在Intersight管理模式下为交换矩阵互联配置安全LDAP访问（HTTP设备控制台和SSH）

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

配置

- 配置LDAP策略
- 配置网络连接策略
- 配置证书管理策略

确认

- 测试设备控制台登录
- 测试FI的SSH登录

相关信息

简介

本文档介绍如何使用LDAP策略在Intersight SaaS实例中配置域LDAP身份验证。

先决条件

要求

了解以下主题：

- 轻型目录访问协议(LDAP)协议。
- 域名服务器(DNS)服务器。
- Cisco Intersight

使用的组件

- Cisco Intersight SaaS实例
- Microsoft Active Directory
- DNS 服务器
- Microsoft Active Directory证书服务(AD CS)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

LDAP是一种公知协议，用于通过网络从目录访问资源。这些目录存储有关用户、组织和资源的信息。LDAP提供标准流程，用于访问和管理可用于身份验证和授权流程的信息。

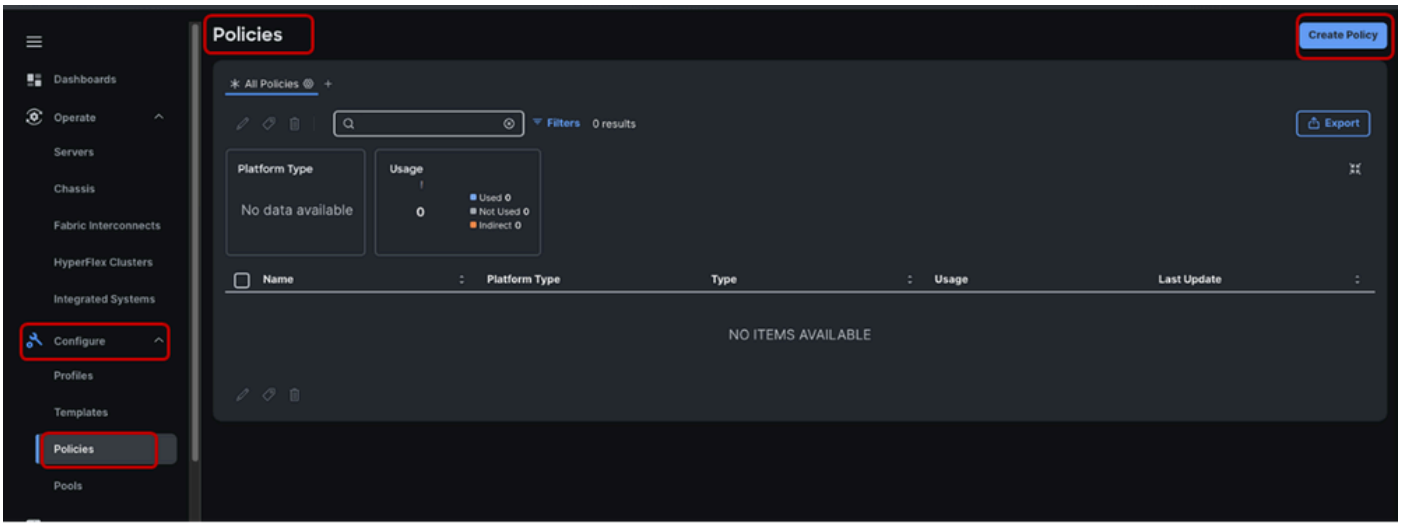
本文档介绍在思科智能互联管理模式下，通过安全LDAP向对等交换矩阵互联设备控制台或CLI（分别为HTTP或SSH）进行远程身份验证的配置过程。

配置

配置LDAP策略

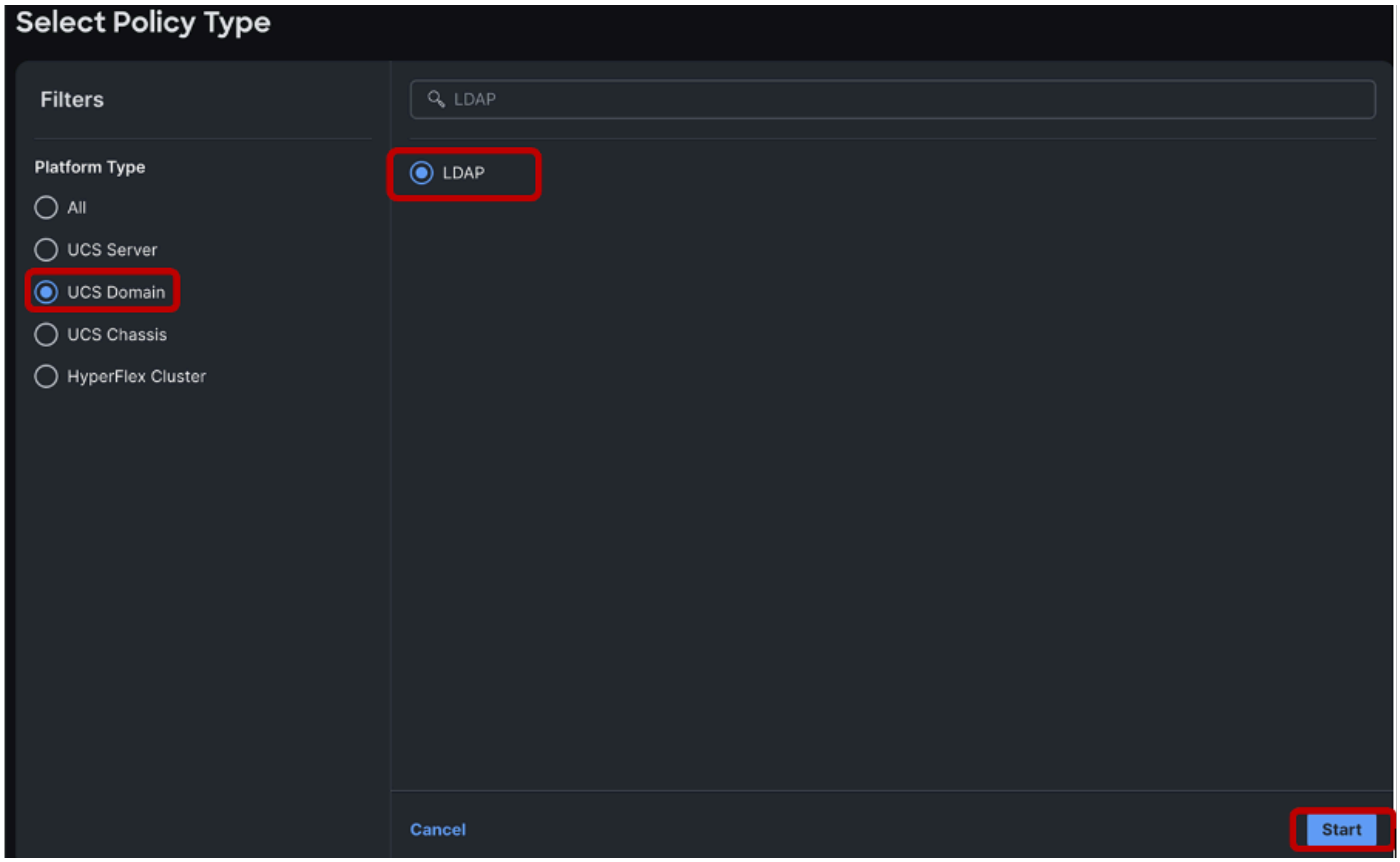
要配置LDAP策略，请登录到Intersight SaaS实例。

导航到Configure（配置）部分> Click Policies(点击策略)。
定位至“策略”窗口>选择创建策略。

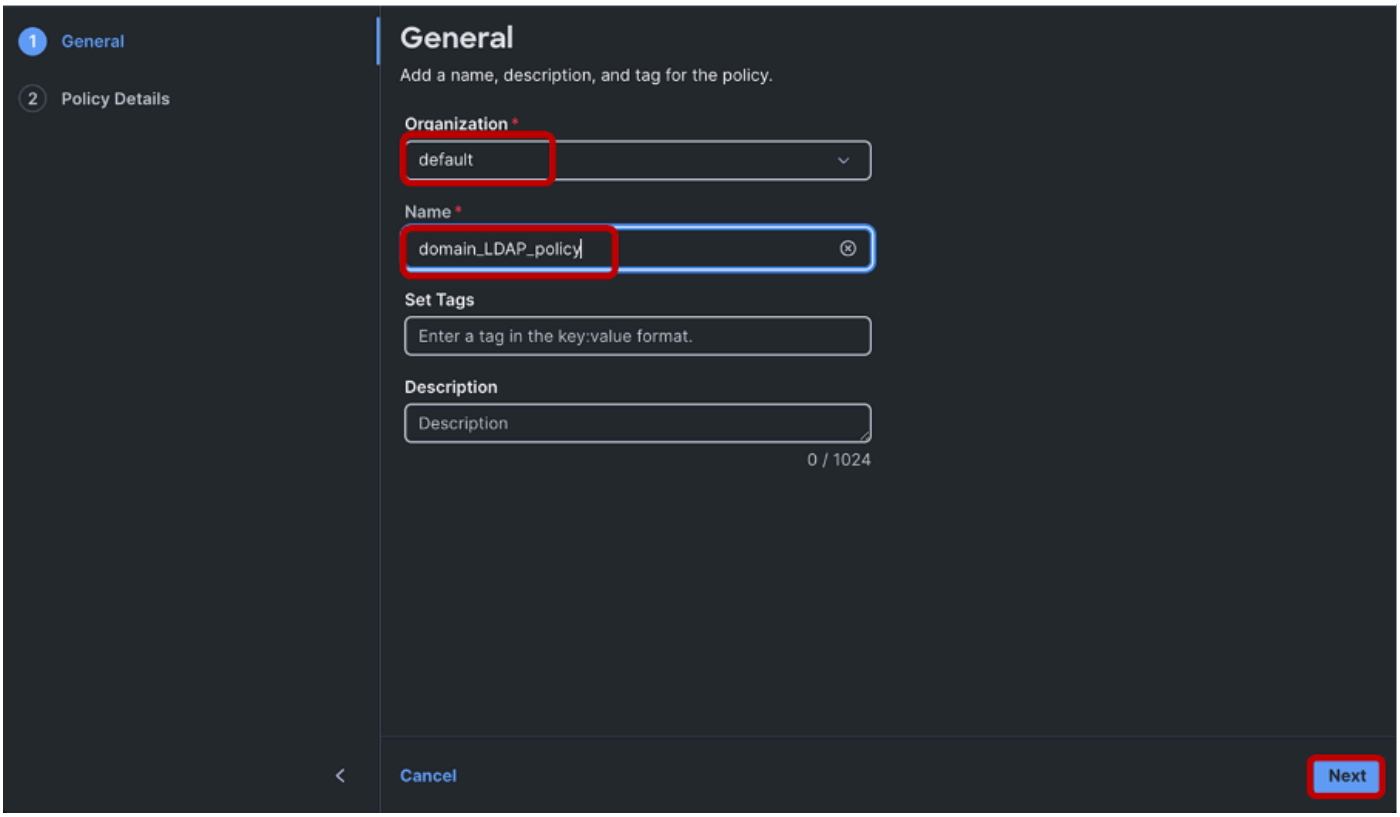


在搜索栏中，搜索“LDAP”。

选择LDAP单选按钮>点击开始。

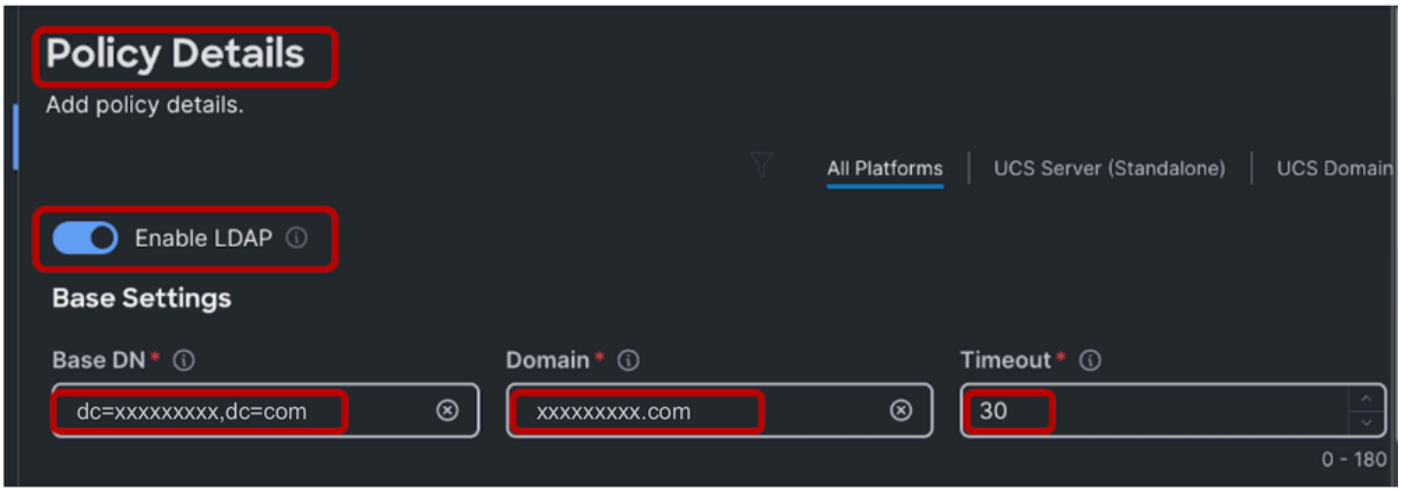


在“创建”窗口>选择所需的组织>命名LDAP策略>点击下一步：



在Policy Details部分>选择Enable LDAP滑块> Populate the Base DN， Domain and Timeout值。

Timeout值设置在0到29之间时，自动默认为30秒。对于此演示，“xxxxxxxxx.com”是已在LDAP服务器上配置的所需域，并且已指定30秒超时值。



要配置安全LDAP，请启用启用加密单选按钮。

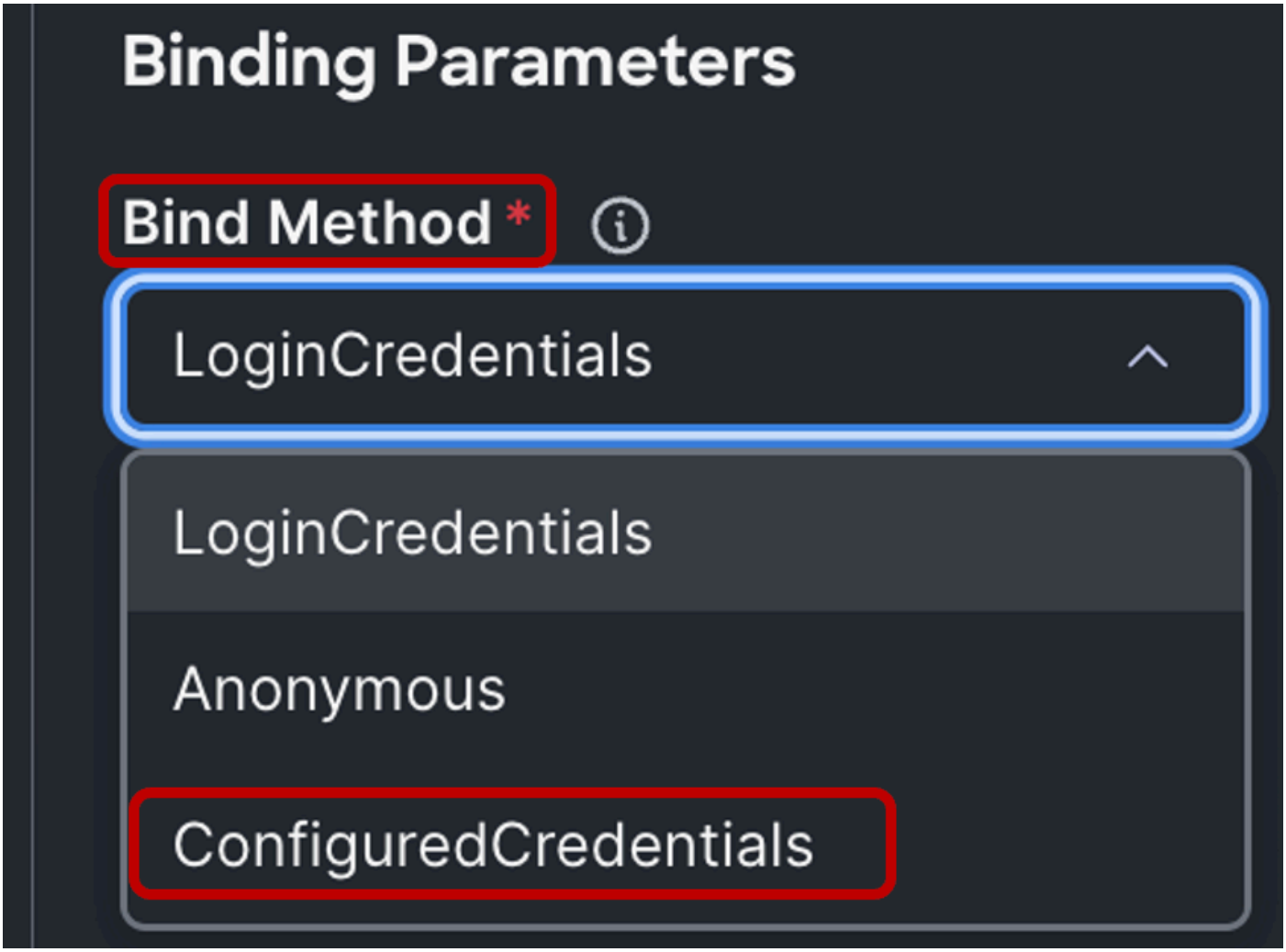
注意：通常的LDAP配置可以使用IP地址或FQDN，但不需要签名证书。因此，在配置“标准”LDAP时，可以忽略Enable Encryption选项、DNS Server Network Connectivity Policy和

Certificate Management Policy配置中的证书。安全LDAP需要为LDAP服务器名称解析配置的DNS服务器和根证书。



在Binding Parameters部分下，默认设置为LoginCredentials，它使用个人对绑定操作的用户LDAP凭据进行身份验证。这样就无需配置专用绑定用户。

在本演示中，配置了Bind用户。因此，“绑定方法”更改为“配置的凭证”。

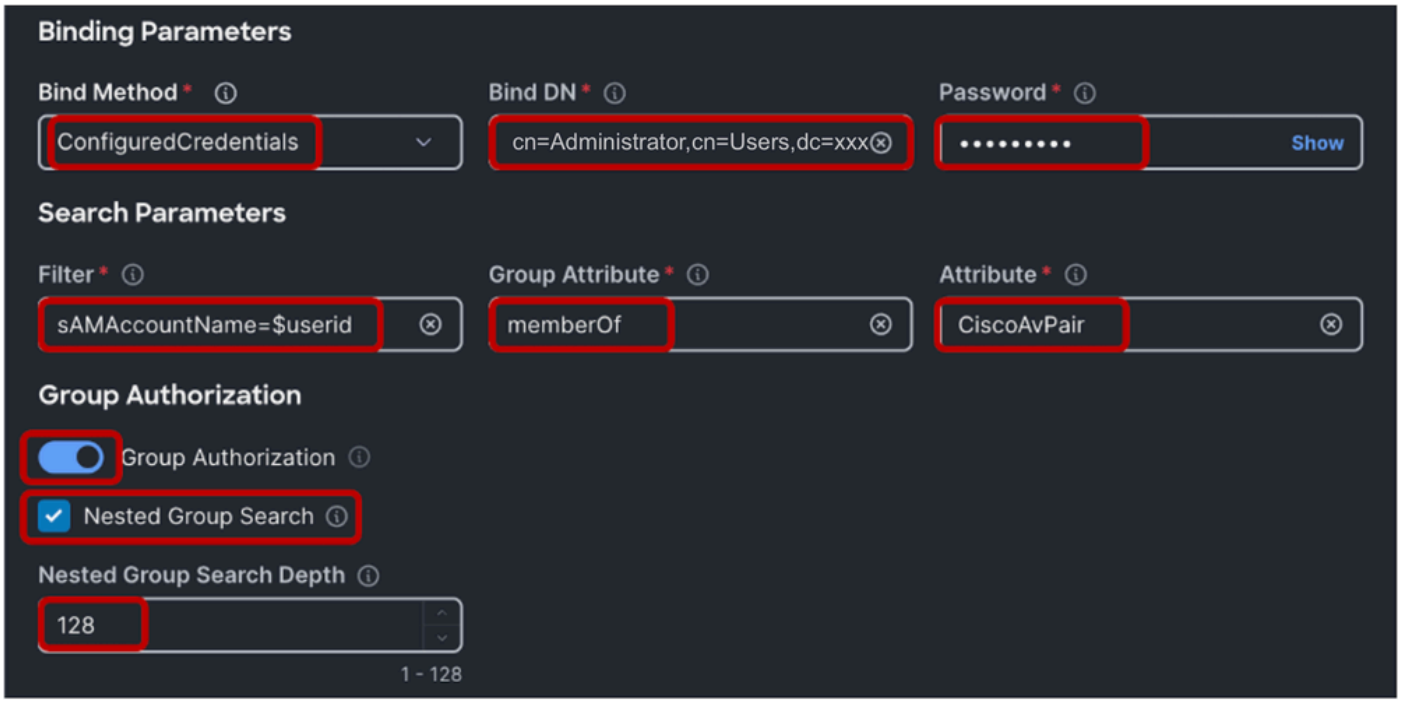


接下来，添加绑定DN（绑定用户）和绑定用户密码。这可以是Windows Active Directory上配置的任何用户。在本演示中，使用Administrator用户。

'cn=Administrator，cn=Users，dc=xxxxxxxxx，dc=com'。

在Search Parameters部分的Filter下，输入“sAMAccountName=$userid”。

对于Group Attributes，添加“memberOf”，并在Attribute字段中添加“CiscoAvPair”。根据您的LDAP服务器配置，您可以启用组授权和嵌套组搜索。对于此演示，使用默认嵌套组搜索深度128。



在“配置LDAP服务器”(Configure LDAP Servers)部分>输入LDAP服务器IP地址或FQDN（对于安全LDAP是必需的）和端口号(389)内。

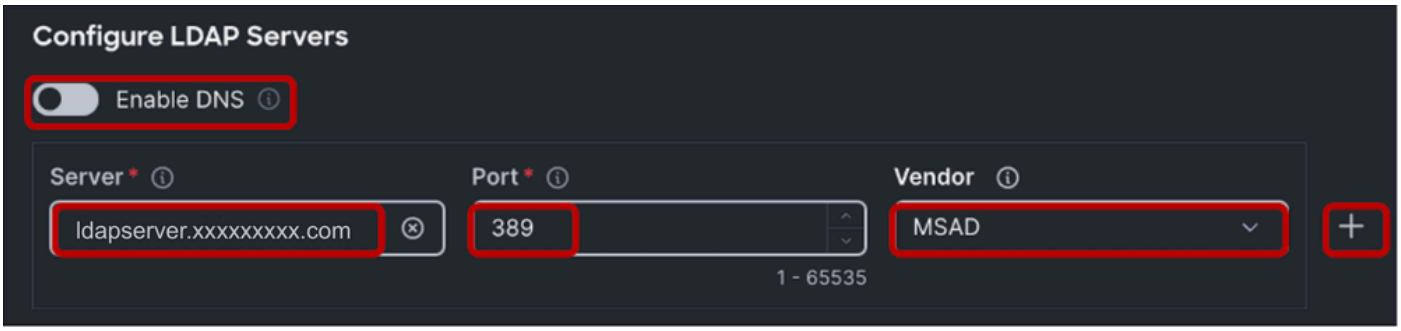
UCS中的安全LDAP使用STARTTLS启用使用端口389的加密通信。

请注意，将端口从389更改为636可能会导致身份验证错误。Cisco UCS在端口636上为SSL执行TLS协商；但是，初始连接始终在端口389上建立时未加密。

选择LDAP服务器供应商。可用的供应商选项为OpenLDAP和MSAD(Microsoft Active Directory)。在本演示中，由于使用的LDAP服务器是Windows Server 2019，因此使用了MSAD。

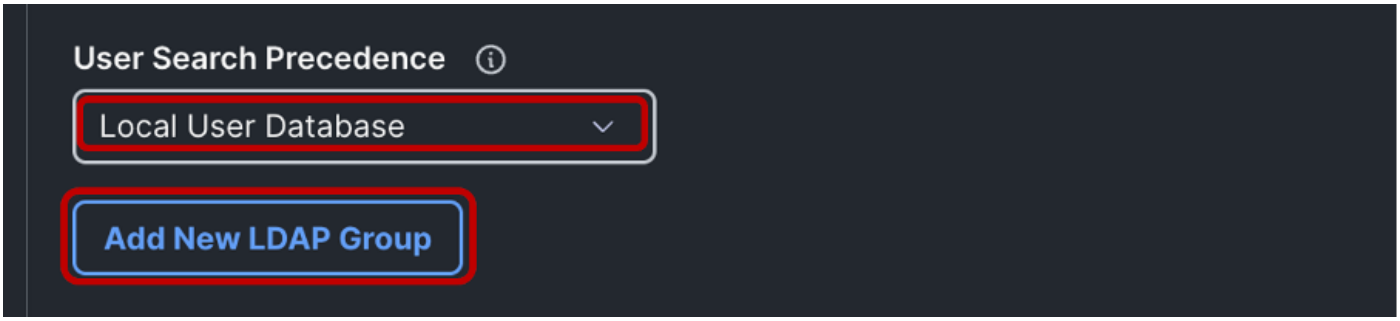
关闭“启用DNS”按钮，因为此选项不适用于UCS域中的LDAP配置。

通过点击已配置LDAP服务器最右侧的“+”图标，可以配置多个LDAP服务器。

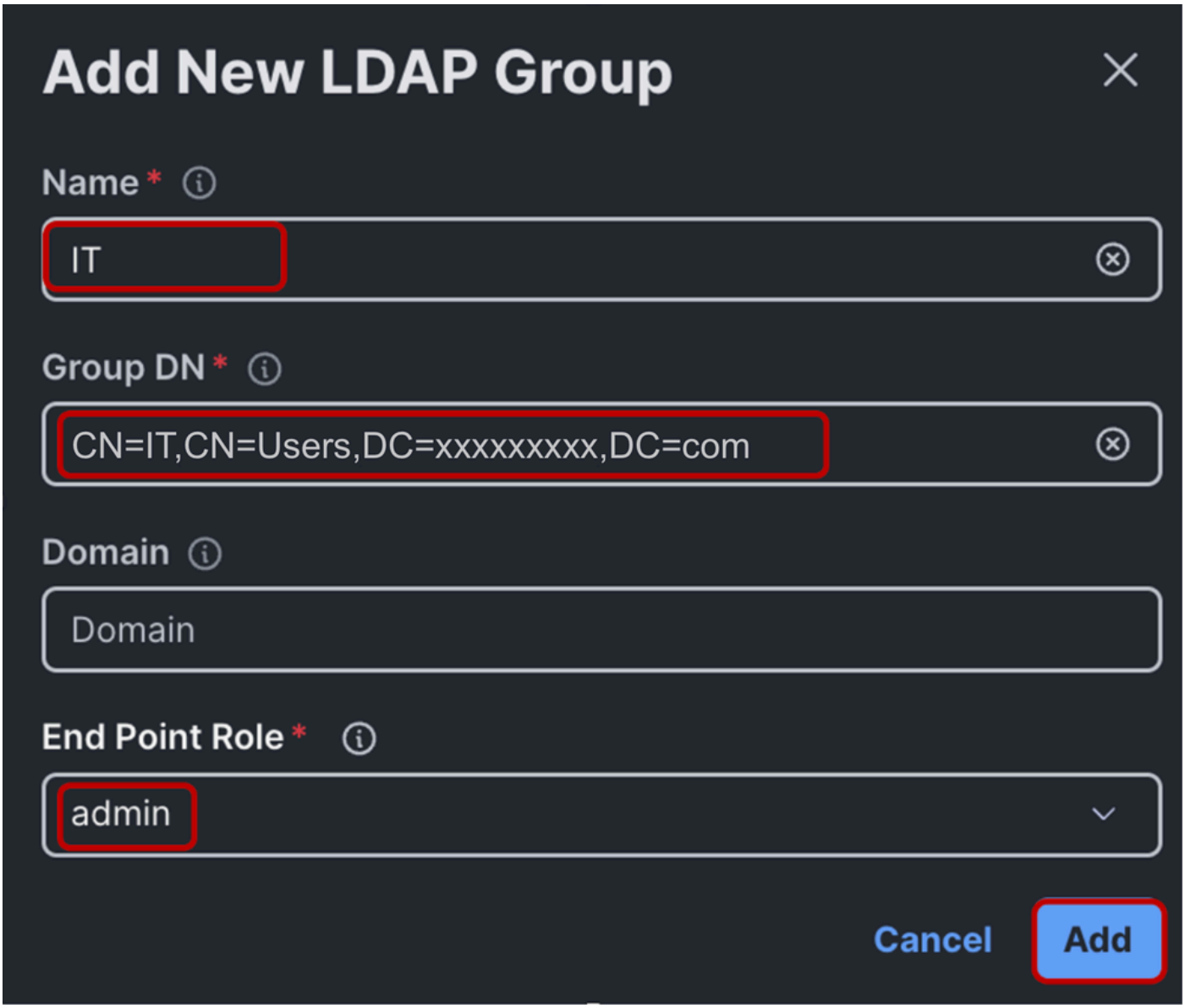


注意：您可以保留用户搜索优先级作为本地用户数据库，也可以将其更改为LDAP用户数据库，具体取决于您的使用案例。

接下来，通过点击Add New LDAP Group按钮，继续添加与LDAP服务器中配置的组对应的组DN。



命名组，添加从LDAP服务器接收的组DN，并选择所需的终端角色。

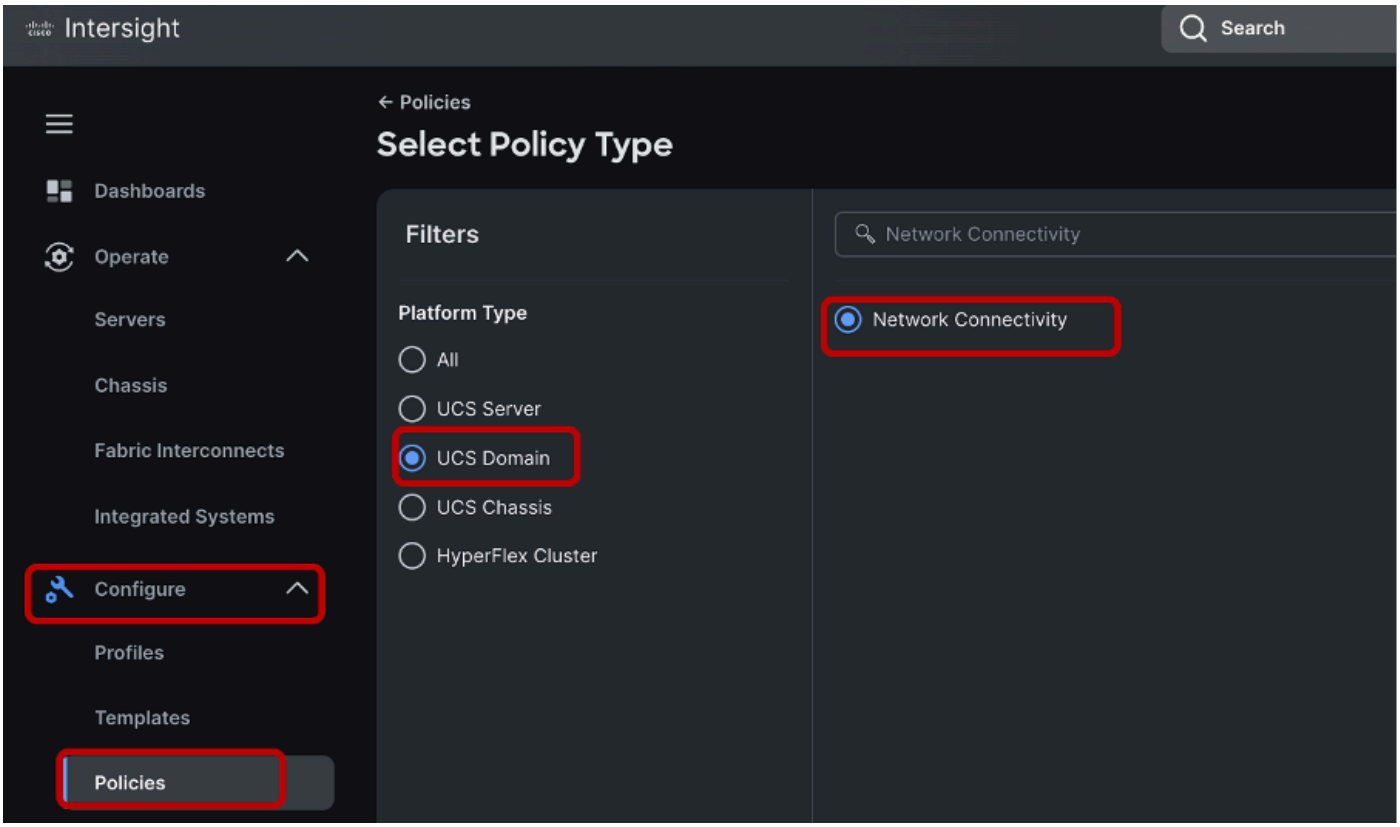


点击Add > Select Create以创建LDAP策略

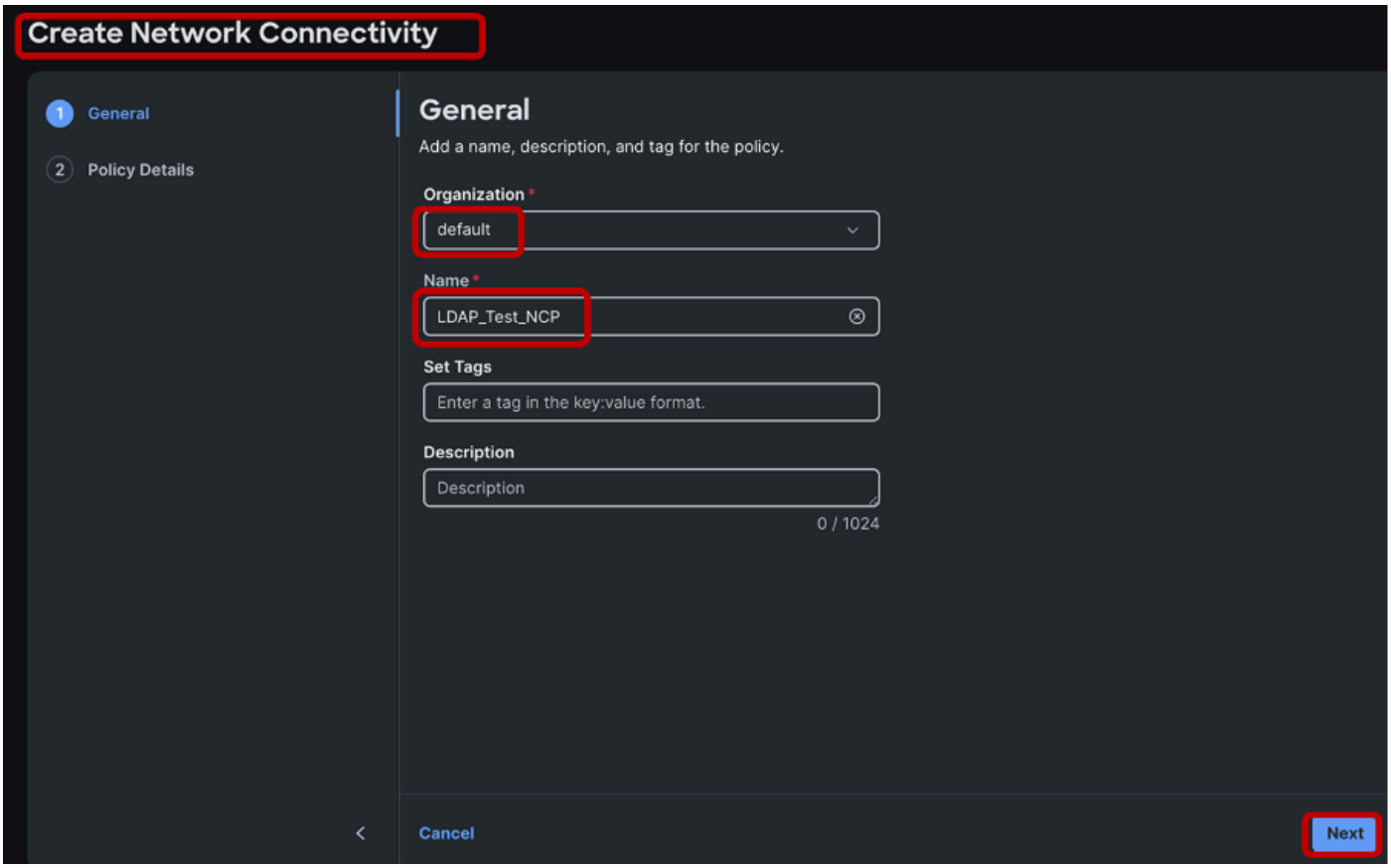
注意：对于域LDAP策略配置，截至本文创建时，唯一支持的终端角色为“admin”。

配置网络连接策略

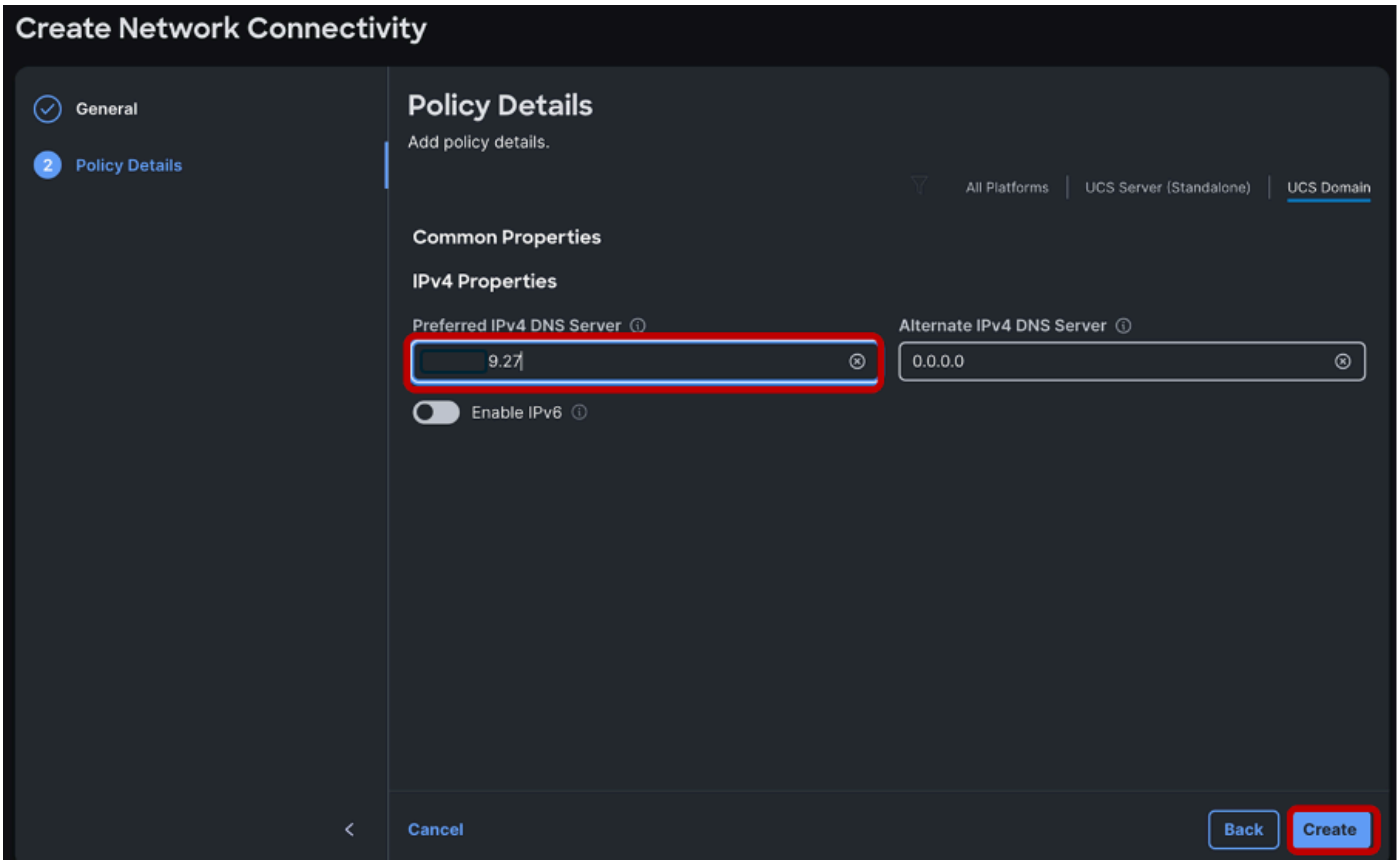
通过创建网络连接策略为UCS域配置DNS服务器。



选择适当的组织>输入策略名称>单击下一步。



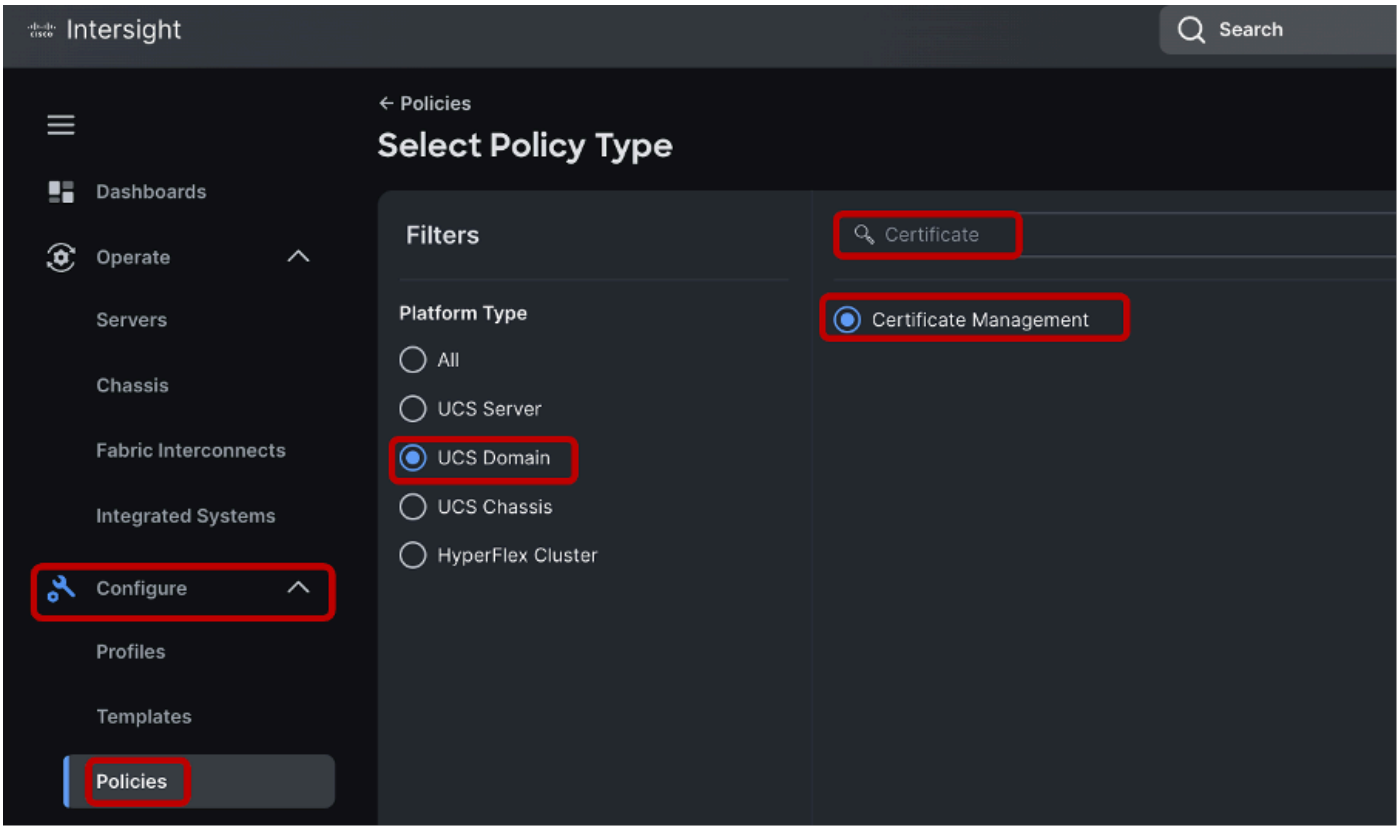
定义首选DNS服务器IPv4地址，然后点击Create保存策略。



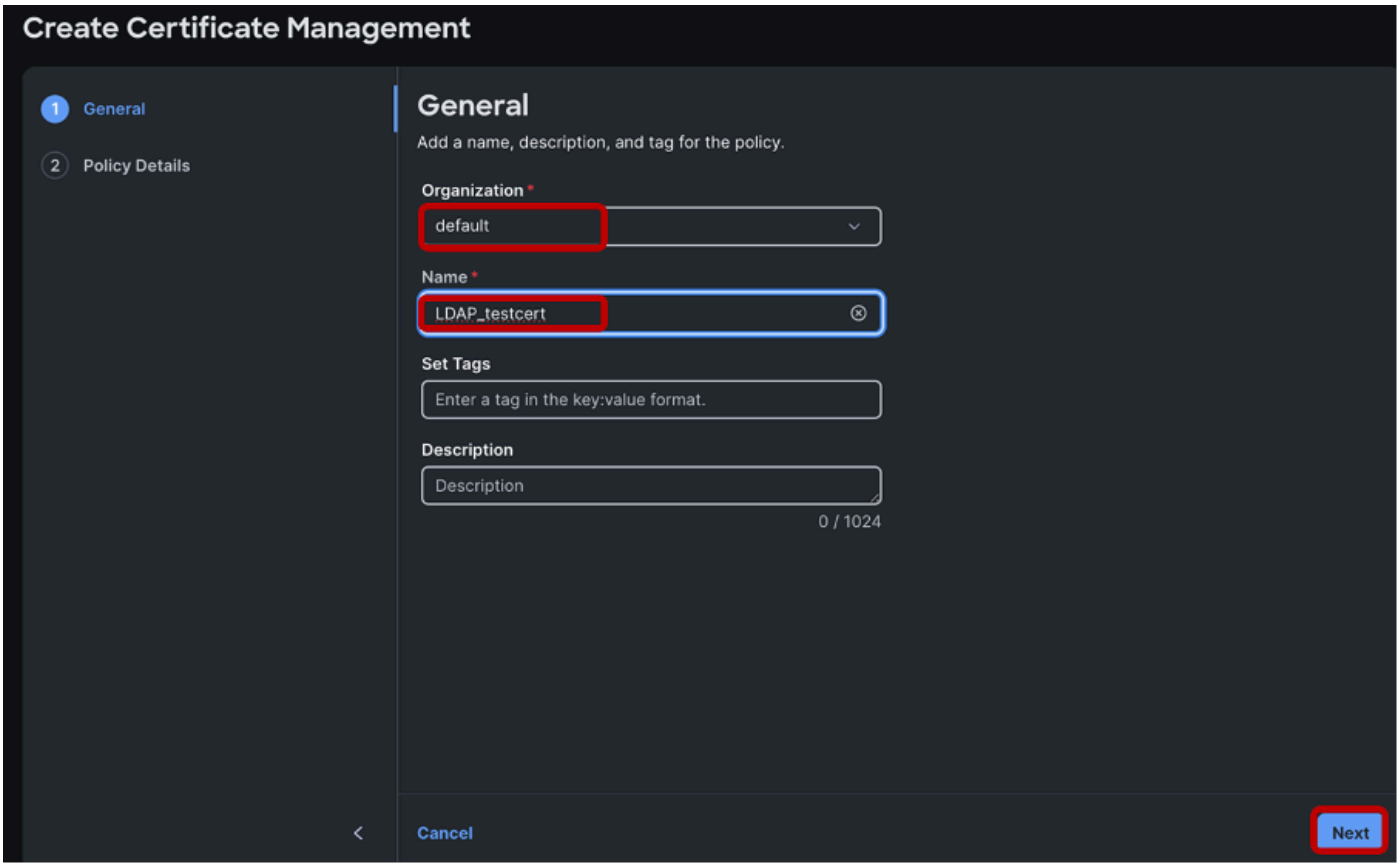
确保配置了DNS服务器IP地址并且可访问以进行名称解析。确保域名解析对域内的LDAP服务器和交换矩阵互联有效。在本演示中，DNS服务器与LDAP服务器位于同一Windows计算机实例上。

配置证书管理策略

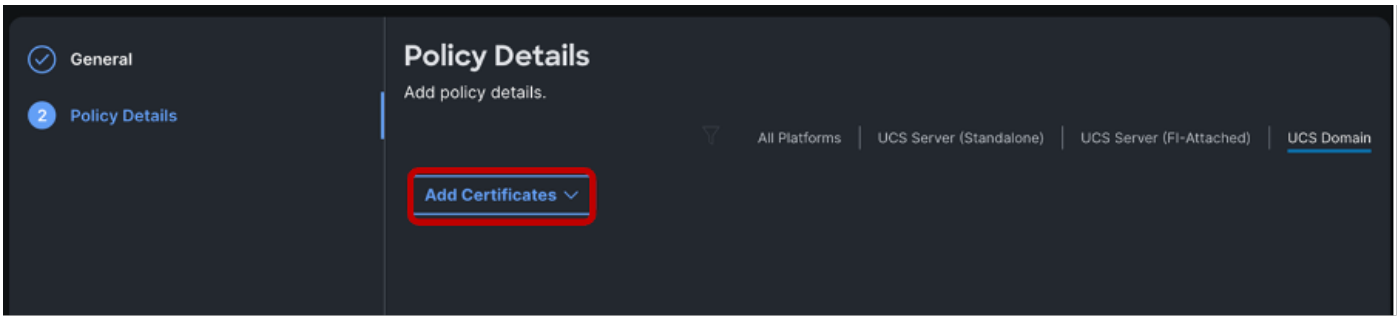
然后配置证书管理策略。要使LDAP加密正常工作，这是必需的。



选择适当的组织，命名策略>点击“下一步”

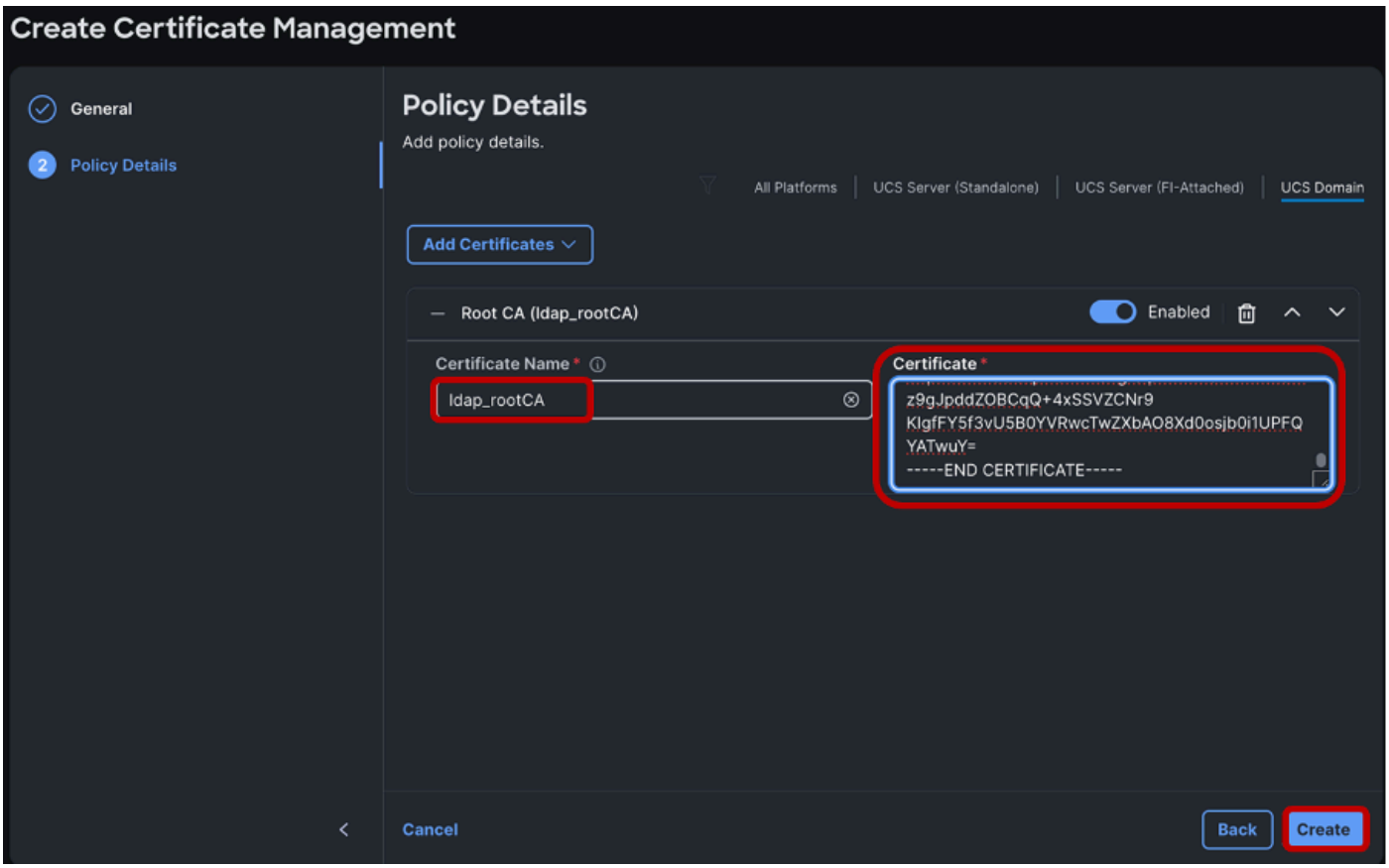


点击Add Certificates。

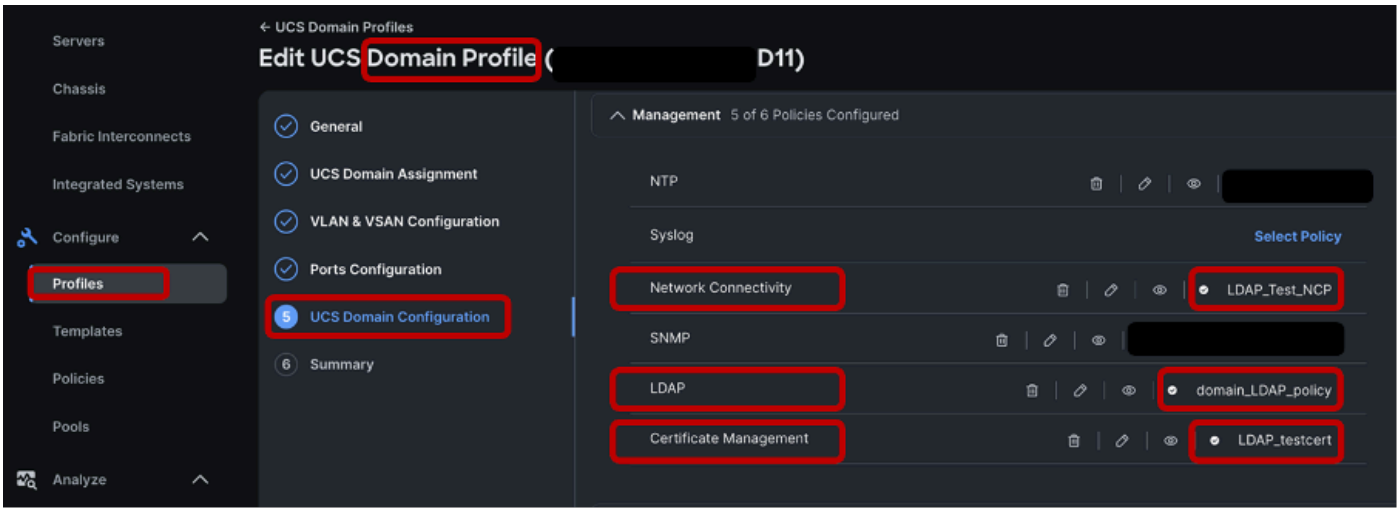


命名证书并粘贴到Microsoft Active Directory证书服务的根证书中。

Click Create.



创建LDAP、网络连接和证书管理策略后，请参阅所需域配置文件中“UCS域配置”部分中新创建的策略，如下所示。



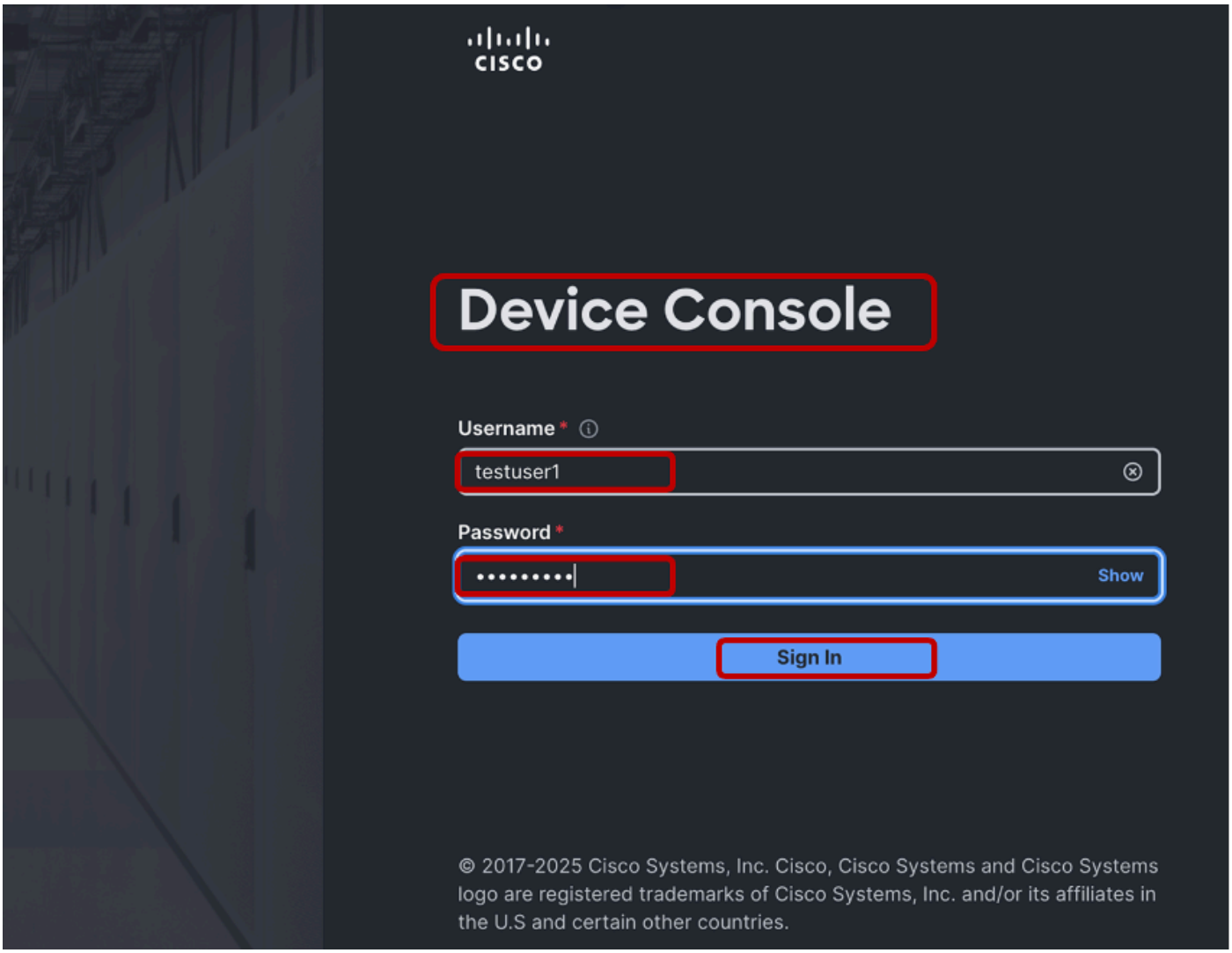
点击下一步，保存并部署域配置文件。

成功部署域配置文件后，IMM域的安全LDAP配置完成。

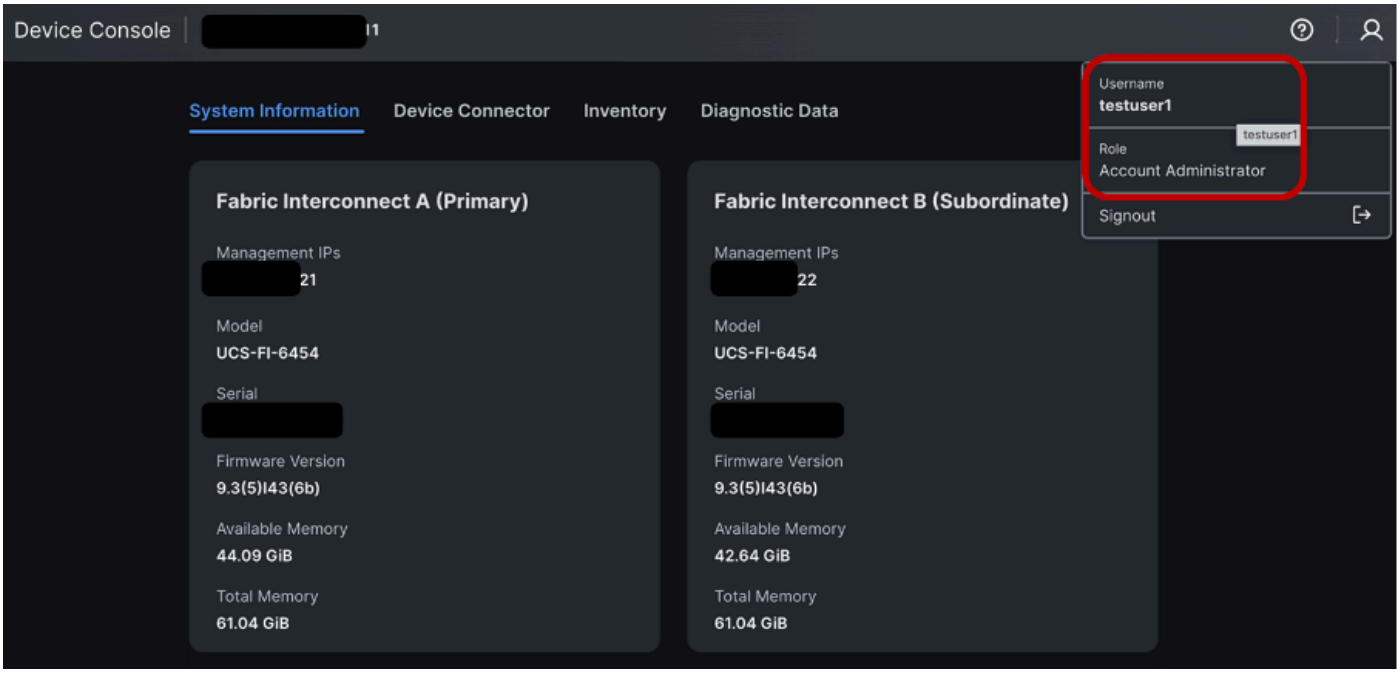
确认

要进行验证，请尝试使用其中一个已配置的LDAP/Active Directory用户登录到设备控制台GUI和交换矩阵互联CLI。

测试设备控制台登录

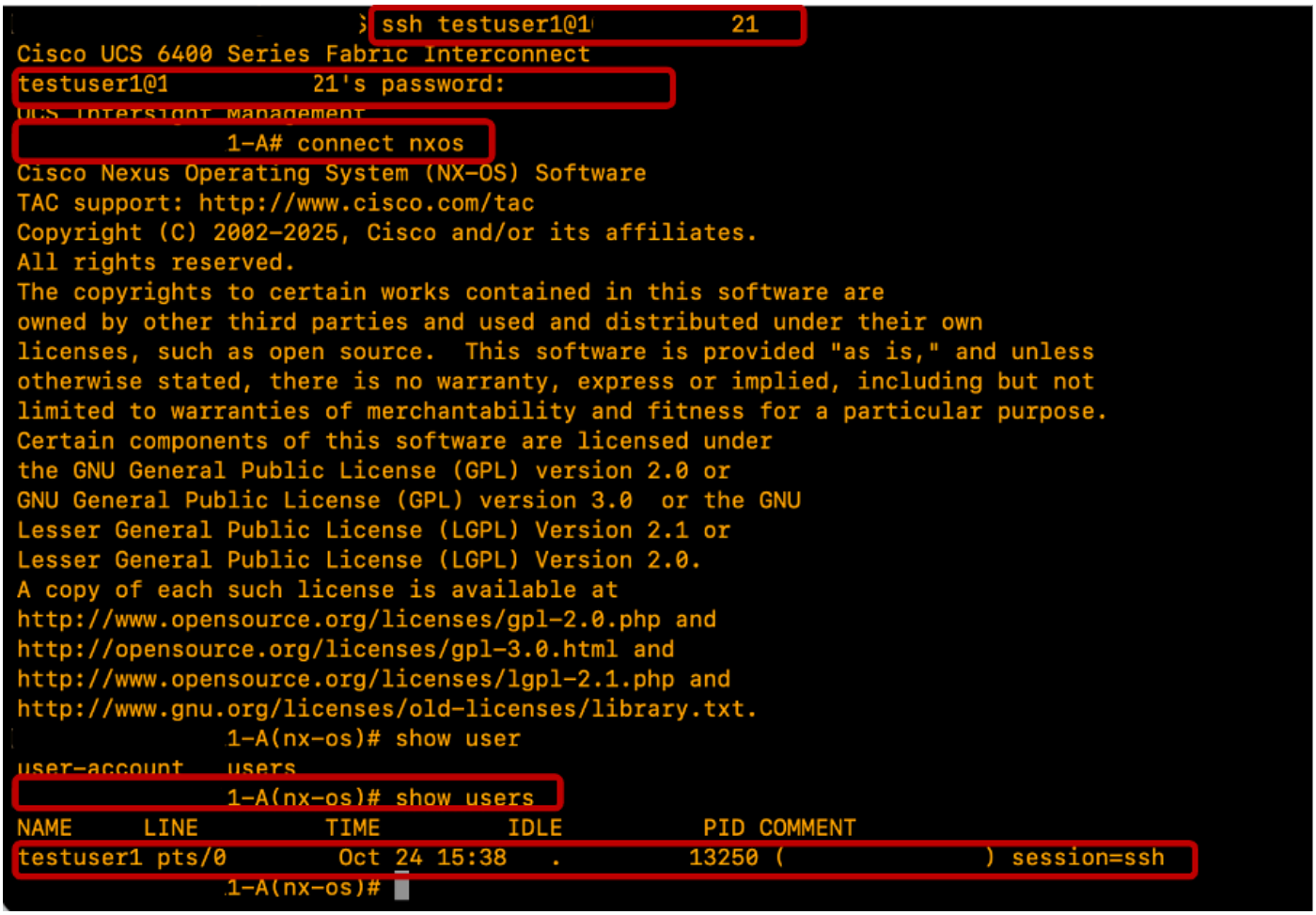


Testuser1设备控制台登录成功。



测试FI的SSH登录

Testuser1 SSH登录成功。



相关信息

- Intersight帮助中心
- Cisco Intersight管理模式交换矩阵互联管理指南

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。