

# Configurar acesso LDAP seguro para interconexões em malha no modo de gerenciamento de interceptação (Console de dispositivo HTTP e SSH)

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configuração](#)

[Configurar a política LDAP](#)

[Configurar Política de Conectividade de Rede](#)

[Configurar Política de Gerenciamento de Certificados](#)

[Verificação](#)

[Testar login do console do dispositivo](#)

[Testar o login do SSH dos FIs](#)

[Informações Relacionadas](#)

---

## Introdução

Este documento descreve como configurar a autenticação LDAP de domínio em uma instância do SaaS da Intersight usando a Política LDAP.

## Pré-requisitos

### Requisitos

Conhecimento destes tópicos:

- Lightweight Directory Access Protocol (LDAP)
- Servidor DNS (Domain Name Server).
- Entrevista da Cisco

## Componentes Utilizados

- Instância Cisco Intersight SaaS
- Microsoft Active Directory
- Servidor DNS
- Serviços de Certificados do Active Directory (AD CS) da Microsoft

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Informações de Apoio

O LDAP é um protocolo bem conhecido usado para acessar recursos de um diretório na rede. Esses diretórios armazenam informações sobre usuários, organizações e recursos. O LDAP fornece um processo padrão para acessar e gerenciar essas informações que podem ser usadas para processos de autenticação e autorização.

Este documento descreve o processo de configuração para autenticação remota através de LDAP seguro para o Console do dispositivo ou CLI (HTTP ou SSH, respectivamente) de um par de interconexões de estrutura no modo gerenciado de interceptação.

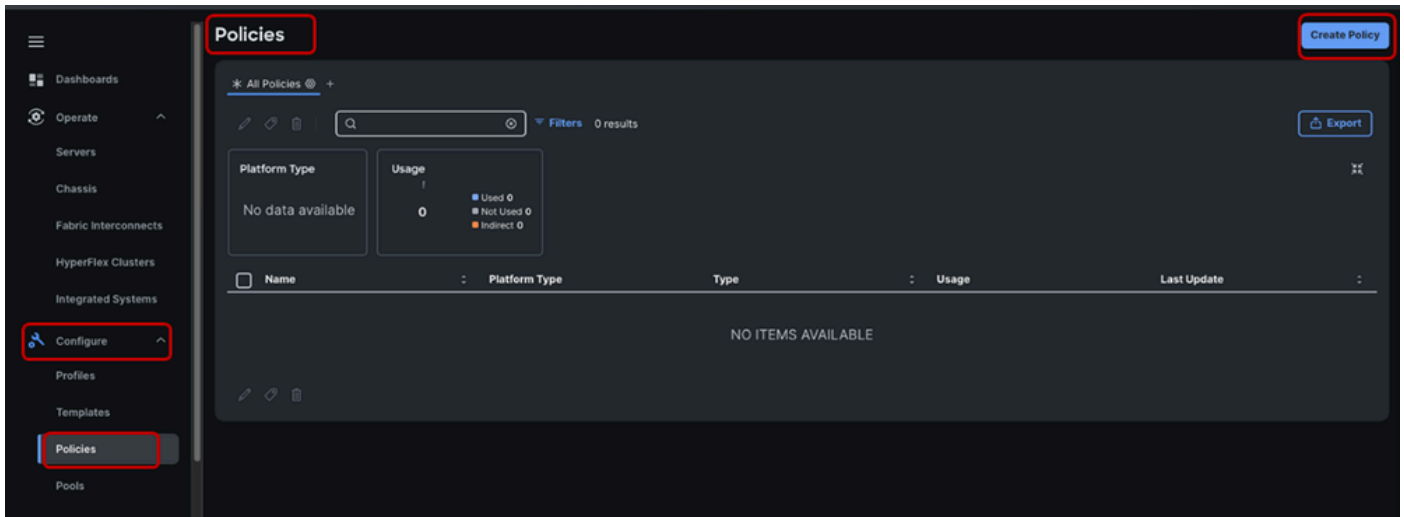
## Configuração

### Configurar a política LDAP

Para configurar a política LDAP, faça login na instância do SaaS da Intersight.

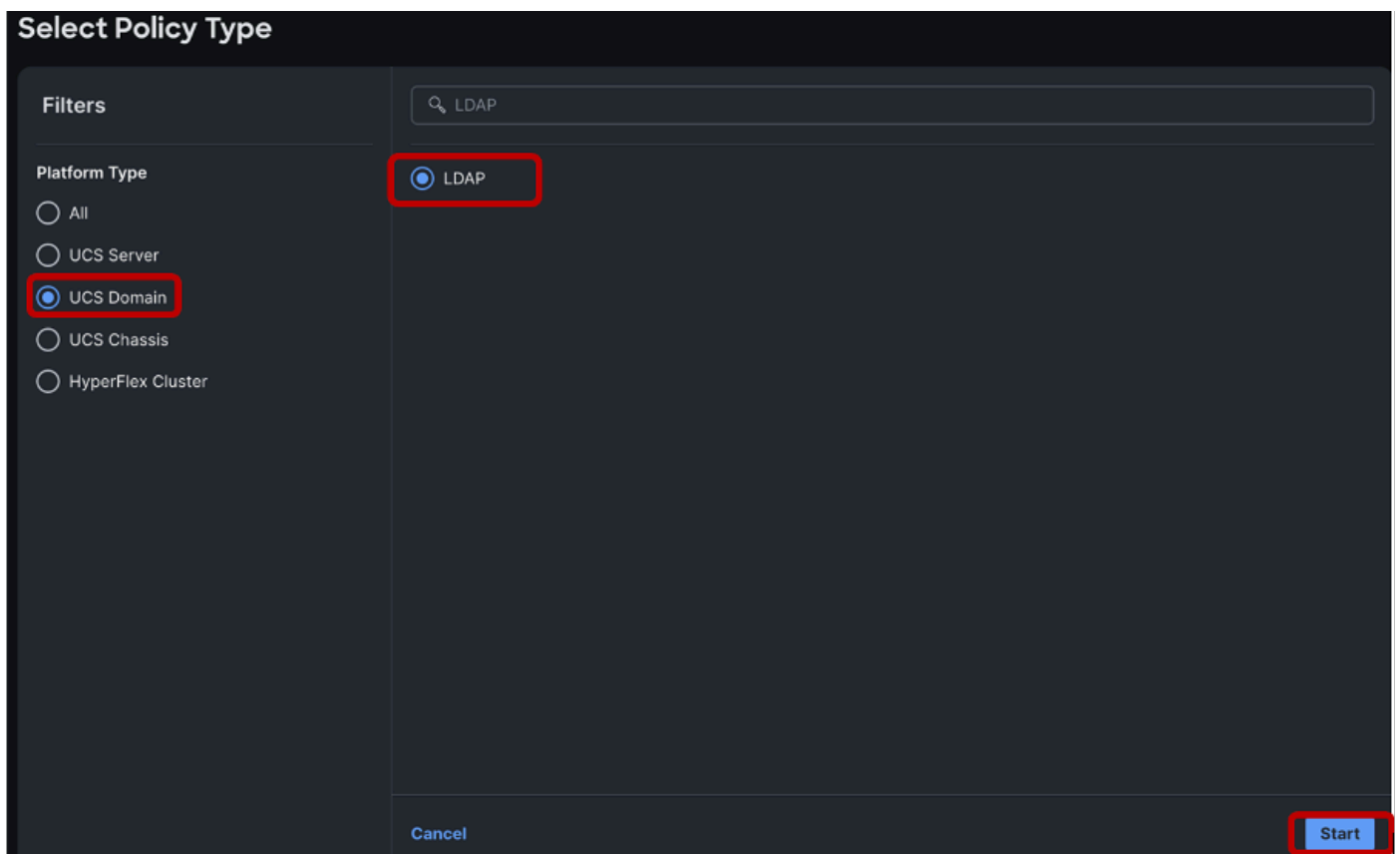
Navegue até a seção Configurar > Clique em Políticas.

Navegue até a janela Políticas > Selecione Criar política.



Na barra de pesquisa, procure por "LDAP".

Selecione o botão de opção LDAP > Clique em Iniciar.



Na janela Criar > Escolha sua organização desejada > Nome a política LDAP > Clique em Avançar:

**1** General

**2** Policy Details

## General

Add a name, description, and tag for the policy.

**Organization \***  
default

**Name \***  
domain\_LDAP\_policy

**Set Tags**  
Enter a tag in the key:value format.

**Description**  
Description  
0 / 1024

[Cancel](#) [Next](#)

Na seção Detalhes da política > Selecione o controle deslizante Habilitar LDAP > Preencher os valores DN base, Domínio e Tempo limite.

Os valores de tempo limite quando definidos entre 0 e 29, automaticamente assumem o padrão de 30 segundos. Para esta demonstração, "xxxxxxxx.com" é o domínio desejado já configurado no servidor LDAP e um valor de tempo limite de 30 segundos foi especificado.

## Policy Details

Add policy details.

All Platforms | UCS Server (Standalone) | UCS Domain

Enable LDAP ⓘ

### Base Settings

**Base DN \*** ⓘ  
dc=xxxxxxxx,dc=com

**Domain \*** ⓘ  
xxxxxxxx.com

**Timeout \*** ⓘ  
30

0 - 180

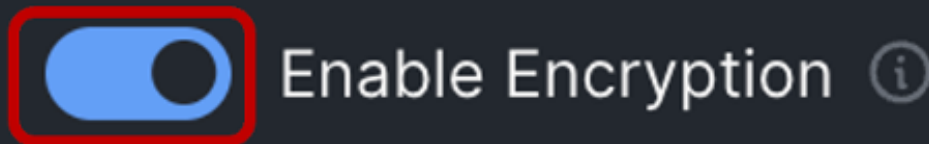
Para configurar o LDAP seguro, habilite o botão de opção Habilitar criptografia.



---

Note: A configuração LDAP comum pode utilizar um endereço IP ou um FQDN, mas um certificado assinado não é um requisito. Portanto, ao configurar o LDAP "Padrão", a opção Habilitar Criptografia, a Política de Conectividade de Rede do Servidor DNS e um Certificado nas configurações da Política de Gerenciamento de Certificados podem ser ignorados. O LDAP seguro requer um servidor DNS configurado para a resolução de nomes de servidores LDAP e um certificado raiz.

---



Na seção Parâmetros de vinculação, a configuração padrão é LoginCredentials, que utiliza a autenticação individual das credenciais LDAP do usuário para a operação de vinculação. Isso elimina a necessidade de configurar um usuário de vinculação dedicado.

Para esta demonstração, um usuário de vinculação é configurado. Portanto, o "Método de vinculação" é alterado para "ConfiguredCredentials".

# Binding Parameters

**Bind Method \***



LoginCredentials



LoginCredentials

Anonymous

ConfiguredCredentials

Em seguida, adicione um DN de vinculação (um Usuário de vinculação) e a Senha de usuário de vinculação. Pode ser qualquer usuário configurado no Windows Active Directory. Nesta demonstração, o usuário Administrador é usado.

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

Na seção Parâmetros de pesquisa, em Filtro, insira "sAMAccountName=\$userid".

Para Atributos de grupo, adicione "memberOf" e, no campo Attribute, adicione "CiscoAvPair". Dependendo da configuração do servidor LDAP, você pode habilitar a Autorização de grupo e a Pesquisa de grupo aninhado. Para esta demonstração, é usada a Profundidade de pesquisa do grupo aninhado padrão em 128.

**Binding Parameters**

Bind Method \* ⓘ  
ConfiguredCredentials

Bind DN \* ⓘ  
cn=Administrator,cn=Users,dc=xxx

Password \* ⓘ  
..... Show

**Search Parameters**

Filter \* ⓘ  
sAMAccountName=\$userid

Group Attribute \* ⓘ  
memberOf

Attribute \* ⓘ  
CiscoAvPair

**Group Authorization**

Group Authorization ⓘ

Nested Group Search ⓘ

Nested Group Search Depth ⓘ  
128

1 - 128

Na seção "Configure LDAP Servers" (Configurar servidores LDAP), insira o endereço IP ou o FQDN do servidor LDAP (necessário para LDAP seguro) e o número da porta (389).

O LDAP seguro no UCS usa STARTTLS para permitir a comunicação criptografada usando a porta 389.

Observe que modificar a porta de 389 para 636 pode causar erros de autenticação. O Cisco UCS executa a negociação TLS na porta 636 para SSL; no entanto, a conexão inicial é sempre estabelecida sem criptografia na porta 389.

Selecione o fornecedor do servidor LDAP. As opções de fornecedor disponíveis são OpenLDAP e MSAD (Microsoft Active Directory). Para esta demonstração, como o servidor LDAP em uso é o Windows Server 2019, o MSAD é usado.

Deixe o botão Enable DNS (Habilitar DNS) DESLIGADO, pois essa opção não se aplica à configuração LDAP no domínio do UCS.

Vários servidores LDAP podem ser configurados clicando no ícone "+" à extrema direita do servidor LDAP configurado.

### Configure LDAP Servers

Enable DNS ⓘ

Server * ⓘ	Port * ⓘ	Vendor ⓘ	
ldapservr.xxxxxxxxx.com ⓘ	389	MSAD	+

1 - 65535



Note: Você pode manter a Precedência de pesquisa do usuário como Banco de dados de usuário local ou alterá-la para Banco de dados de usuário LDAP, dependendo do caso de uso.

Em seguida, prossiga para adicionar um DN de grupo correspondente ao grupo configurado no servidor LDAP, clicando no botão Adicionar novo grupo LDAP.

### User Search Precedence ⓘ

Local User Database

**Add New LDAP Group**

Nomeie o grupo, adicione o DN do grupo recebido do servidor LDAP e selecione a função de ponto final desejada.

# Add New LDAP Group ✕

Name \* ⓘ

Group DN \* ⓘ

Domain ⓘ

End Point Role \* ⓘ

Cancel Add

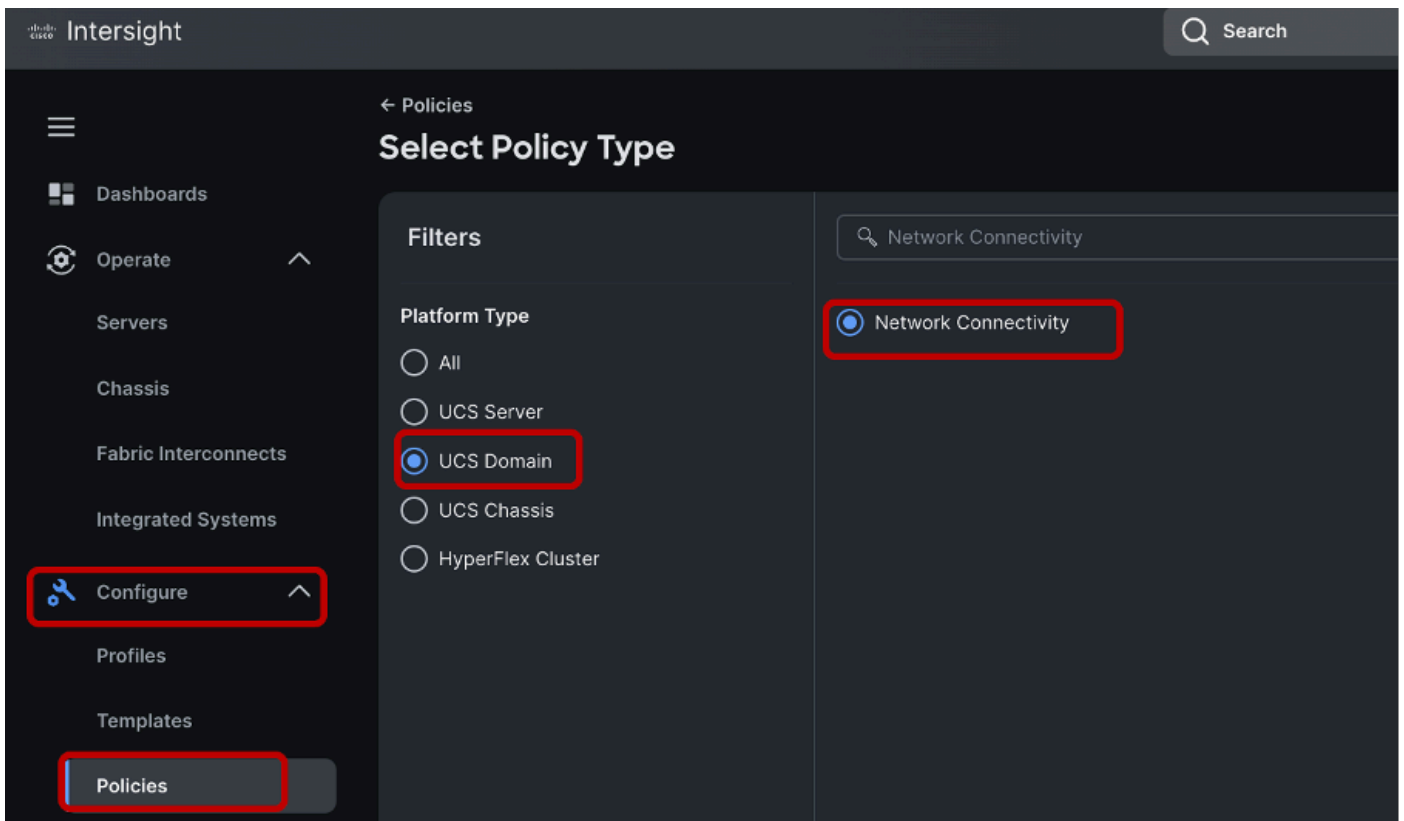
Clique em Adicionar > Selecionar Criar para criar a política LDAP



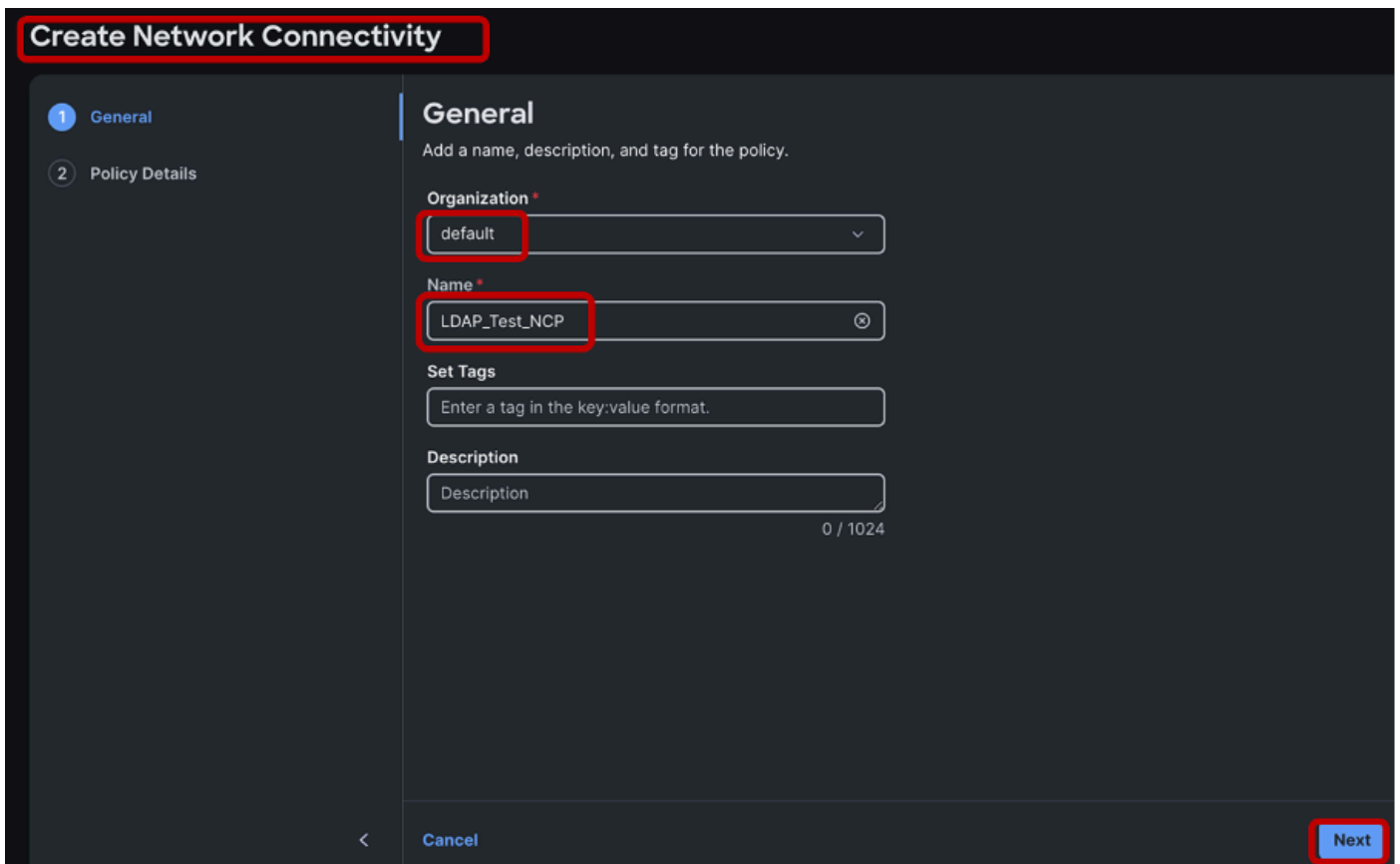
Note: Para a Configuração de Política LDAP do Domínio, a única Função de Ponto de Extremidade com suporte é "admin" no momento da criação deste documento.

## Configurar Política de Conectividade de Rede

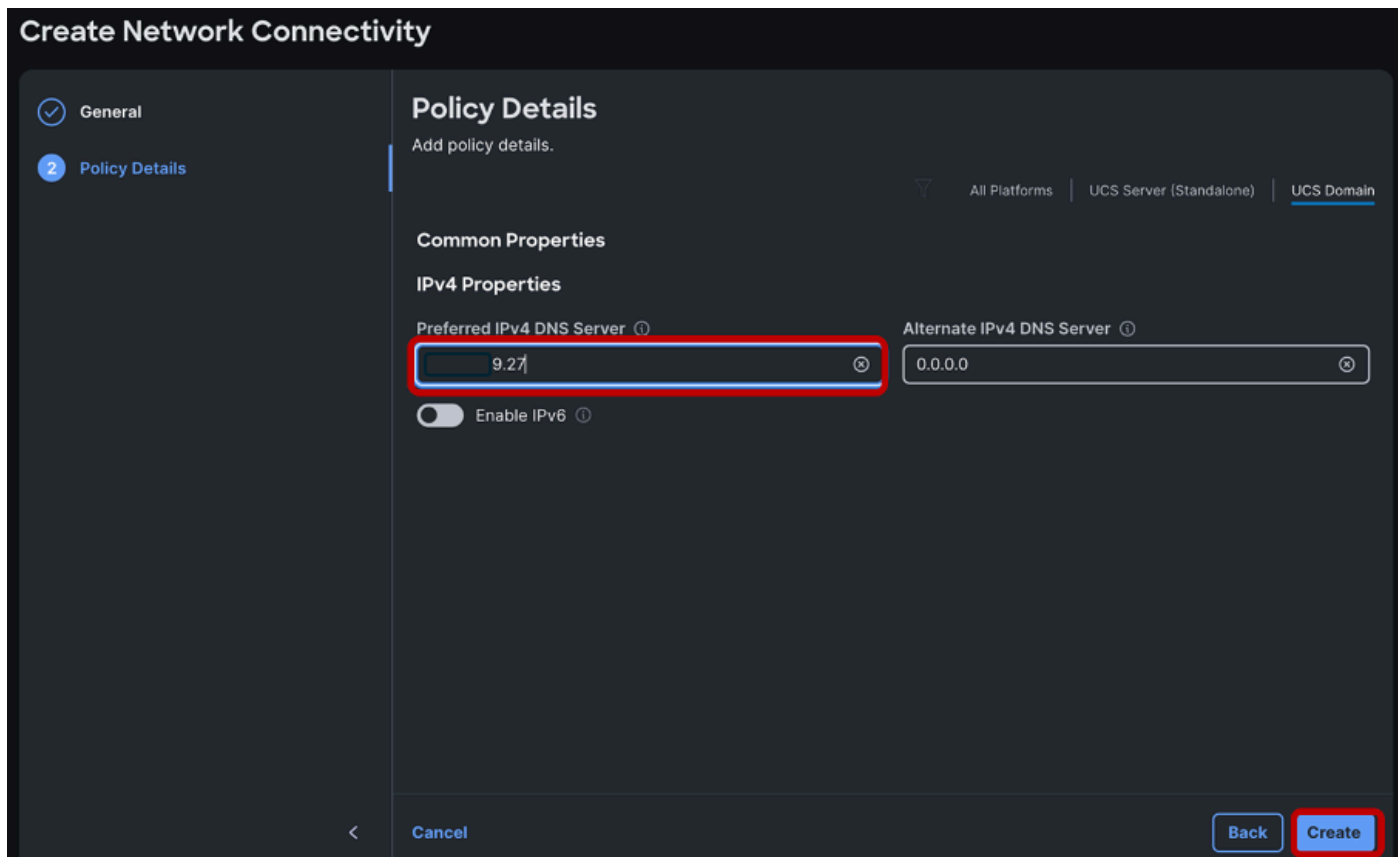
Configure um servidor DNS para o domínio do UCS criando uma Política de Conectividade de Rede.



Selecione a organização apropriada > Digite o nome da política > Clique em Avançar.



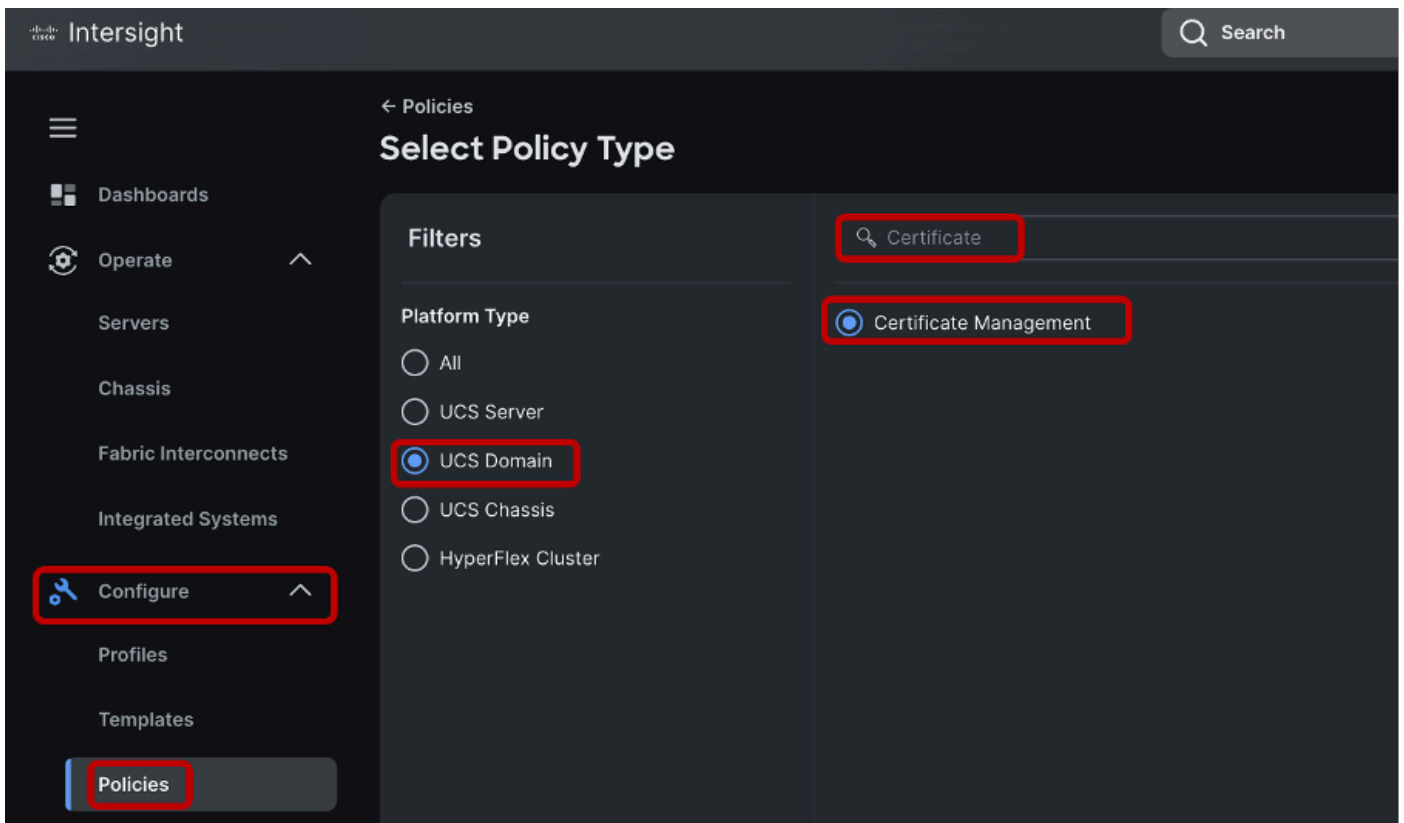
Defina um endereço IPv4 de servidor DNS preferencial e clique em Criar para salvar a diretiva.



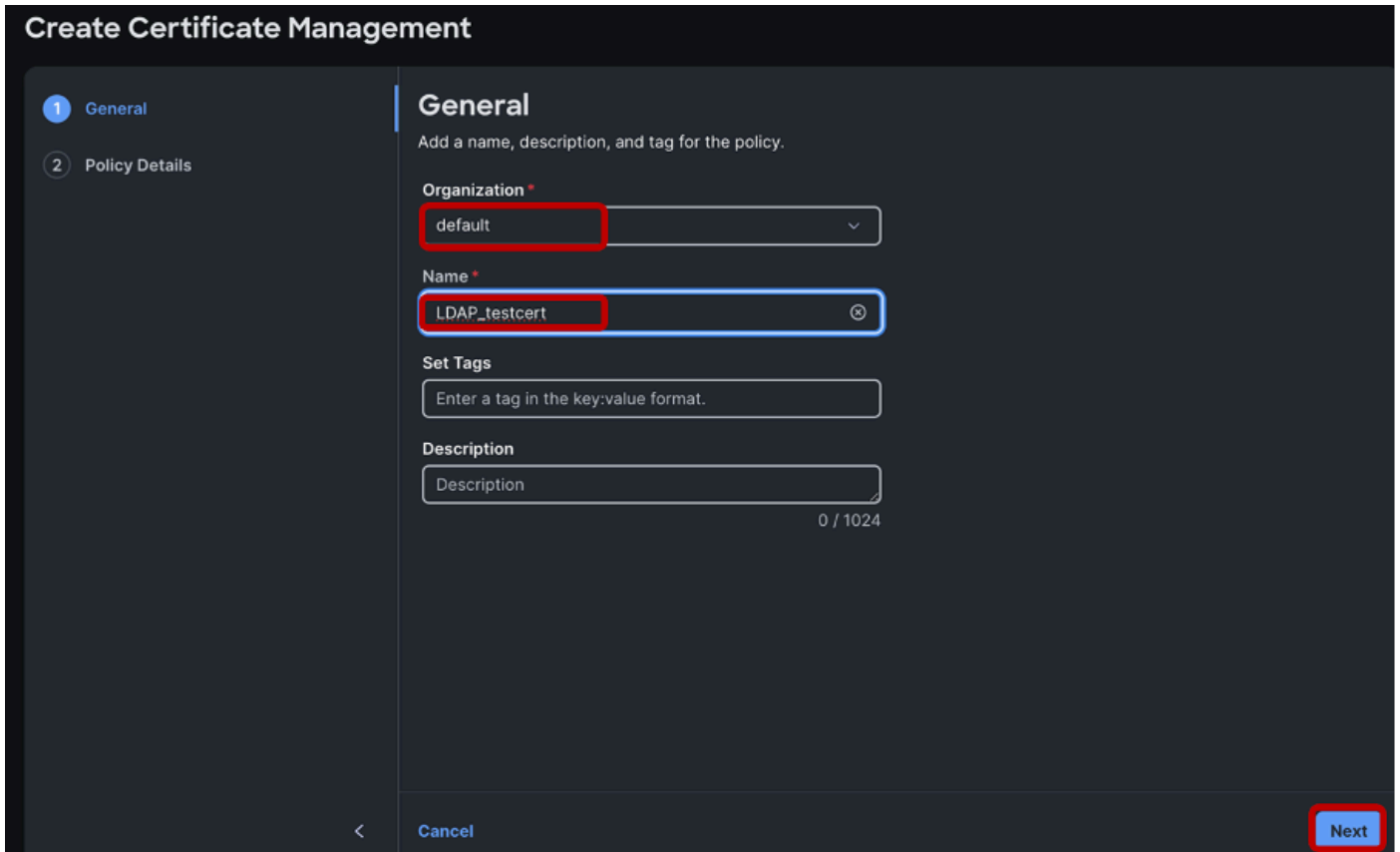
Verifique se um endereço IP do servidor DNS está configurado e acessível para a resolução de nomes. Certifique-se de que a resolução de nomes seja funcional para o servidor LDAP e as interconexões em malha dentro do domínio. Para esta demonstração, o servidor DNS está na mesma instância de máquina Windows que o servidor LDAP.

## Configurar Política de Gerenciamento de Certificados

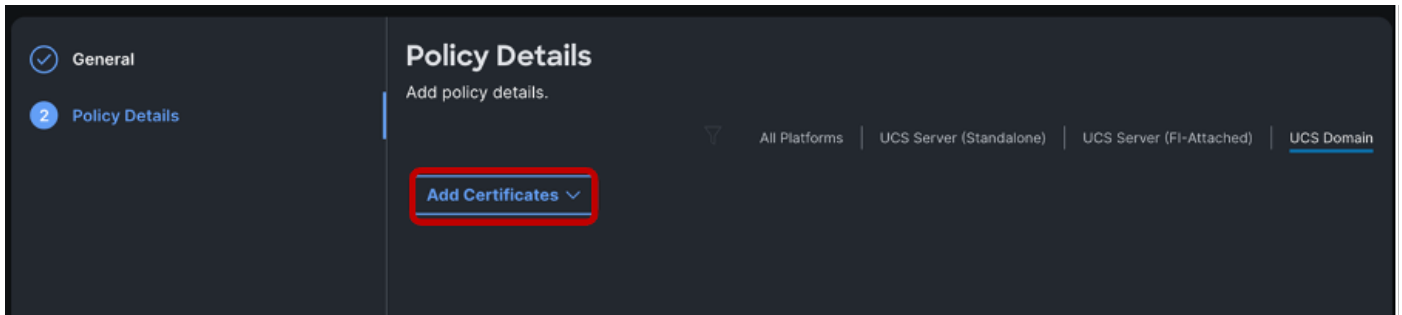
Em seguida, configure uma política de gerenciamento de certificados. Isso é necessário para a criptografia LDAP funcionar.



Selecione a organização apropriada, nomeie a política > Clique em Avançar

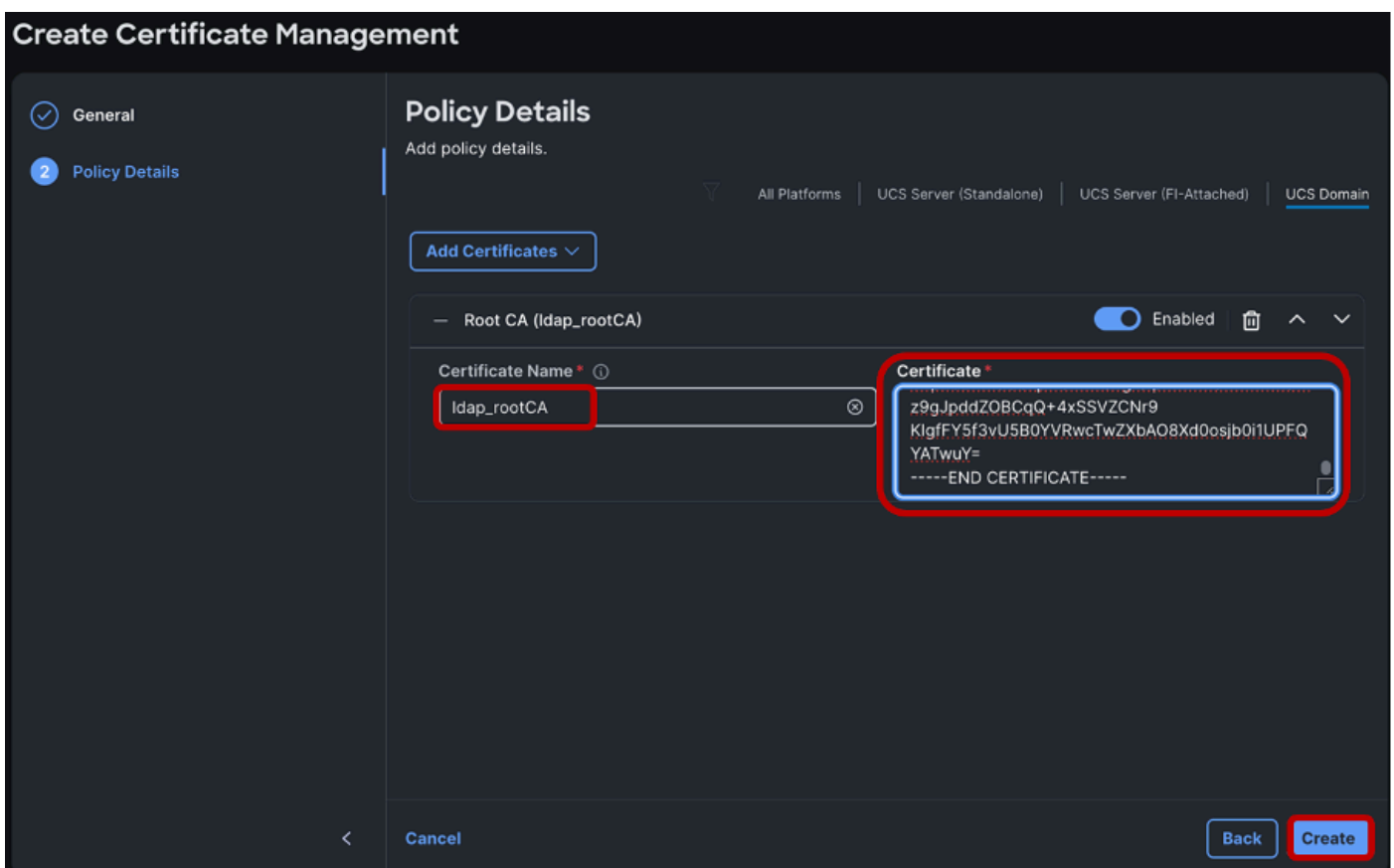


Clique em Adicionar certificados.

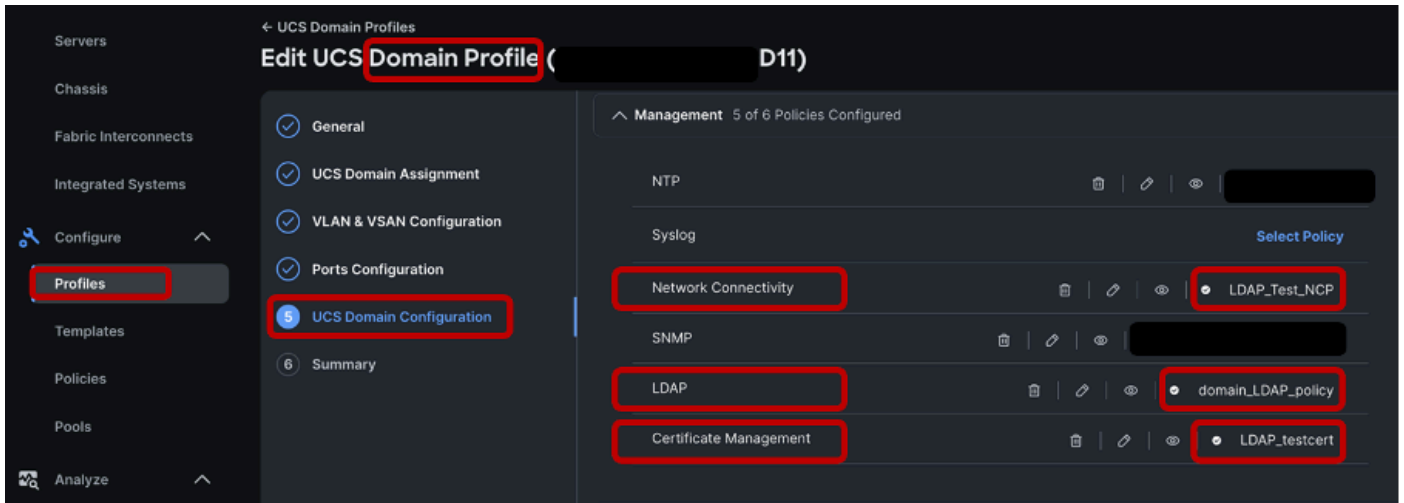


Nomeie o certificado e cole-o no Certificado Raiz dos Serviços de Certificados do Microsoft Active Directory.

Clique em Criar.



Depois que as políticas LDAP, de conectividade de rede e de gerenciamento de certificado tiverem sido criadas, consulte as políticas recém-criadas no perfil de domínio desejado, na seção "Configuração de domínio UCS", conforme mostrado.



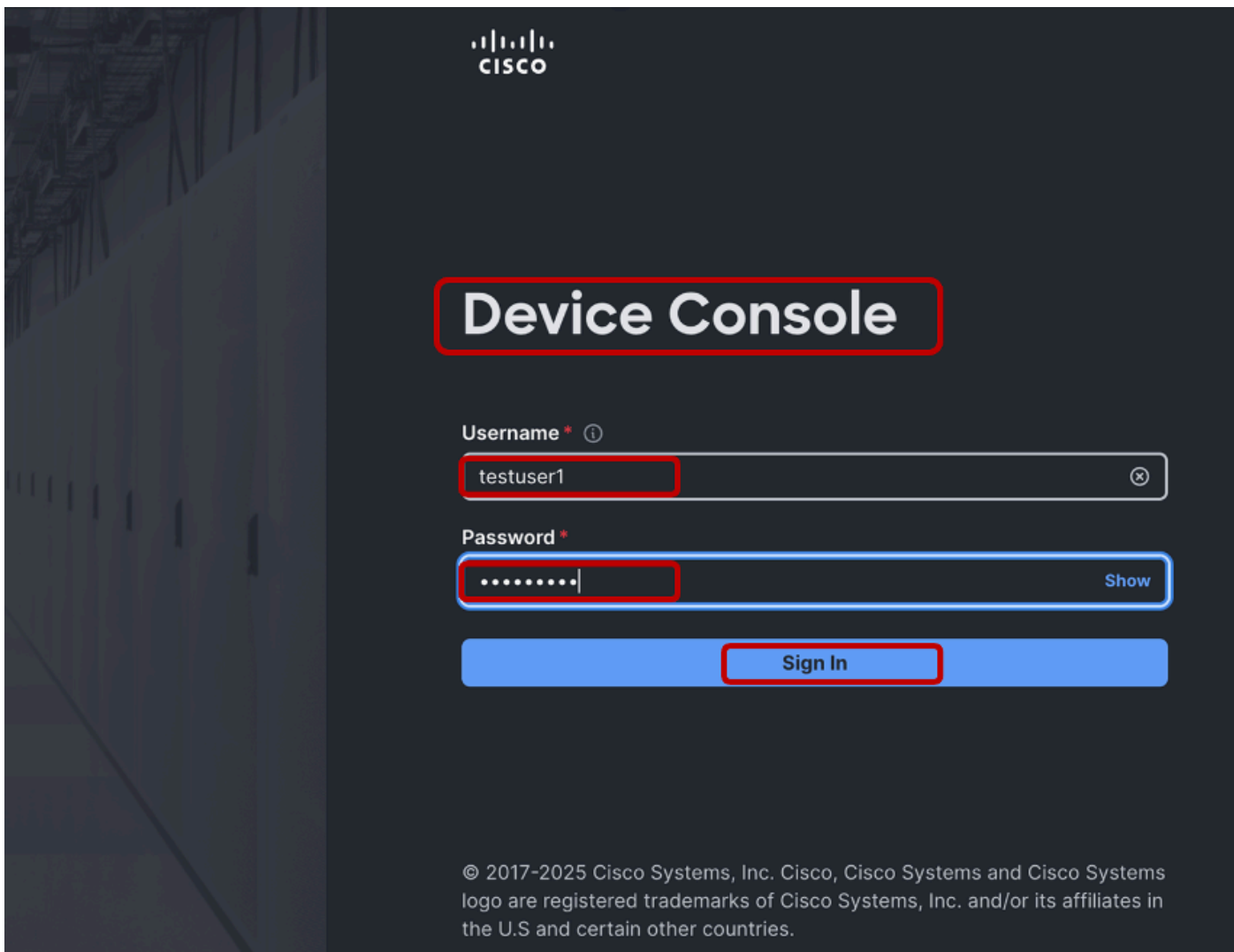
Clique em Avançar, Salvar e implantar o perfil de domínio.

Após a implantação bem-sucedida do perfil de domínio, a configuração LDAP segura para o domínio IMM é concluída.

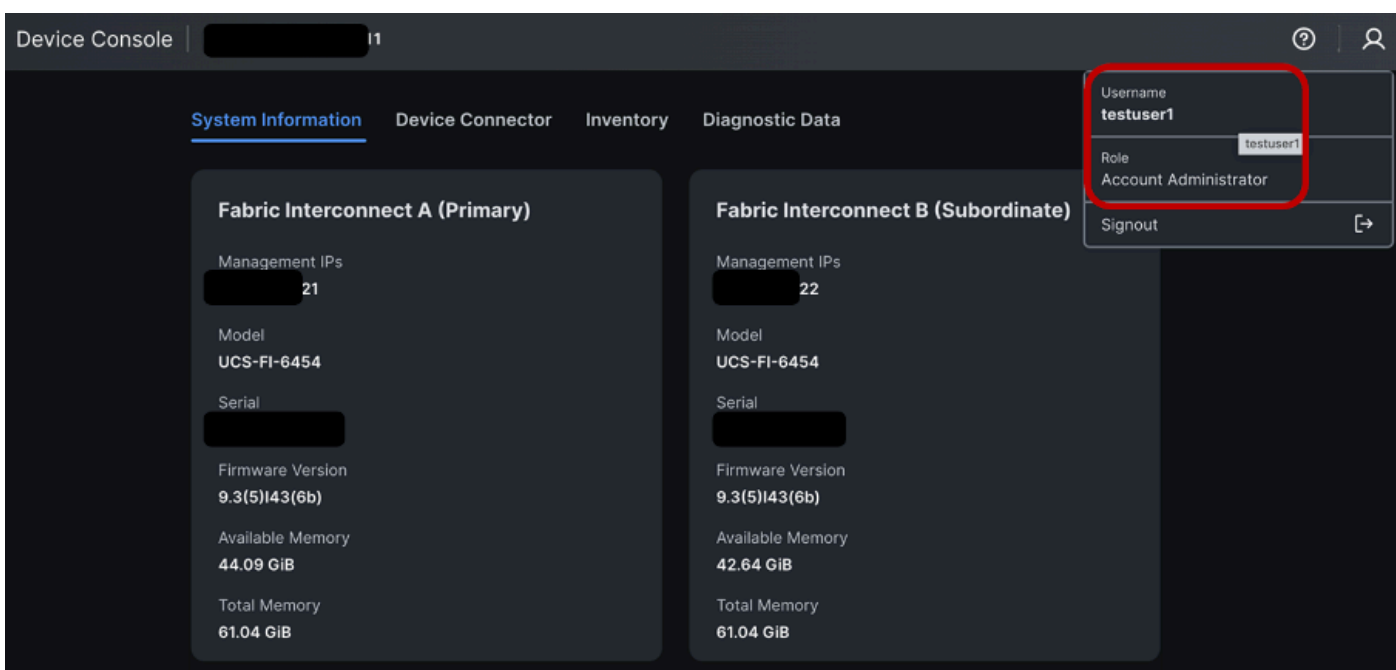
## Verificação

Para verificar, tente fazer login na GUI do Console do dispositivo e na CLI de interconexões em malha usando um dos usuários configurados do LDAP/Ative Directory.

Testar logon do console do dispositivo



O logon do console do dispositivo testuser1 foi bem-sucedido.



## Testar o login do SSH dos FIs

Êxito no login de SSH do testuser1.

```

> ssh testuser1@1 21
Cisco UCS 6400 Series Fabric Interconnect
testuser1@1 21's password:
UCS Intersight management
1-A# connect nxos
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2025, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source. This software is provided "as is," and unless
otherwise stated, there is no warranty, express or implied, including but not
limited to warranties of merchantability and fitness for a particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.
1-A(nx-os)# show user
user-account users
1-A(nx-os)# show users
NAME      LINE      TIME      IDLE      PID COMMENT
testuser1 pts/0      Oct 24 15:38 .      13250 (      ) session=ssh
1-A(nx-os)#
```

## Informações Relacionadas

- [Central de ajuda do Intersight](#)
- [Guia de administração do Cisco Intersight Managed Mode Fabric Interconnect](#)

## Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.