Beveiligde LDAP-toegang configureren voor verbindingsverbindingen in de Intersight Manage-modus (HTTP-apparaatconsole en SSH)

Inhoud

Inleiding

In dit document wordt beschreven hoe domein-LDAP-verificatie in een Intersight SaaS-instantie kan worden geconfigureerd met behulp van het LDAP-beleid.

Voorwaarden

Vereisten

Kennis van deze onderwerpen:

- Het Lightweight Directory Access Protocol (LDAP) protocol.
- DNS-server (Domain Name Server).
- Cisco Intersight

Gebruikte componenten

- Cisco Intersight SaaS-exemplaar
- Microsoft Active Directory
- DNS-server
- Microsoft Active Directory Certificate Services (AD CS)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

LDAP is een bekend protocol dat wordt gebruikt om toegang te krijgen tot bronnen vanuit een directory via het netwerk. Deze mappen slaan informatie op over gebruikers, organisaties en bronnen. LDAP biedt een standaardproces voor toegang tot en beheer van die informatie die kan worden gebruikt voor authenticatie- en autorisatieprocessen.

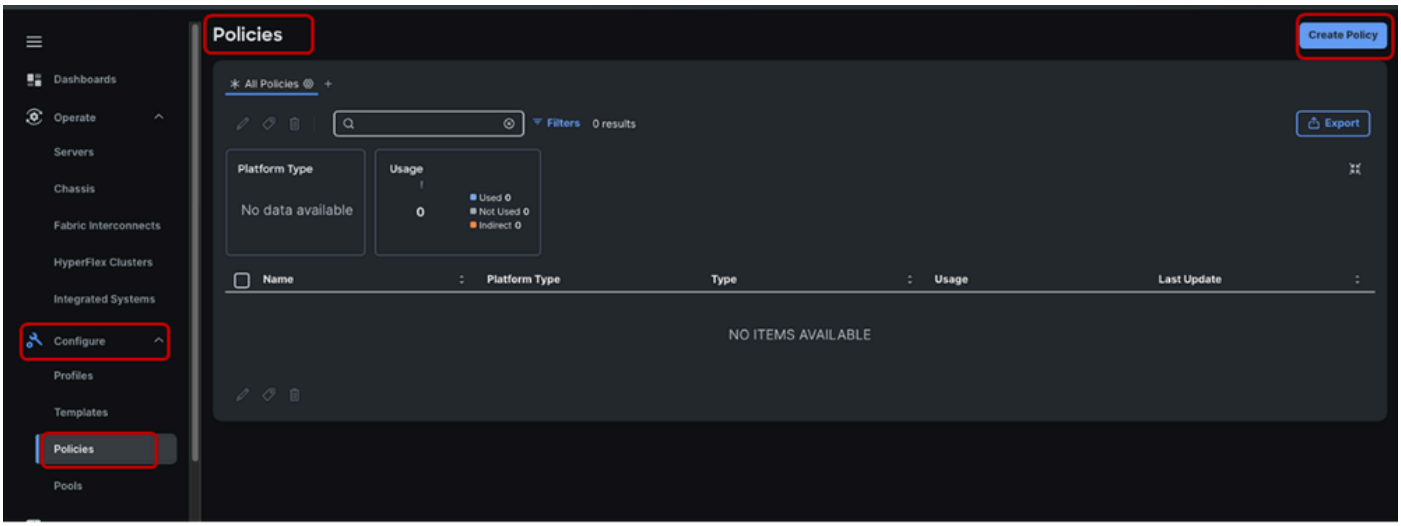
In dit document wordt het configuratieproces beschreven voor externe verificatie via beveiligde LDAP naar de apparaatconsole of CLI (respectievelijk HTTP of SSH) van een peer of Fabric Interconnects in de beheerde modus Intersight.

Configuratie

Het LDAP-beleid configureren

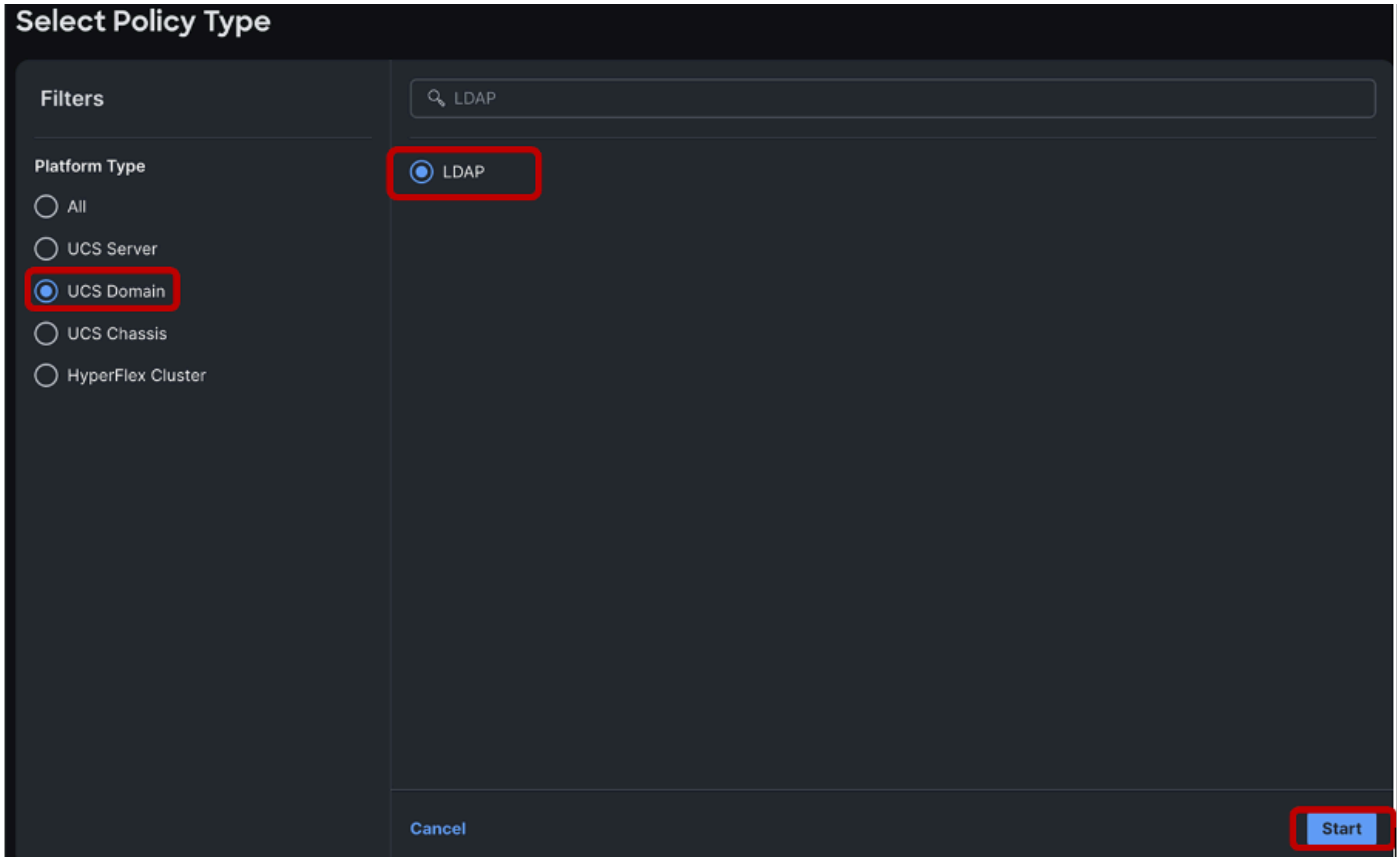
Als u het LDAP-beleid wilt configureren, meldt u zich aan bij de instantie Intersight SaaS.

Navigeer naar de sectie Configureren > Klik op Beleid.
Navigeer naar het venster Beleid > Selecteer Beleid maken.

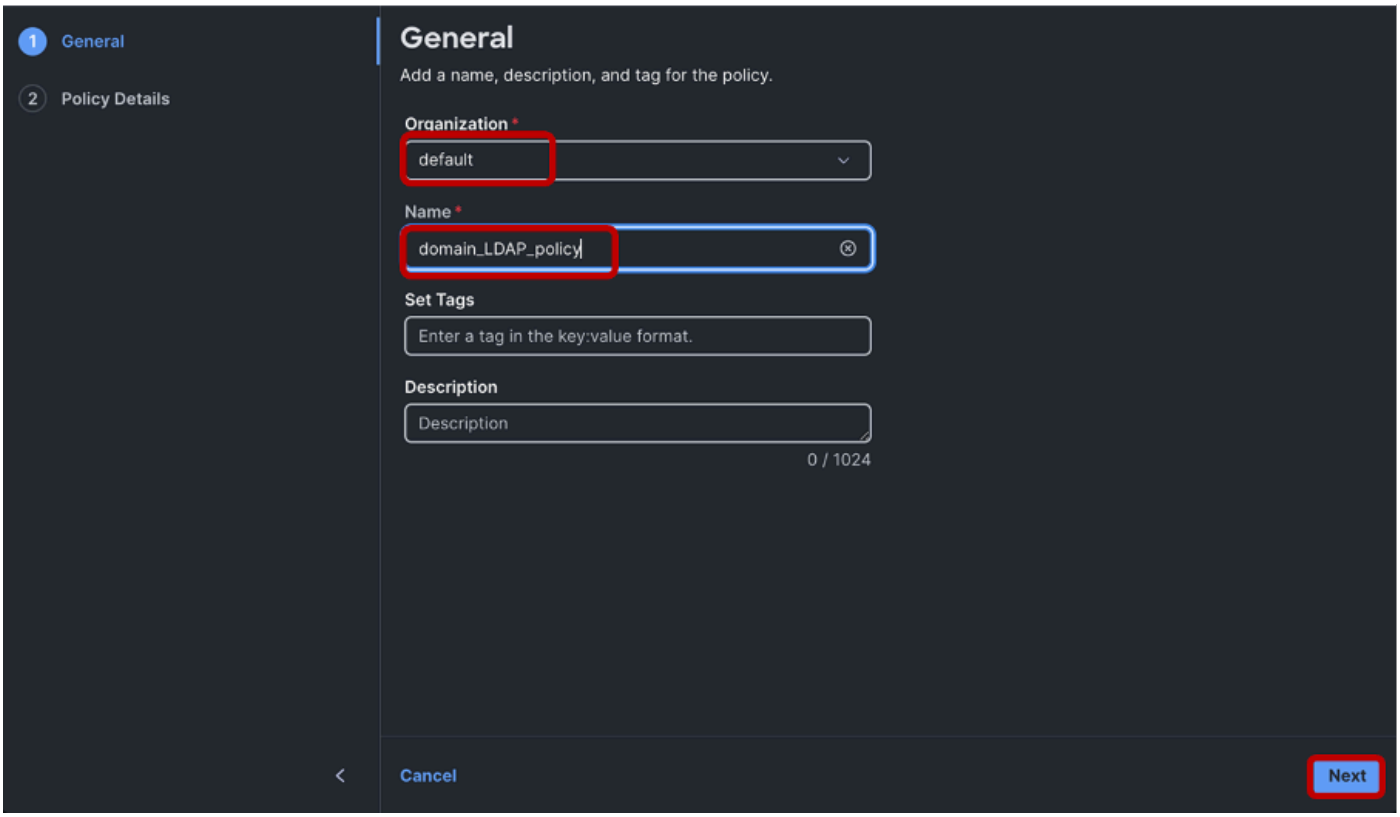


Zoek in de zoekbalk naar "LDAP".

Selecteer het keuzerondje LDAP > Klik op Starten.

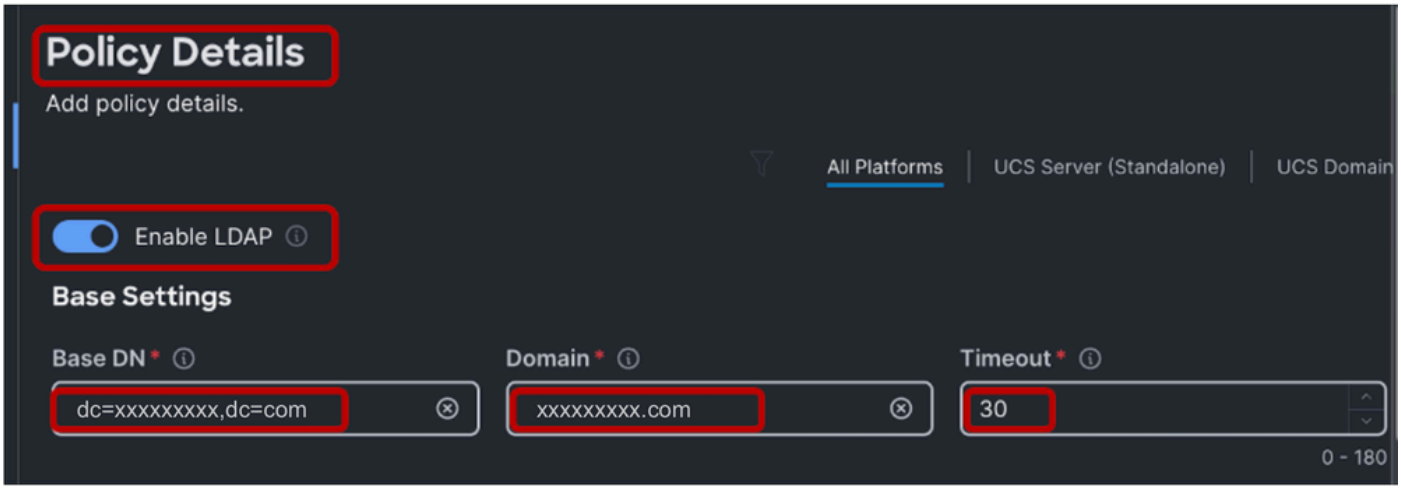


Kies in het venster Maken > Uw gewenste organisatie > Naam van het LDAP-beleid > Klik op Volgende:



Selecteer in de sectie Beleidsdetails > Selecteer de schuifregelaar LDAP inschakelen > De waarden voor basis-DN, domein en time-out populeren.

De waarde voor de time-out wordt standaard ingesteld op 30 seconden wanneer deze wordt ingesteld tussen 0 en 29. Voor deze demonstratie is "xxxxxxxxx.com" het gewenste domein dat al is geconfigureerd op de LDAP-server en is een time-outwaarde van 30 seconden opgegeven.

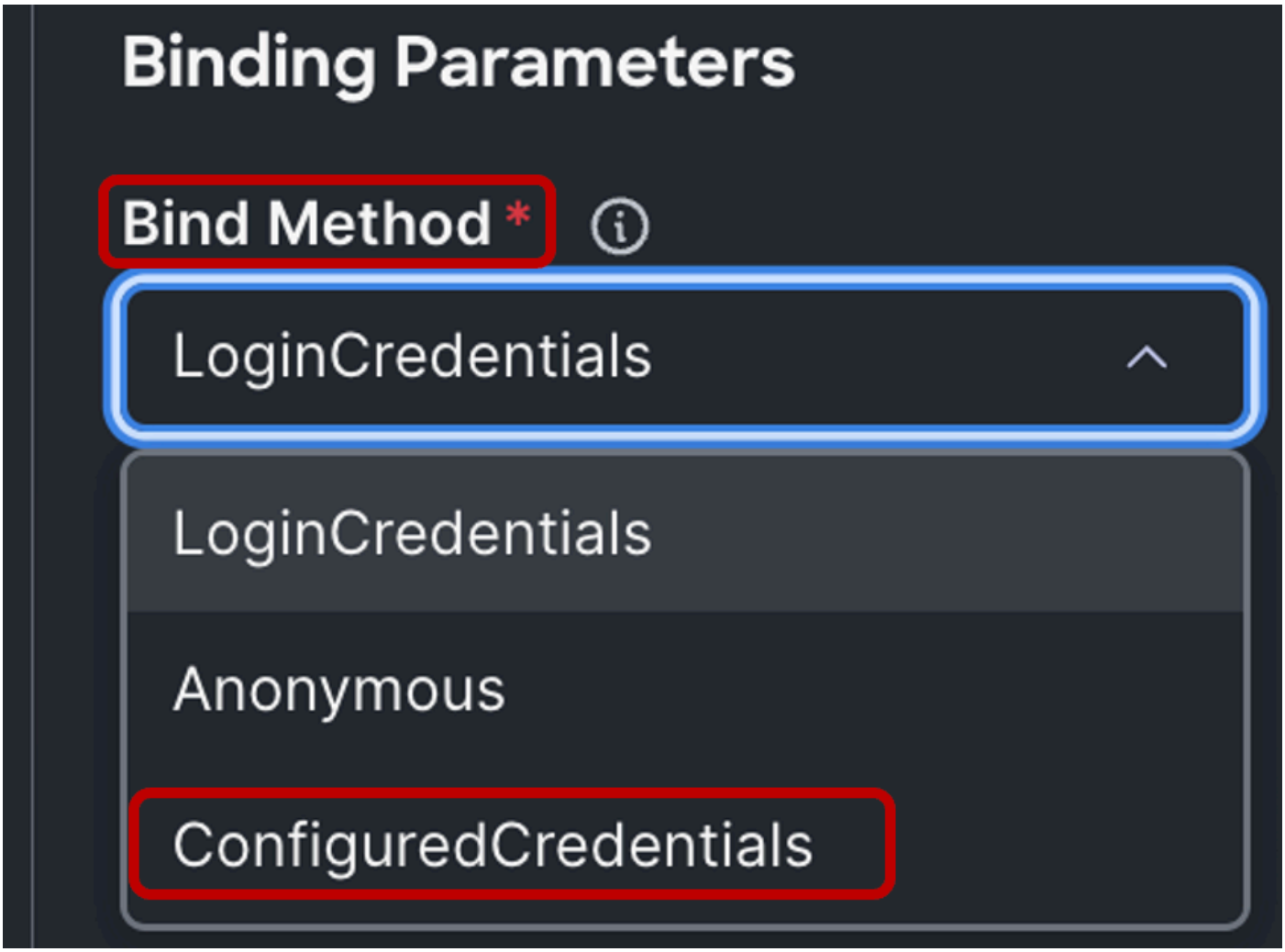


Als u Secure LDAP wilt configureren, schakelt u het keuzerondje Encryptie inschakelen in.

Opmerking: de gebruikelijke LDAP-configuratie kan een IP-adres of een FQDN gebruiken, maar een ondertekend certificaat is geen vereiste. Daarom kunnen bij het configureren van "Standaard" LDAP de optie Codering inschakelen, het netwerkverbindingsbeleid van DNS Server en een certificaat in configuraties voor certificaatbeheer worden genegeerd. Voor Secure LDAP is een DNS-server vereist die is geconfigureerd voor de naamresolutie van de LDAP-server en een basiscertificaat.

Onder de sectie Bindende parameters is de standaardinstelling LoginCredentials, waarbij de individuele verificatie van de LDAP-referenties van de gebruiker wordt gebruikt voor de bindbewerking. Hierdoor hoeft u geen speciale Bindende gebruiker te configureren.

Voor deze demonstratie wordt een Bindende gebruiker geconfigureerd. Daarom wordt de "Bindmethode" gewijzigd in "Geconfigureerde referenties".

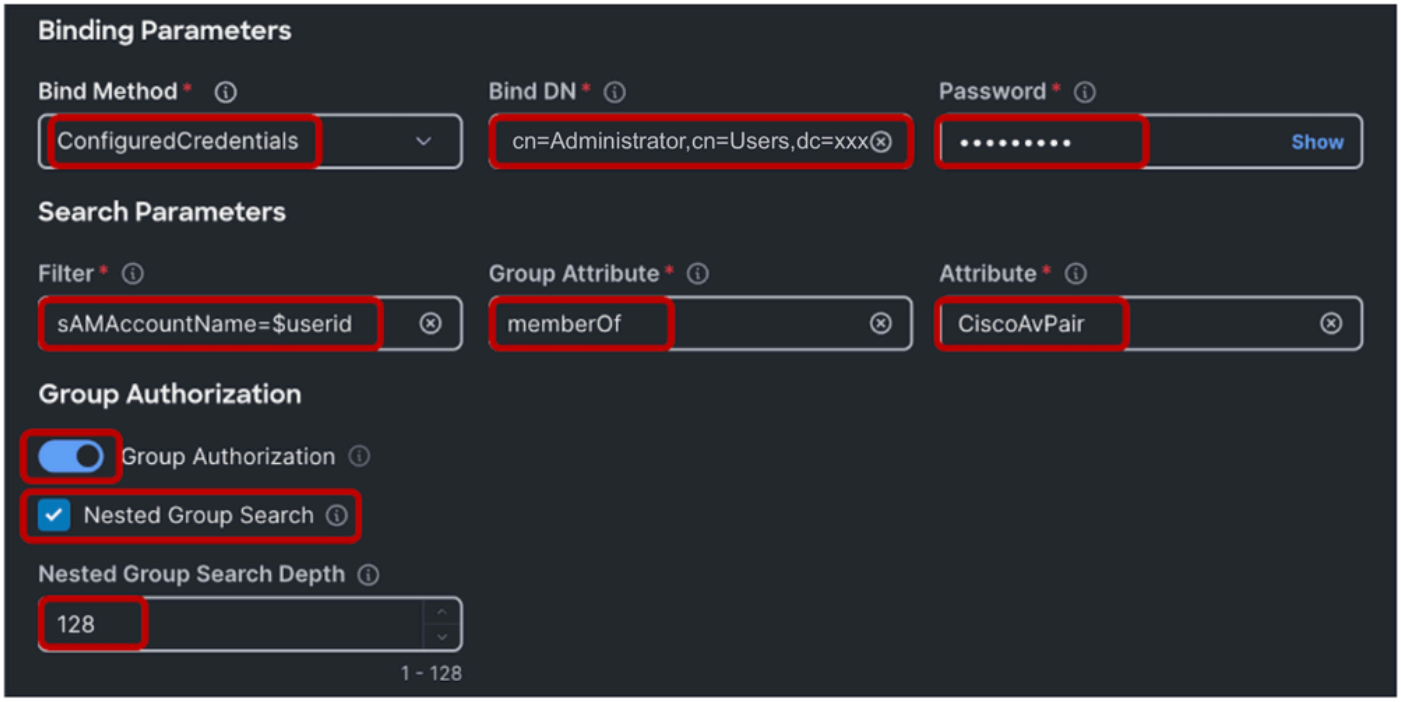


Voeg vervolgens een bindend DN (een gebonden gebruiker) en het wachtwoord voor een gebonden gebruiker toe. Dit kan elke gebruiker configureren in Windows Active Directory. In deze demonstratie wordt de gebruiker Administrator gebruikt.

"cn=Administrator, cn=Users, dc=xxxxxxxx, dc=com".

Voer in de sectie Zoekparameters onder Filter "sAMAaccountName=$userid" in.

Voeg voor Groepskenmerken "memberOf" toe en voeg in het veld Attributen "CiscoAvPair" toe. Afhankelijk van de configuratie van uw LDAP-server kunt u Groepsautorisatie en Zoeken in geneste groepen inschakelen. Voor deze demonstratie wordt de standaardzoekdiepte voor geneste groepen op 128 gebruikt.



In de sectie "Configure LDAP Servers" (LDAP-servers configureren) > Voer het IP-adres of FQDN van de LDAP-server in (vereist voor Secure LDAP) en het poortnummer (389).

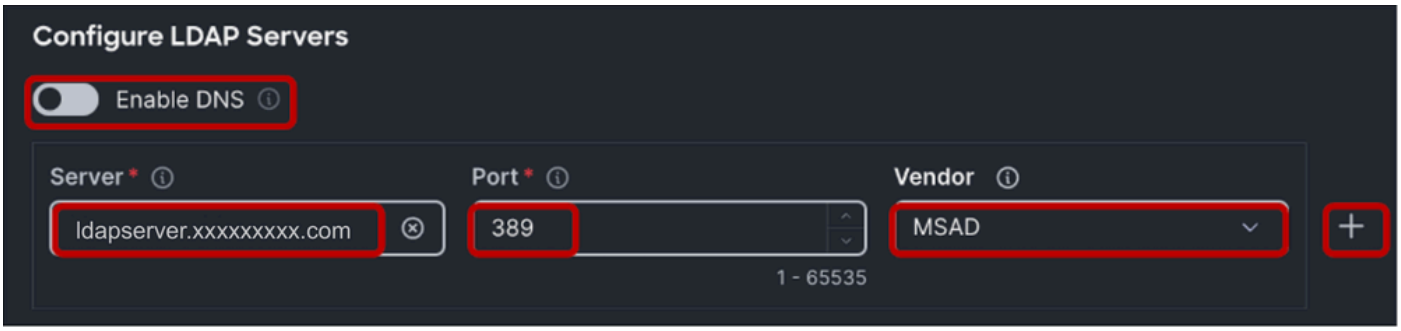
Secure LDAP in UCS maakt gebruik van STARTTLS om gecodeerde communicatie mogelijk te maken met behulp van poort 389.

Houd er rekening mee dat het wijzigen van de poort van 389 naar 636 authenticatiefouten kan veroorzaken. Cisco UCS voert TLS-onderhandelingen uit op poort 636 voor SSL; de eerste verbinding wordt echter altijd ongecodeerd tot stand gebracht op poort 389.

Selecteer de LDAP-serverleverancier. De beschikbare opties voor leveranciers zijn OpenLDAP en MSAD (Microsoft Active Directory). Voor deze demonstratie wordt MSAD gebruikt omdat de LDAP-server die wordt gebruikt Windows Server 2019 is.

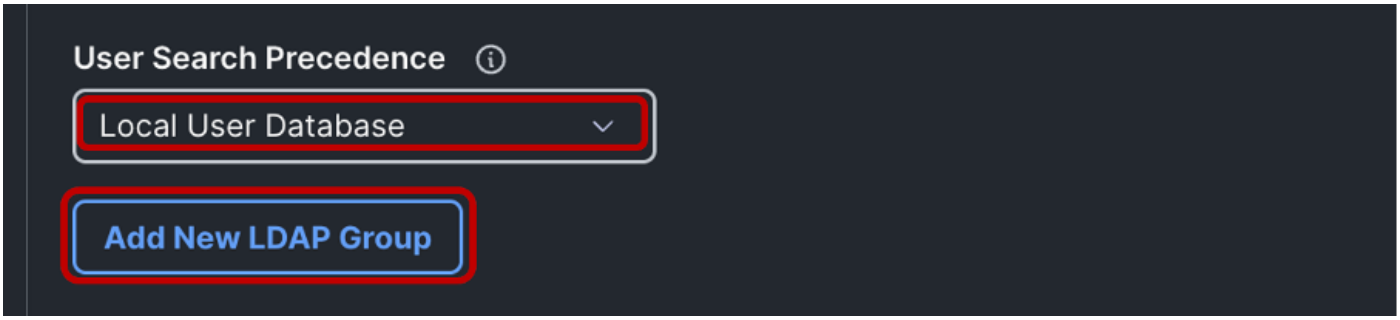
Laat de knop DNS inschakelen uitgeschakeld omdat deze optie niet van toepassing is op LDAP-configuratie in UCS-domein.

Meerdere LDAP-servers kunnen worden geconfigureerd door te klikken op het "+"-pictogram uiterst rechts van de geconfigureerde LDAP-server.

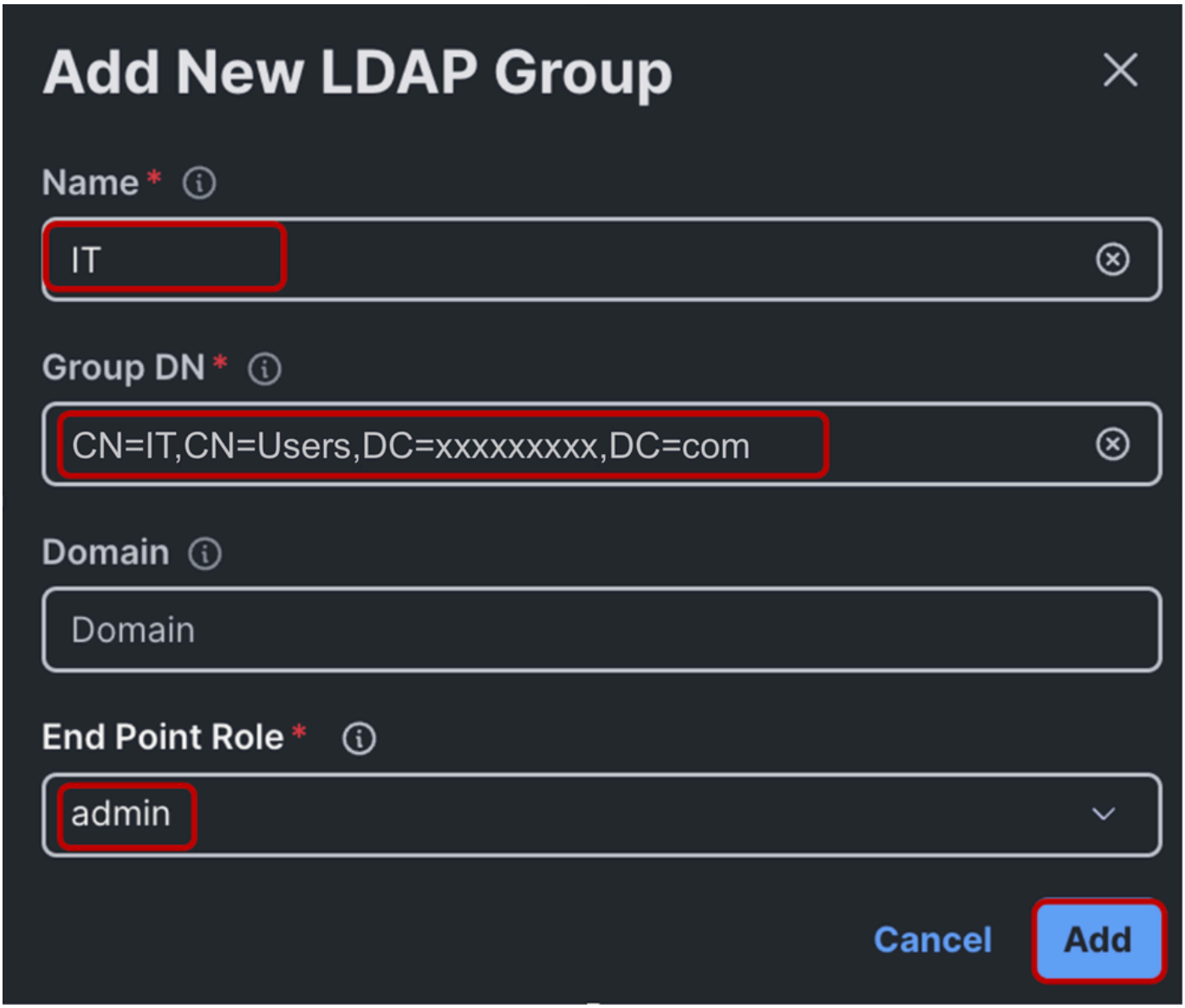


Opmerking: U kunt de voorrang voor zoekopdrachten van gebruikers behouden als lokale gebruikersdatabase of wijzigen in LDAP-gebruikersdatabase, afhankelijk van uw gebruikssituatie.

Ga vervolgens verder met het toevoegen van een groep-DN die overeenkomt met de groep die is geconfigureerd in de LDAP-server, door op de knop Nieuwe LDAP-groep toevoegen te klikken.



Geef de groep een naam, voeg de groep-DN toe die u van de LDAP-server hebt ontvangen en selecteer de gewenste eindpuntrol.

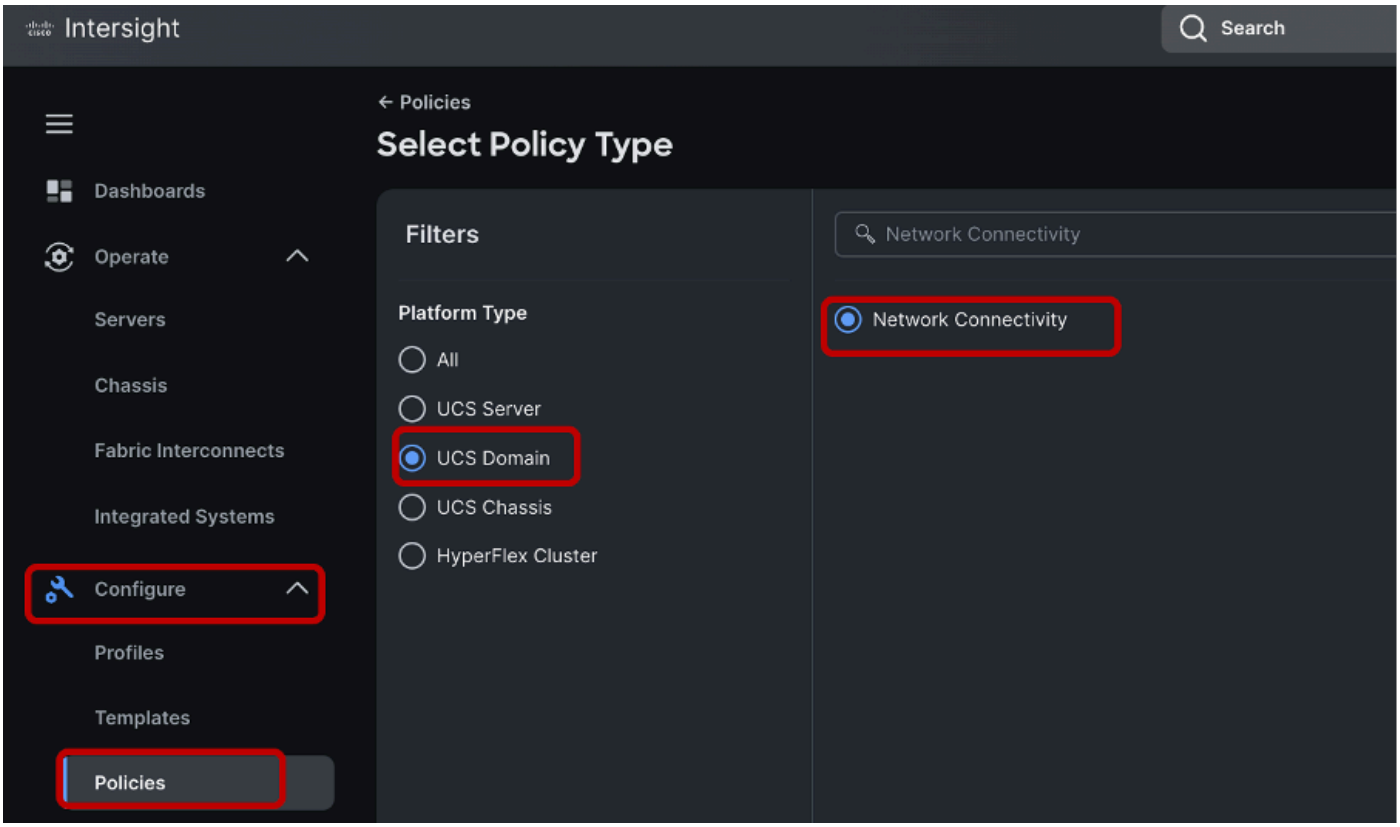


Klik op Toevoegen > Aanmaken om het LDAP-beleid te maken

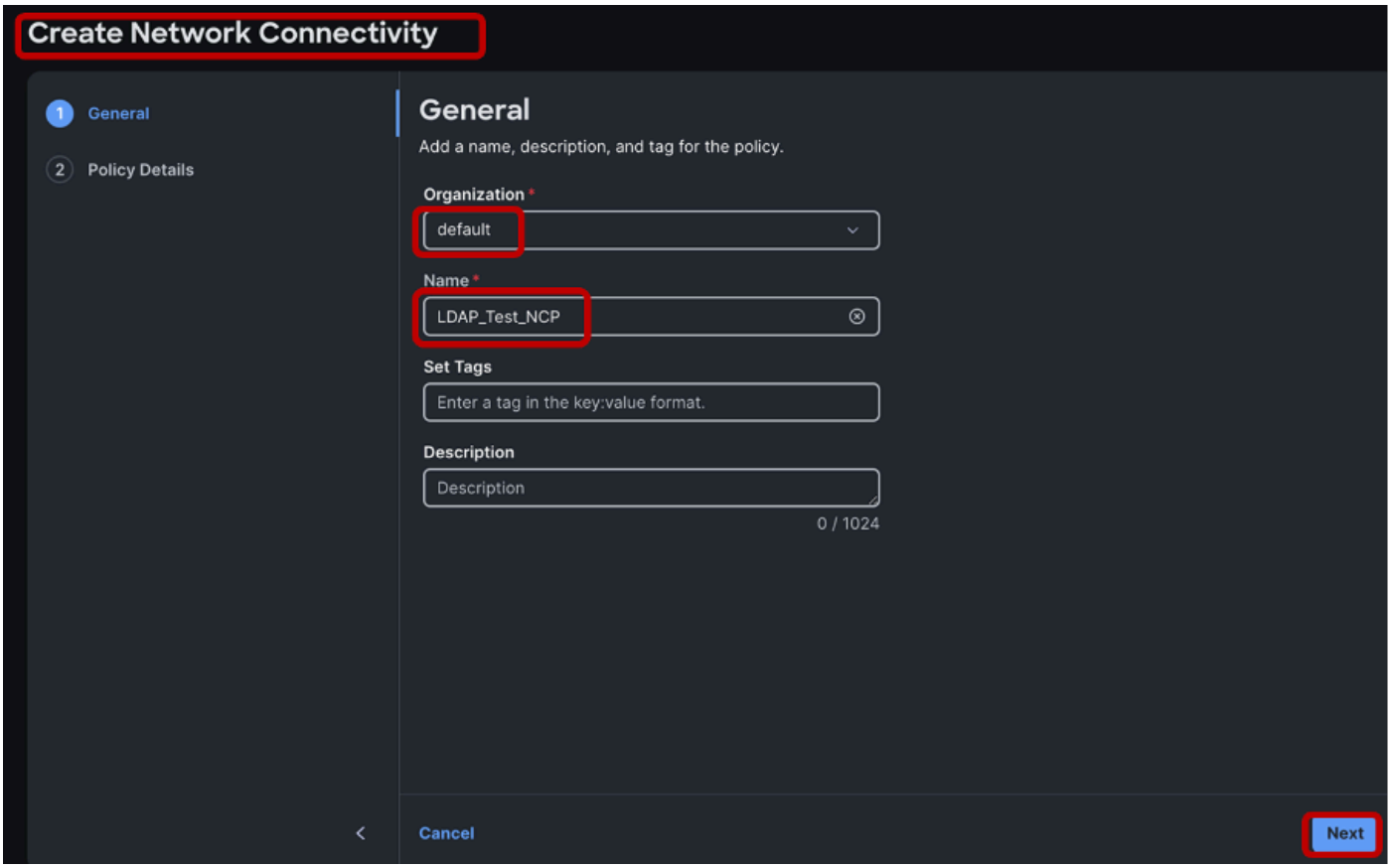
Opmerking: voor domein-LDAP-beleidsconfiguratie is de enige ondersteunde eindpuntrol "admin" vanaf het moment dat dit document wordt gemaakt.

Beleid voor netwerkconnectiviteit configureren

Configureer een DNS-server voor het UCS-domein door een netwerkverbindingsbeleid te maken.

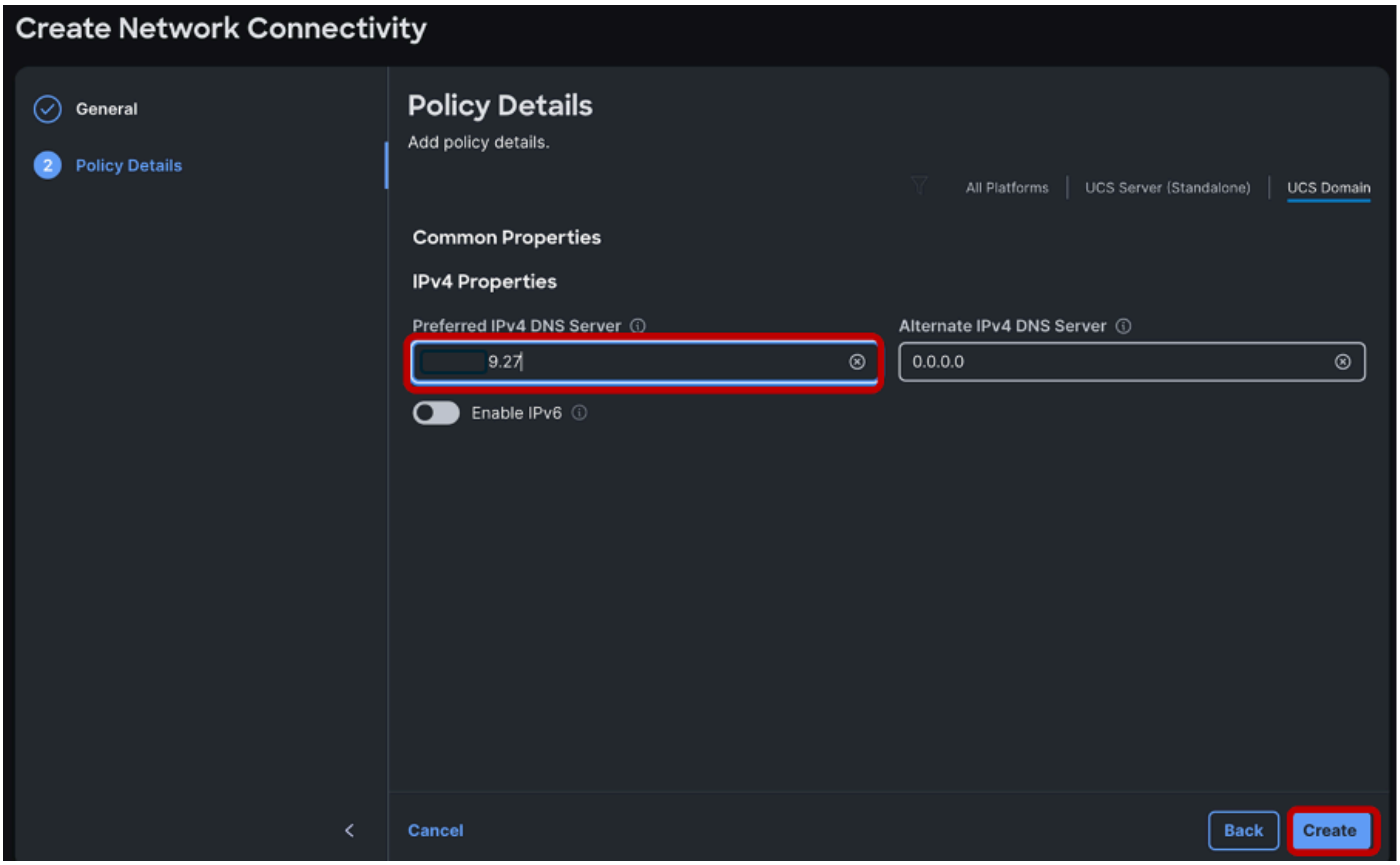


Selecteer de juiste organisatie > Voer de naam van het beleid in > Klik op Volgende.



Definieer een IPv4-adres voor de voorkeurs-DNS-server en klik op Maken om het beleid op te

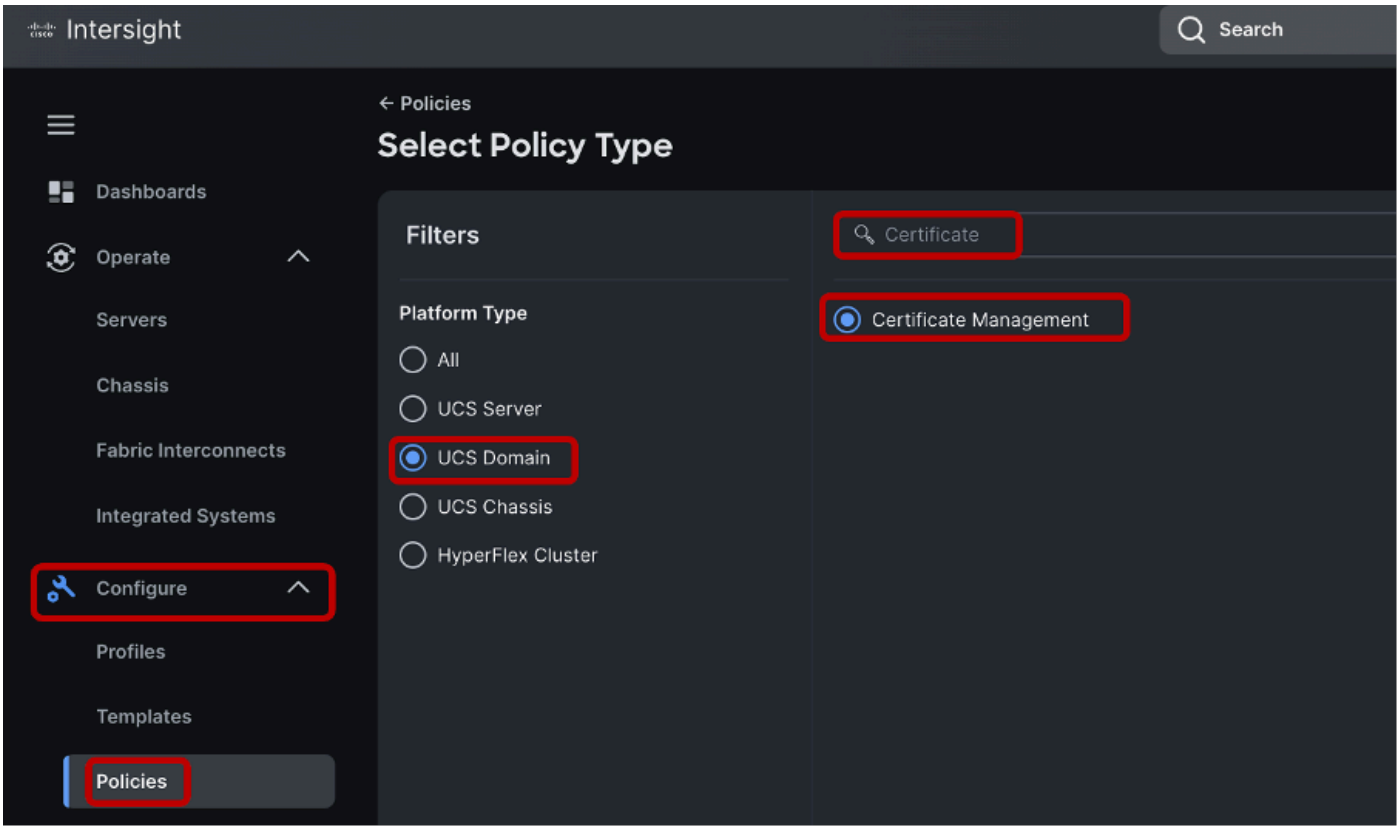
slaan.



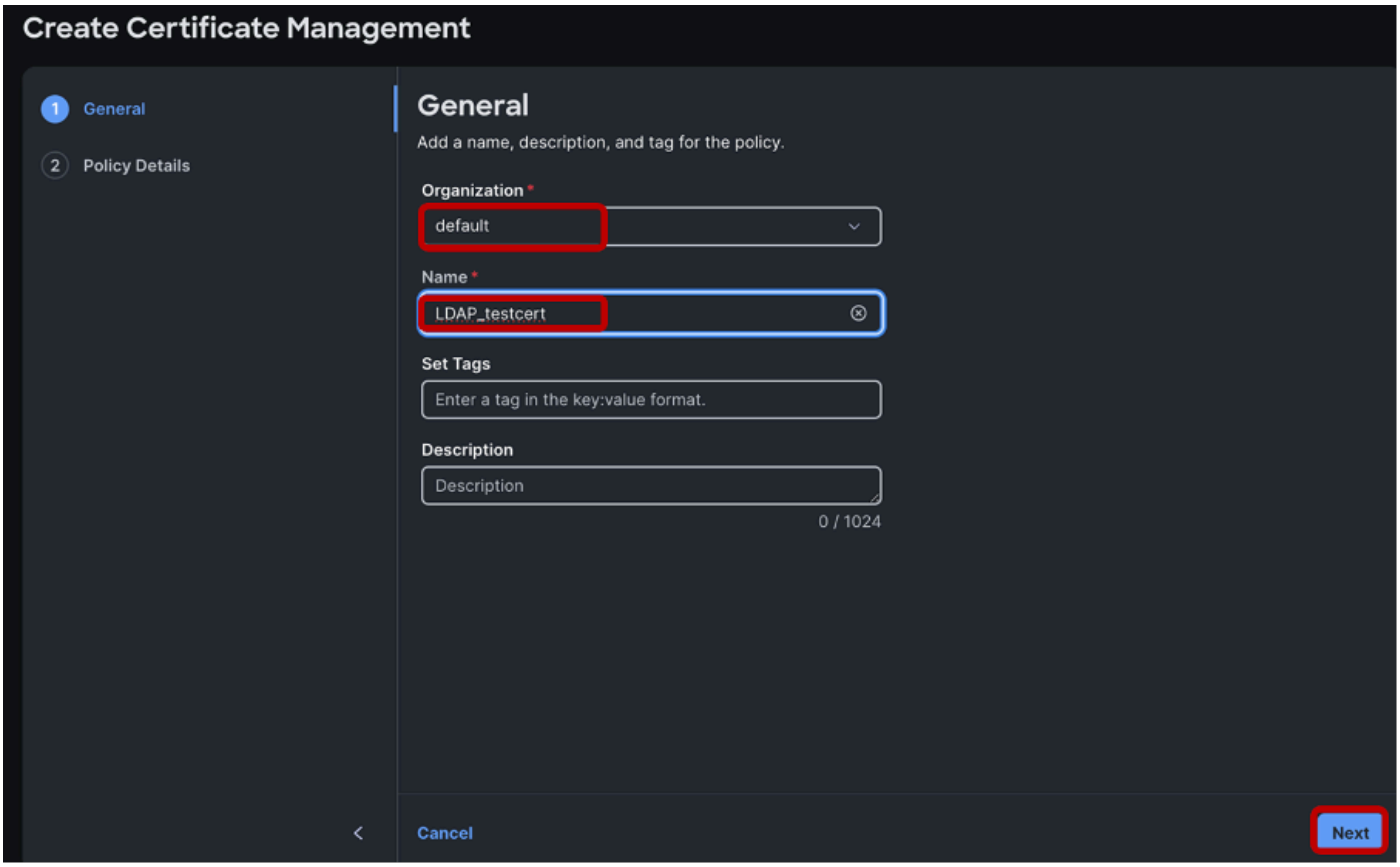
Zorg ervoor dat het IP-adres van een DNS-server is geconfigureerd en bereikbaar is voor naamresolutie. Zorg ervoor dat de naamresolutie functioneel is voor de LDAP-server en de verbindingslijnen binnen het domein. Voor deze demonstratie bevindt de DNS-server zich op dezelfde Windows-systeeminstantie als de LDAP-server.

Certificaatbeheerbeleid configureren

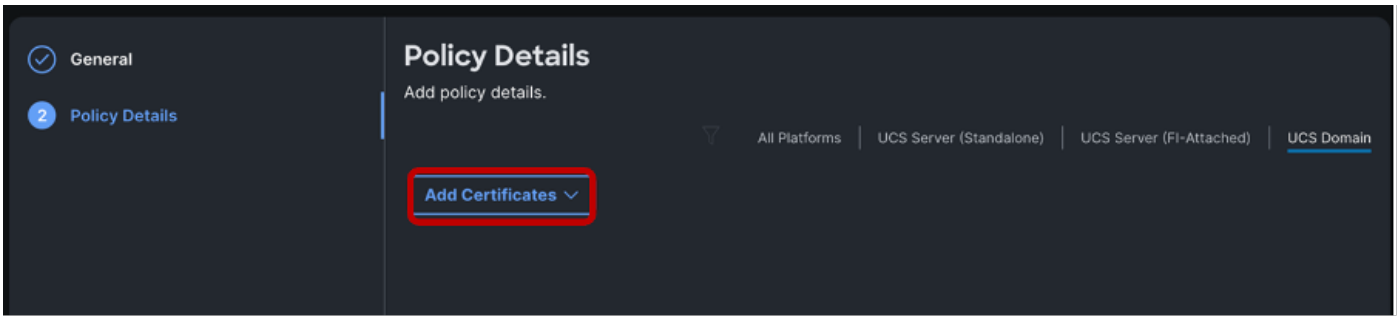
Configureer vervolgens een beleid voor certificaatbeheer. Dit is nodig om LDAP-codering te laten functioneren.



Selecteer de juiste organisatie, noem het beleid > Klik op Volgende

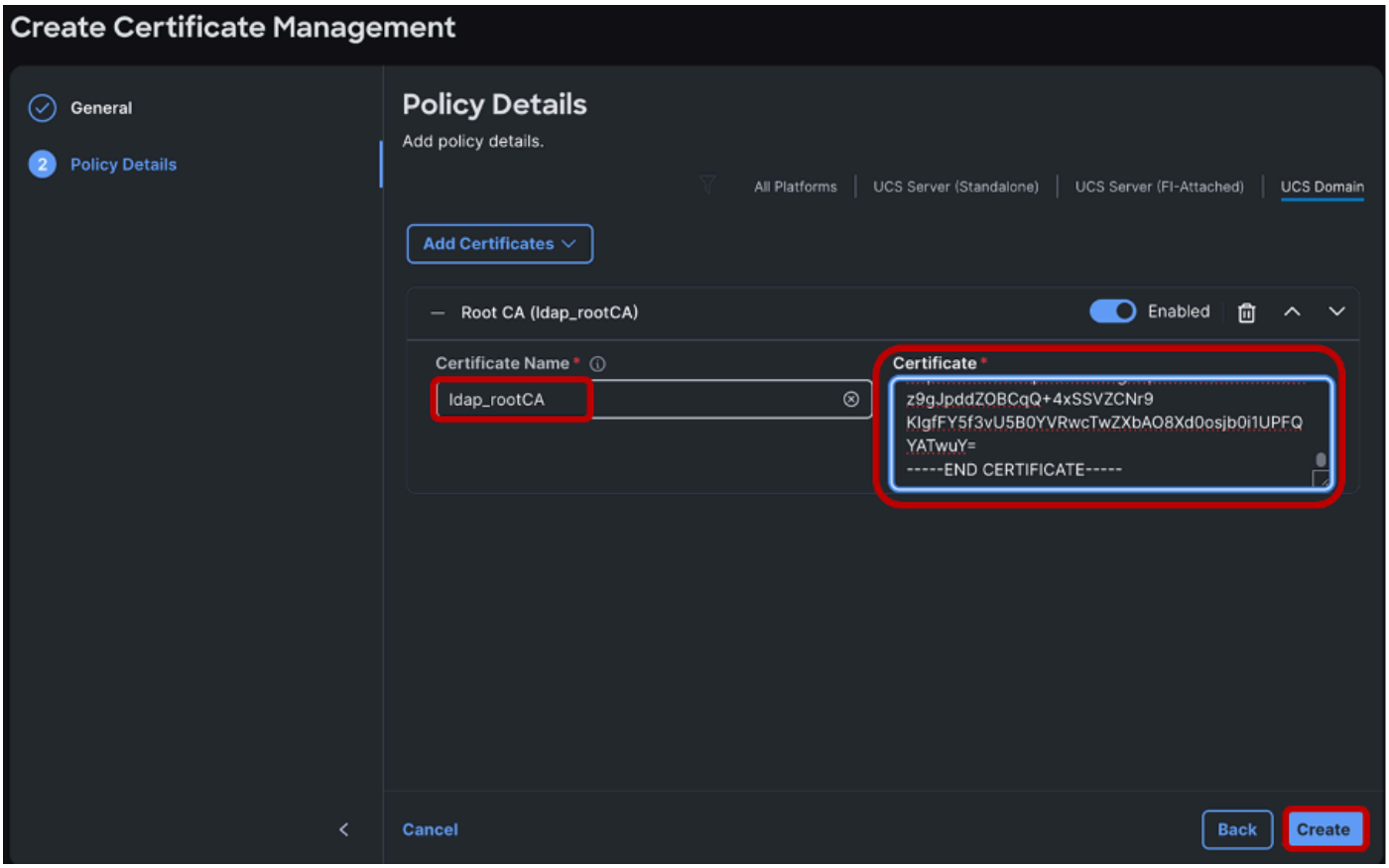


Klik op Certificaten toevoegen.

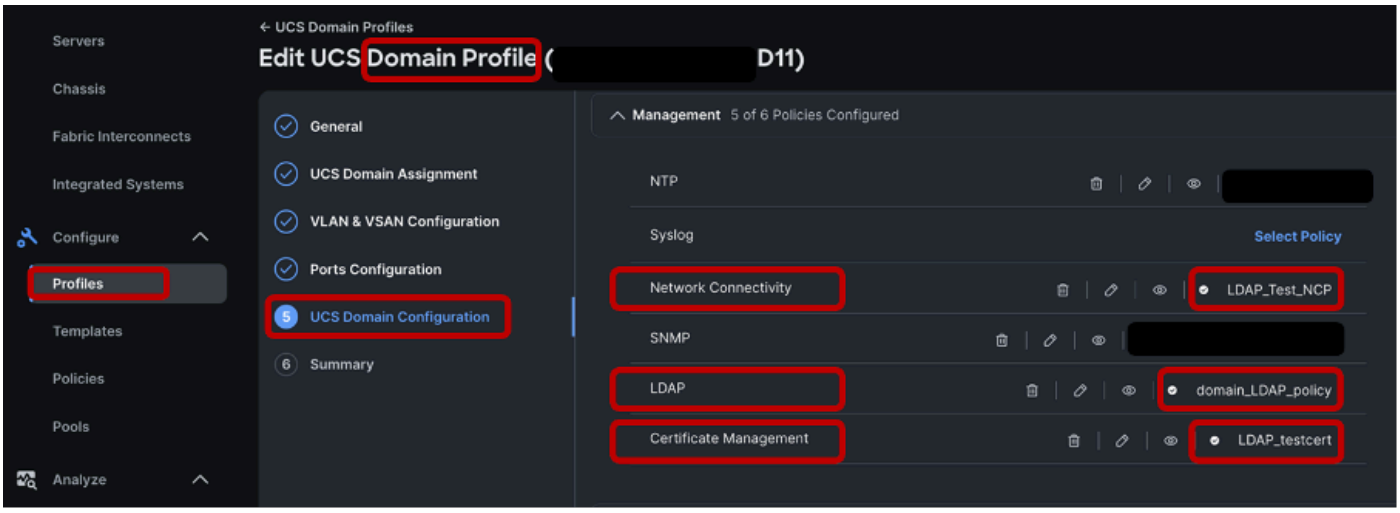


Geef het certificaat een naam en plak het in het hoofdcertificaat van de Microsoft Active Directory Certificate Services.

Klik op Maken.



Nadat het LDAP-, Network Connectivity- en Certificate Management-beleid is gemaakt, verwijst u naar het nieuw gemaakte beleid in het gewenste domeinprofiel onder de sectie "UCS Domain Configuration", zoals wordt weergegeven.



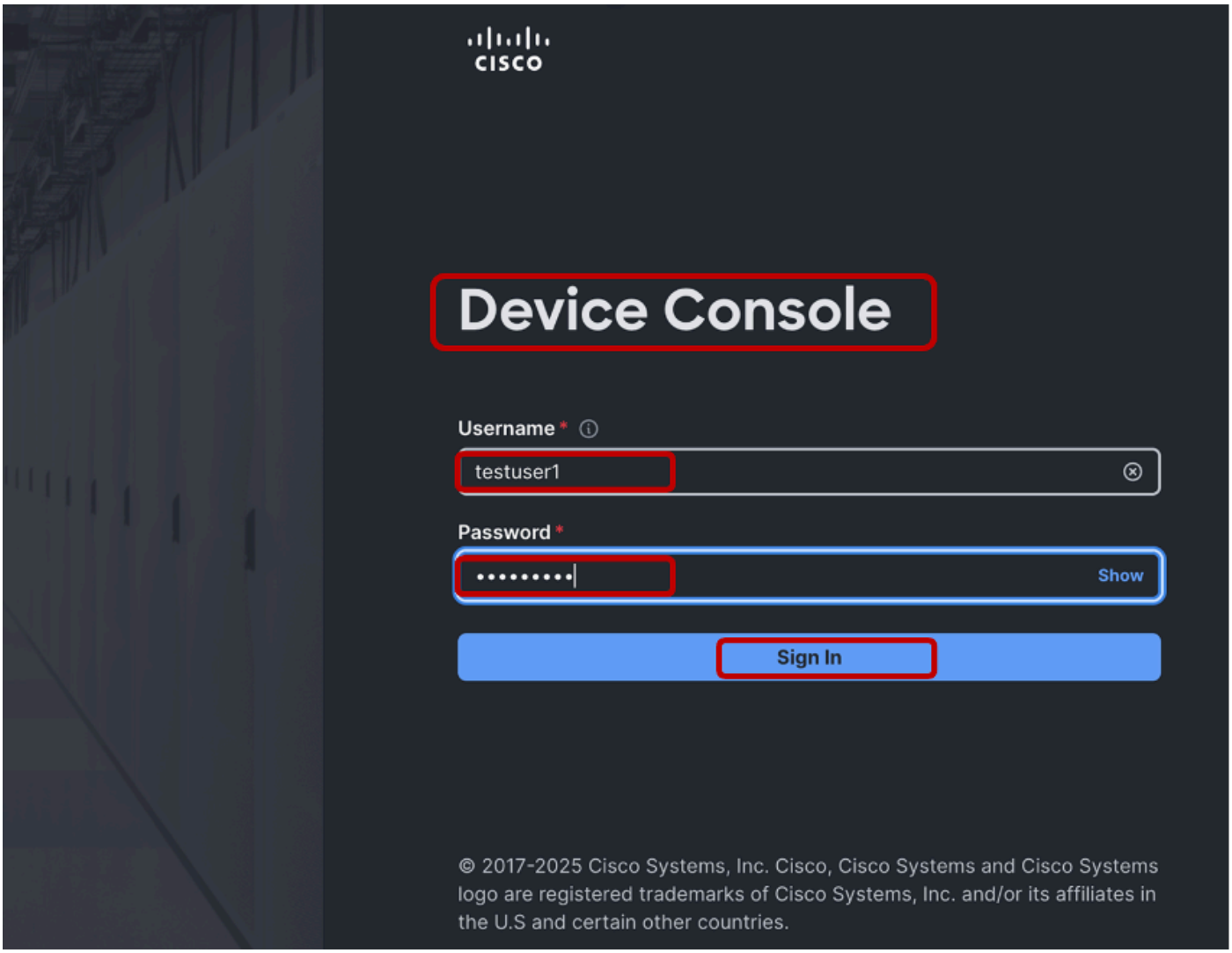
Klik op Volgende, Sla het domeinprofiel op en implementeer het.

Na succesvolle implementatie van het domeinprofiel is de beveiligde LDAP-configuratie voor het IMM-domein voltooid.

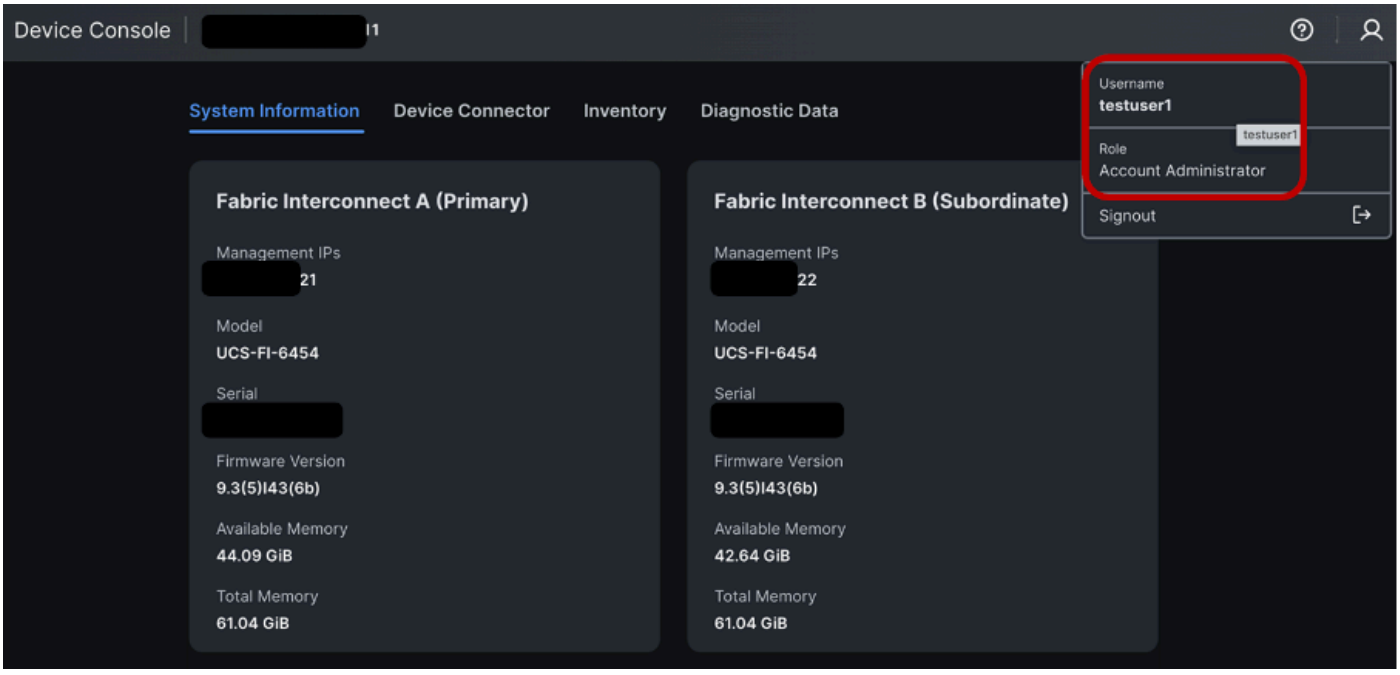
Verificatie

Om dit te controleren, probeert u zich aan te melden bij de apparaatconsole-GUI en verbind u de CLI met een van de geconfigureerde LDAP/Active Directory-gebruikers.

Aanmelding apparaatconsole testen

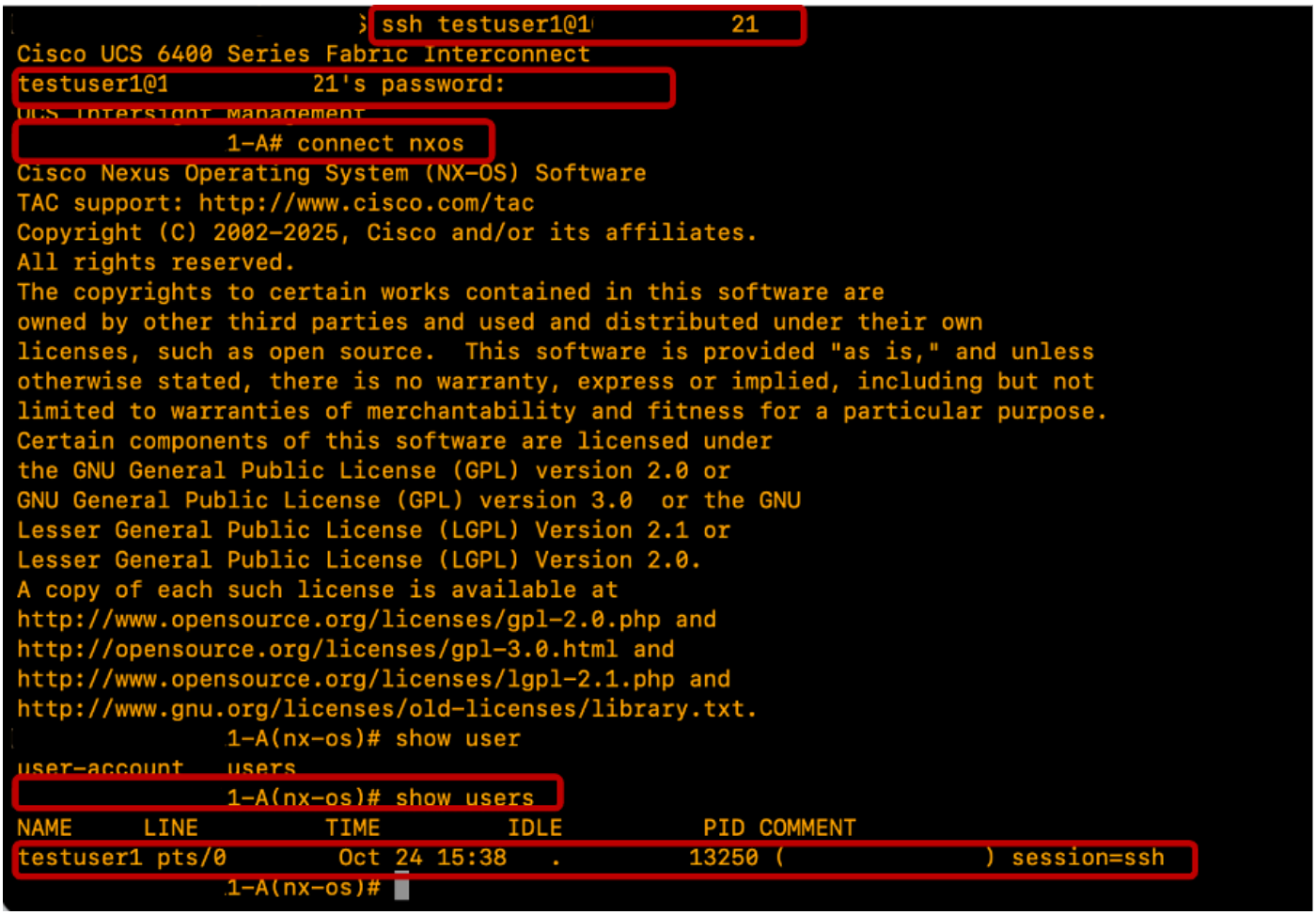


De aanmelding voor de testuser1-apparaatconsole is voltooid.



Aanmelden bij FI's SSH testen

De aanmelding bij Testuser1 SSH is succesvol.



Gerelateerde informatie

- Helpcentrum Intersight
- Cisco Intersight Managed Mode Fabric Interconnect-beheerdershandleiding

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.