

Aprovisionamiento seguro de dispositivos de red

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Generar e instalar certificado SSL en DNAC](#)

[Procedimiento](#)

[Configuración del Servidor DHCP](#)

[Información Relacionada](#)

Introducción

Este documento describe el enfoque paso a paso para que un dispositivo Cisco incorpore la red de forma segura a través de la búsqueda de DNS.

Prerequisites

Requirements

- Conocimientos básicos de la gestión de Cisco DNA Center (DNAC)
- Conocimiento básico de Certificados SSL

Componentes Utilizados

Este documento se basa en la versión 2.1.x de Cisco DNA Center (DNAC).

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

La búsqueda de DNS es una forma recomendada de integración cuando el dispositivo de red y el controlador Cisco DNA Center (DNAC) se encuentran en sitios remotos y desea aprovisionar un dispositivo de red a través de Internet pública.

Hay diferentes formas de incorporar un dispositivo de red con el uso de Cisco Plug & Play Day0.

- Opciones específicas del proveedor de DHCP
- búsqueda de DNS

- Cisco Cloud Redirection

Para tener una comunicación segura a través de la Internet pública, debe instalar un certificado seguro en DNAC. Siga este documento para configurar un servidor DHCP, un servidor DNS, generar e instalar un certificado SSL. Si ya tiene la clave certificate + y solo necesita instalarla en DNAC, siga el documento del paso 11. En este documento:

- El dispositivo Cat9K es el agente PNP.
- pnpserver.cisco.com es el nombre FQDN del controlador DNAC.
- El switch de Cisco está configurado como servidor DNS y servidor DHCP.

Generar e instalar certificado SSL en DNAC

De forma predeterminada, DNAC viene con un certificado autofirmado preinstalado válido para los dispositivos de red integrados en una red privada. Sin embargo, Cisco recomienda que importe un certificado X.509 válido de su CA interna para una comunicación segura con el dispositivo de red incorporado desde una ubicación remota a través de Internet pública.

Este es un ejemplo para descargar e instalar el certificado Open SSL emitido por Cisco en DNAC.

Para descargar el certificado, primero debe crear una CSR.

Procedimiento

Paso 1. Utilice un cliente SSH para iniciar sesión en el clúster de Cisco DNA Center y crear una carpeta temporal en `/home/maglev`; por ejemplo, ingrese el comando `mkdir tls-cert;cd tls-cert` mientras se encuentra en el directorio principal.

Paso 2. Antes de continuar, asegúrese de que el nombre de host (FQDN) del Cisco DNA Center esté configurado en el momento de la configuración del Cisco DNA Center con el uso del comando `maglev cluster network display`:

Input :

```
$maglev cluster network display
```

Output :

```
cluster_network:  
cluster_dns: 169.254.20.10  
cluster_hostname: fqdn.cisco.com
```

Nota: Debe tener privilegios de root para ejecutar este comando.

Si el campo de salida `cluster_hostname` está vacío o no es lo que desea, agregue o cambie el nombre de host (FQDN) de Cisco DNA Center con el uso del comando `maglev cluster config update`:

Input :

```
$maglev-config update
```

Output:

Maglev Config Wizard GUI

Nota: Debe tener privilegios de root para ejecutar este comando.

Haga clic en **Next** hasta que vea el paso titulado MAGLEV CLUSTER DETAILS que contiene el mensaje de entrada Cluster hostname. Establezca el nombre de host en el FQDN del Cisco DNA Center que desee. Haga clic en **Next** y continúe hasta que Cisco DNA Center se reconfigure con el nuevo FQDN.

Paso 3. Utilice un editor de texto de su elección, cree un archivo llamado **openssl.cnf** y cárguelo en el directorio que creó en el paso anterior. Utilice este ejemplo como guía, pero ajústelo para adaptarlo a su implementación.

- Ajuste `default_bits` y `default_md` si el equipo de administración de la autoridad certificadora requiere 2048/sha256 en su lugar.
- Especifique valores para cada campo de las secciones `req_distinguido_name` y `alt_names`. La única excepción es el campo OU, que es opcional. Omita el campo OU si el equipo de administración de la autoridad certificadora no lo requiere.
- El campo de dirección de correo electrónico es opcional; omítalo si el equipo de administración de la autoridad de certificación no lo requiere.
- `alt_names`: Los requisitos de configuración del certificado varían en función de la versión de Cisco DNA Center.

El soporte completo de FQDN en el certificado del Centro de ADN de Cisco está disponible a partir de Cisco DNA Center 2.1.1. Para las versiones de Cisco DNA Center anteriores a la 2.1.1, necesita un certificado con direcciones IP definidas en el campo Nombre alternativo del sujeto (SAN). Las configuraciones de la sección `alt_names` para las versiones 2.1.1 y posteriores de Cisco DNA Center y las versiones anteriores a la 2.1.1 de Cisco DNA Center son las siguientes:

Cisco DNA Center versiones 2.1.1 y posteriores:

1. Preste mucha atención a la sección `alt_names`, que debe contener todos los nombres DNS (que incluye el FQDN de Cisco DNA Center) que se utilizan para acceder a Cisco DNA Center, ya sea mediante un navegador web o mediante un proceso automatizado como PnP o Cisco ISE. La primera entrada DNS de la sección `alt_names` debe contener el FQDN del centro de DNA de Cisco (`DNS.1 = FQDN-de-Cisco-DNA-Center`). No puede agregar una entrada de DNS comodín en lugar del FQDN del centro de DNA de Cisco, pero puede usar un comodín en las entradas de DNS subsiguientes en la sección de nombres alternativos (para PnP y otras entradas de DNS). Por ejemplo, `*.example.com` es una entrada válida.

Importante: si utiliza el mismo certificado para la configuración de recuperación ante desastres, no se permiten comodines mientras agrega una entrada DNS para un sitio del sistema de recuperación ante desastres en la sección `alt_names`. Sin embargo, se recomienda utilizar un certificado independiente para una configuración de recuperación ante desastres. Para obtener más información, consulte la sección "Add Disaster Recovery Certificate" (Agregar certificado de recuperación ante desastres) de la [Guía del administrador de Cisco DNA Center](#).

2. La sección `alt_names` debe contener `FQDN-of-Cisco-DNA-Center` como entrada DNS y debe coincidir con el nombre de host (FQDN) del centro DNA de Cisco establecido en el momento de la configuración del centro DNA de Cisco a través del asistente de configuración (en el campo de entrada "Nombre de host del clúster"). Actualmente, Cisco DNA Center sólo admite un nombre de

host (FQDN) para todas las interfaces. Si utiliza tanto el puerto de administración como el de empresa de Cisco DNA Center para la conexión de dispositivos a Cisco DNA Center en su red, debe configurar la política GeoDNS para resolver la IP de administración/IP virtual e IP empresarial/IP virtual para el nombre de host (FQDN) de Cisco DNA Center basado en la red desde la que se recibe la consulta DNS. La configuración de la política GeoDNS no es necesaria si utiliza únicamente el puerto empresarial de Cisco DNA Center para la conexión de dispositivos a Cisco DNA Center en la red.

Nota: Si ha habilitado la recuperación ante desastres para Cisco DNA Center, debe configurar la política GeoDNS para resolver la IP virtual de administración de recuperación ante desastres y la IP virtual empresarial de recuperación ante desastres para el nombre de host (FQDN) de Cisco DNA Center basado en la red desde la que se recibe la consulta DNS.

3. Cisco DNA Center versiones anteriores a la 2.1.1:

Preste mucha atención a la sección `alt_names`, que debe contener todas las direcciones IP y nombres DNS que se utilizan para acceder a Cisco DNA Center, ya sea mediante un navegador web o mediante un proceso automatizado como PnP o Cisco ISE. (En este ejemplo se supone que hay un clúster de Cisco DNA Center de tres nodos. Si tiene un dispositivo independiente, utilice las redes SAN solo para ese nodo y el VIP. Si agrupa el dispositivo más adelante, debe volver a crear el certificado para incluir las direcciones IP de los nuevos miembros del clúster.)

Si no se configura una interfaz de nube, omita los campos del puerto de nube.

- En la extensión `extendedKeyUsage`, los atributos `serverAuth` y `clientAuth` son obligatorios. Si omite alguno de los atributos, Cisco DNA Center rechazará el certificado SSL.
- Si importa un certificado autofirmado (no recomendado), debe contener la extensión "CA:TRUE" de Restricciones básicas de X.509.

Ejemplo `openssl.cnf` (aplicable para Cisco DNA Center versiones 2.1.1 y posteriores):

```
req_extensions = v3_req
distinguished_name = req_distinguished_name
default_bits = 4096
default_md = sha512
prompt = no

[req_distinguished_name]

C = <two-letter-country-code>
ST = <state-or-province>
L = <city>
O = <company-name>
OU = MyDivision
CN = FQDN-of-Cisco-DNA-Center
emailAddress = responsible-user@mycompany.tld

[ v3_req ]

basicConstraints = CA:FALSE
keyUsage = digitalSignature, keyEncipherment
extendedKeyUsage=serverAuth,clientAuth
subjectAltName = @alt_names
```

```

[alt_names]

DNS.1 = FQDN-of-Cisco-DNA-Center
DNS.2 = pnpserver.DomainAssignedByDHCPDuringPnP.tld
DNS.3 = *.example.com

!--- Example openssl.cnf (Applicable for Cisco DNA Center versions earlier than 2.1.1)

req_extensions = v3_req
distinguished_name = req_distinguished_name
default_bits = 4096
default_md = sha512
prompt = no

[req_distinguished_name]

C = <two-letter-country-code>
ST = <state-or-province>
L = <city> O = <company-name>
OU = MyDivision
CN = FQDN-of-Cisco-DNA-Center
emailAddress = responsible-user@mycompany.tld

[ v3_req ]

basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
extendedKeyUsage=serverAuth,clientAuth
subjectAltName = @alt_names

[alt_names]

DNS.1 = FQDN-of-Cisco-DNA-Center
DNS.2 = pnpserver.DomainAssignedByDHCPDuringPnP.tld
IP.1 = Enterprise port IP node #1
IP.2 = Enterprise port IP node #2
IP.3 = Enterprise port IP node #3
IP.4 = Enterprise port VIP
IP.5 = Cluster port IP node #1
IP.6 = Cluster port IP node #2
IP.7 = Cluster port IP node #3
IP.8 = Cluster port VIP
IP.9 = GUI port IP node #1
IP.10 = GUI port IP node #2
IP.11 = GUI port IP node #3
IP.12 = GUI port VIP
IP.13 = Cloud port IP node #1
IP.14 = Cloud port IP node #2
IP.15 = Cloud port IP node #3
IP.16 = Cloud port VIP

```

Nota: Si no incluye las direcciones IP del clúster en el archivo **openssl.cnf**, no puede programar la activación de la imagen de software. Para solucionar este problema, agregue las direcciones IP del clúster como SAN al certificado.

Utilice un editor de texto de su elección, cree un archivo llamado **openssl.cnf** y cárguelo en el directorio que creó en el paso anterior. Utilice este ejemplo como guía, pero ajústelo para adaptarlo a su implementación.

- Ajuste **default_bits** y **default_md** si el equipo de administración de la autoridad certificadora requiere 2048/sha256 en su lugar.

- Especifique valores para cada campo de las secciones req_distinguido_name y alt_names. La única excepción es el campo OU, que es opcional. Omita el campo OU si el equipo de administración de la autoridad certificadora no lo requiere.
- El campo direcciónDeCorreoElectrónico es opcional; omítalo si el equipo de administración de la autoridad de certificación no lo requiere.
- alt_names: Los requisitos de configuración del certificado varían en función de la versión de Cisco DNA Center.
- El soporte de FQDN está disponible desde Cisco DNA Center 2.1.1 en adelante. Para las versiones de Cisco DNA Center anteriores a la 2.1.1, se necesita un certificado con direcciones IP en el nombre alternativo del sujeto (SAN). Las configuraciones de la sección alt_names para las versiones 2.1.1 y posteriores de Cisco DNA Center y las versiones anteriores a la 2.1.1 de Cisco DNA Center son las siguientes:
 - Cisco DNA Center versiones 2.1.1 y posteriores: Preste mucha atención a la sección alt_names, que debe contener todos los nombres DNS (que incluye el FQDN de Cisco DNA Center) que se utilizan para acceder a Cisco DNA Center, ya sea mediante un navegador web o mediante un proceso automatizado como PnP o Cisco ISE. La primera entrada DNS de la sección alt_names debe contener el FQDN de Cisco DNA Center (DNS.1 = FQDN-of-Cisco-DNA-Center). No puede agregar una entrada de DNS comodín en lugar del FQDN de Cisco DNA Center. Sin embargo, puede utilizar un comodín en las entradas DNS subsiguientes de la sección alt-names (para PnP y otras entradas DNS). Por ejemplo, *.ejemplo.com es una entrada válida.

Importante: si utiliza el mismo certificado para la configuración de recuperación ante desastres, no se permiten comodines mientras agrega una entrada DNS para un sitio del sistema de recuperación ante desastres en la sección alt_names. Sin embargo, se recomienda utilizar un certificado independiente para una configuración de recuperación ante desastres. Para obtener más información, consulte la sección "Add Disaster Recovery Certificate" (Agregar certificado de recuperación ante desastres) de la [Guía del administrador de Cisco DNA Center](#).

- La sección alt_names debe contener FQDN-of-Cisco-DNA-Center como entrada DNS y debe coincidir con el nombre de host (FQDN) del centro DNA de Cisco establecido en el momento de la configuración del centro DNA de Cisco a través del asistente de configuración (en el campo de entrada "Nombre de host del clúster").

Actualmente, Cisco DNA Center sólo admite un nombre de host (FQDN) para todas las interfaces. Debe configurar la política GeoDNS para resolver la dirección IP/IP virtual y la dirección IP/IP virtual empresarial para el nombre de host (FQDN) del centro de DNA de Cisco basado en la red desde la que se recibe la consulta DNS.

Nota: Si ha habilitado la recuperación ante desastres para Cisco DNA Center, debe configurar la política GeoDNS para resolver la IP virtual de administración de recuperación ante desastres y la IP virtual empresarial de recuperación ante desastres para el nombre de host (FQDN) de Cisco DNA Center basado en la red desde la que se recibe la consulta DNS.

- Cisco DNA Center versiones anteriores a la 2.1.1:

Preste mucha atención a la sección alt_names, que debe contener todas las direcciones IP y nombres DNS que se utilizan para acceder a Cisco DNA Center, ya sea mediante un navegador web o mediante un proceso automatizado como PnP o Cisco ISE. (En este ejemplo se supone que hay un clúster de Cisco DNA Center de tres nodos. Si tiene un dispositivo independiente,

utilice las redes SAN solo para ese nodo y el VIP. Si agrupa el dispositivo más adelante, debe volver a crear el certificado para incluir las direcciones IP de los nuevos miembros del clúster.)

- Si no se configura una interfaz de nube, omita los campos del puerto de nube.
 - En la extensión `extendedKeyUsage`, los atributos `serverAuth` y `clientAuth` son obligatorios. Si omite alguno de los atributos, Cisco DNA Center rechazará el certificado SSL.
 - Si importa un certificado autofirmado (no recomendado), debe contener la extensión "CA:TRUE" de Restricciones básicas de X.509.

Ejemplo `openssl.cnf` (aplicable para las versiones 2.1.1 y posteriores de Cisco DNA Center)

```
req_extensions = v3_reqdistinguished_name = req_distinguished_namedefault_bits = 4096default_md = sha512prompt = no[req_distinguished_name]C = <two-letter-country-code>ST = <state-or-province>L = <city>O = <company-name>OU = MyDivisionCN = FQDN-of-Cisco-DNA-CenteremailAddress = responsible-user@mycompany.tld [ v3_req ]basicConstraints = CA:FALSEkeyUsage = digitalSignature, keyEnciphermentextendedKeyUsage=serverAuth,clientAuthsubjectAltName = @alt_names[alt_names]DNS.1 = FQDN-of-Cisco-DNA-CenterDNS.2 = pnpserver.DomainAssignedByDHCPDuringPnP.tldDNS.3 = *.example.com
```

Ejemplo `openssl.cnf` (Aplicable para las versiones de Cisco DNA Center anteriores a la 2.1.1)

```
req_extensions = v3_reqdistinguished_name = req_distinguished_namedefault_bits = 4096default_md = sha512prompt = no[req_distinguished_name]C = <two-letter-country-code>ST = <state-or-province>L = <city>O = <company-name>OU = MyDivisionCN = FQDN-of-Cisco-DNA-Centeron-GUI-portemailAddress = responsible-user@mycompany.tld[ v3_req ]basicConstraints = CA:FALSEkeyUsage = nonRepudiation, digitalSignature, keyEnciphermentextendedKeyUsage=serverAuth,clientAuthsubjectAltName = @alt_names[alt_names]DNS.1 = FQDN-of-Cisco-DNA-Center-on-GUI-portDNS.2 = FQDN-of-Cisco-DNA-Center-on-enterprise-portDNS.3 = pnpserver.DomainAssignedByDHCPDuringPnP.tldIP.1 = Enterprise port IP node #1IP.2 = Enterprise port IP node #2IP.3 = Enterprise port IP node #3IP.4 = Enterprise port VIPIP.5 = Cluster port IP node #1IP.6 = Cluster port IP node #2IP.7 = Cluster port IP node #3IP.8 = Cluster port VIPIP.9 = GUI port IP node #1IP.10 = GUI port IP node #2IP.11 = GUI port IP node #3IP.12 = GUI port VIPIP.13 = Cloud port IP node #1IP.14 = Cloud port IP node #2IP.15 = Cloud port IP node #3IP.16 = Cloud port VIP
```

Nota: Si no incluye las direcciones IP del clúster en el archivo `openssl.cnf`, no puede programar la activación de la imagen de software. Para solucionar este problema, agregue las direcciones IP del clúster como SAN al certificado.

En este caso, el siguiente resultado es la configuración de mi archivo `openssl.conf`

```
req_extensions = v3_req
distinguished_name = req_distinguished_name
default_bits = 4096
default_md = sha512
prompt = no

[req_distinguished_name]

C = US
ST = California
```

```
L = Milpitas
O = Cisco Systems Inc.
OU = MyDivision
CN = noc-dnac.cisco.com
emailAddress = sit-noc-team@cisco.com
```

```
[ v3_req ]
```

```
basicConstraints = CA:FALSE
keyUsage = digitalSignature, keyEncipherment
extendedKeyUsage=serverAuth,clientAuth
subjectAltName = @alt_names
```

```
[alt_names]
```

```
DNS.1 = noc-dnac.cisco.com
DNS.2 = pnpserver.cisco.com
IP.1 = 10.10.0.160
IP.2 = 10.29.51.160
```

Paso 4. Introduzca este comando para crear una clave privada. Ajuste la longitud de la clave a 2048 si lo requiere el equipo de administración de la autoridad de certificación. **openssl genrsa -out csr.key 4096**

Paso 5. Después de rellenar los campos en el archivo **openssl.cnf**, utilice la clave privada que creó en el paso anterior para generar la solicitud de firma de certificado.

```
openssl req -config openssl.cnf -new -key csr.key -out DNAC.csr
```

Paso 6. Verifique el contenido de la Solicitud de firma de certificado y asegúrese de que los nombres DNS (y las direcciones IP para la versión del Cisco DNA Center anterior a la 2.1.1) se rellenan correctamente en el campo Nombre alternativo del sujeto.

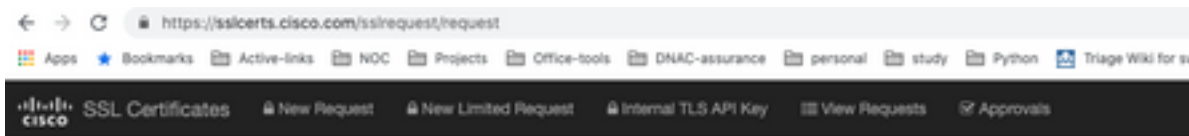
```
openssl req -text -noout -verify -in DNAC.csr
```

Paso 7. Copie la solicitud de firma de certificado y péguela en una CA (por ejemplo, Cisco Open SSL).

Vaya al vínculo para descargar el certificado. [Certificados Cisco SSL](#)

Haga clic en "Solicitar certificado" para descargar el certificado permanente.

O haga clic en "Solicitar certificado de prueba limitado" para un propósito limitado.



El usuario recibe un correo electrónico con la información del certificado. Haga clic con el botón derecho del ratón y descargue los tres archivos PEM del portátil. En este caso, he recibido 3 archivos independientes, así que omita el paso 8 y continúe con el paso 9.

Paso 8. Si el emisor del certificado proporciona la cadena completa del certificado (servidor y CA) en p7b:

Descargue el paquete p7b en formato DER y guárdelo como **dnac-chain.p7b**.

Copie el certificado dnac-chain.p7b en el clúster de Cisco DNA Center mediante SSH.

Ingrese este comando:

```
openssl pkcs7 -in dnac-chain.p7b -inform DER -out dnac-chain.pem -print_certs
```

Paso 9. Si el emisor del certificado proporciona el certificado y su cadena de CA de emisor en archivos sueltos:

Descargue los archivos PEM (base64) o utilice openssl para convertir DER a PEM.

Concatenar el certificado y su CA emisora, comenzar con el certificado, seguido por la CA subordinada, hasta la CA raíz, y enviarla al archivo dnac-chain.pem.

```
cat certificate.cer subCA.cer rootCA.cer > dnac-chain.pem
```

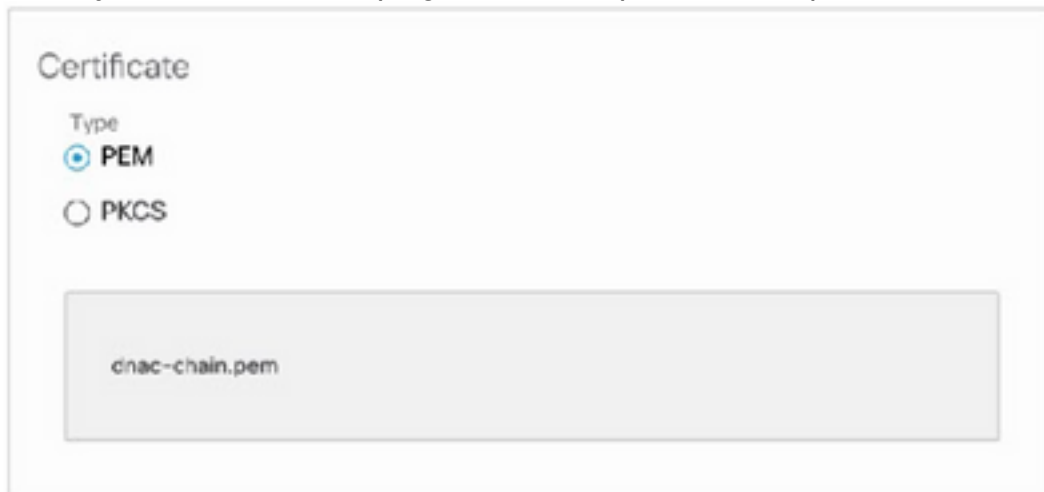
Paso 10. Copie el archivo dnac-chain.pem de su laptop a Cisco DNA Center en el directorio tls-cert creado anteriormente.

Paso 11. En la GUI de Cisco DNA Center, haga clic en el icono del menú () y seleccione System > Settings > Certificates.

Paso 12. Haga clic en Reemplazar certificado.

Paso 13. En el campo Certificado, haga clic en el botón de opción PEM y realice las siguientes tareas.

- Para el campo Certificate (Certificado), importe el archivo **dnac-chain.pem**, simplemente arrastre y suelte este archivo en el campo Drag n' Drop a File Here (Arrastrar y soltar un archivo aquí).
- Para el campo Private Key (Clave privada), importe la clave privada (csr.key); sólo tiene que arrastrar y soltar este archivo en el campo Drag n' Drop a File Here (Arrastrar y soltar un archivo aquí).
- Elija No en la lista desplegable Cifrado para la clave privada.



Certificate

Type

PEM

PKCS

dnac-chain.pem



Private Key

csr.key

Encrypted

NO

Paso 14. Haga clic en Cargar/Activar. Cierre la sesión y vuelva a iniciarla en DNAC.

Configuración del Servidor DHCP

Configure un conjunto de servidores DHCP para asignar una dirección IP al DUT. También configura el servidor DHCP

para enviar el nombre de dominio y la dirección IP del servidor DNS.

```
ip dhcp pool PNP-A4
network 192.0.2.0 255.255.255.252
default-router 192.0.2.2
domain-name cisco.com
dns-server 203.0.113.23
```

Configuración del servidor DNS. Configure un servidor DNS en la red para resolver el nombre FQDN del DNAC.

```
ip dns server
ip host pnpserver.cisco.com <dnac-controller-ip>
```

Paso 1. El nuevo dispositivo que se va a incorporar está cableado y encendido. Dado que la configuración de inicio en la NVRAM está vacía, el agente PnP se activa y envía "Cisco PnP" en la opción DHCP 60 en el mensaje DHCP DISCOVER.

Paso 2. El servidor DHCP no está configurado para reconocer "Cisco PnP" en la opción 60, ignora la opción 60. El servidor DHCP asigna una dirección IP y envía la oferta DHCP junto con el nombre de dominio configurado y la dirección IP del servidor DNS.

Paso 3. El agente PnP lee el nombre de dominio y formula el nombre de host del servidor PnP completo y anexa el nombre de dominio a la cadena "pnpserver". Si el nombre de dominio es "example.com", el nombre de host totalmente calificado del servidor PnP sería "pnpserver.example.com". El agente PnP resuelve "pnpserver.example.com" para su dirección IP con el servidor DNS recibido en las opciones DHCP.

Ejemplo cuando se activa el agente pnp para la incorporación:

Encienda un nuevo switch o "borre escritura" seguido de recarga en caso de una implementación de campo marrón

Verifique el siguiente flujo de trabajo en la consola del switch.

```
Would you like to enter the initial configuration dialog? [yes/no]:
```

```
*Jan 19 22:23:21.981: %IOSXE-0-PLATFORM: R0/0: udev: disk0: has been inserted
```

```
Autoinstall trying DHCPv6 on Vlan1
```

```
Autoinstall trying DHCPv4 on Vlan1
```

```
Autoinstall trying DHCPv6 on Vlan1
```

```
Redundant RPs -
```

```
Autoinstall trying DHCPv6 on Vlan119
```

```
Autoinstall trying DHCPv6 on Vlan119
```

```
Acquired IPv4 address 192.0.2.3 on Interface Vlan119
```

```
Received following DHCPv4 options:
```

```
    domain-name      : cisco.com
    dns-server-ip    : 203.0.113.23
    si-addr          : 203.0.113.21
```

```
stop Autoip process
```

```
OK to enter CLI now...
```

```
pnp-discovery can be monitored without entering enable mode
```

```
Entering enable mode will stop pnp-discovery
```

```
Autoinstall trying DHCPv6 on Vlan119
```

Guestshell destroyed successfully

Autoinstall trying DHCPv6 on Vlan119

Press RETURN to get started!

Información Relacionada

- [detección de servidor PnP](#)
- [Guía de prácticas recomendadas de seguridad de Cisco DNA Center](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).