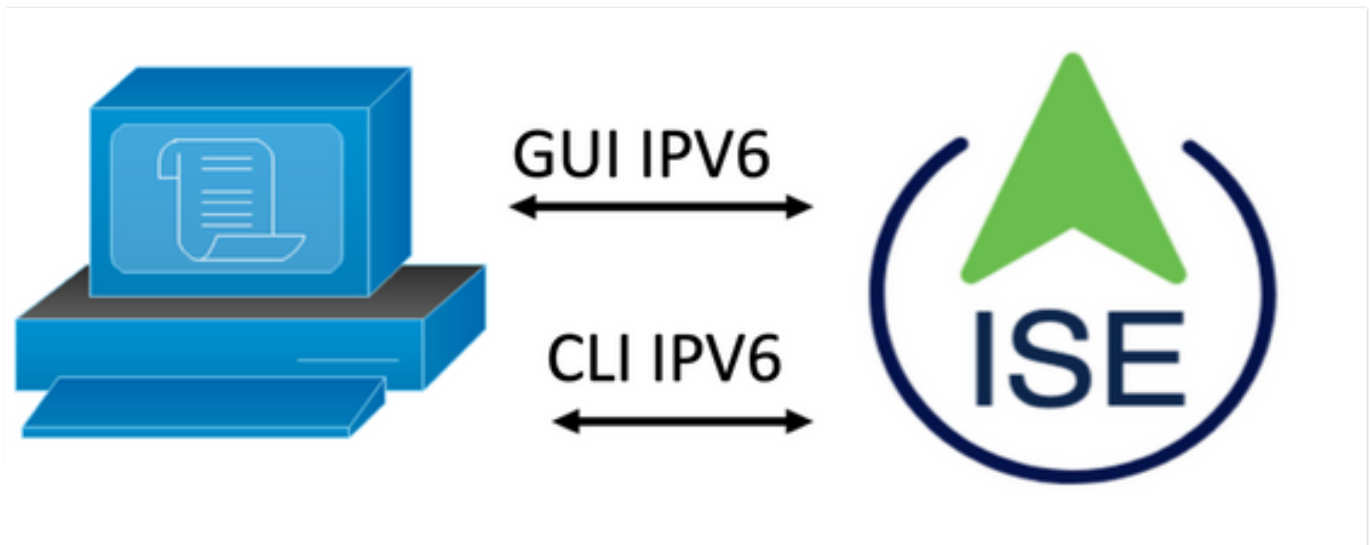
configura la dirección IPv6, se recomienda configurar una dirección IPv4 (además de la dirección IPv6) para la comunicación del nodo Cisco ISE. Por lo tanto, se requiere una doble pila (combinación de IPv4 e IPv6).

Es posible configurar Secure Socket Shell (SSH) con direcciones IPv6. Cisco ISE admite varias direcciones IPv6 en cualquier interfaz y estas direcciones IPv6 se pueden configurar y administrar mediante CLI.

Configurar

Diagrama de la red

La imagen proporciona un ejemplo de un diagrama de red



Configuración de ISE

Nota: De forma predeterminada, la opción de dirección ipv6 está activada en todas las interfaces ISE. Es una práctica recomendada desactivar esta opción si no se planea utilizarla ejecute **no ipv6 address autoconfig** y/o **no ipv6 enable** si procede. Utilice el comando **show run** para validar qué interfaces tienen ipv6 habilitado.

Nota: La configuración considera que Cisco ISE ya está configurado con direccionamiento IPv4.

```
ems-ise-mnt001/admin# Configure terminal
```

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

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

% El cambio de la dirección IP puede hacer que se reinicie el servicio ise

¿Desea continuar con el cambio de dirección IP? Y/N [N]:Y

Nota: Al agregar o cambiar el direccionamiento IP en una interfaz, los servicios se reinician

Paso 2. Una vez que se hayan reiniciado los servicios, ejecute el comando **show application status ise** para validar los servicios que se están ejecutando:

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

ID DE PROCESO DE NOMBRE DE PROCESO ISE

—

Receptor de base de datos que ejecuta 1252

Servidor de base de datos que ejecuta 74 PROCESOS

Servidor de aplicaciones que ejecuta 11134

Base de datos del generador de perfiles ejecutando 6897

ISE Indexing Engine que ejecuta 14121

Conector AD que ejecuta 17184

Base de datos de sesiones de M&T que ejecuta 6681

Procesador de registro de M&T que ejecuta 11337

Servicio de autoridad certificadora que ejecuta 17044

Servicio EST ejecutando 10559

Servicio de motor SXP desactivado

Docker Daemon ejecutando 3579

Servicio TC-NAC desactivado

servicio de infraestructura pxGrid que ejecuta 9712

servicio de suscriptor de editor de pxGrid que ejecuta 9791

administrador de conexiones pxGrid que ejecuta 9761

controlador pxGrid que ejecuta 9821

Servicio WMI de ID pasivo deshabilitado

Servicio de registro del sistema pasivoID deshabilitado

Servicio de API pasivoID deshabilitado

Servicio de agente pasivoID deshabilitado

Servicio de terminal PasivoID desactivado

Servicio SPAN PasivoID deshabilitado

Servidor DHCP (dhcpd) deshabilitado

Servidor DNS (denominado) deshabilitado

Servicio de mensajería ISE ejecutando 4260

ISE API Gateway Database Service con 5805

ISE API Gateway Service que ejecuta 8973

Servicio de política de segmentación deshabilitado

Servicio de autenticación de REST desactivado

Conector SSE desactivado

Paso 3. Ejecute el comando show run para validar IPv6 se ha configurado en Eth0 (Interfaz):

ems-ise-mnt001/admin# show run

Generando configuración...

!

hostname ems-ise-mnt001

!

ip domain-name ise.com

!

ipv6 enable

!

interface GigabitEthernet 0

IP address 10.52.13.175 255.255.255.0

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

ipv6 address autoconfig

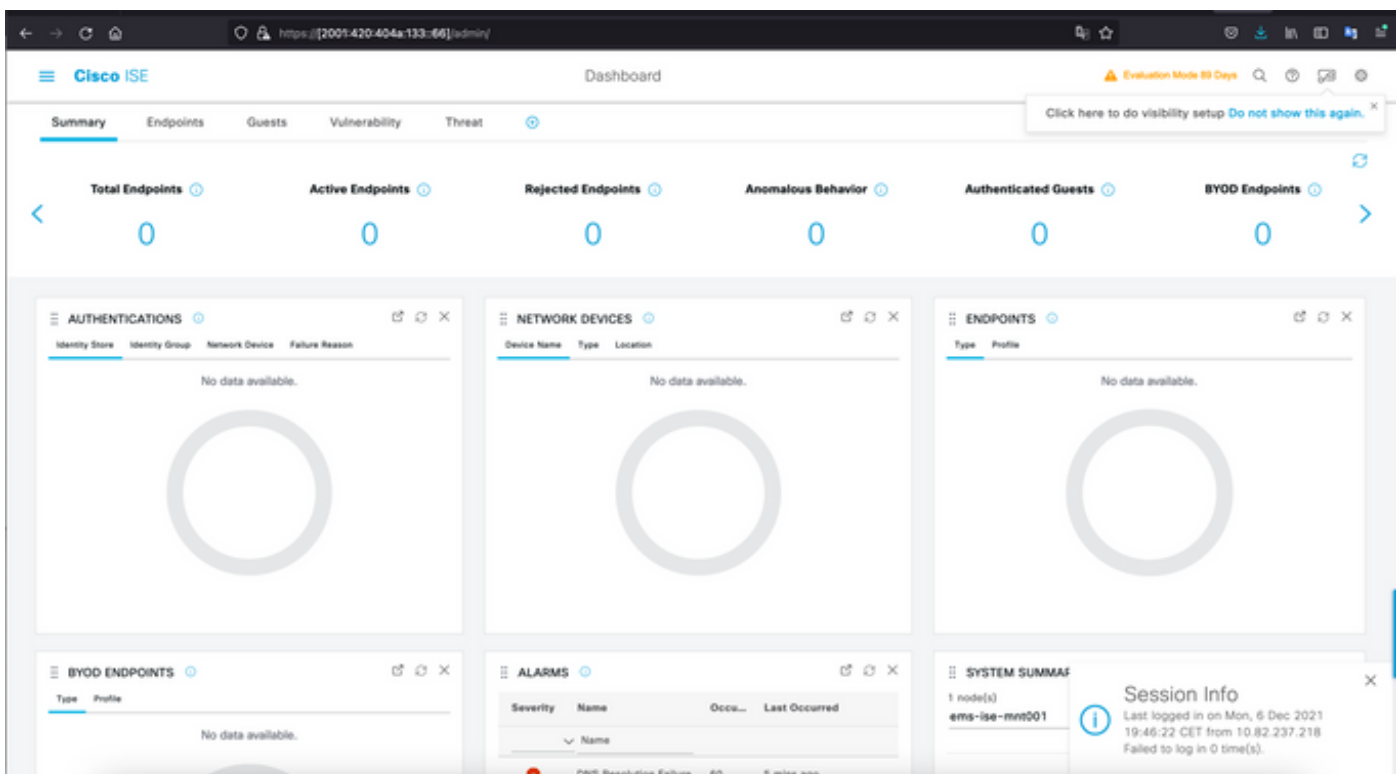
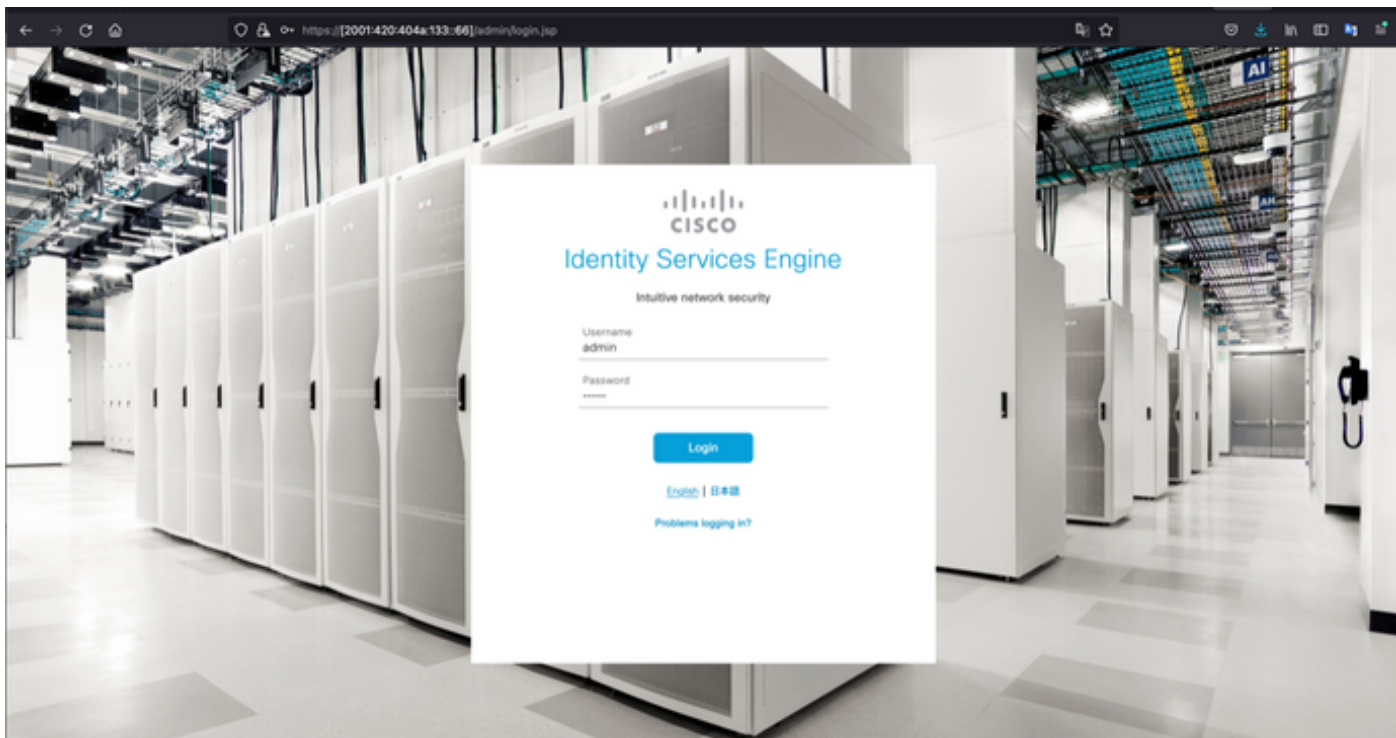
ipv6 enable

!

Verificación

Interfaz de usuario de Cisco ISE

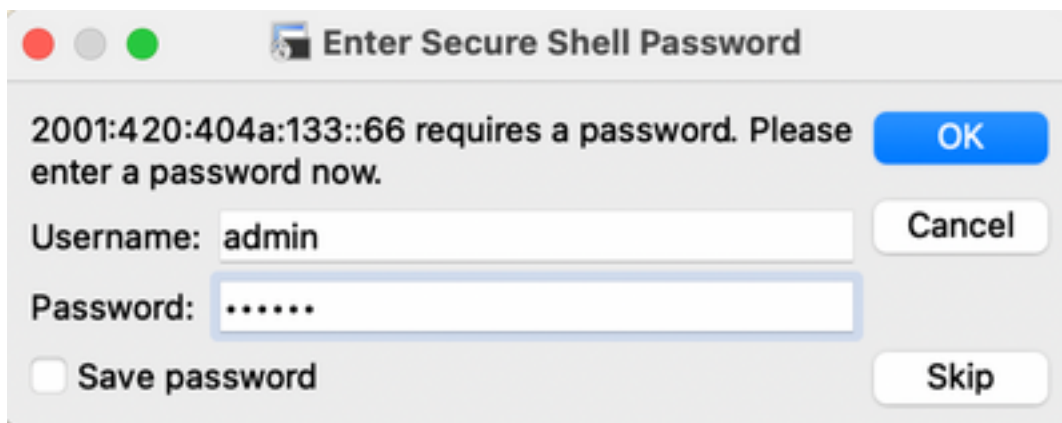
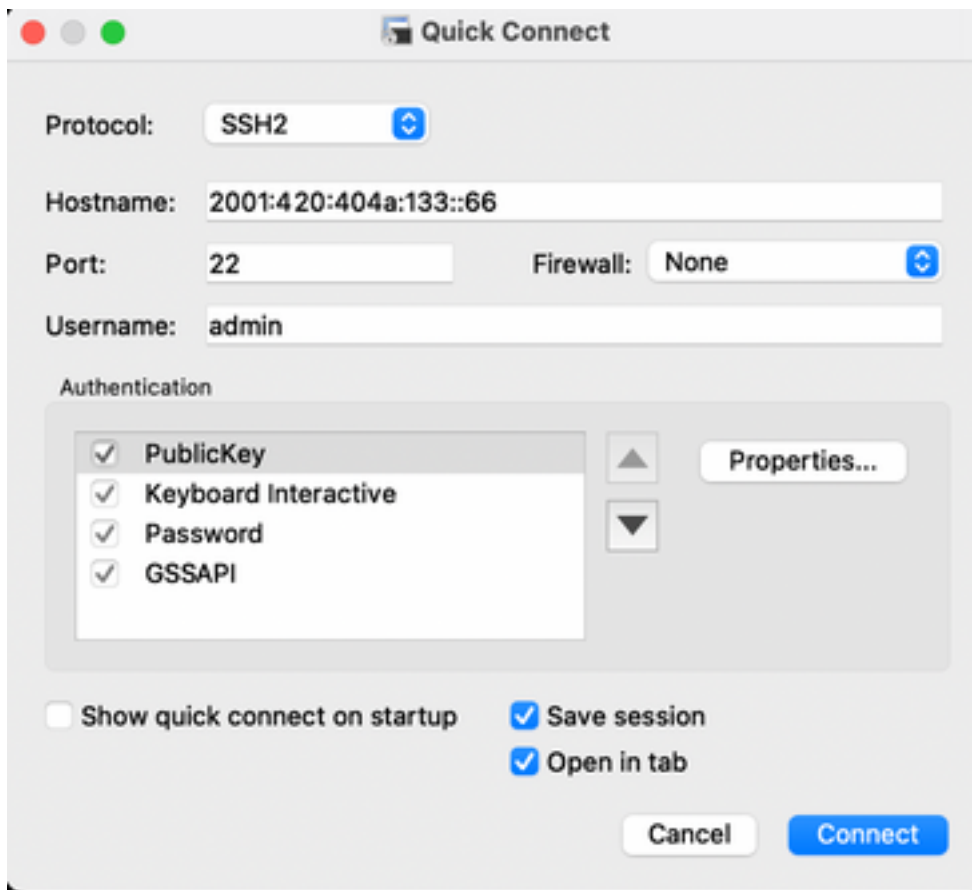
Paso 1. Abra un nuevo navegador de ventanas y escriba [https://\[2001:420:404a:133::66\]](https://[2001:420:404a:133::66]). Tenga en cuenta que la dirección IPv6 debe estar entre paréntesis.



SSH de Cisco ISE

Nota: En este ejemplo se utiliza Secure CRT.

Paso 1. Abra una nueva sesión SSH y escriba la dirección IPv6 seguida del nombre de usuario y la contraseña Admin.



Paso 2. Ejecute el comando `show interface gigabitEthernet 0` para validar la dirección IPv6 configurada en Eth0 (Interface):

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

```
GigabitEthernet 0
```

```
indicadores=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
```

```
inet 10.52.13.175 netmask 255.255.255.0 broadcast 10.52.13.255
```

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

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

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

Paquetes RX 17683390 bytes 15013193200 (13,9 GiB)

Los errores RX 0 descartaron 7611 sobrecarga 0 frame 0

Paquetes TX 16604234 bytes 2712406084 (2,5 GiB)

TX errors 0 drop 0 sobrecarga 0 carrier 0 colisiones 0

Paso 3. Ejecute el comando `show users` para validar la dirección IPv6 de origen.

```
ems-ise-mnt001/admin# show users
```

```
USERNAME ROLE HOST TTY LOGIN DATETIME
```

```
admin Admin 10.82.237.218 pts/0 Mon Dic 6 19:47:38 2021
```

```
admin Admin 2001:420:c0c4:1005::589 pts/2 Mon Dic 6 20:09:04 20
```

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Validación de la comunicación con el uso de ping para la dirección IPv6 en MacOS

Paso 1. Abra un terminal y utilice el comando `ping6 <IPv6 Address>` para validar la respuesta de comunicación de ISE

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

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

```
16 bytes de 2001:420:404a:133::66, icmp_seq=0 hlim=51 tiempo=229.774 ms
```

```
16 bytes de 2001:420:404a:133::66, icmp_seq=1 hlim=51 tiempo=231.262 ms
```

```
16 bytes de 2001:420:404a:133::66, icmp_seq=2 hlim=51 tiempo=230.545 ms
```

```
16 bytes de 2001:420:404a:133::66, icmp_seq=3 hlim=51 tiempo=320.207 ms
```

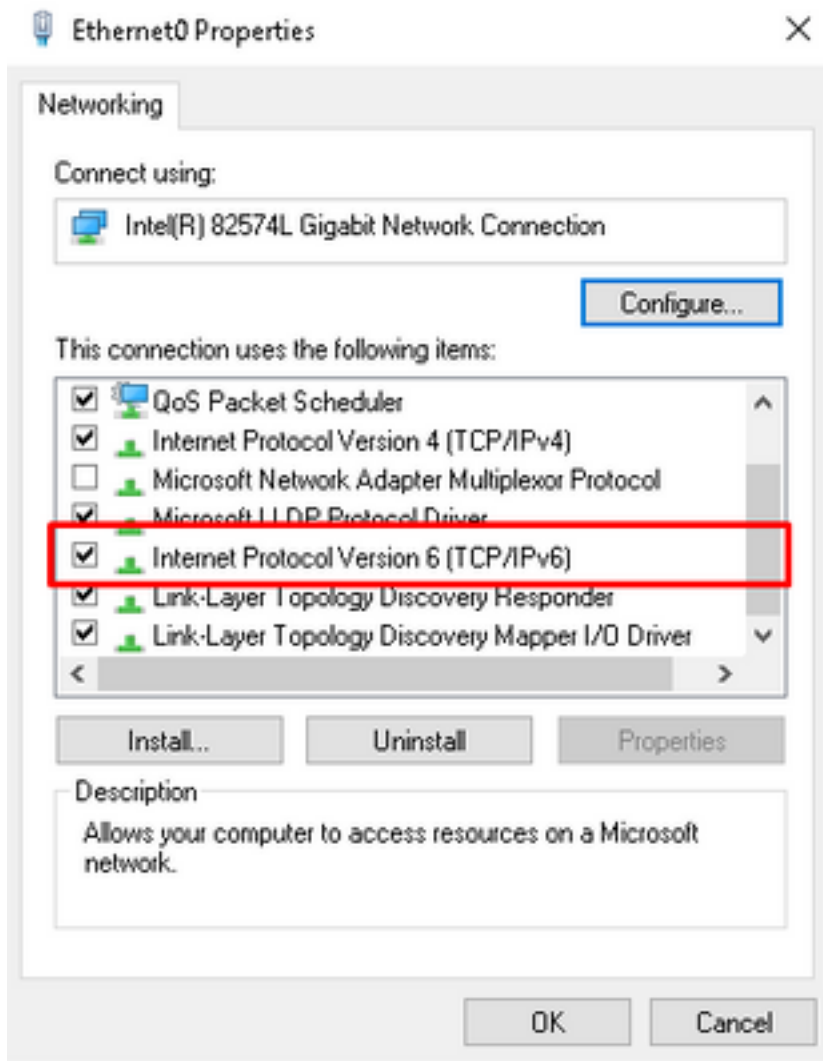
```
16 bytes de 2001:420:404a:133::66, icmp_seq=4 hlim=51 tiempo=236.246
```

Validación de la comunicación con el uso de ping para la dirección IPv6 en Windows

Para que el comando ping IPv6 funcione, se debe habilitar Ipv6 en la configuración de red.

Paso 1. Seleccione Start > Settings > Control Panel > Network and Internet > Network and Sharing Center > Change adapter settings .

Paso 2. Validar el protocolo de Internet versión 6 (TCP/IPv6) está activado. Haga clic en la casilla de verificación en caso de que esta opción esté desactivada.



Paso 3: Abra un terminal y utilice el comando `ping <IPv6 Address>` o `ping -6 <ise_node_fqdn>` para validar la respuesta de comunicación de ISE

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

Validación de la comunicación con el uso de ping para la dirección IPv6 en Ping IPv6 In Linux (Ubuntu, Debian, Mint, CentOS, RHEL).

Paso 1. Abra un terminal y utilice el comando `ping <IPv6 Address>` o `ping -6 <ise_node_fqdn>` para validar la respuesta de comunicación de ISE

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

Validación de la comunicación con el uso de ping para la dirección IPv6 en Ping IPv6 en Cisco (IOS)

Nota: Cisco proporciona el comando ping en modo exec para verificar la conectividad con los destinos IPv6. El comando ping requiere el parámetro `ipv6` y la dirección IPv6 del destino.

Paso 1. Inicie sesión en el dispositivo Cisco IOS en el modo exec y ejecute el comando `ping ipv6 <IPv6 Address>` para validar la respuesta de comunicación de ISE

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


Nota: Además, también puede tomar paquetes de ISE para validar los ingresos del tráfico IPv6

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