Configuración del Acceso LDAP Seguro para Fabric Interconnects en el Modo Administrado de Intersight (Consola de Dispositivo HTTP y SSH)

Contenido

Introducción

Este documento describe cómo configurar la autenticación LDAP de dominio en una instancia de Intersight SaaS usando la política LDAP.

Prerequisites

Requirements

Conocimiento de estos temas:

- Protocolo ligero de acceso a directorios (LDAP).
- Servidor de nombre de dominio (DNS).
- Cisco Intersight

Componentes Utilizados

- Instancia de Cisco Intersight SaaS
- Microsoft Active Directory
- Servidor DNS
- Servicios de certificados de Microsoft Active Directory (AD CS)

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

LDAP es un protocolo conocido que se utiliza para acceder a los recursos desde un directorio a través de la red. Estos directorios almacenan información sobre usuarios, organizaciones y recursos. LDAP proporciona un proceso estándar para acceder y administrar esa información que se puede utilizar para los procesos de autenticación y autorización.

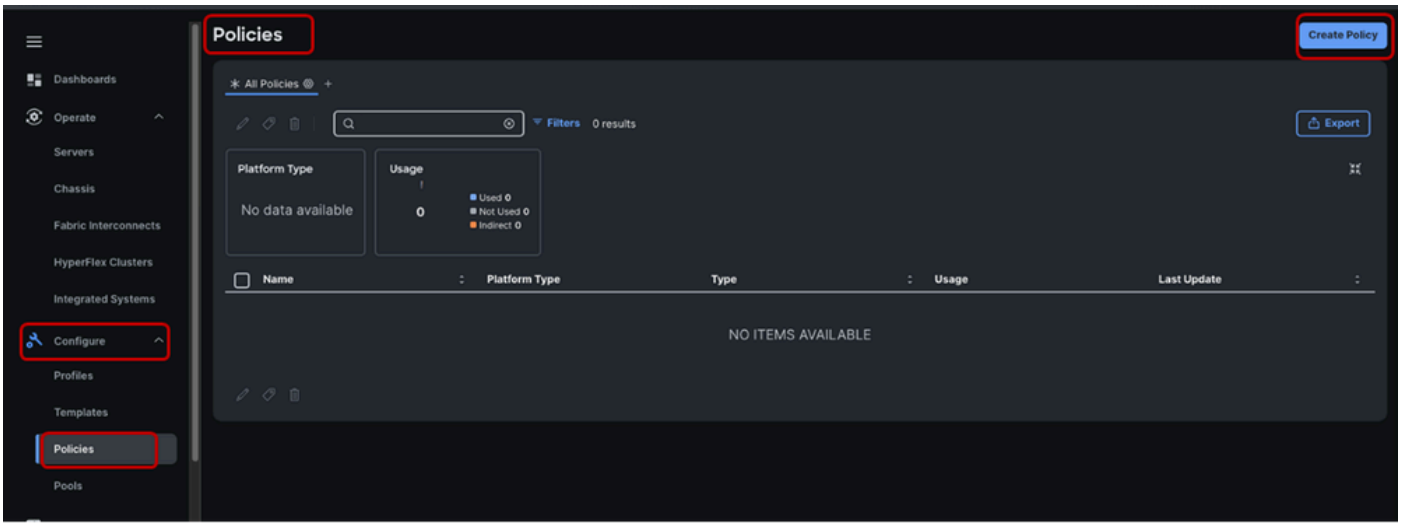
Este documento describe el proceso de configuración para la autenticación remota a través de LDAP seguro a la consola del dispositivo o CLI (HTTP o SSH respectivamente) de un par de Fabric Interconnects en el modo administrado de intersección.

Configuración

Configuración de la política LDAP

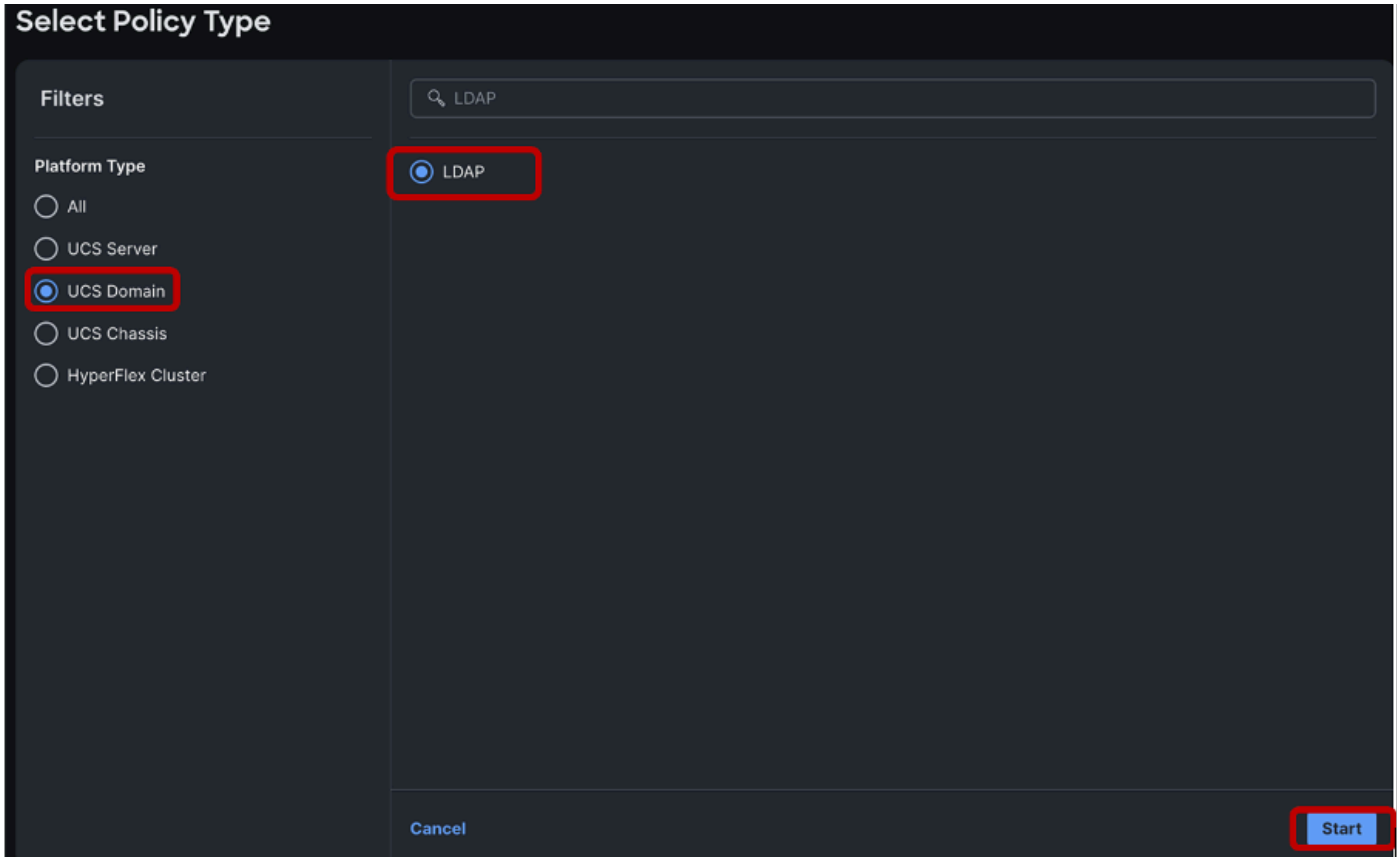
Para configurar la política LDAP, inicie sesión en la instancia SaaS de Intersight.

Vaya a la sección Configurar > Haga clic en Políticas.
Acceda a la ventana Políticas > Seleccione Crear Política.

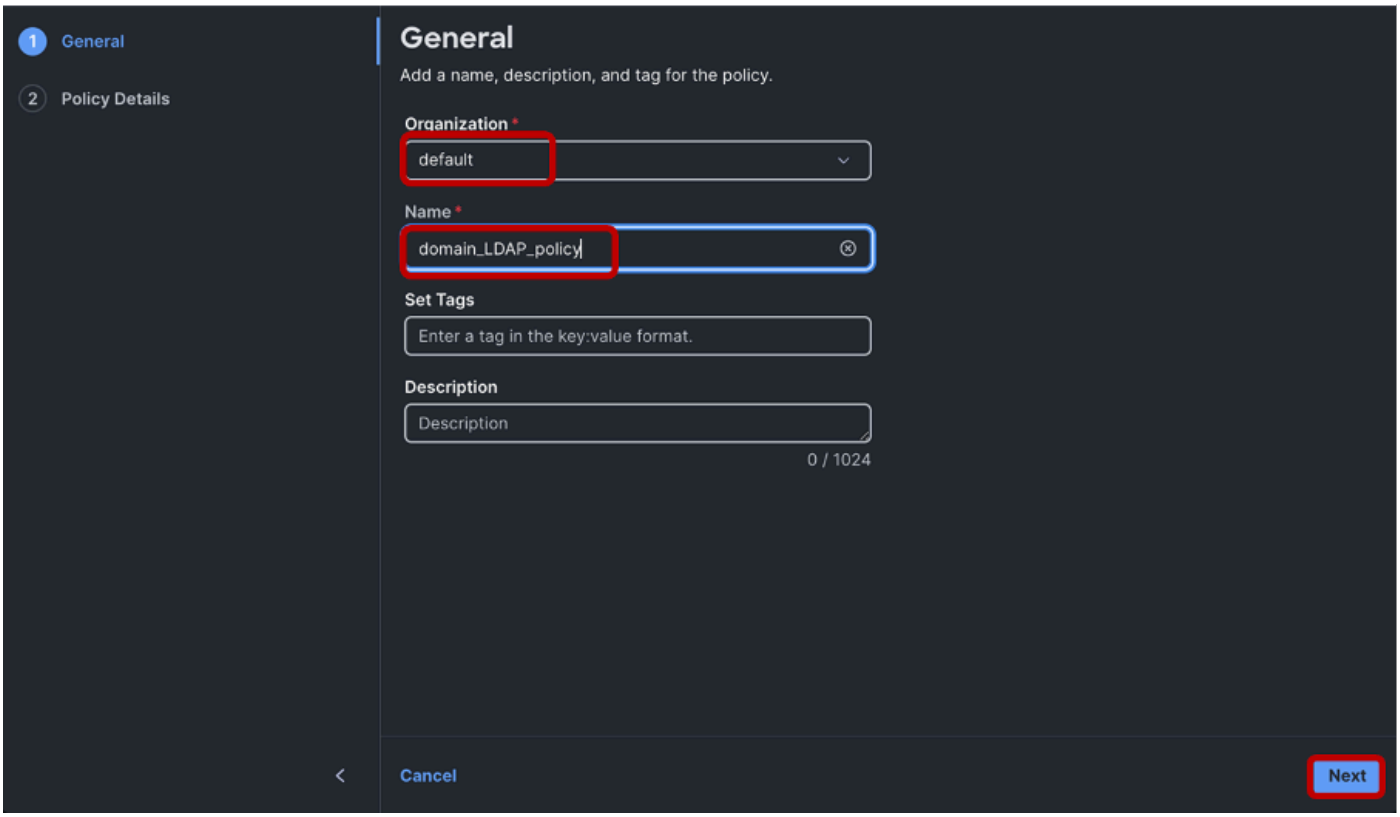


En la barra de búsqueda, busque "LDAP".

Seleccione el botón de opción LDAP > Haga clic en Inicio.

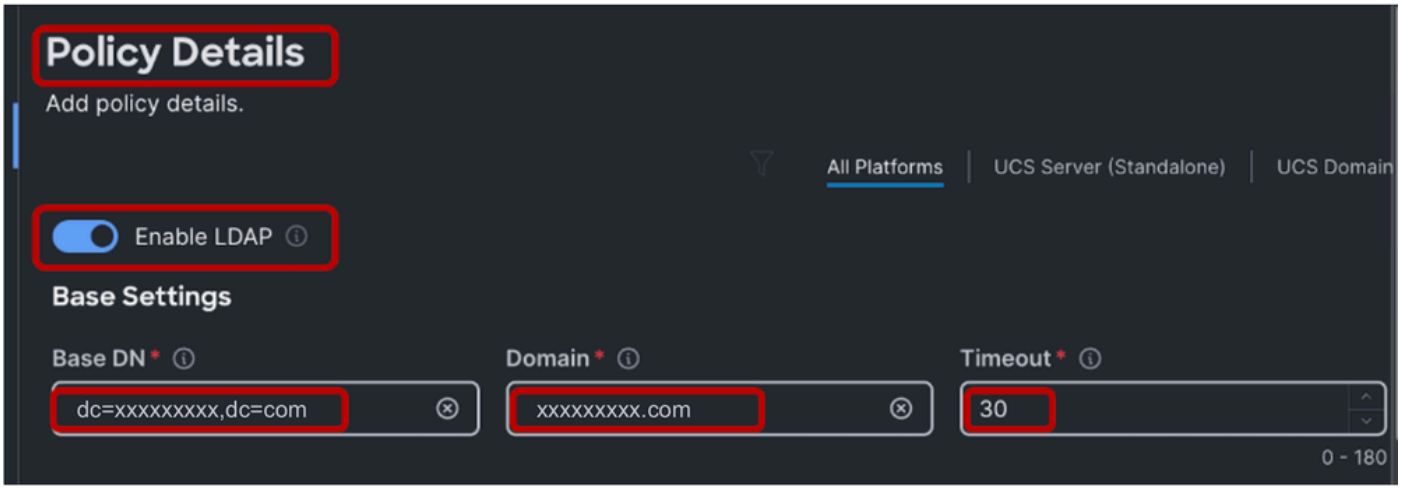


En la ventana Create > Choose your desired Organization > Name the LDAP policy > Click Next:



En la sección Detalles de política > Seleccione el control deslizante Enable LDAP > Populate the Base DN, Domain and Timeout values.

Los valores de tiempo de espera, cuando se establecen entre 0 y 29, se establecen automáticamente de forma predeterminada en 30 segundos. Para esta demostración, "xxxxxxxx.com" es el dominio deseado ya configurado en el servidor LDAP y se ha especificado un valor de tiempo de espera de 30 segundos.

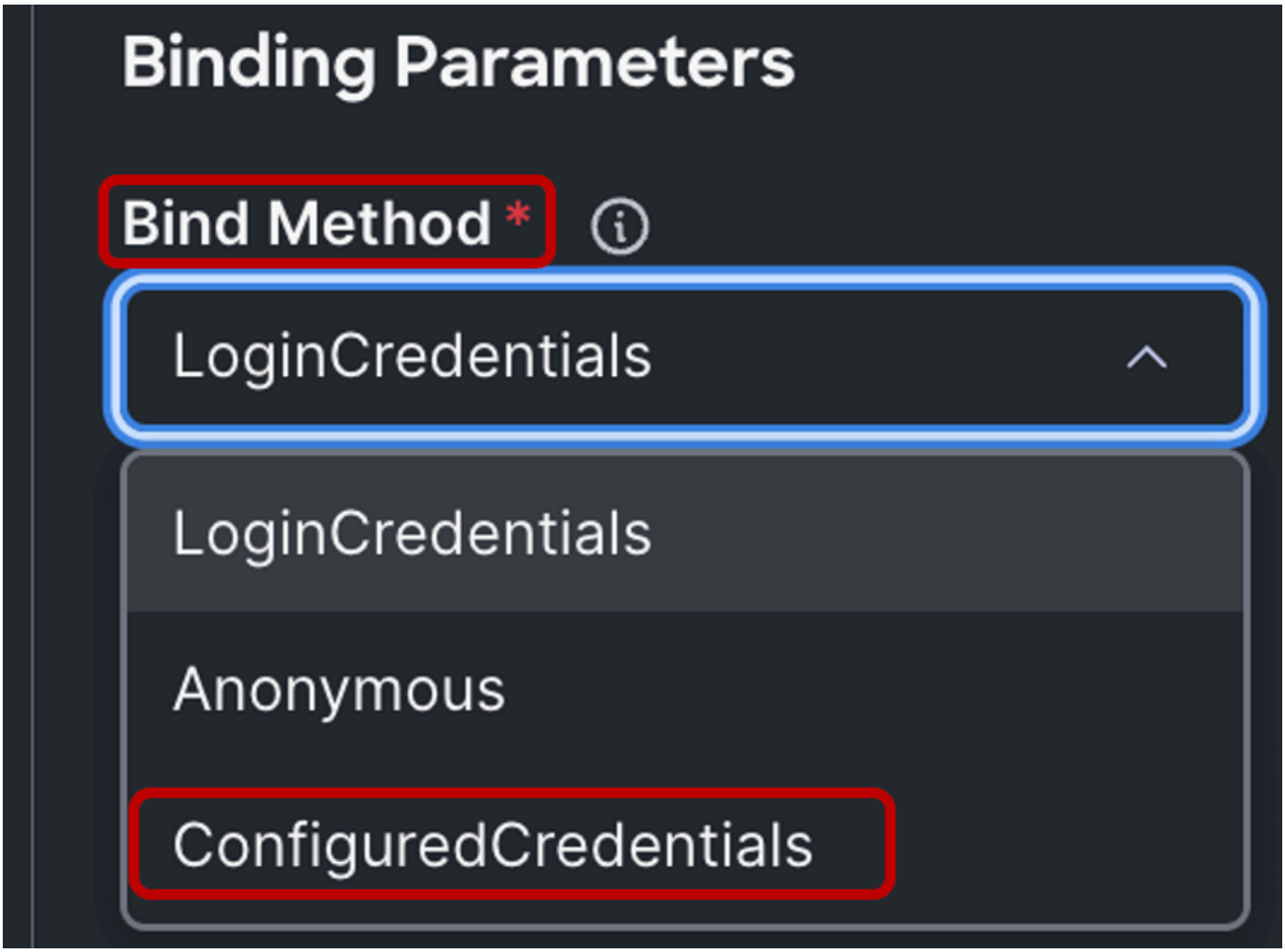


Para configurar LDAP seguro, active el botón de radio Enable Encryption (Activar cifrado).

Nota: La configuración LDAP habitual puede utilizar una dirección IP o un FQDN, pero un certificado firmado no es un requisito. Por lo tanto, al configurar LDAP "Estándar", se pueden omitir la opción Habilitar cifrado, la directiva de conectividad de red de servidor DNS y un certificado en las configuraciones de directiva de administración de certificados. LDAP seguro requiere un servidor DNS configurado para la resolución de nombres de servidor LDAP y un certificado raíz.

En la sección Parámetros de enlace, la configuración predeterminada es LoginCredentials, que utiliza la autenticación individual de las credenciales LDAP del usuario para la operación de enlace. Esto elimina la necesidad de configurar un usuario de enlace dedicado.

Para esta demostración, se ha configurado un usuario Bind. Por lo tanto, el "Método de enlace" se cambia a "Credenciales configuradas".

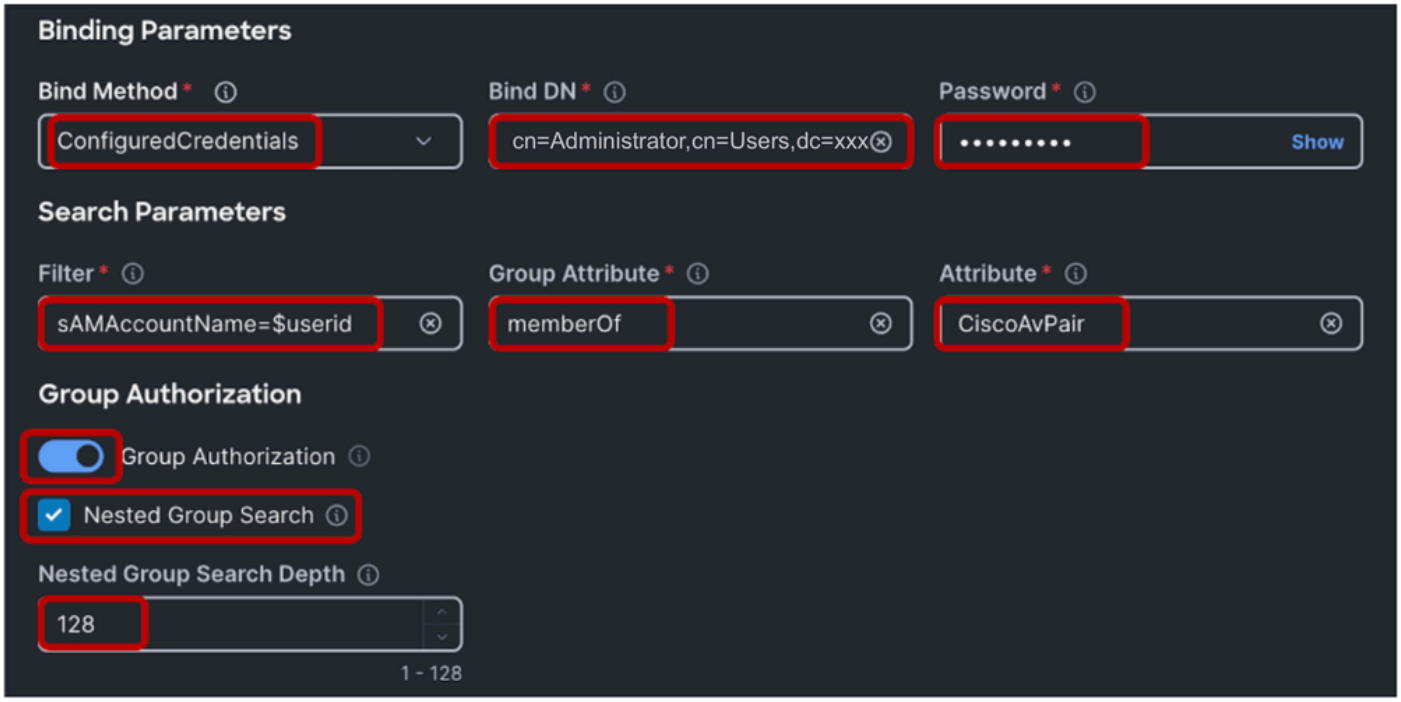


A continuación, agregue un DN de enlace (un usuario de enlace) y la contraseña de enlace de usuario. Puede ser cualquier usuario configurado en Windows Active Directory. En esta demostración se utiliza el usuario Administrator.

‘cn=Administrator,cn=Users,dc=xxxxxxxxx,dc=com’.

En la sección Buscar parámetros, en Filtro, introduzca "sAMAccountName=$userid".

En Atributos de grupo, agregue "memberOf" y en el campo Atributo, "CiscoAvPair". Dependiendo de la configuración del servidor LDAP, puede activar la autorización de grupo y la búsqueda de grupos anidados. Para esta demostración se utiliza la Profundidad de búsqueda de grupos anidados predeterminada, 128.



En la sección "Configurar servidores LDAP" > Introduzca la dirección IP o FQDN del servidor LDAP (requerido para LDAP seguro) y el número de puerto (389).

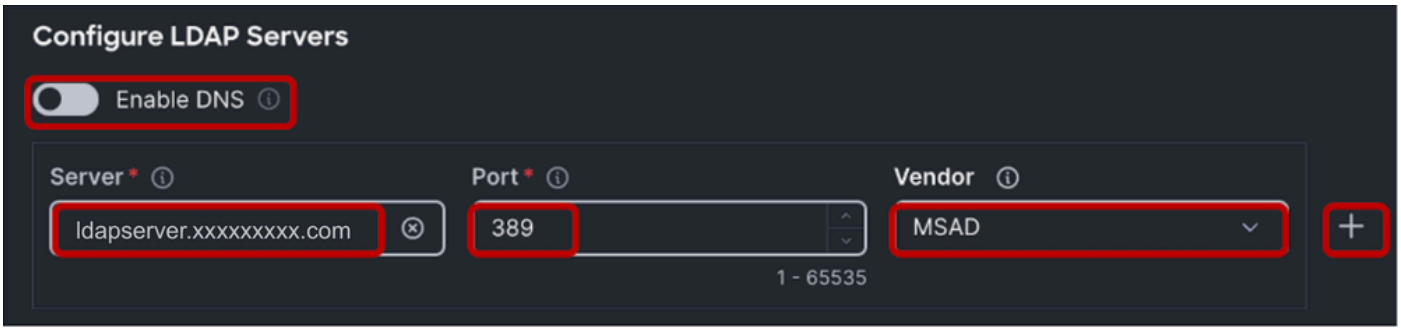
LDAP seguro en UCS utiliza STARTTLS para habilitar la comunicación cifrada mediante el puerto 389.

Tenga en cuenta que modificar el puerto de 389 a 636 puede causar errores de autenticación. Cisco UCS realiza la negociación de TLS en el puerto 636 para SSL; sin embargo, la conexión inicial siempre se establece sin cifrar en el puerto 389.

Seleccione el proveedor del servidor LDAP. Las opciones de proveedor disponibles son OpenLDAP y MSAD (Microsoft Active Directory). Para esta demostración, se utiliza MSAD, ya que el servidor LDAP que se utiliza es Windows Server 2019.

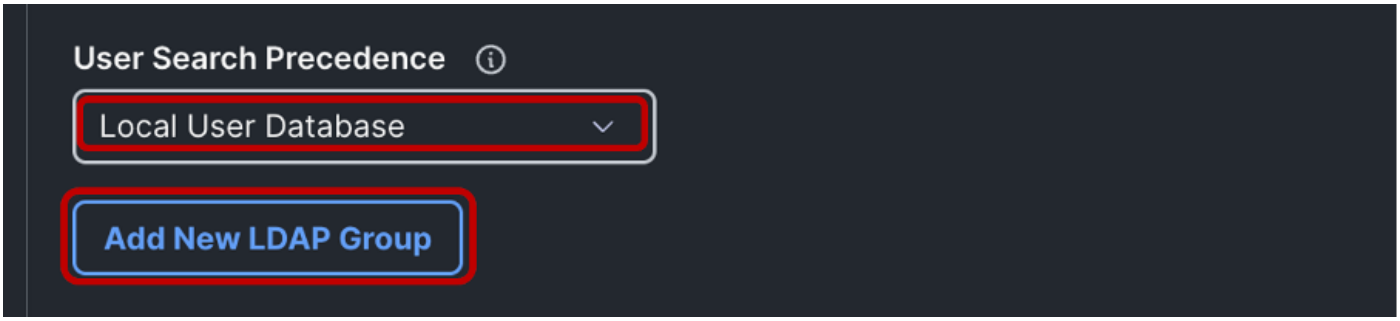
Deje el botón Enable DNS (Activar DNS) apagado, ya que esta opción no es aplicable a la configuración LDAP en el dominio UCS.

Para configurar varios servidores LDAP, haga clic en el icono "+" que se encuentra en el extremo derecho del servidor LDAP configurado.

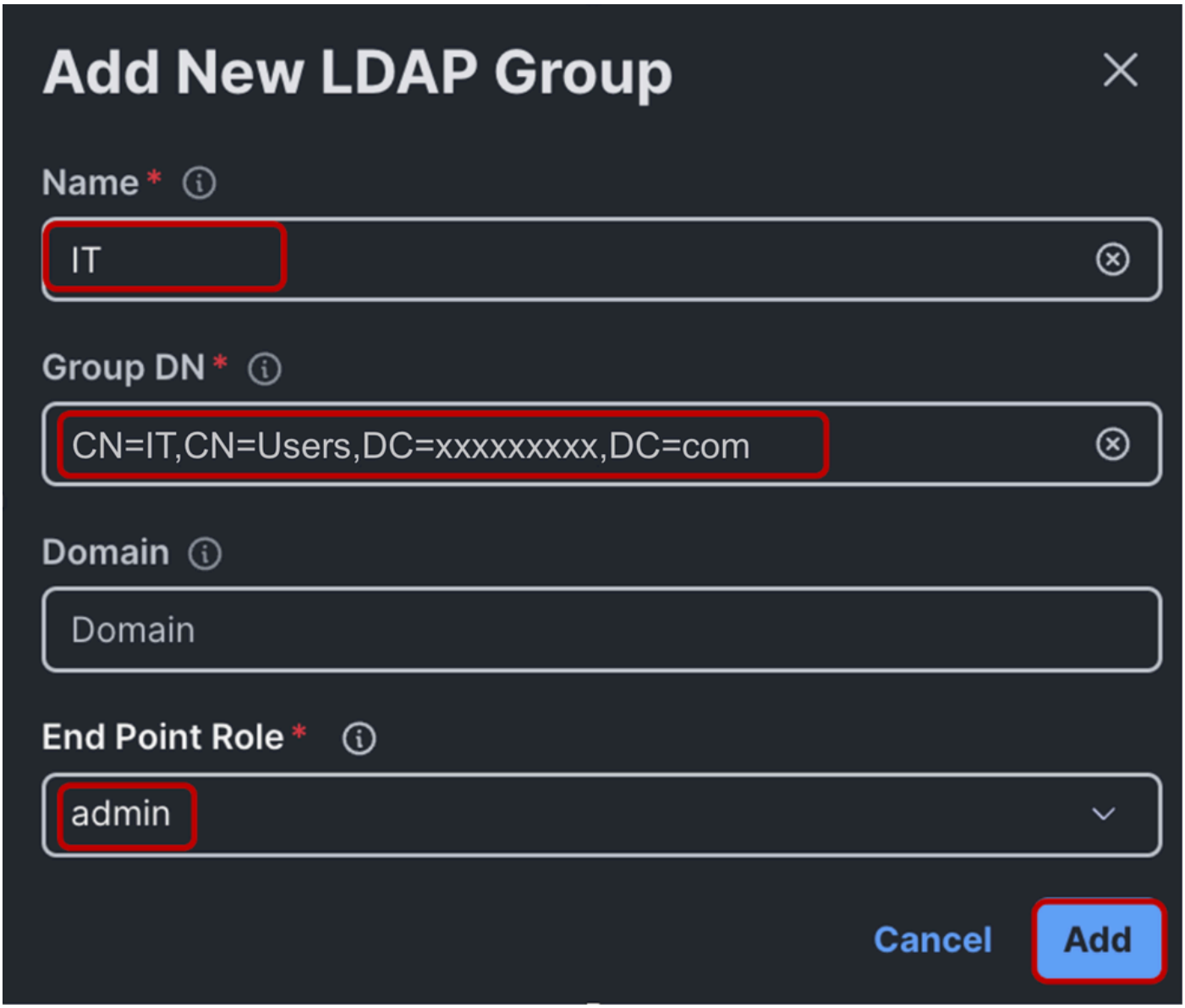


Nota: Puede mantener la Precedencia de Búsqueda de Usuario como Base de Datos de Usuario Local o cambiarla a Base de Datos de Usuario LDAP dependiendo de su caso de uso.

A continuación, vaya a agregar un DN de grupo correspondiente al grupo configurado en el servidor LDAP; para ello, haga clic en el botón Add New LDAP Group (Agregar nuevo grupo LDAP).



Asigne un nombre al grupo, agregue el DN de grupo recibido del servidor LDAP y seleccione el rol de punto final que desee.

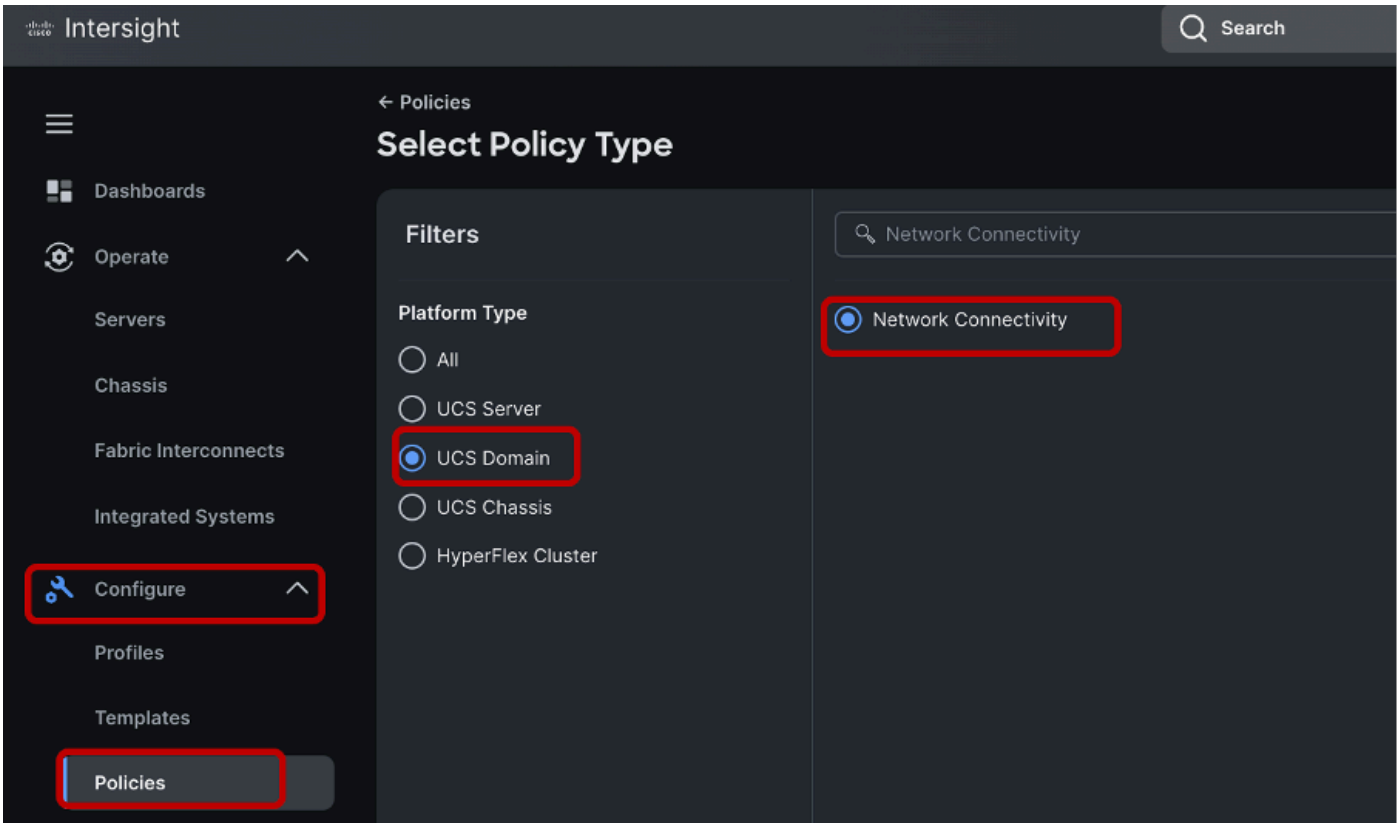


Haga clic en Agregar > Seleccionar Crear para crear la política LDAP

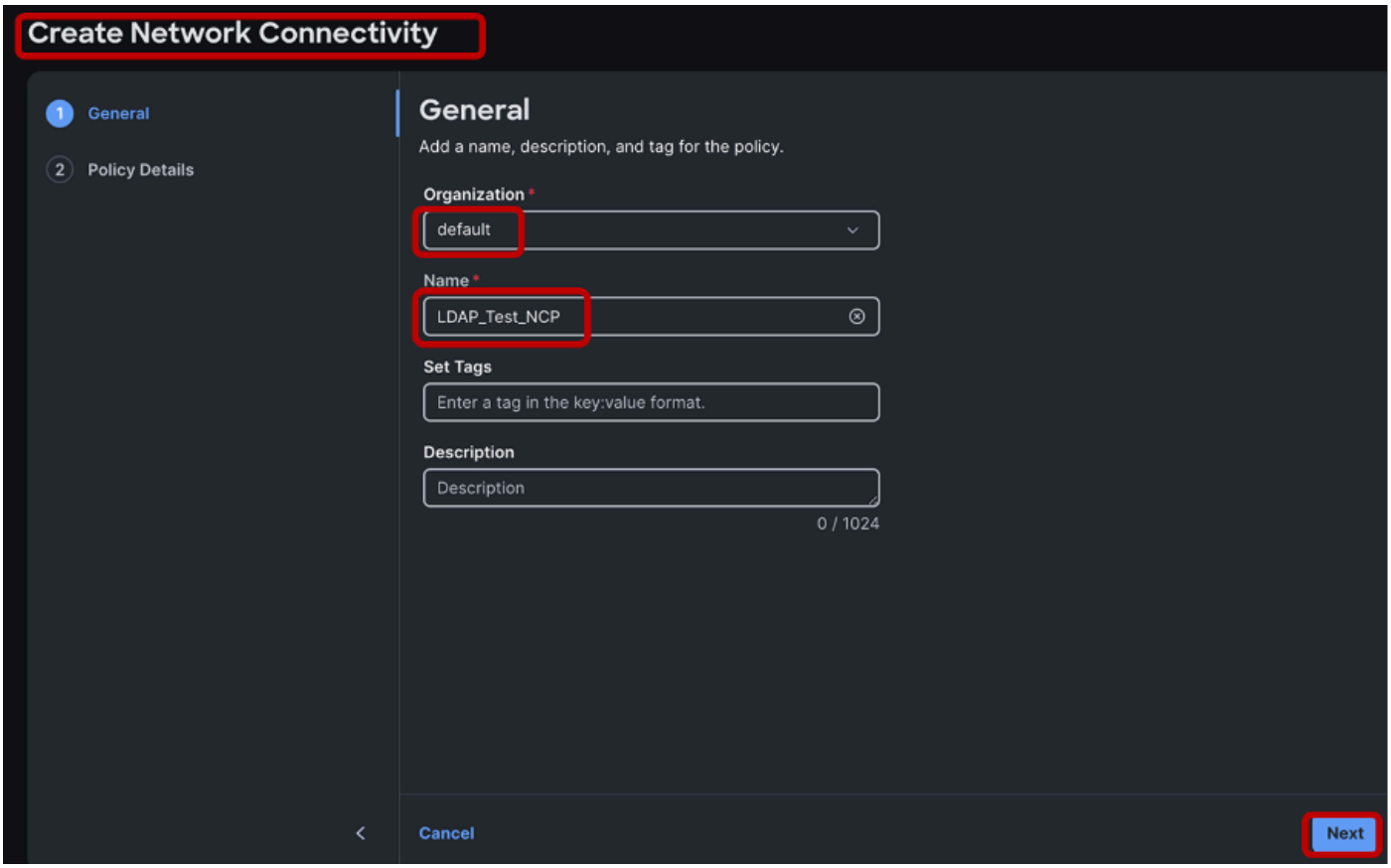
Nota: Para la configuración de la política LDAP de dominio, el único rol de punto final admitido es "admin" en el momento de la creación de este documento.

Configurar directiva de conectividad de red

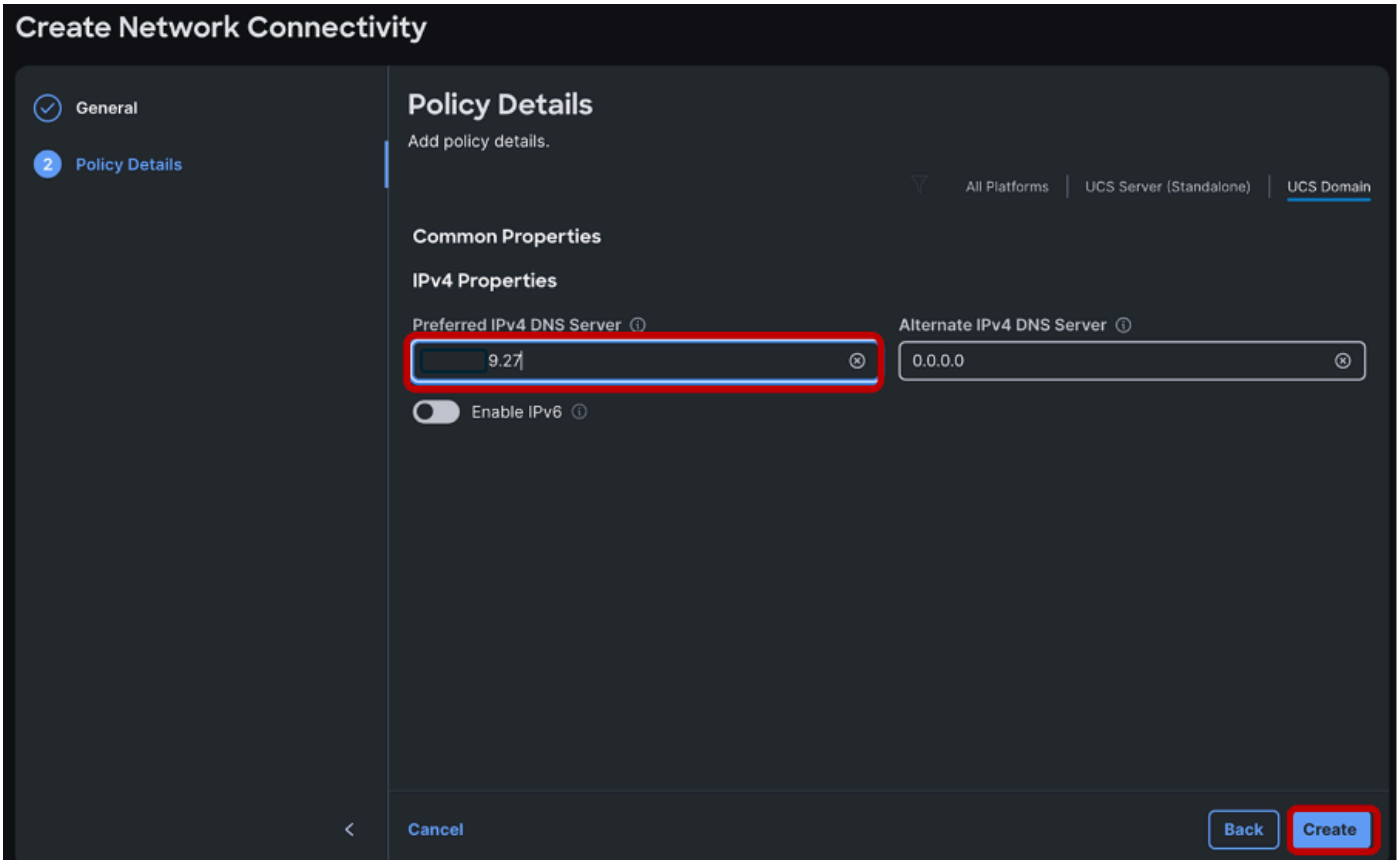
Configure un servidor DNS para el dominio UCS mediante la creación de una directiva de conectividad de red.



Seleccione la organización adecuada > Introduzca el nombre de la política > Haga clic en Next (Siguiente).



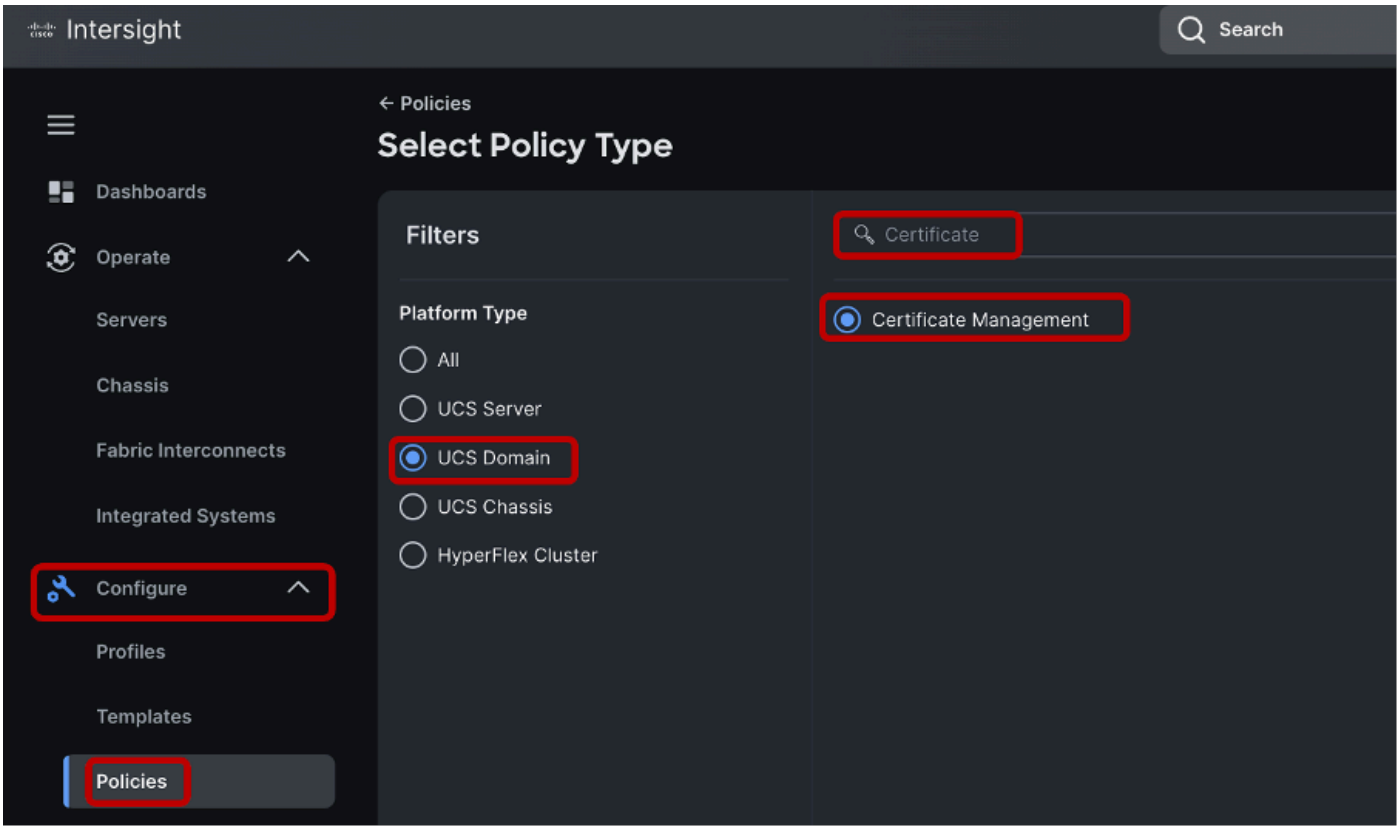
Defina una dirección IPv4 del servidor DNS preferido y haga clic en Create (Crear) para guardar la directiva.



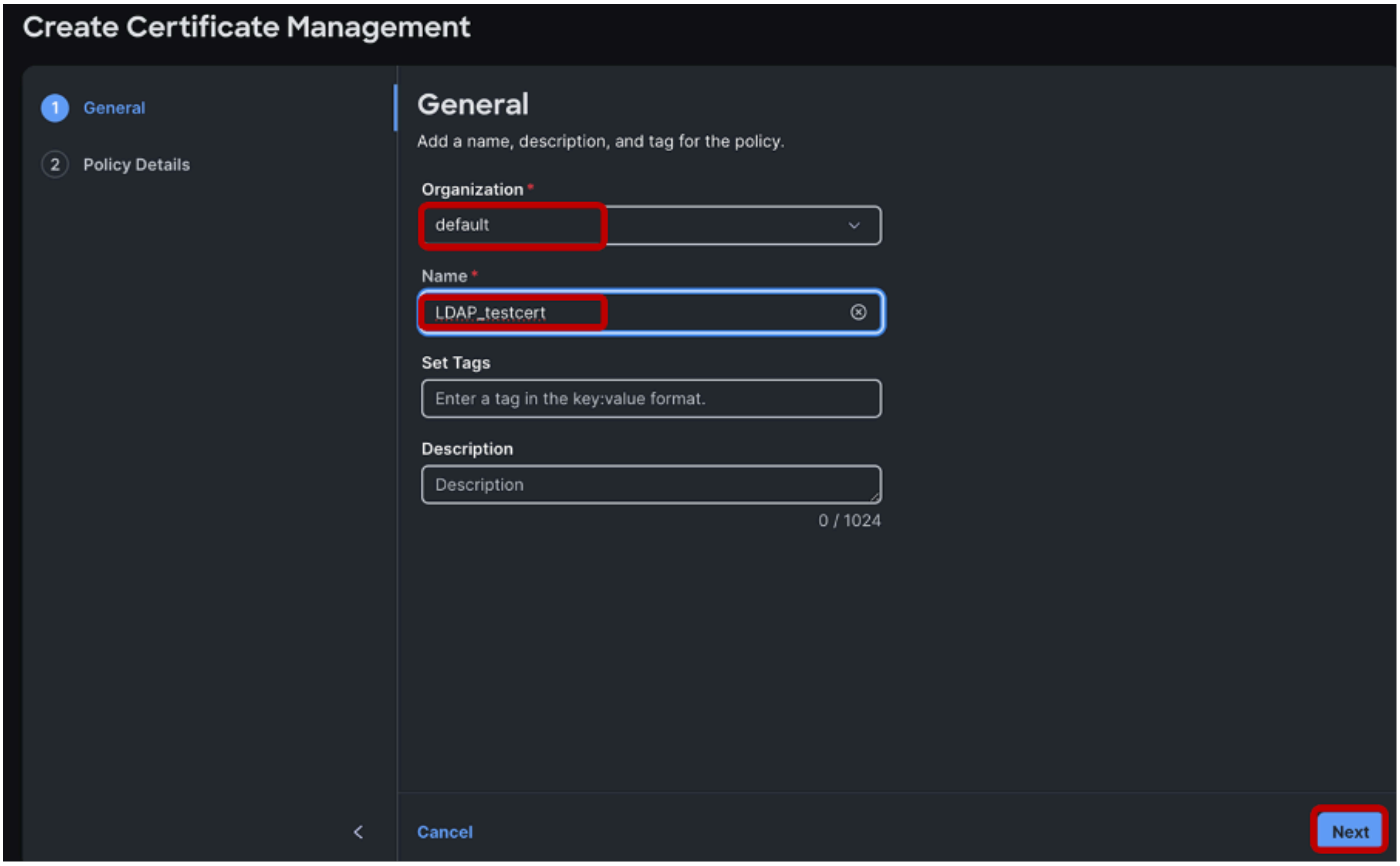
Asegúrese de que se haya configurado una dirección IP de servidor DNS y de que sea accesible para la resolución de nombres. Asegúrese de que la resolución de nombres sea funcional para el servidor LDAP y las Fabric Interconnects dentro del dominio. Para esta demostración, el servidor DNS se encuentra en la misma instancia del equipo Windows que el servidor LDAP.

Configurar directiva de administración de certificados

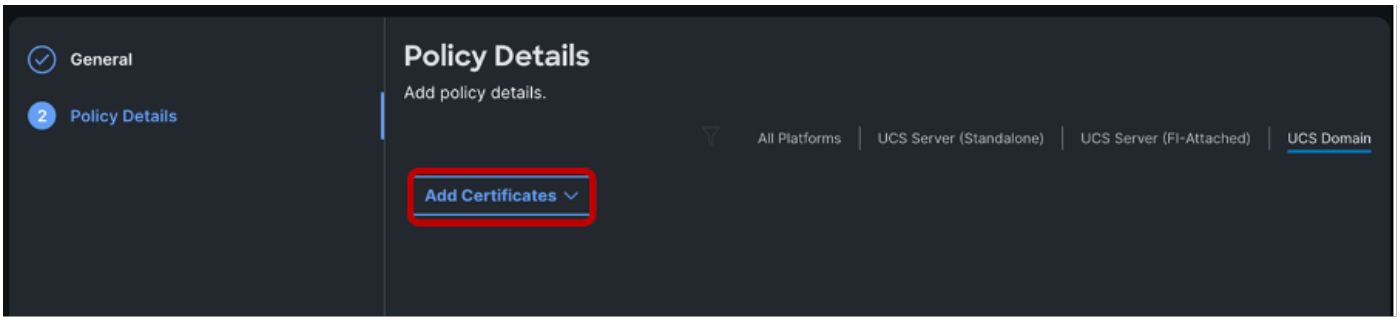
A continuación, configure una directiva de administración de certificados. Esto es necesario para que funcione el cifrado LDAP.



Seleccione la organización adecuada, asigne un nombre a la política > Haga clic en Next (Siguiente)

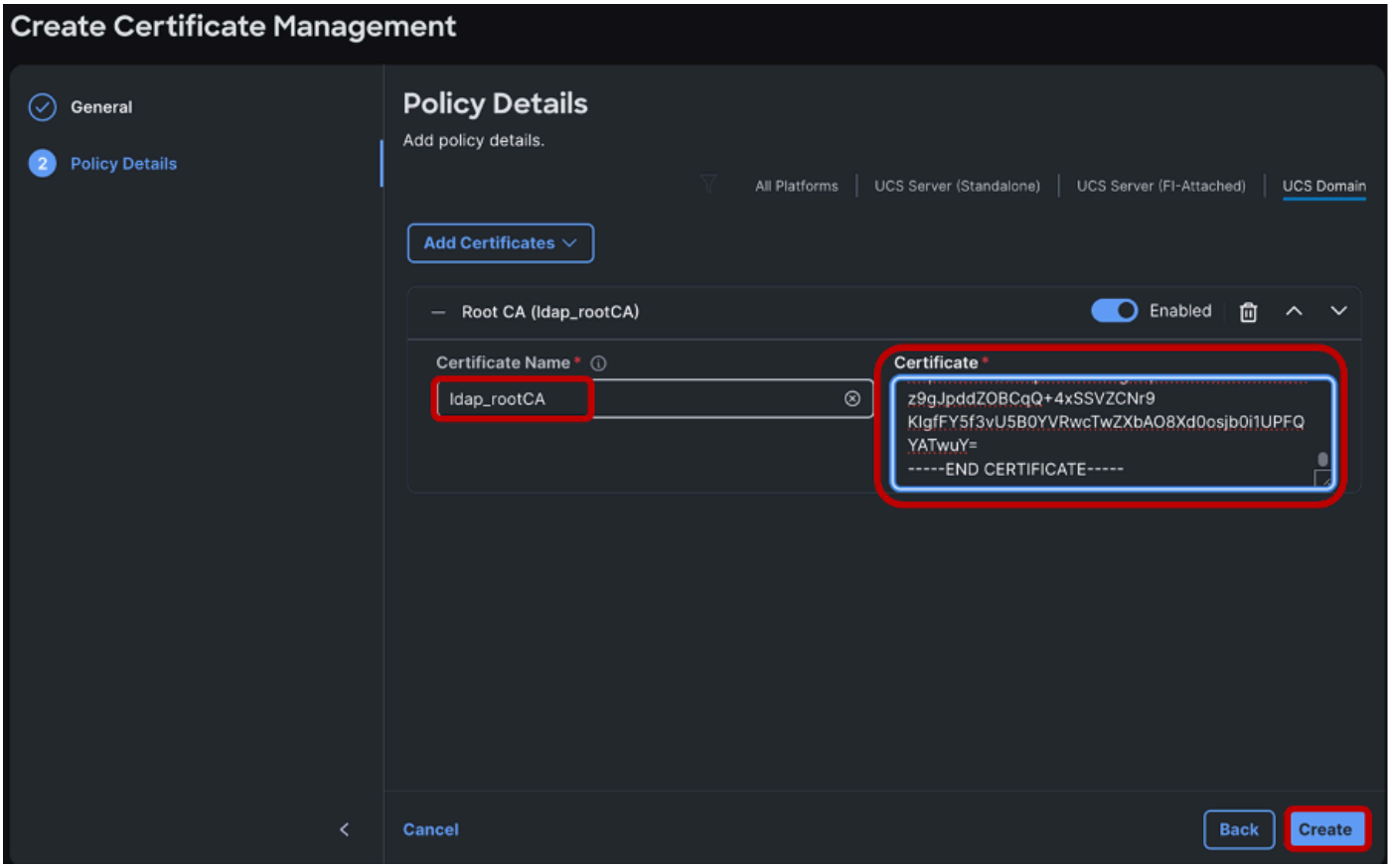


Haga clic en Agregar certificados.

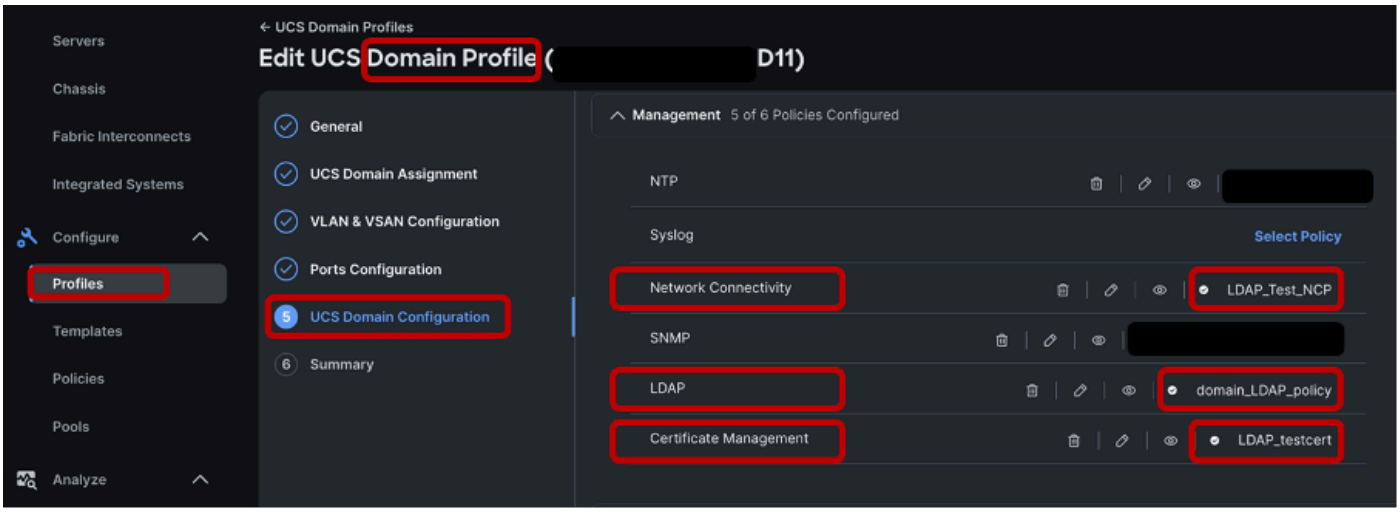


Dé un nombre al certificado y péguelo en el certificado raíz de los Servicios de certificados de Microsoft Active Directory.

Haga clic en Crear.



Una vez creadas las directivas de LDAP, conectividad de red y administración de certificados, haga referencia a las directivas recién creadas en el perfil de dominio deseado, en la sección "Configuración de dominio UCS", como se muestra.



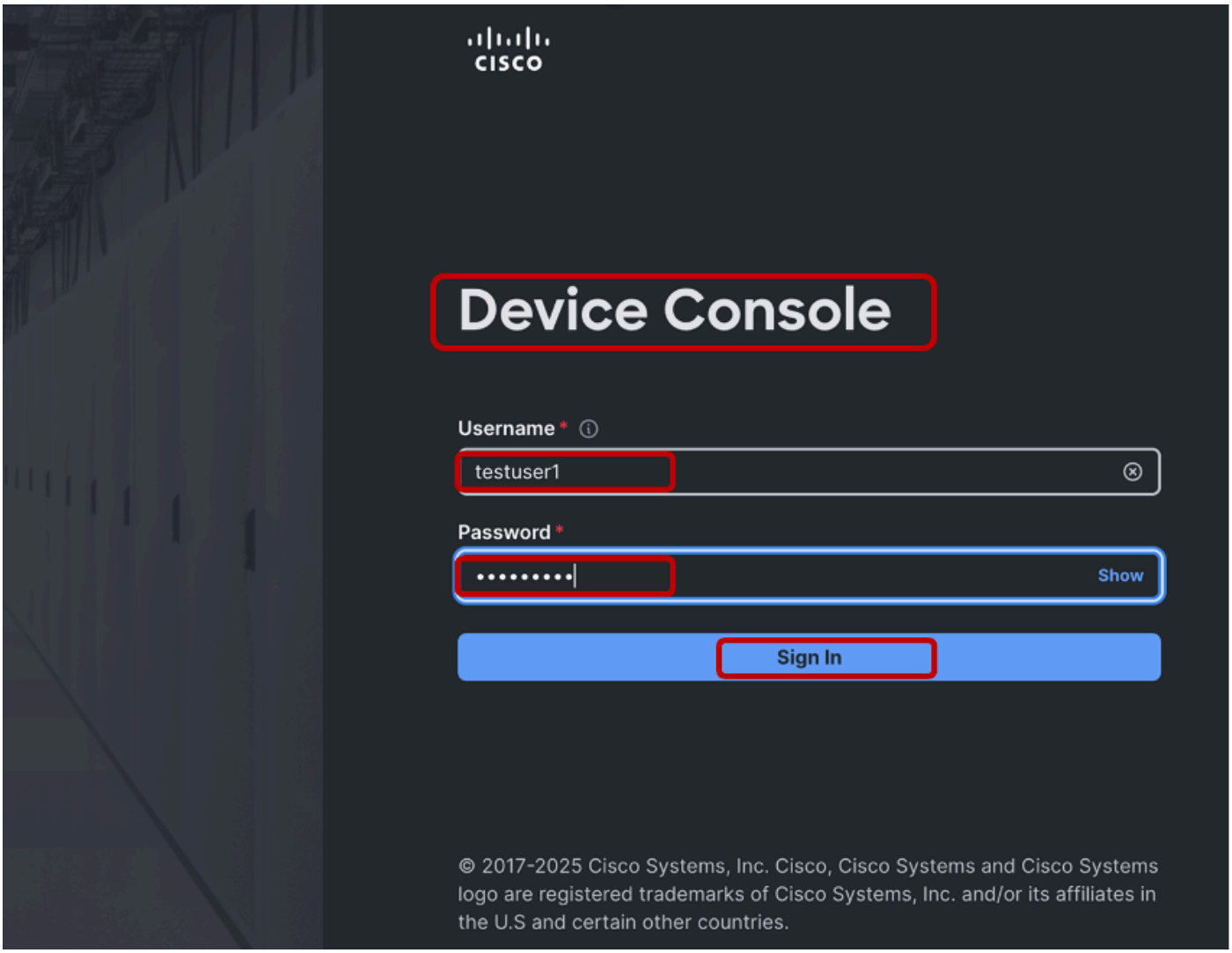
Haga clic en Next (Siguiente), Save and Deploy the domain profile.

Una vez implementada correctamente el perfil de dominio, se completa la configuración LDAP segura para el dominio IMM.

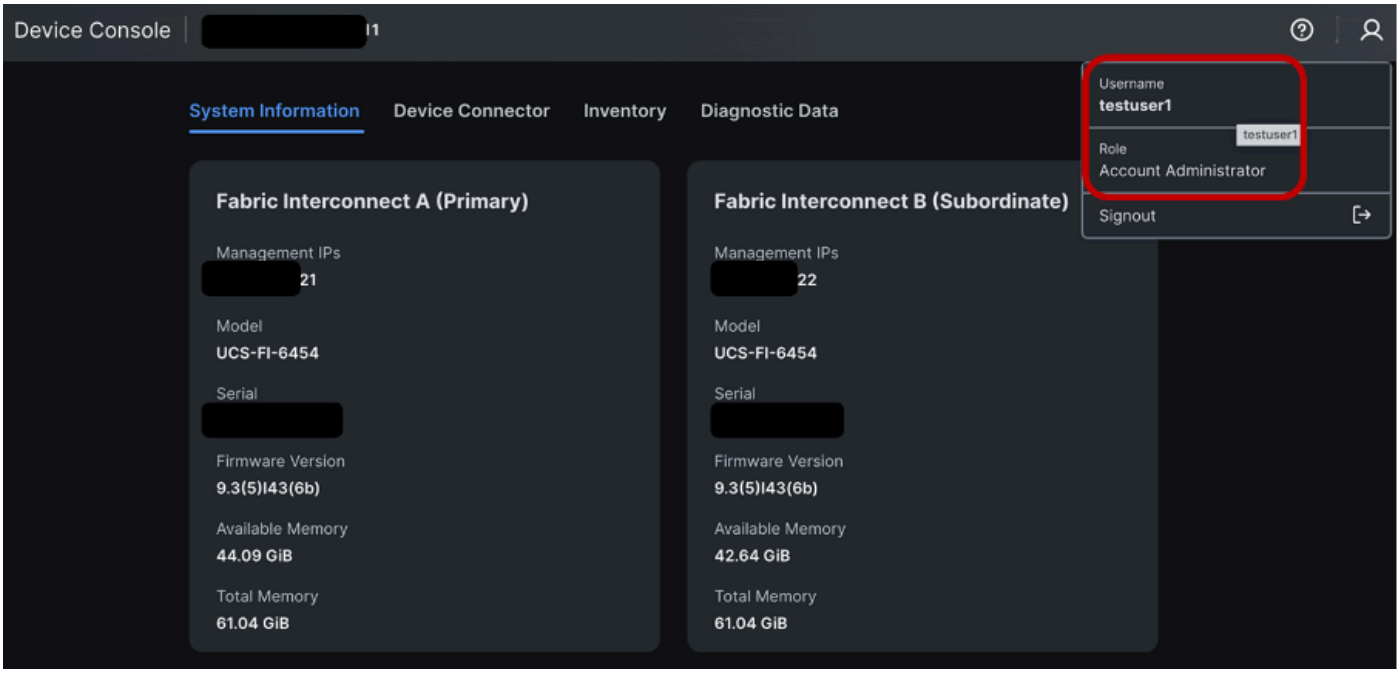
Verificación

Para verificarlo, intente iniciar sesión en la GUI de Device Console y en la CLI de Fabric Interconnects mediante uno de los usuarios LDAP/Active Directory configurados.

Probar inicio de sesión de Device Console

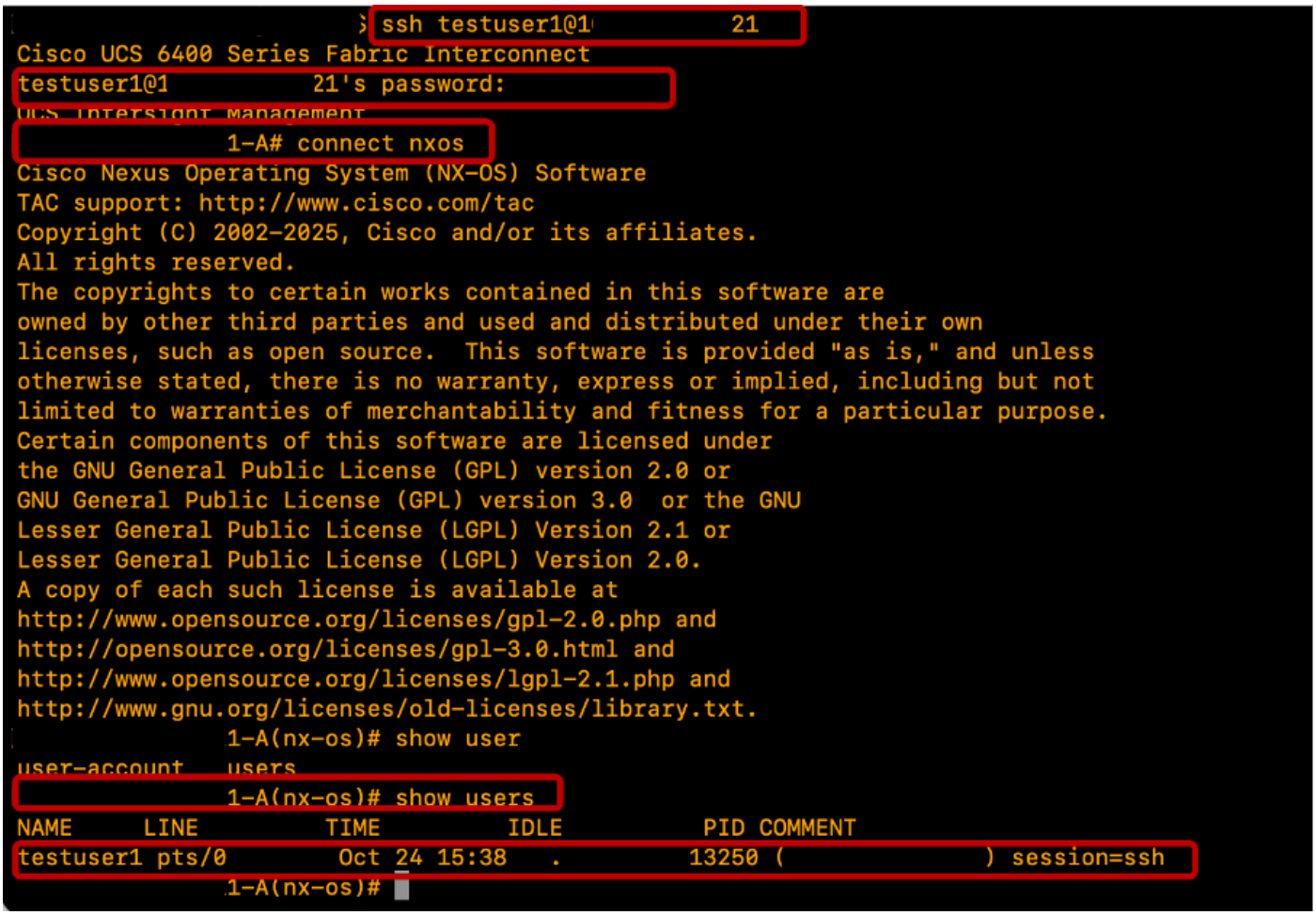


El inicio de sesión en la consola del dispositivo Testuser1 se ha realizado correctamente.



Test FIs SSH Login

El inicio de sesión SSH de Testuser1 se ha realizado correctamente.



Información Relacionada

- Centro de ayuda de Intersight
- Guía de administración de Fabric Interconnect en modo administrado de Cisco Intersight

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).