在Intersight管理模式下為交換矩陣互聯配置安全LDAP訪問（HTTP裝置控制檯和SSH）

目錄

簡介

本文檔介紹如何使用LDAP策略在Intersight SaaS例項中配置域LDAP身份驗證。

必要條件

需求

瞭解以下主題：

- 輕型目錄訪問協定(LDAP)協定。
- 網域名稱伺服器(DNS)伺服器。
- Cisco Intersight

採用元件

- Cisco Intersight SaaS例項
- Microsoft Active Directory
- DNS伺服器
- Microsoft Active Directory憑證服務(AD CS)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

LDAP是一種公知的協定，用於通過網路從目錄訪問資源。這些目錄儲存有關使用者、組織和資源的資訊。LDAP提供標準流程，用於訪問和管理可用於身份驗證和授權流程的資訊。

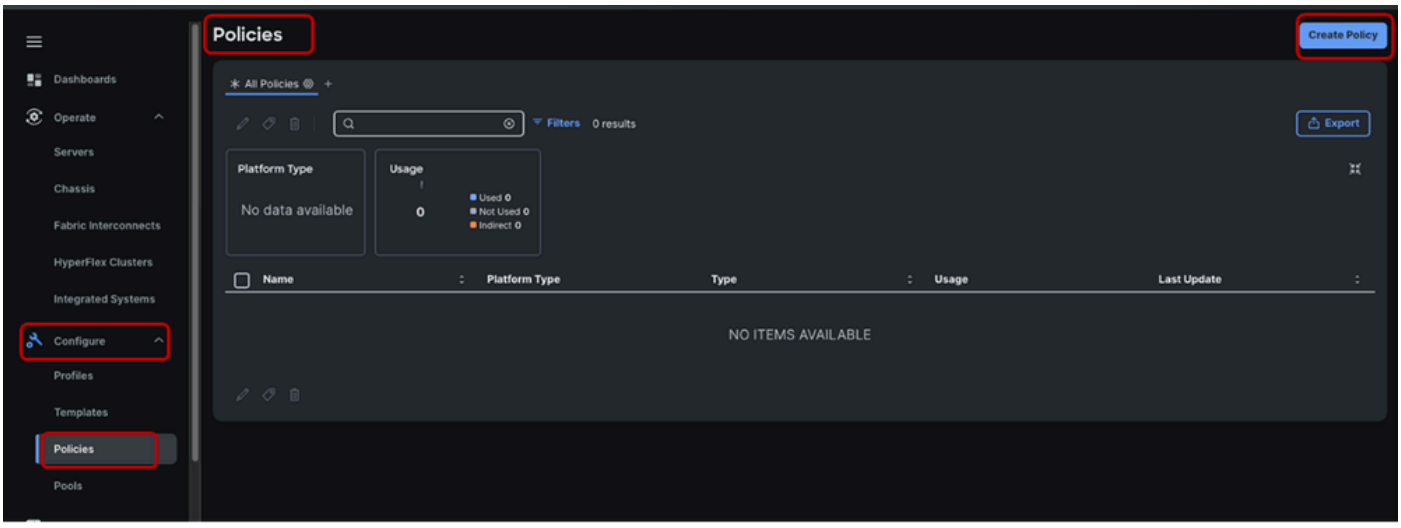
本文檔介紹在Intersight管理模式下通過安全LDAP對對等交換矩陣互聯的裝置控制檯或CLI（分別為HTTP或SSH）進行遠端身份驗證的配置過程。

組態

配置LDAP策略

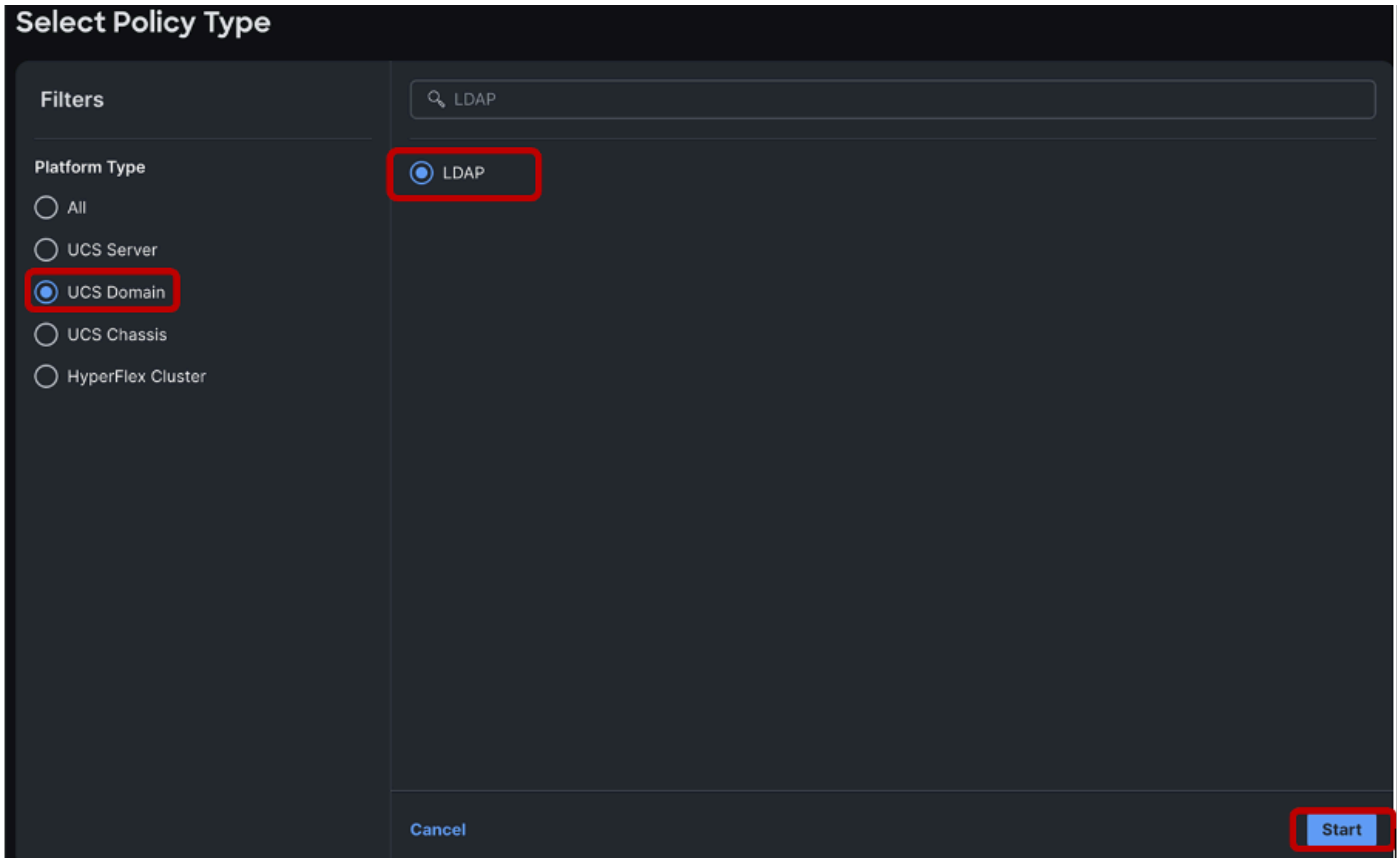
要配置LDAP策略，請登入到Intersight SaaS例項。

導航到Configure部分>單擊Policies。
定位至「策略」視窗>選擇建立策略。

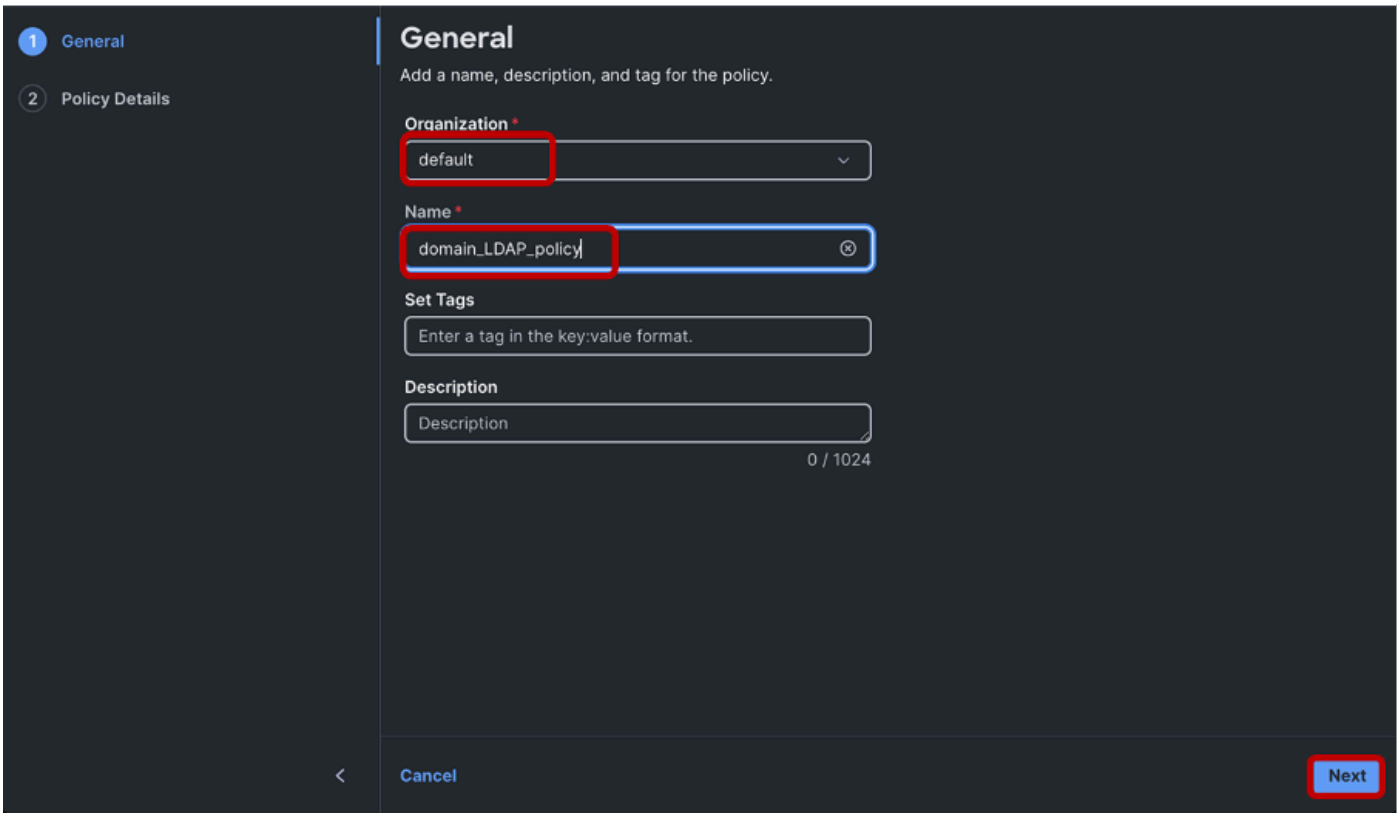


在搜尋欄中，搜尋「LDAP」。

選擇LDAP單選按鈕>單擊開始。

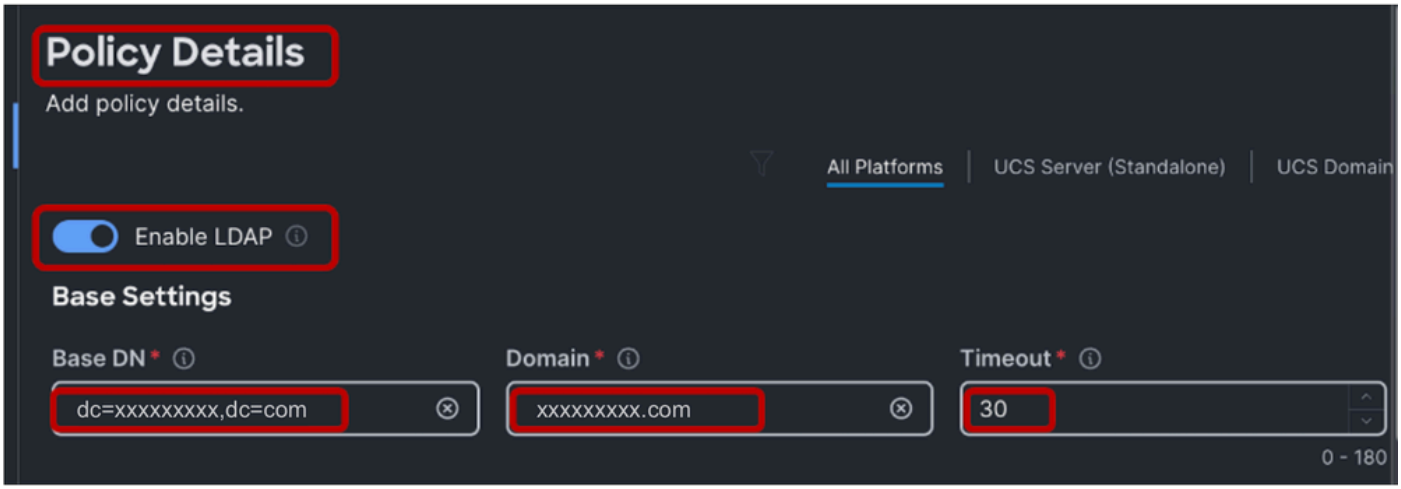


在「建立」視窗>選擇所需的組織>命名LDAP策略>單擊下一步：



在Policy Details部分> Select the Enable LDAP slider > Populate the Base DN， Domain and Timeout values。

設定在0到29之間的超時值會自動預設為30秒。對於此演示，「xxxxxxxxx.com」是已在LDAP伺服器上配置的所需域，並且已指定30秒超時值。



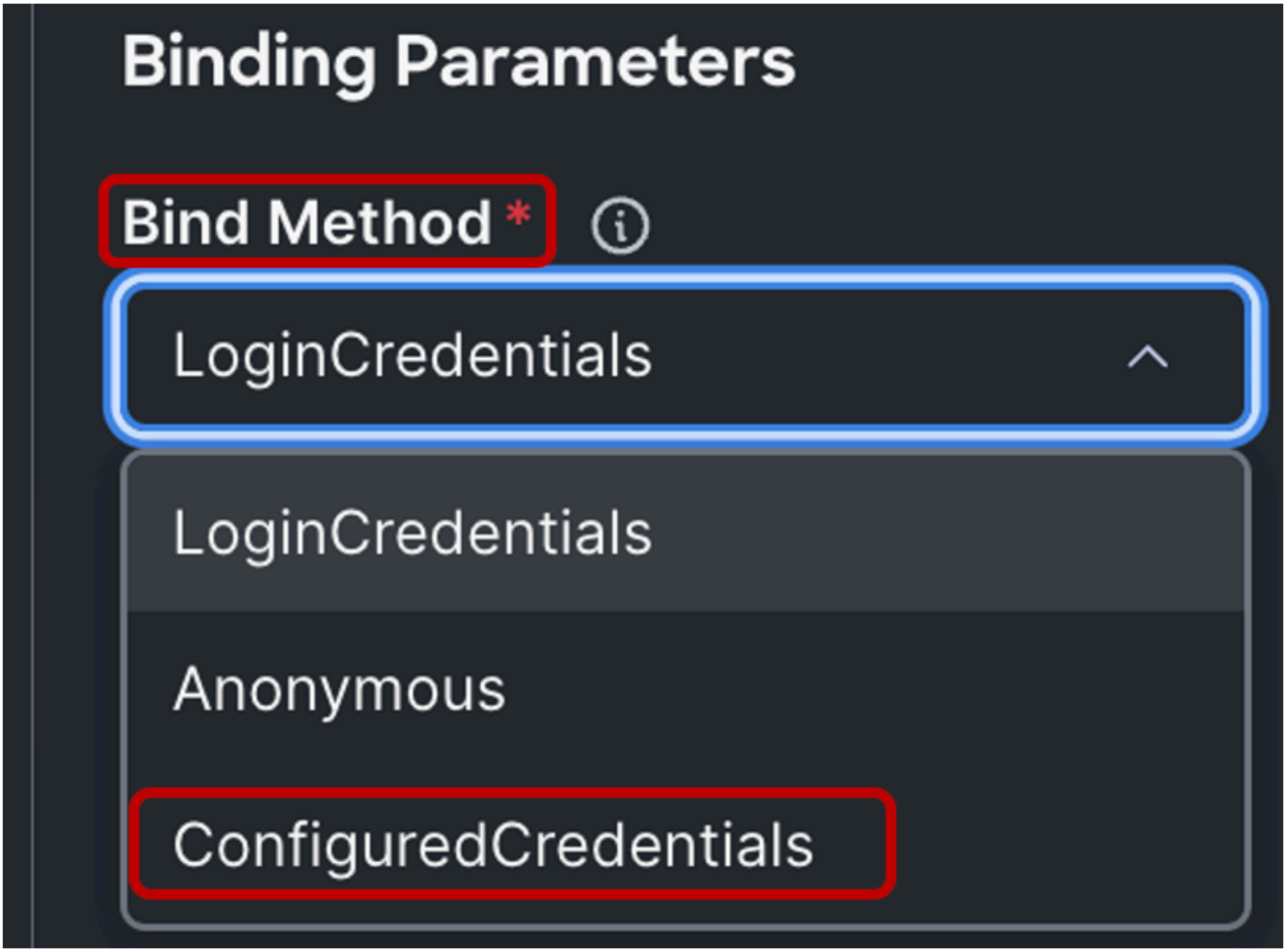
要配置安全LDAP，請啟用Enable Encryption單選按鈕。

附註：通常的LDAP配置可以利用IP地址或FQDN，但簽名證書不是必需的。因此，在配置

「標準」LDAP時，可以忽略Enable Encryption選項、DNS伺服器網路連線策略和證書管理策略配置中的證書。安全LDAP需要為LDAP伺服器名稱解析配置的DNS伺服器和根證書。

在Binding Parameters部分下，預設設定為LoginCredentials，它利用個人對使用者LDAP憑據進行繫結操作。這樣就無需配置專用繫結使用者。

在本演示中，配置了Bind使用者。因此，「繫結方法」更改為「ConfiguredCredentials」。

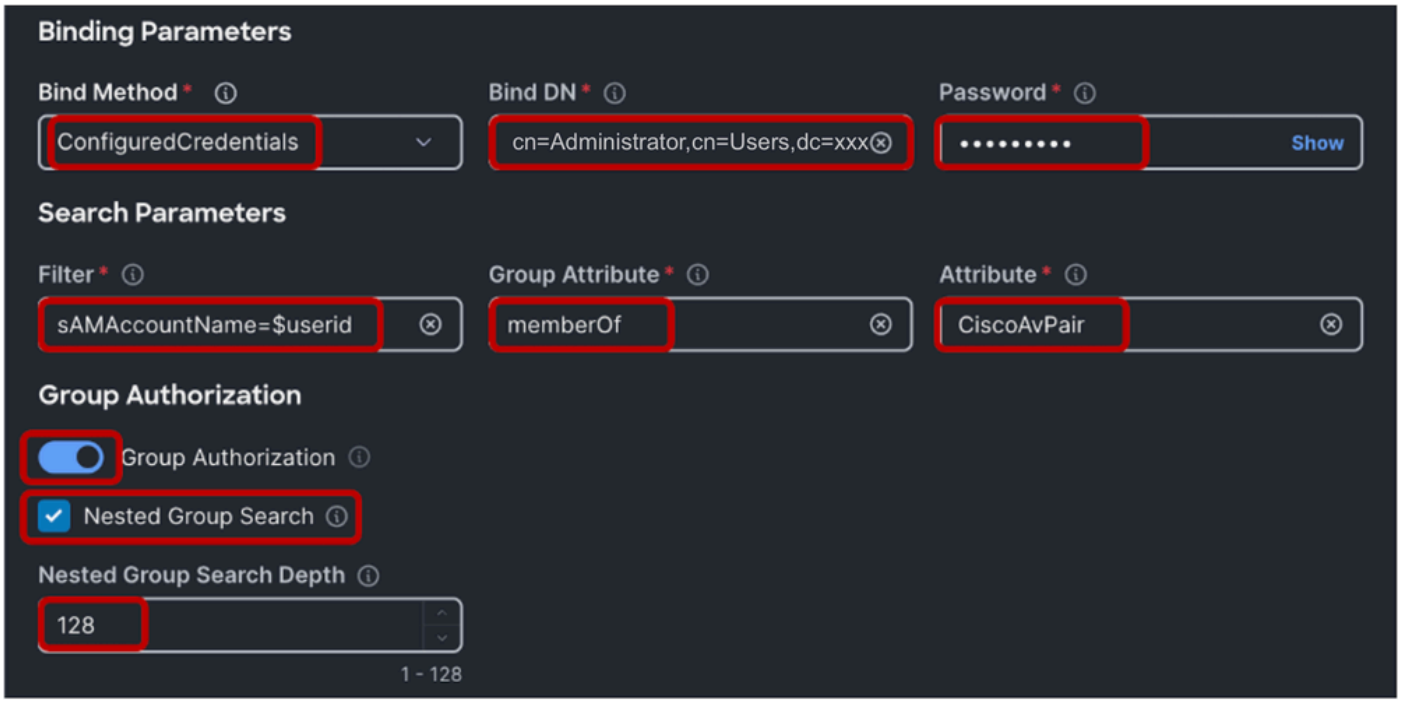


接下來，新增繫結DN（繫結使用者）和繫結使用者密碼。這可以是在Windows Active Directory上配置的任何使用者。在本演示中，使用Administrator使用者。

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

在「搜尋引數」部分的「篩選器」下，輸入「sAMAccountName=$userid」。

對於Group Attributes，新增"memberOf"，並在Attribute欄位中新增"CiscoAvPair"。根據您的LDAP伺服器配置，您可以啟用組授權和巢狀組搜尋。對於此演示，使用預設巢狀組搜尋深度128。



在「配置LDAP伺服器」部分>輸入LDAP伺服器IP地址或FQDN（對於安全LDAP是必需的）和埠號(389)。

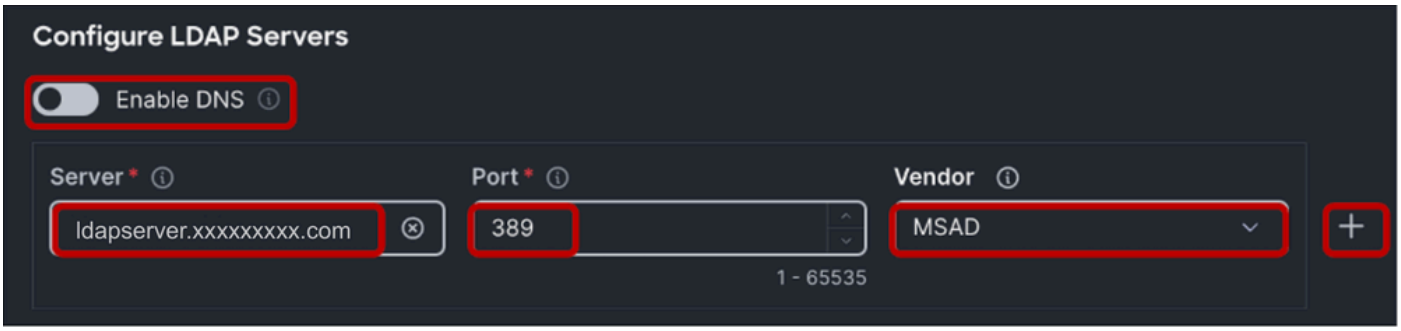
UCS中的安全LDAP使用STARTTLS啟用使用埠389的加密通訊。

請注意，將埠從389更改為636可能會導致身份驗證錯誤。Cisco UCS在埠636上為SSL執行TLS協商；但是，初始連線始終在埠389上建立時未加密。

選擇LDAP伺服器供應商。可用的供應商選項包括OpenLDAP和MSAD(Microsoft Active Directory)。在本演示中，由於使用的LDAP伺服器是Windows Server 2019，因此使用了MSAD。

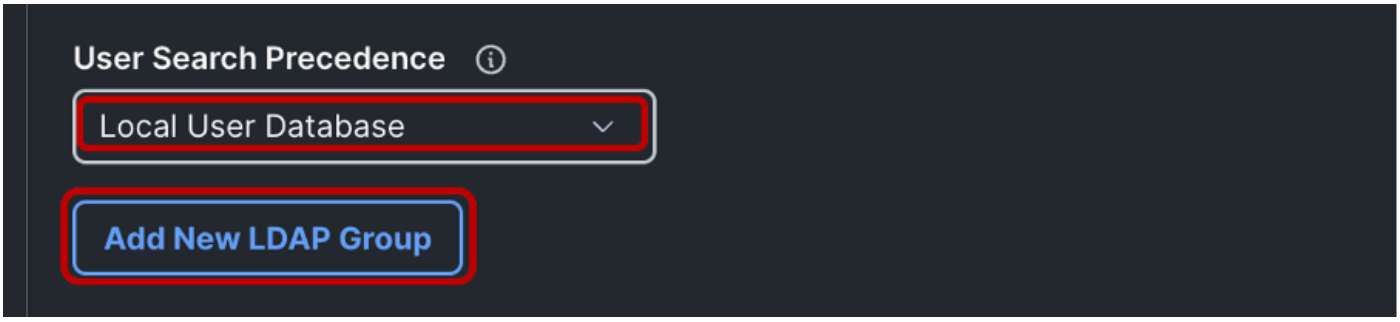
關閉「啟用DNS」按鈕，因為此選項不適用於UCS域中的LDAP配置。

通過按一下已配置LDAP伺服器最右側的「+」圖示，可以配置多個LDAP伺服器。

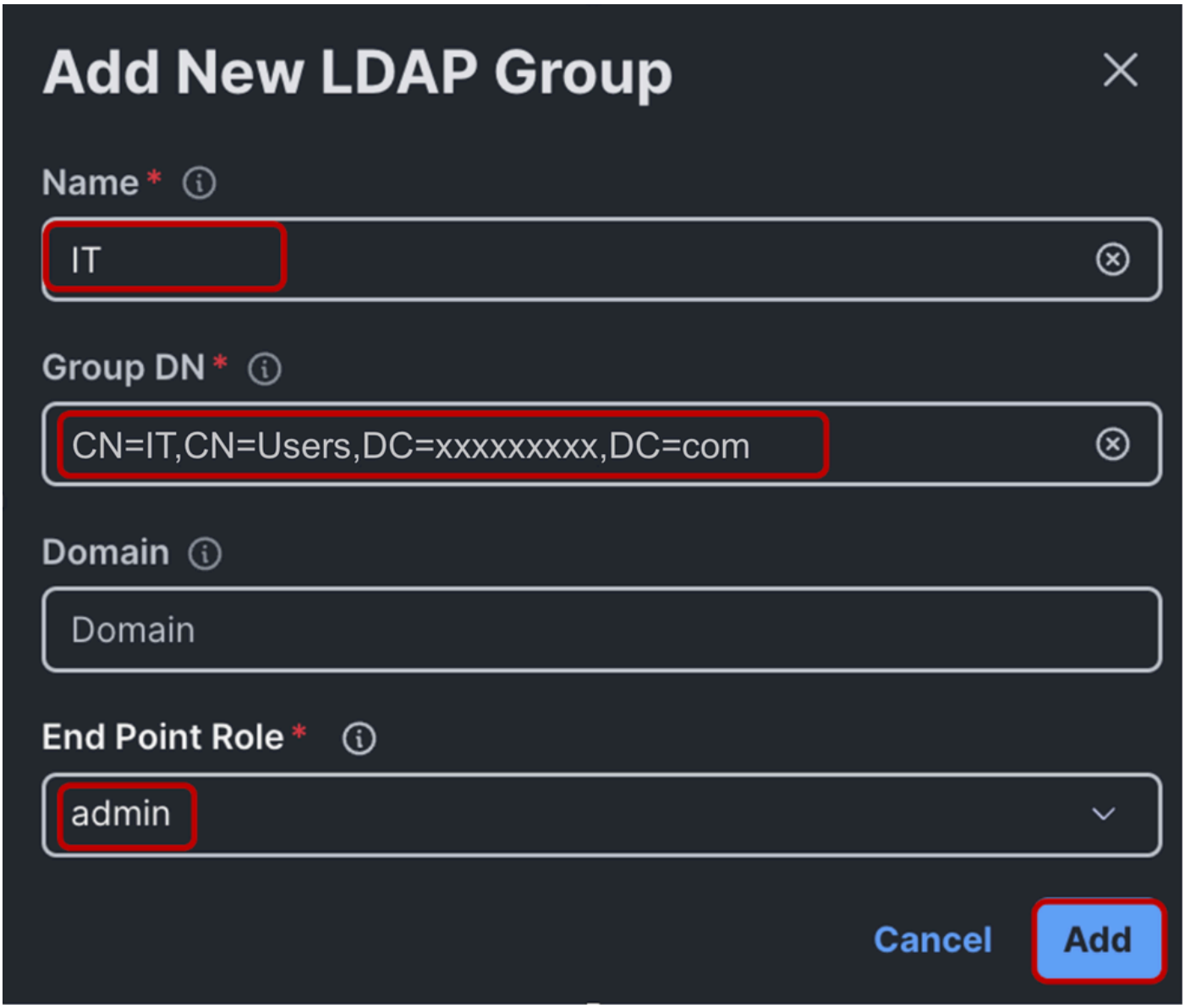


附註：您可以保留「使用者搜尋優先順序」作為「本地使用者資料庫」，也可以將其更改為「LDAP使用者資料庫」，具體取決於您的使用案例。

接下來，通過按一下Add New LDAP Group按鈕，繼續新增與LDAP伺服器中配置的組對應的組DN。



命名組，新增從LDAP伺服器接收的組DN，並選擇所需的終端角色。

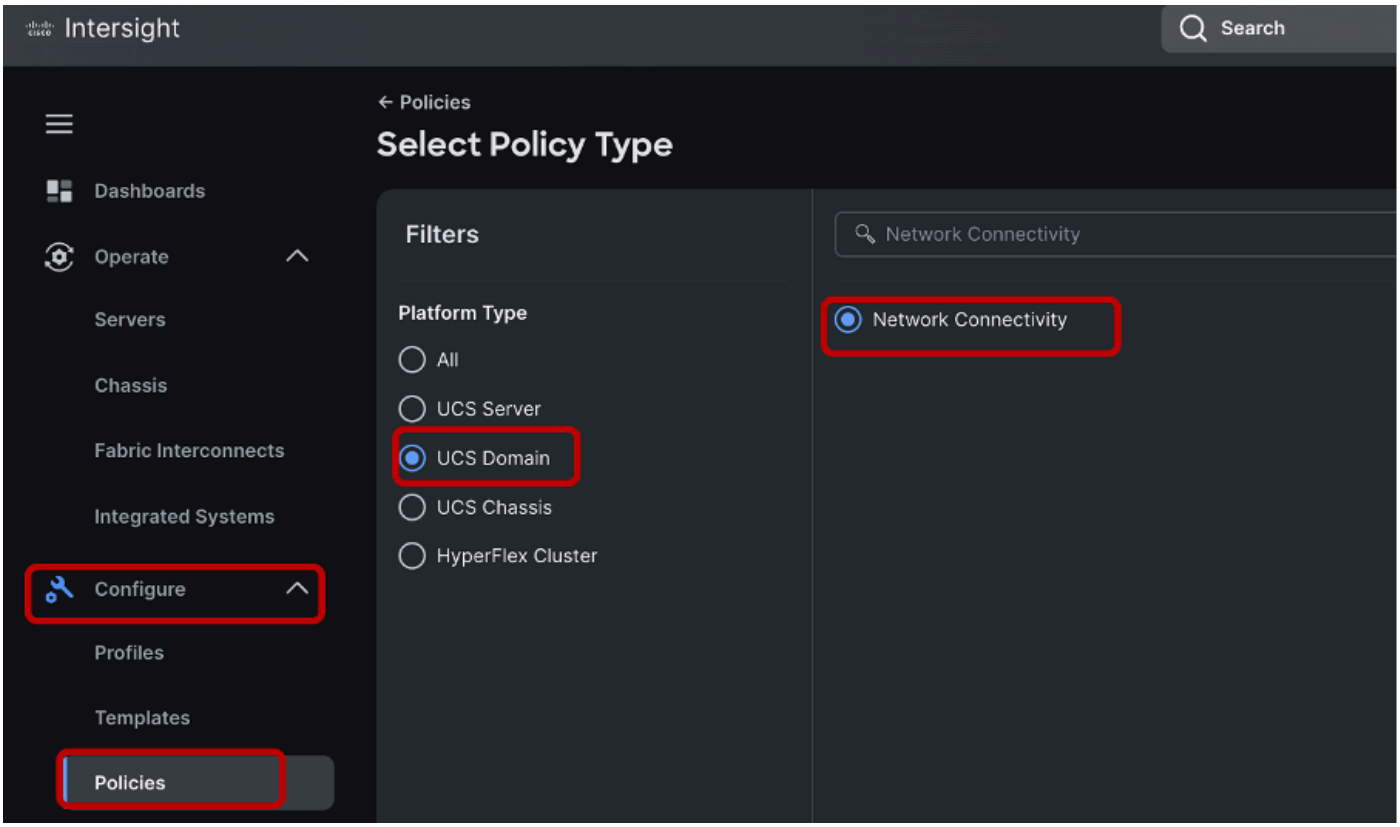


點選Add > Select Create以建立LDAP策略

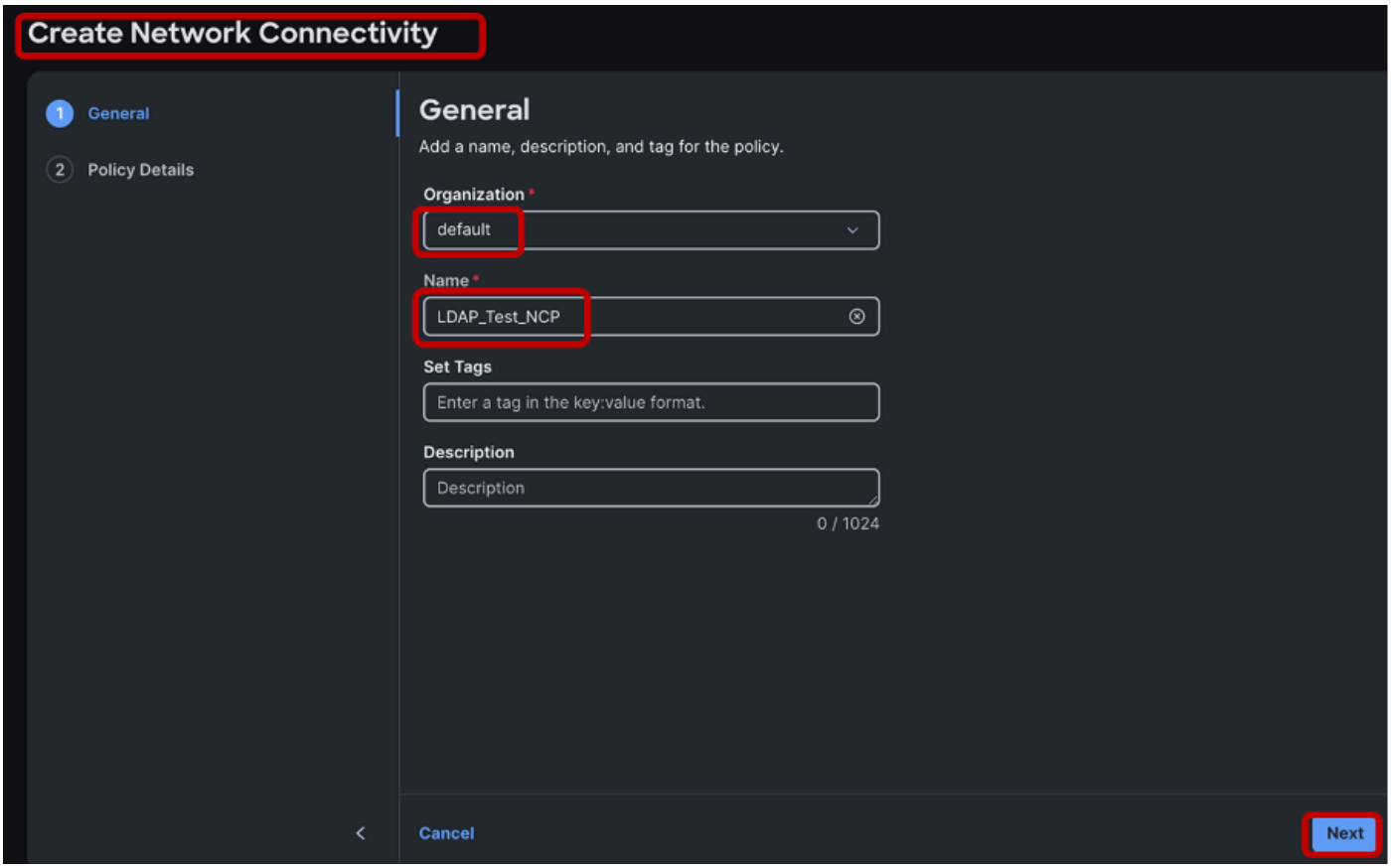
附註：對於域LDAP策略配置，截至此文檔建立時，唯一支援的終端角色為「admin」。

配置網路連線策略

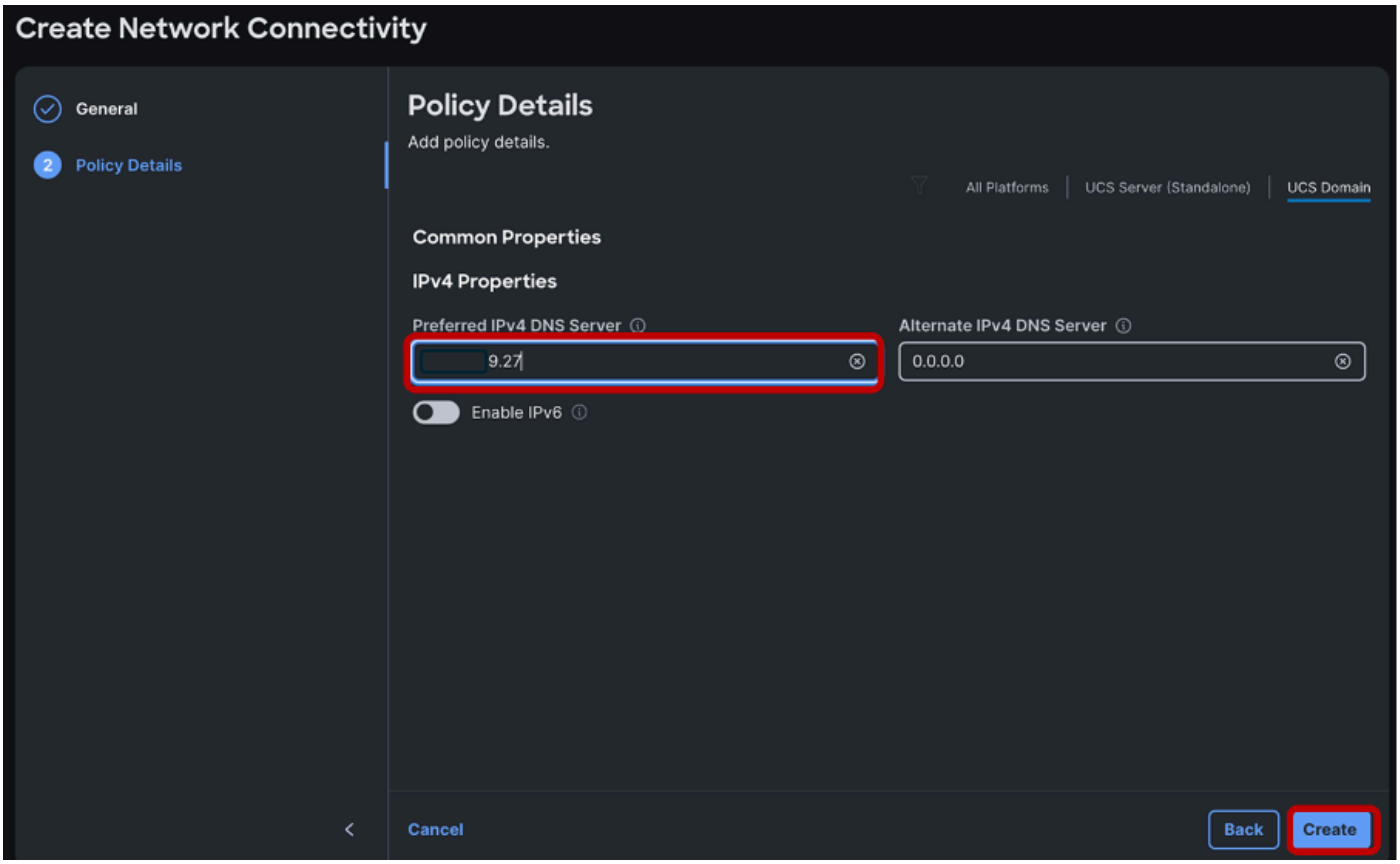
通過建立網路連線策略為UCS域配置DNS伺服器。



選擇適當的組織>輸入策略名稱>按一下下一步。



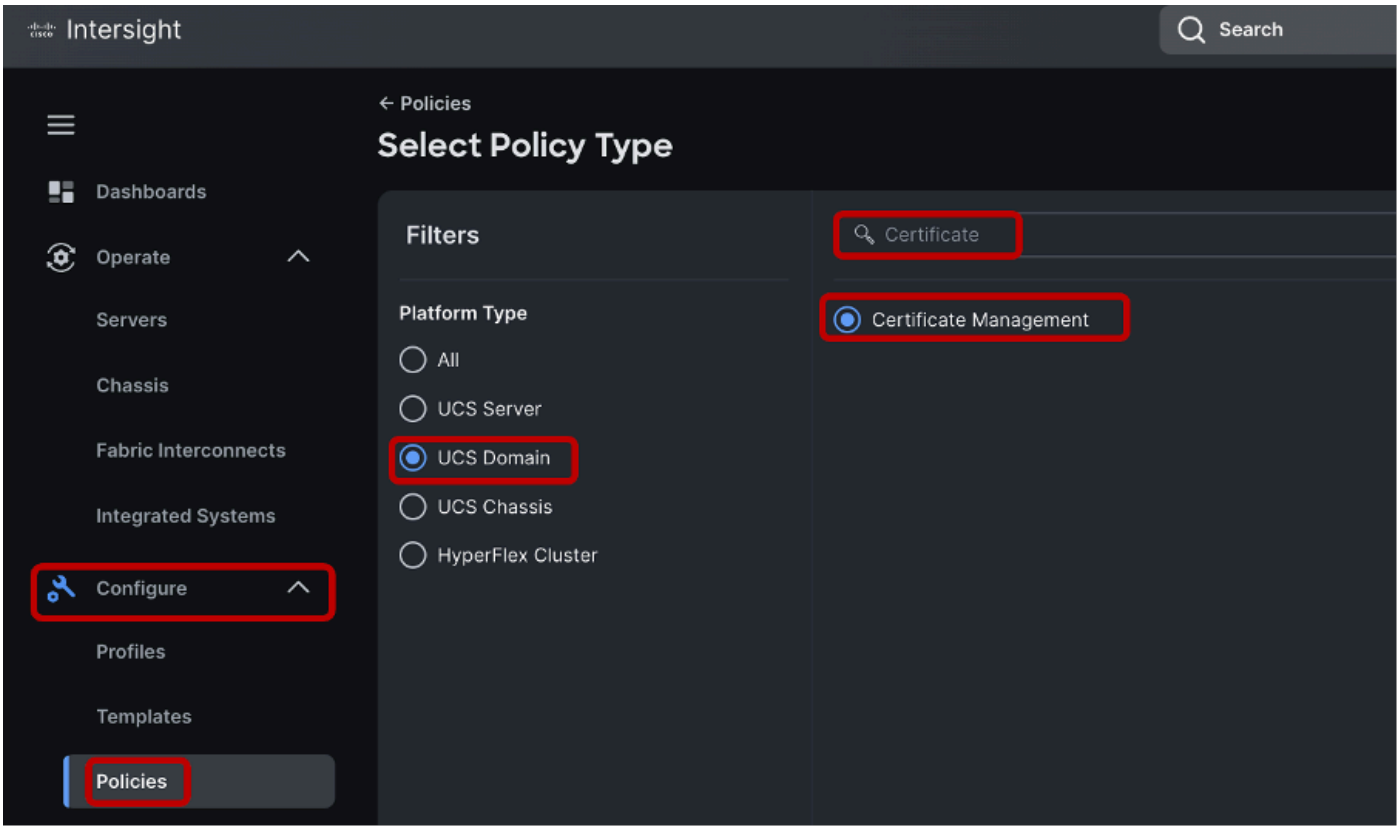
定義首選DNS伺服器IPv4地址，然後按一下Create儲存策略。



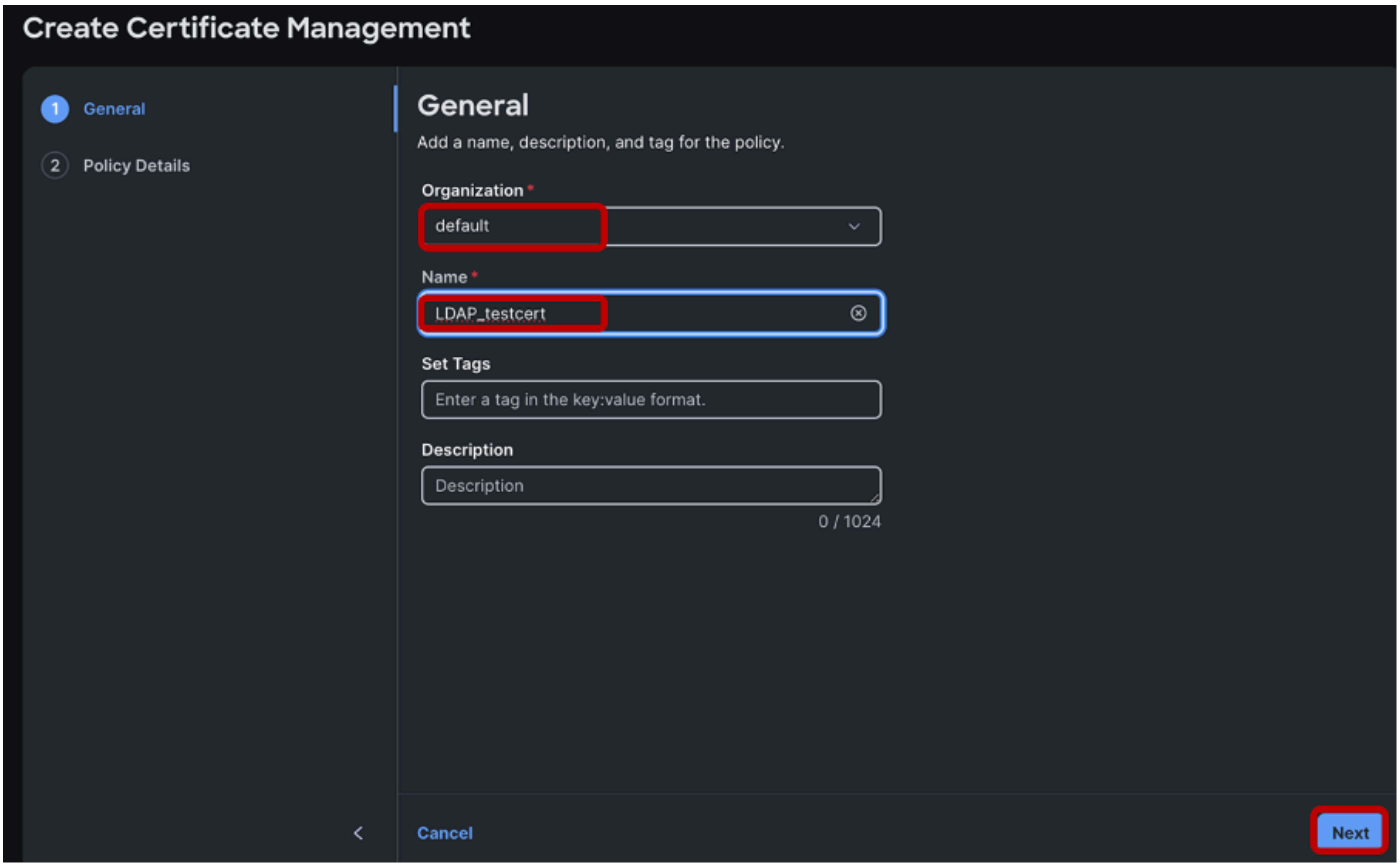
確保配置了DNS伺服器IP地址並且可以訪問以進行名稱解析。確保域名解析對域中的LDAP伺服器和交換矩陣互聯有效。在本演示中，DNS伺服器與LDAP伺服器位於同一個Windows電腦例項上。

配置證書管理策略

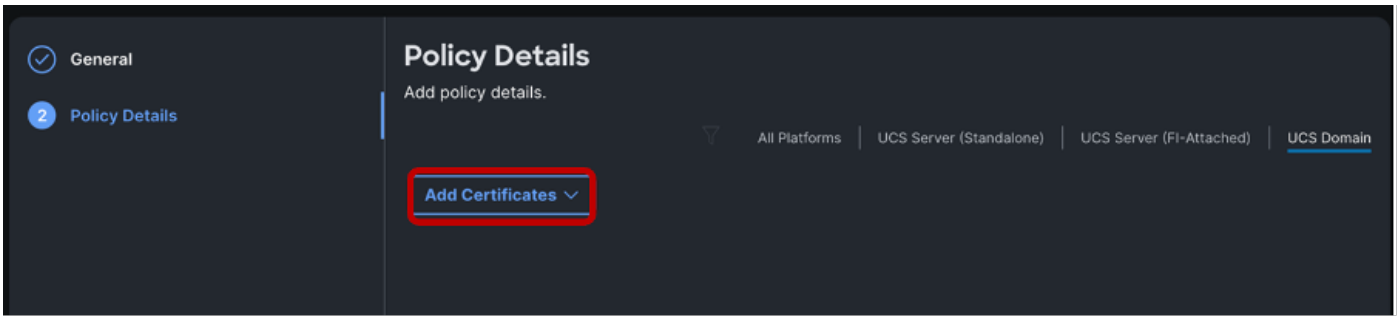
接下來，配置證書管理策略。這是LDAP加密正常運行所必需的。



選擇適當的組織，命名策略>按一下下一步

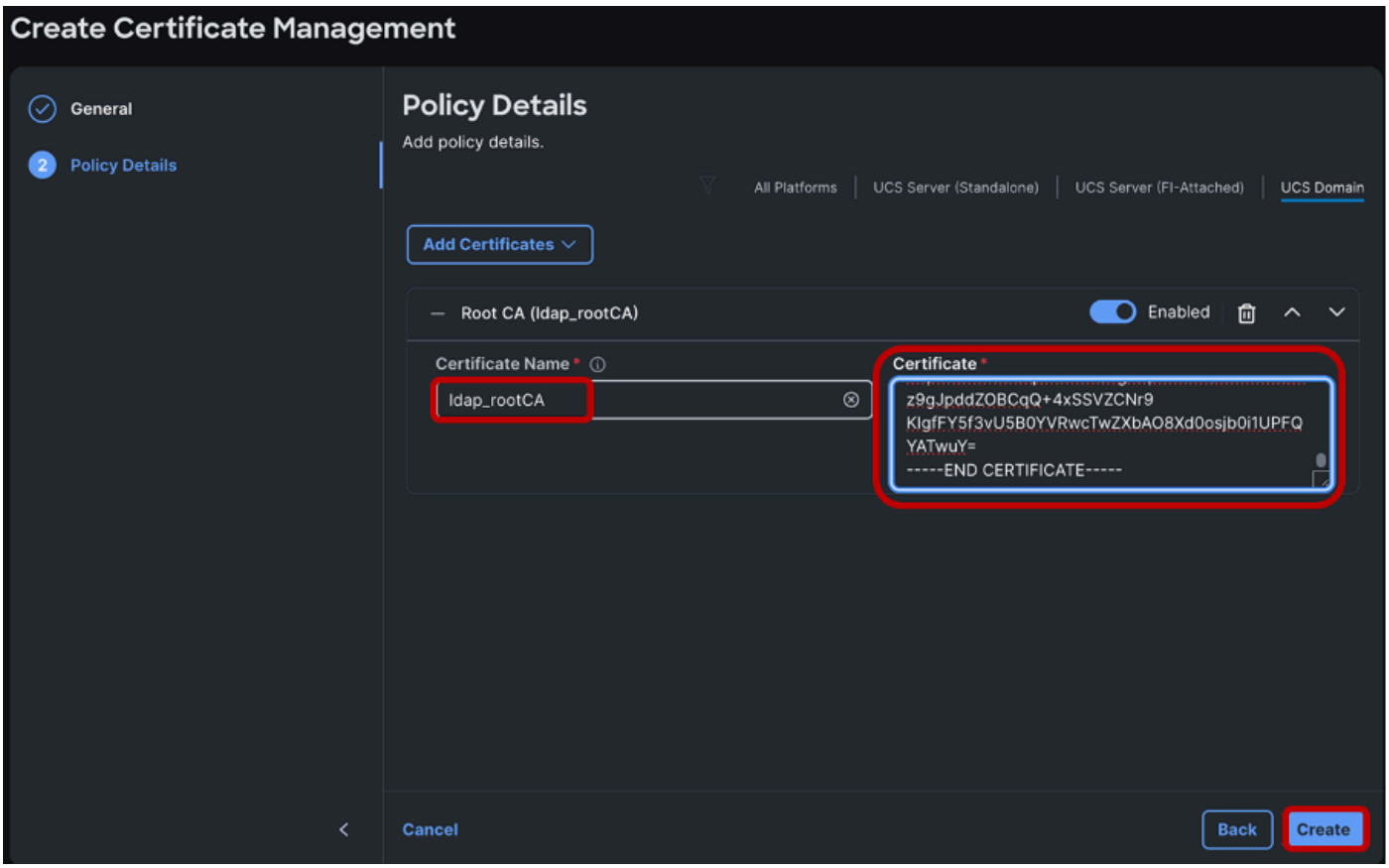


點選Add Certificates。

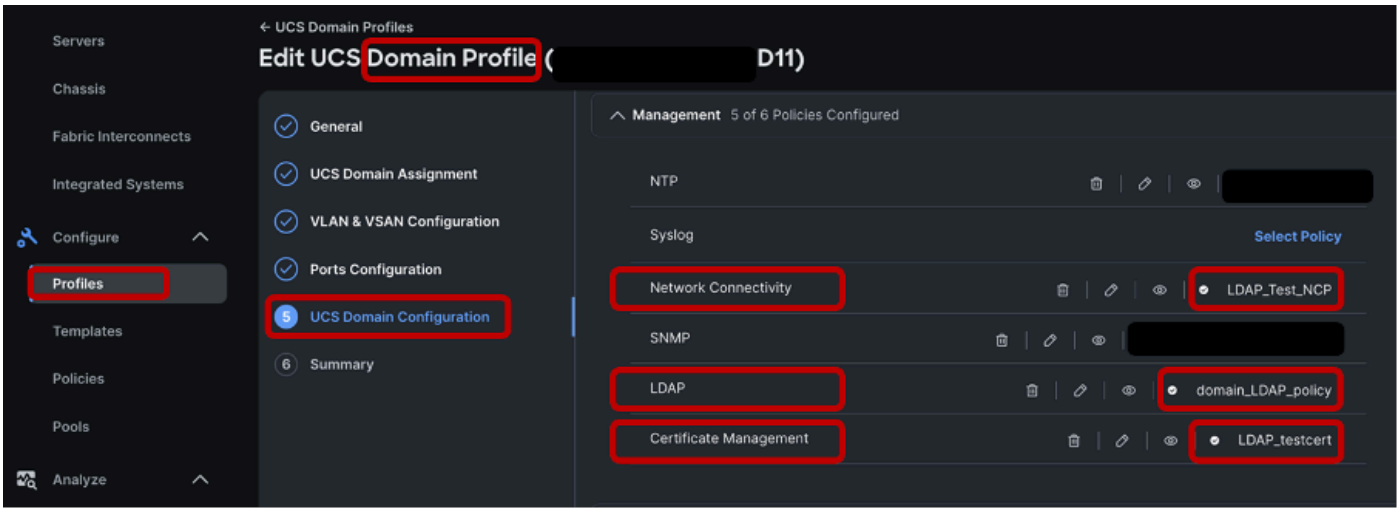


為證書命名，然後從Microsoft Active Directory證書服務貼上到根證書。

按一下「建立」。



建立LDAP、網路連線和證書管理策略後，請參閱所需域配置檔案中「UCS域配置」部分的新建立策略，如圖所示。



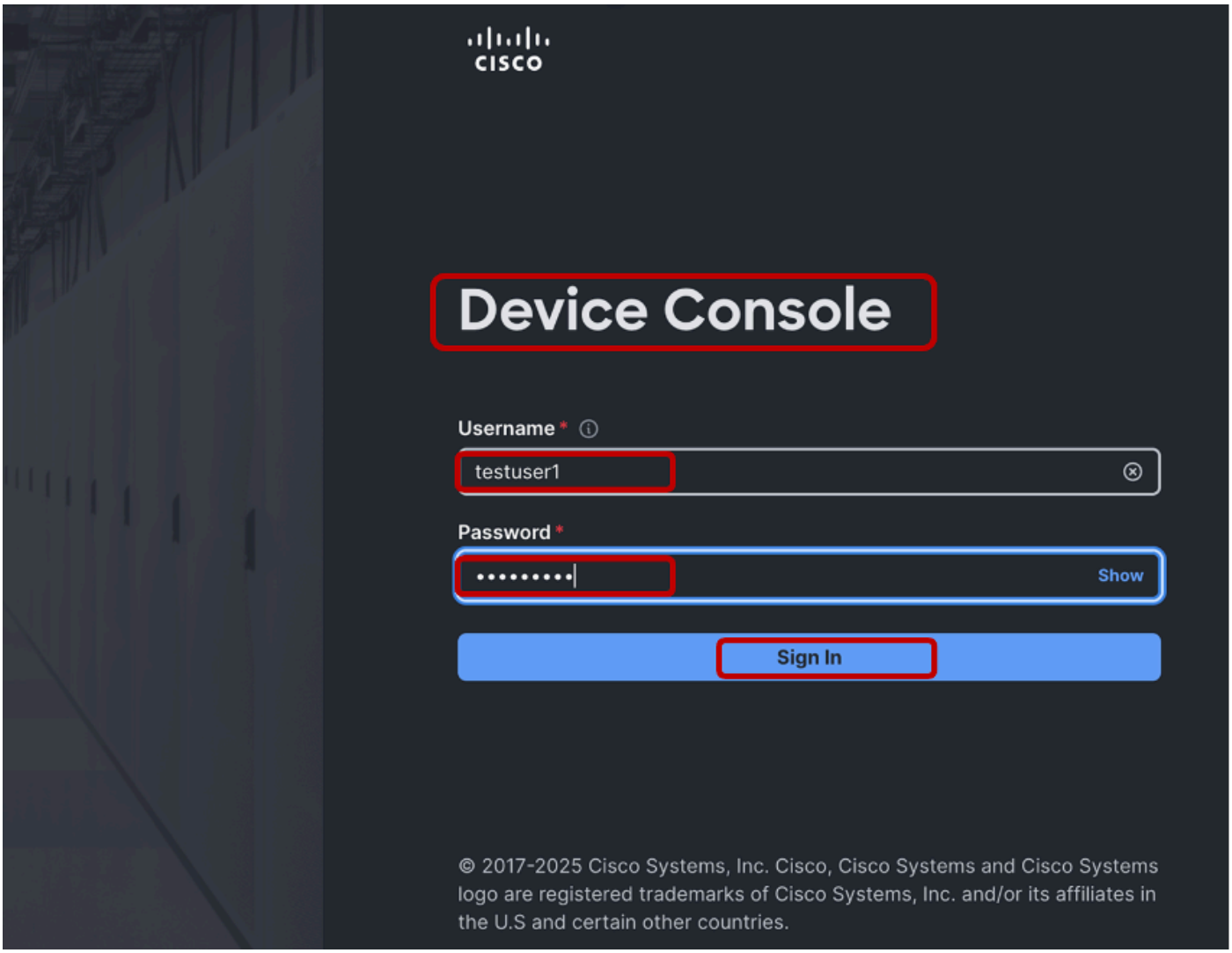
點選Next， Save and Deploy the domain profile。

成功部署域配置檔案後，IMM域的安全LDAP配置完成。

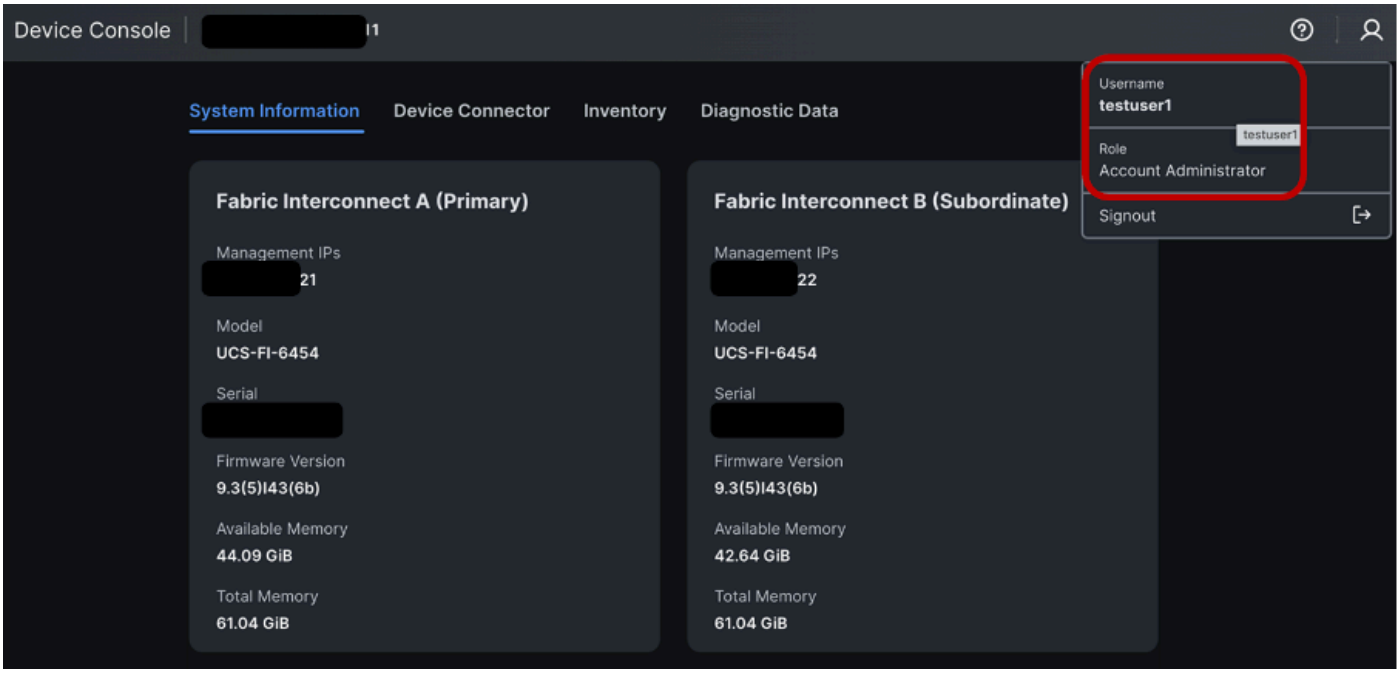
驗證

要驗證，請嘗試使用配置的LDAP/Active Directory使用者之一登入到裝置控制檯GUI和交換矩陣互聯CLI。

測試裝置控制檯登入

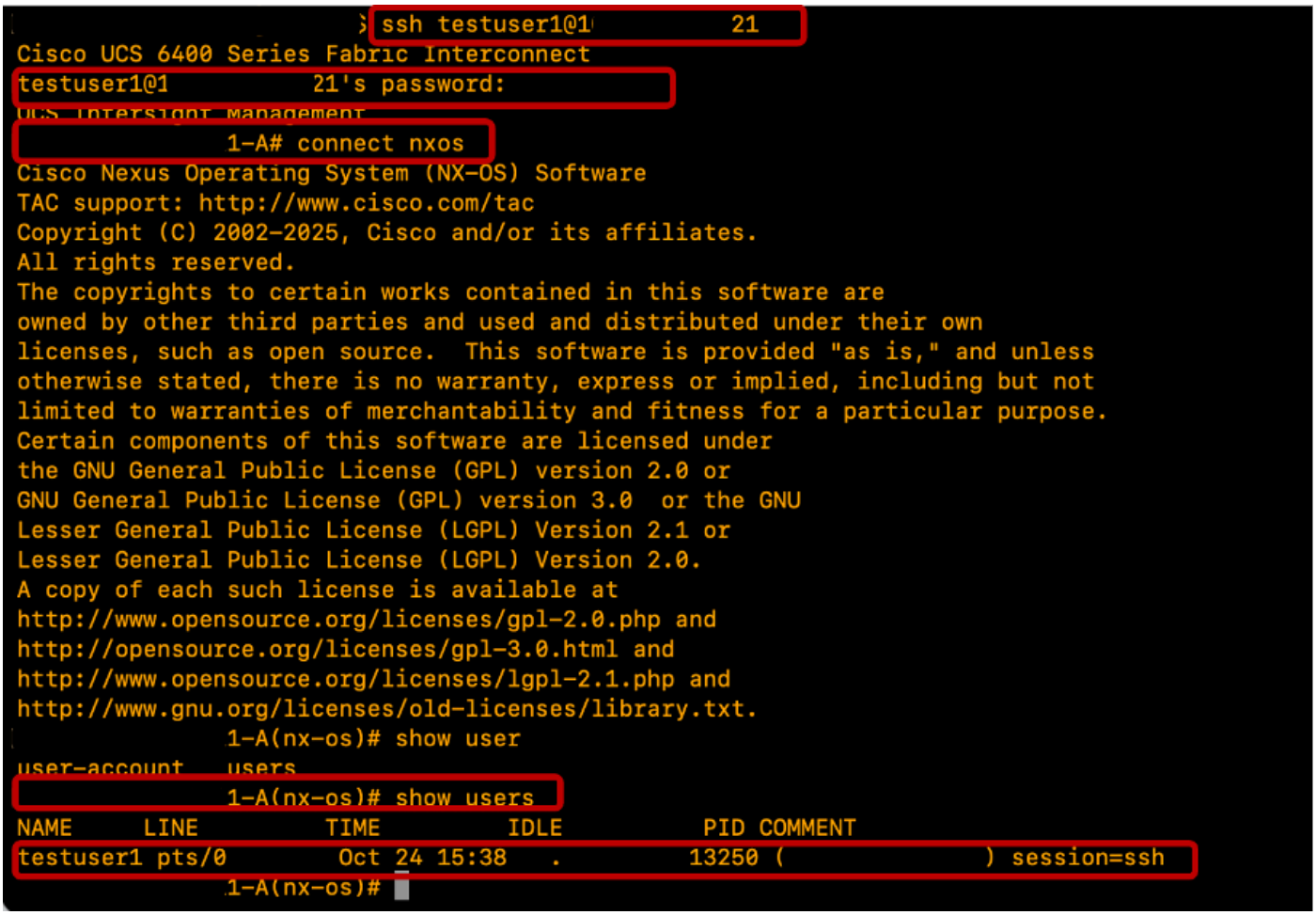


Testuser1裝置控制檯登入成功。



測試FI的SSH登入

Testuser1 SSH登入成功。



相關資訊

- Intersight幫助中心
- Cisco Intersight管理模式交換矩陣互聯管理指南

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。