ACS 5.X:安全LDAP伺服器配置示例

目錄

簡介

輕量型目錄訪問協定(LDAP)是一種用於查詢和修改在TCP/IP和UDP上運行的目錄服務的網路協定。LDAP是一種用於訪問基於x.500的目錄伺服器的輕量級機制。RFC 2251定義LDAP。

訪問控制伺服器(ACS)5.x使用LDAP協定與LDAP外部資料庫（也稱為身份庫）整合。有兩種方法可以連線到LDAP伺服器：純文字檔案（簡單）和SSL（加密）連線。可以使用這兩種方法將ACS 5.x配置為連線到LDAP伺服器。在本文檔中，ACS 5.x配置為使用加密連線連線到LDAP伺服器。

必要條件

需求

本文檔假設ACS 5.x與LDAP伺服器具有IP連線，並且埠TCP 636處於開啟狀態。

需要將Microsoft® Active Directory LDAP伺服器配置為接受埠TCP 636上的安全LDAP連線。本文檔假定您擁有將伺服器證書頒發給Microsoft LDAP伺服器的證書頒發機構(CA)的根證書。有關如何配置LDAP伺服器的詳細資訊，請參閱如何使用第三方證書頒發機構啟用SSL上的LDAP。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco安全ACS 5.x
- Microsoft Active Directory LDAP伺服器

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

背景資訊

目錄服務

目錄服務是一種軟體應用程式，或一組應用程式，用於儲存和組織關於電腦網路使用者和網路資源的資訊。您可以使用目錄服務來管理使用者對這些資源的訪問。

LDAP目錄服務基於客戶端 — 伺服器模型。客戶端通過連線到LDAP伺服器來啟動LDAP會話，並向伺服器傳送操作請求。然後，伺服器傳送其響應。一個或多個LDAP伺服器包含來自LDAP目錄樹或LDAP後端資料庫的資料。

目錄服務管理目錄，即儲存資訊的資料庫。目錄服務使用分散式模型來儲存資訊，該資訊通常在目錄伺服器之間複製。

LDAP目錄以簡單的樹狀層次結構組織，可以分佈在許多伺服器中。每台伺服器都可以擁有定期同步的總目錄的復製版本。

樹中的條目包含一組屬性，其中每個屬性都有一個名稱（屬性型別或屬性說明）和一個或多個值。屬性在架構中定義。

每個條目都有一個唯一的識別符號：其唯一判別名(DN)。 此名稱包含從條目的屬性構建的相對可分辨名稱(RDN)，後跟父條目的DN。您可以將DN視為完整檔名，將RDN視為資料夾中的相對檔名。

使用LDAP進行身份驗證

ACS 5.x可以通過在目錄伺服器上執行繫結操作來查詢和驗證主體，從而根據LDAP身份庫驗證主體。如果身份驗證成功，ACS可以檢索屬於主體的組和屬性。可以在ACS Web介面（LDAP頁面）中配置要檢索的屬性。 ACS可以使用這些組和屬性授權承擔者。

為了驗證使用者或查詢LDAP身份庫，ACS連線到LDAP伺服器並維護連線池。

LDAP連線管理

ACS 5.x支援多個併發LDAP連線。在第一次進行LDAP身份驗證時，會按需開啟連線。為每個LDAP伺服器配置的最大連線數。提前開啟連線可縮短身份驗證時間。

可以設定用於併發繫結連線的最大連線數。每個LDAP伺服器（主或輔助）的已開啟連線數可以不同，並根據為每個伺服器配置的最大管理連線數確定。

ACS會為在ACS中配置的每個LDAP伺服器保留一個開啟的LDAP連線清單（包括繫結資訊）。在身份驗證過程中，連線管理器會嘗試從池中查詢開啟的連線。

如果開啟的連線不存在，則會開啟一個新連線。如果LDAP伺服器關閉了連線，則連線管理器在第一次呼叫搜尋目錄時報告錯誤，並嘗試續訂連線。

身份驗證過程完成後，連線管理器釋放到連線管理器的連線。有關詳細資訊，請參閱ACS 5.X使用手冊。

設定

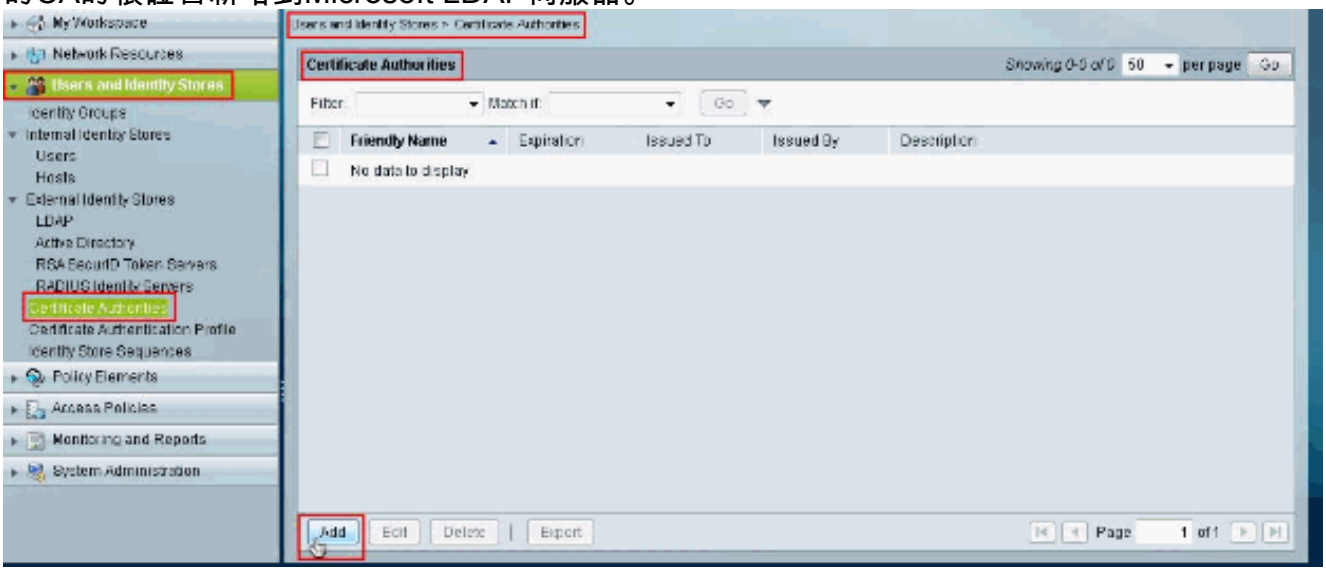
本節提供用於設定本文件中所述功能的資訊。

在ACS 5.x上安裝根CA證書

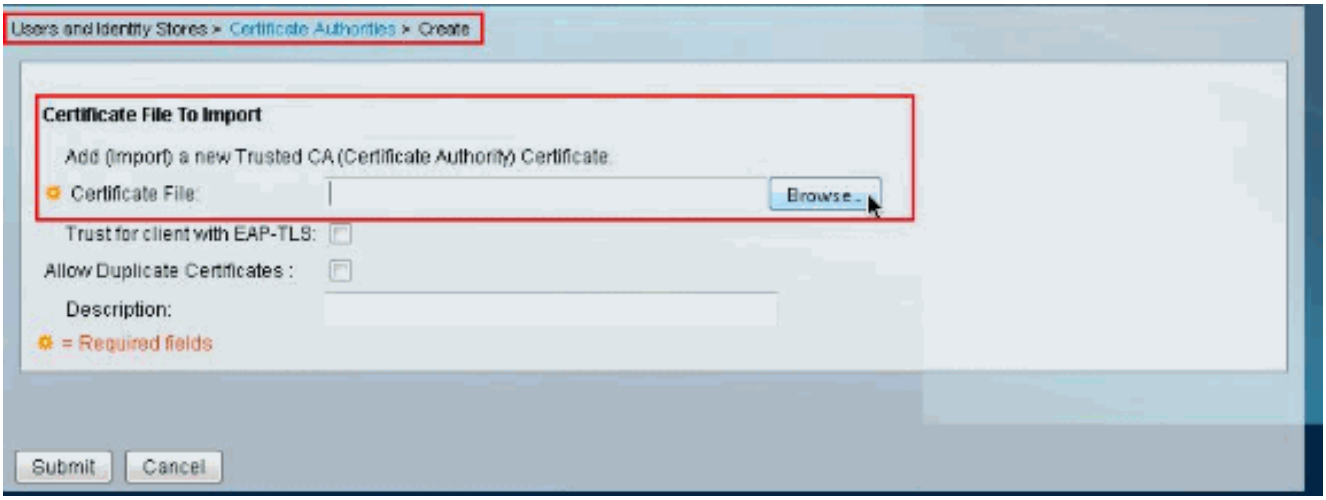
要在Cisco Secure ACS 5.x上安裝根CA證書，請完成以下步驟：

註意：確保LDAP伺服器已預配置為接受埠TCP 636上的加密連線。有關如何配置Microsoft LDAP伺服器的詳細資訊，請參閱如何啟用具有第三方證書頒發機構的SSL上的LDAP。

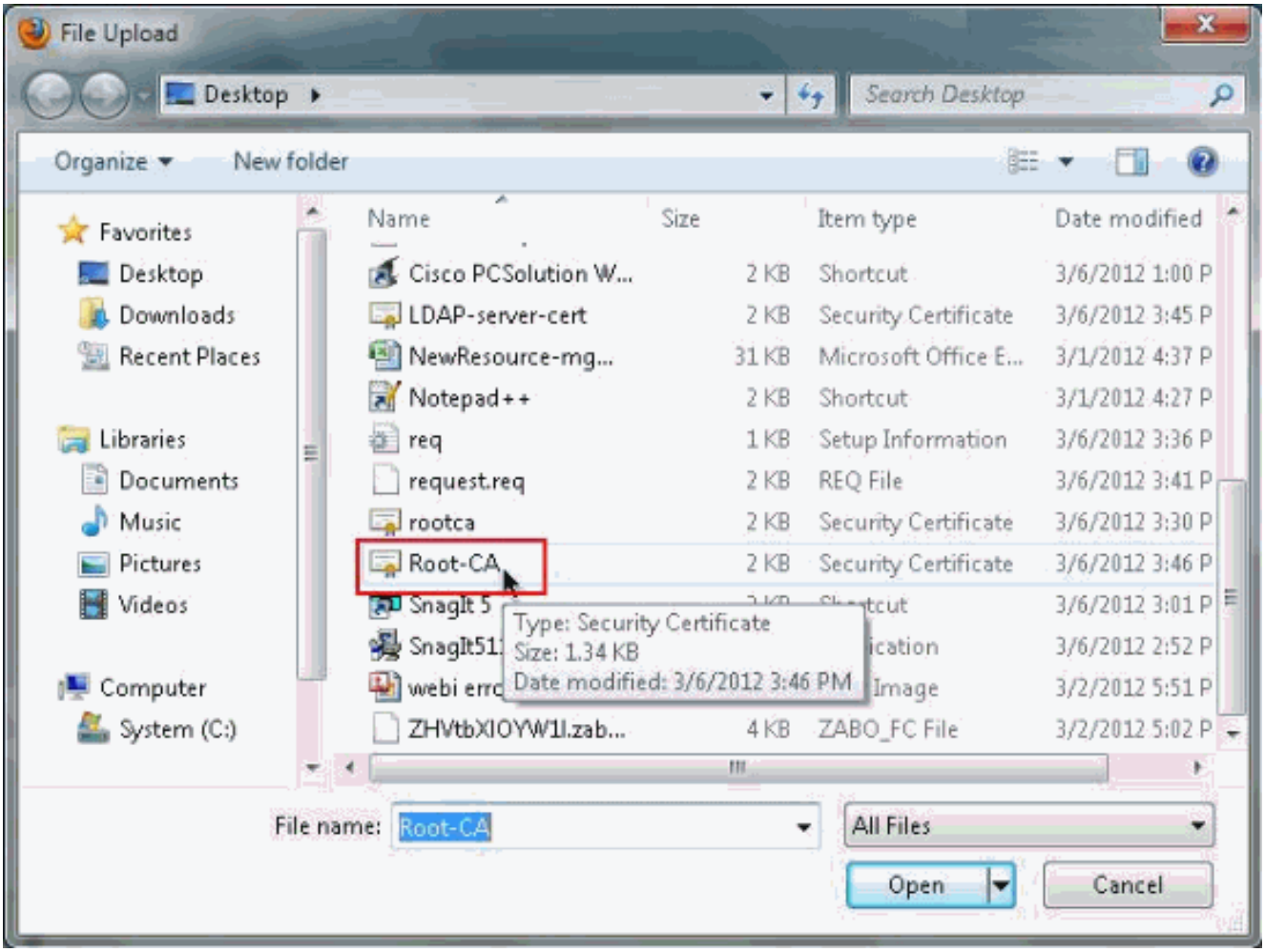
1. 選擇**Users and Identity Stores > Certificate Authorities**，然後按一下**Add**以將頒發伺服器證書的CA的根證書新增到Microsoft LDAP伺服器。



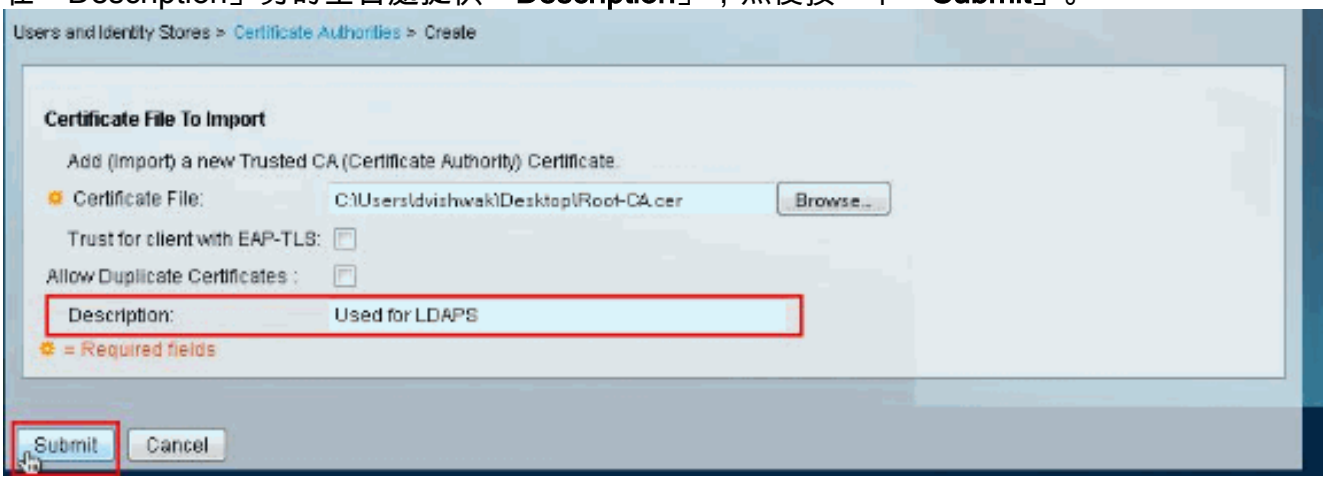
2. 在「**Certificate File to Import**」區段中，按一下「**Certificate File**」旁邊的**Browse**，即可搜尋憑證檔案。



3. 選擇所需的**Certificate file**（將伺服器證書頒發給Microsoft LDAP伺服器的CA的根證書），然後按一下**Open**。

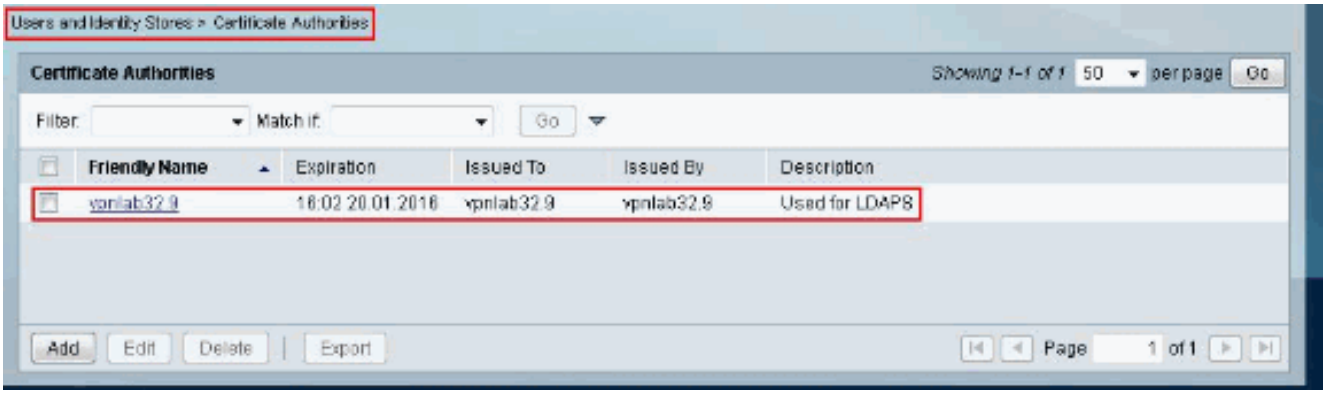


4. 在「Description」旁的空白處提供「**Description**」，然後按一下「**Submit**」。



此圖顯示根憑證已正確安裝

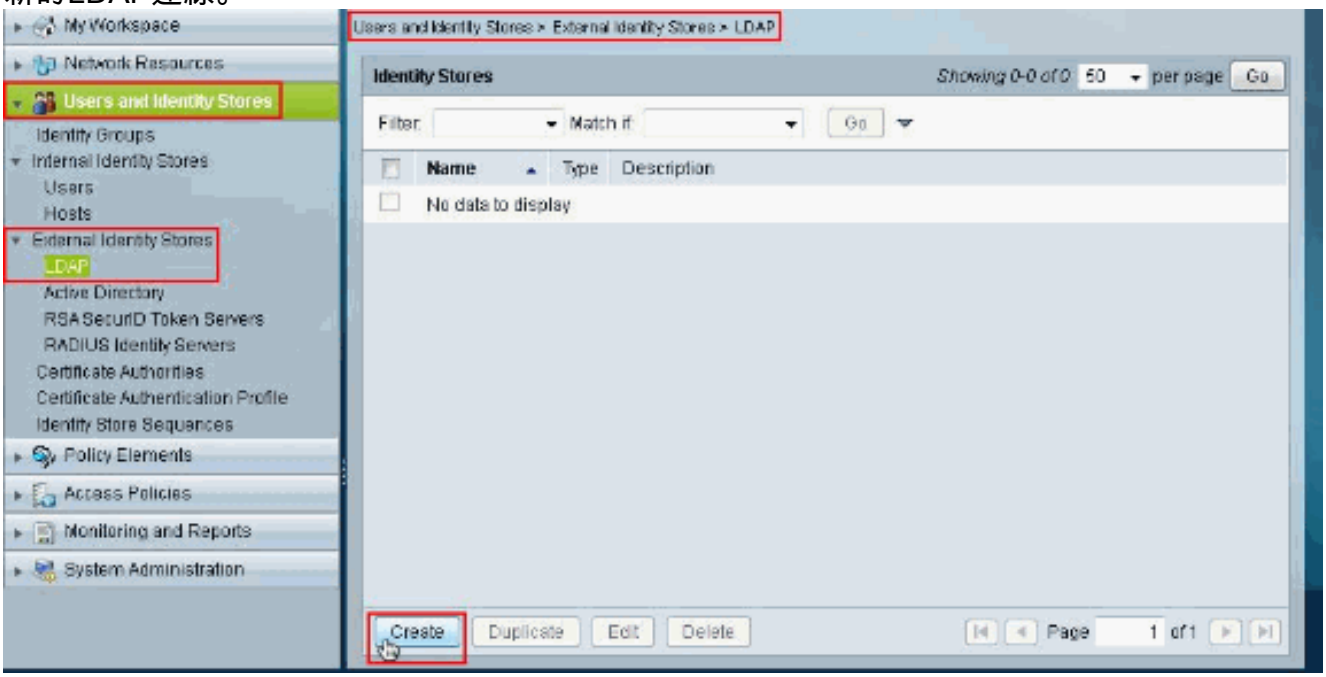
:



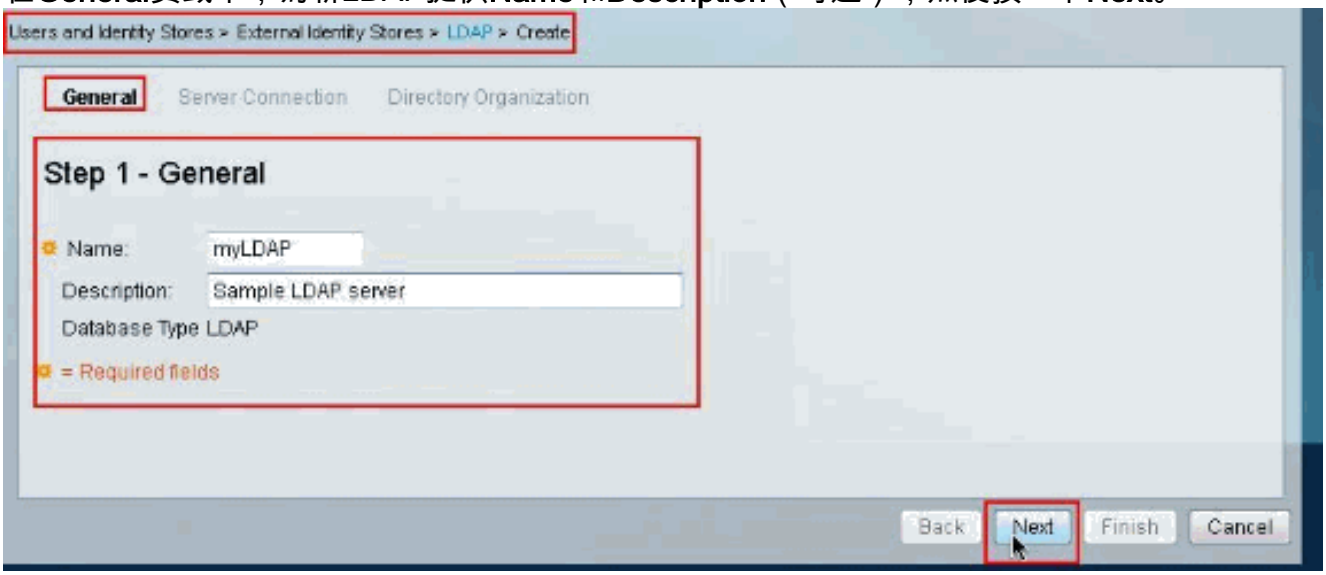
為安全LDAP配置ACS 5.X

完成以下步驟，為安全LDAP配置ACS 5.x:

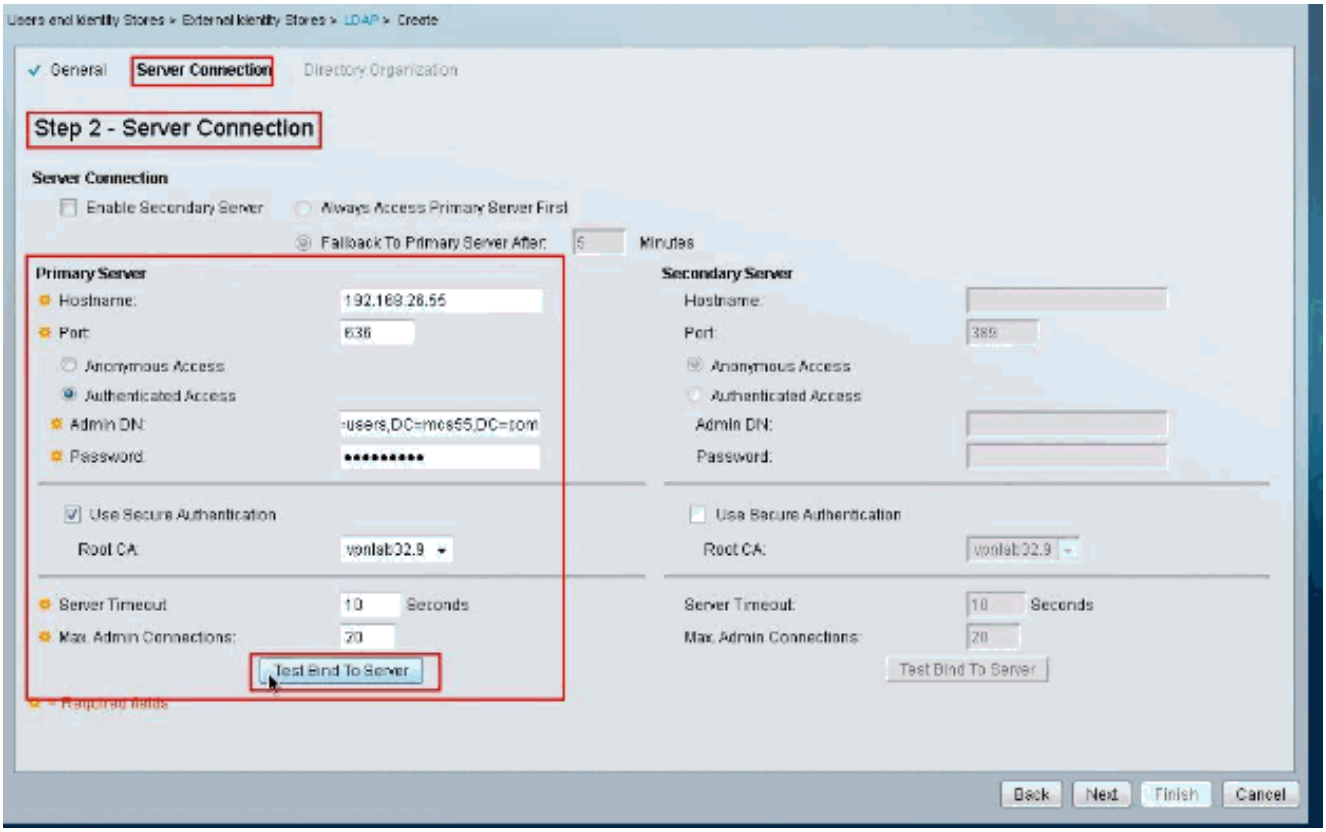
1. 選擇**Users and Identity Stores > External Identity Stores > LDAP**，然後按一下**Create**以建立新的LDAP連線。



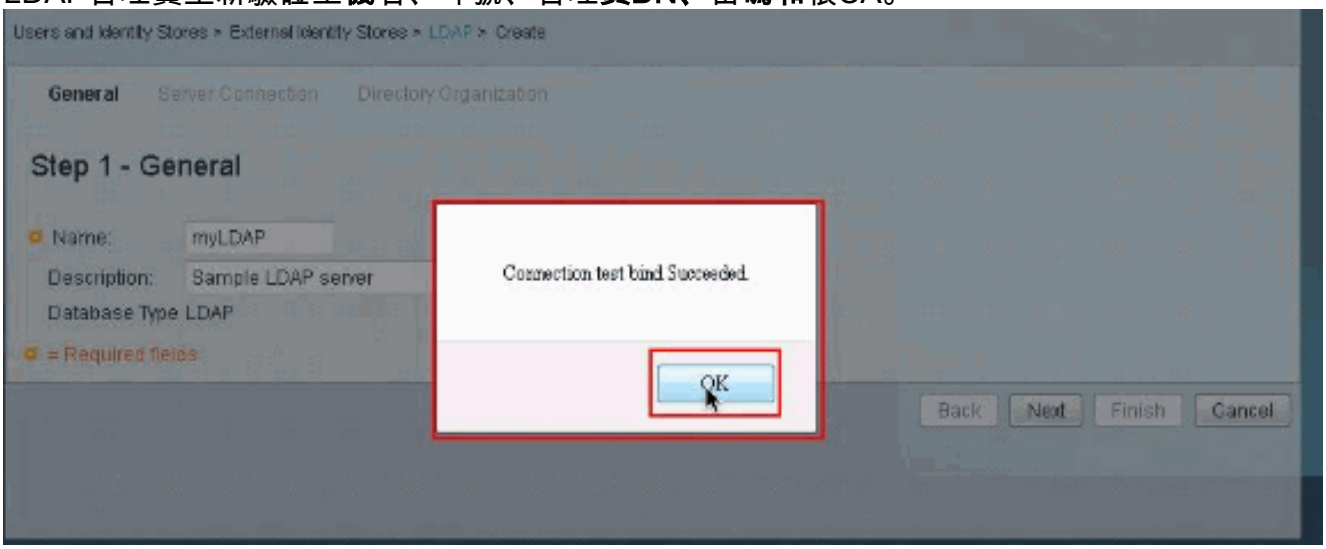
2. 在**General**頁籤中，為新LDAP提供**Name**和**Description**（可選），然後按一下**Next**。



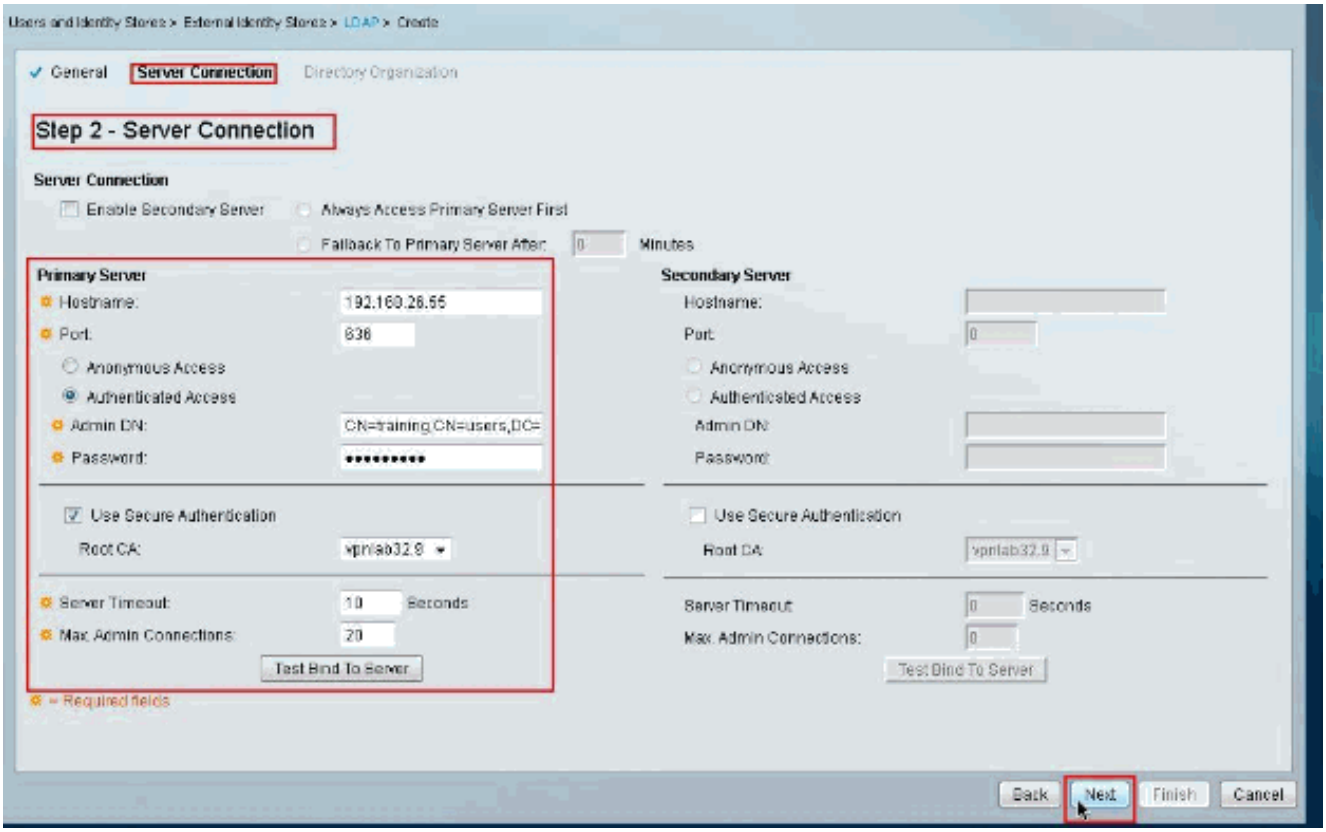
3. 在**主伺服器**部分下的**伺服器連線**頁籤中，提供**主機名、埠、管理員DN和密碼**。確保選中**Use Secure Authentication**旁邊的覈取方塊，並選擇最近安裝的**根CA證書**。按一下**測試繫結到伺服器**。**注意**：IANA為安全LDAP分配的埠號為TCP 636。但是，請從LDAP管理員確認LDAP伺服器使用的埠號。**注意**：管理員DN和密碼應由您的LDAP管理員提供。管理員DN必須對LDAP伺服器上的所有OU具有讀取所有許可權。



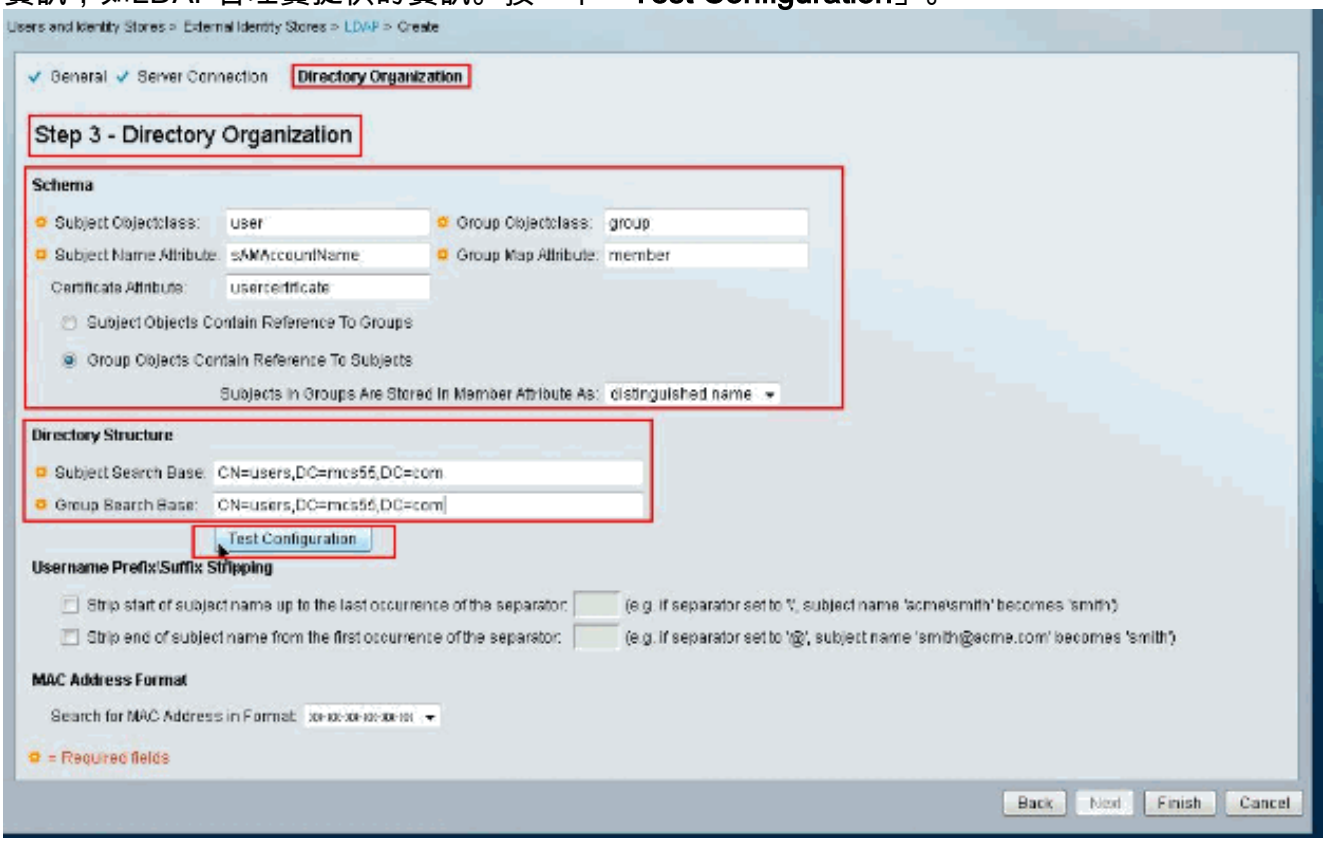
下一張圖顯示Connection Test Bind to the server成功。**注意**：如果測試繫結未成功，請從LDAP管理員重新驗證主機名、埠號、管理員DN、密碼和根CA。



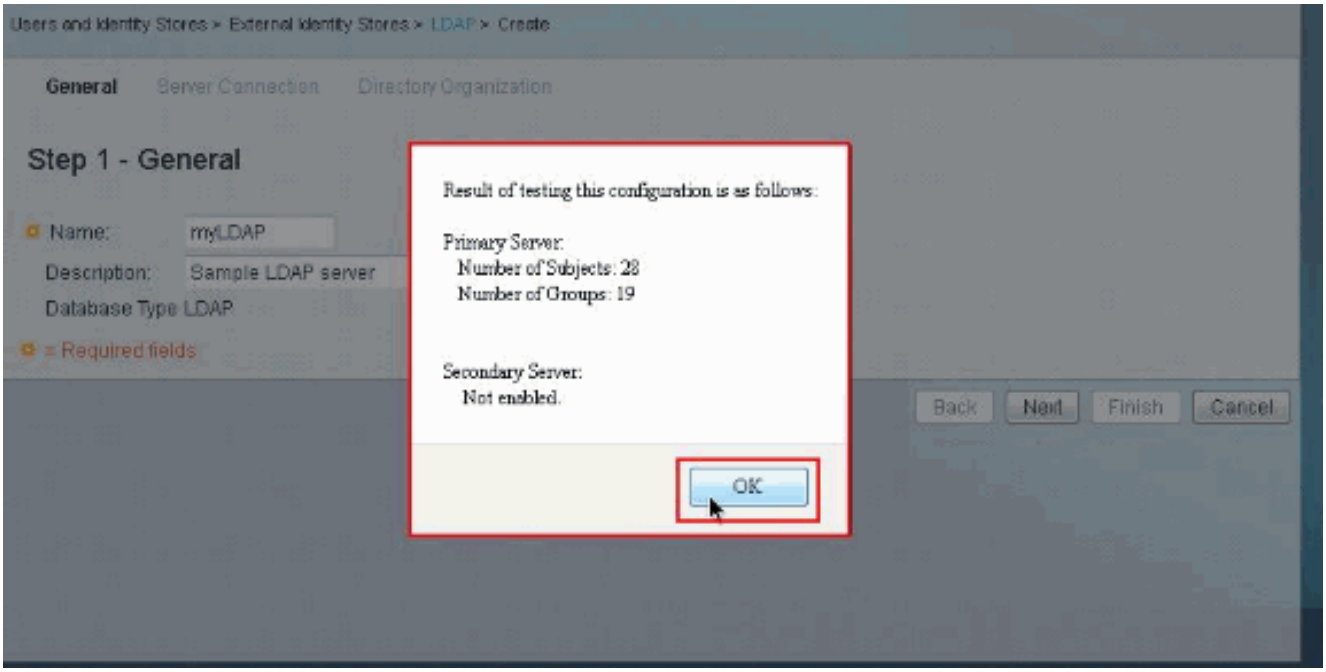
4. 按「**Next**」（下一步）。



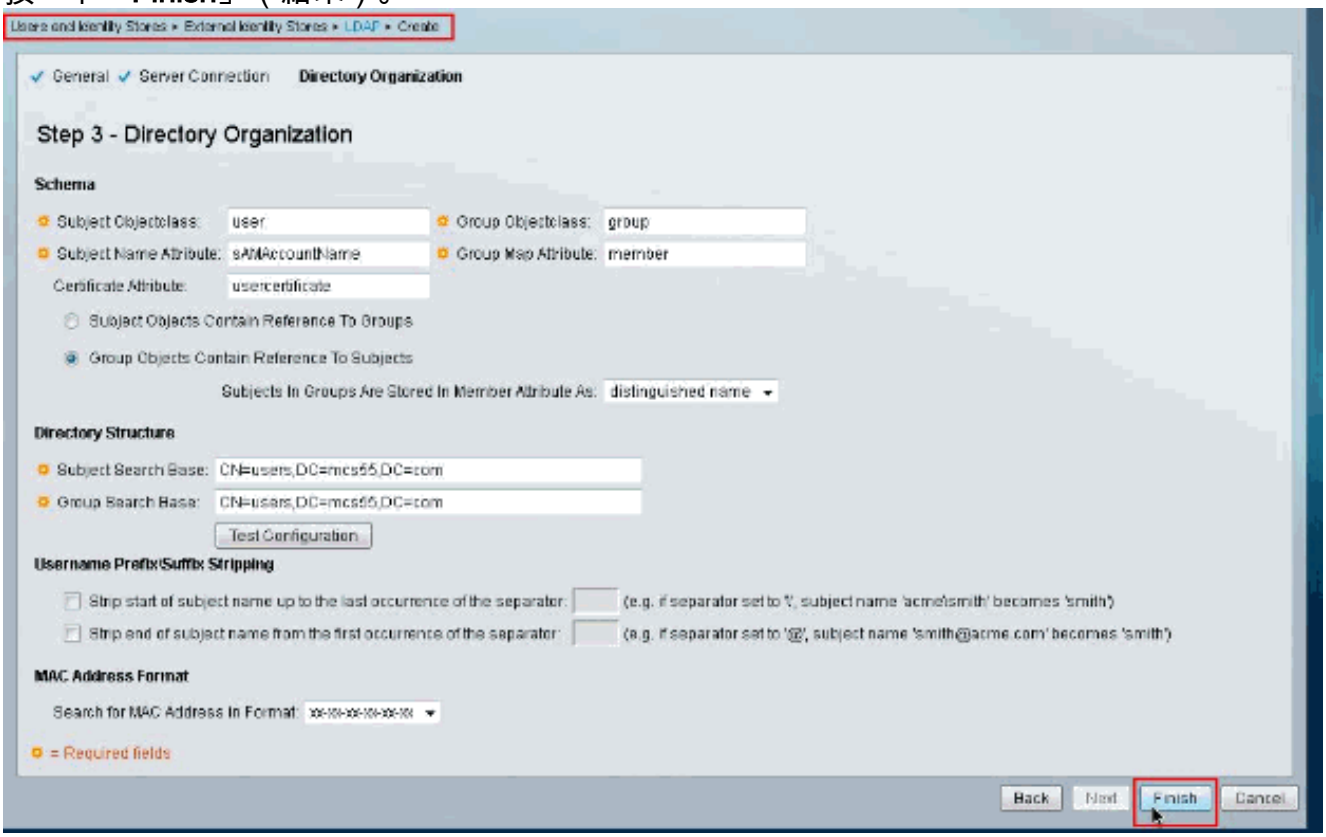
5. 在**架構**部分下的**目錄組織**頁籤中，提供所需的詳細資訊。同樣，在**目錄結構**部分下提供所需的資訊，如LDAP管理員提供的資訊。按一下「**Test Configuration**」。



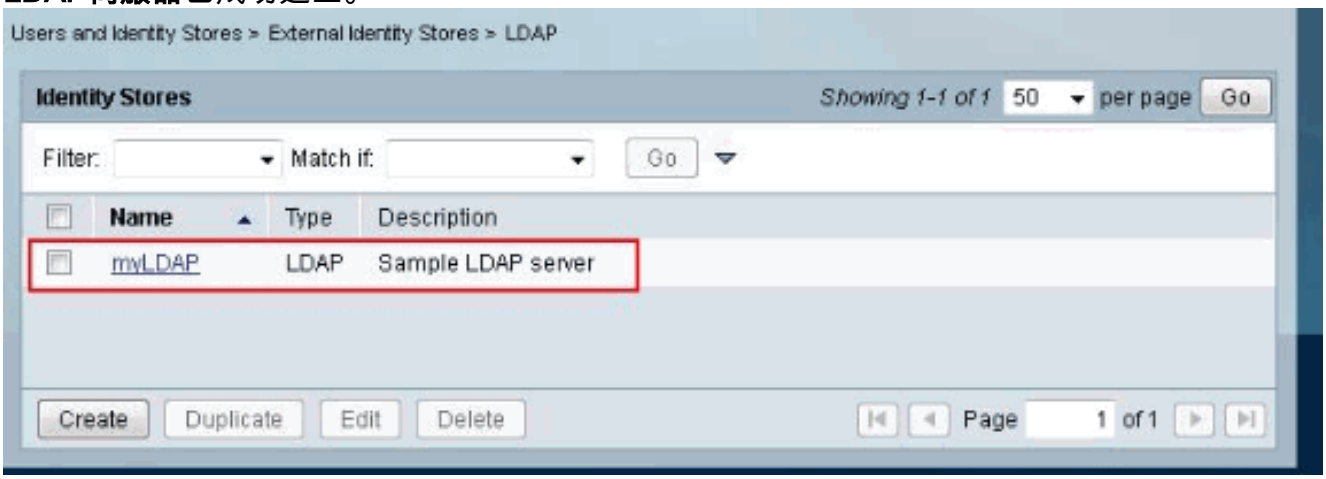
下一張圖顯示**組態測試**成功。**註：如**果配置測試未成功，請從LDAP管理員重新驗證**方案**和目錄**結構**中提供的引數。



6. 按一下「**Finish**」（結束）。



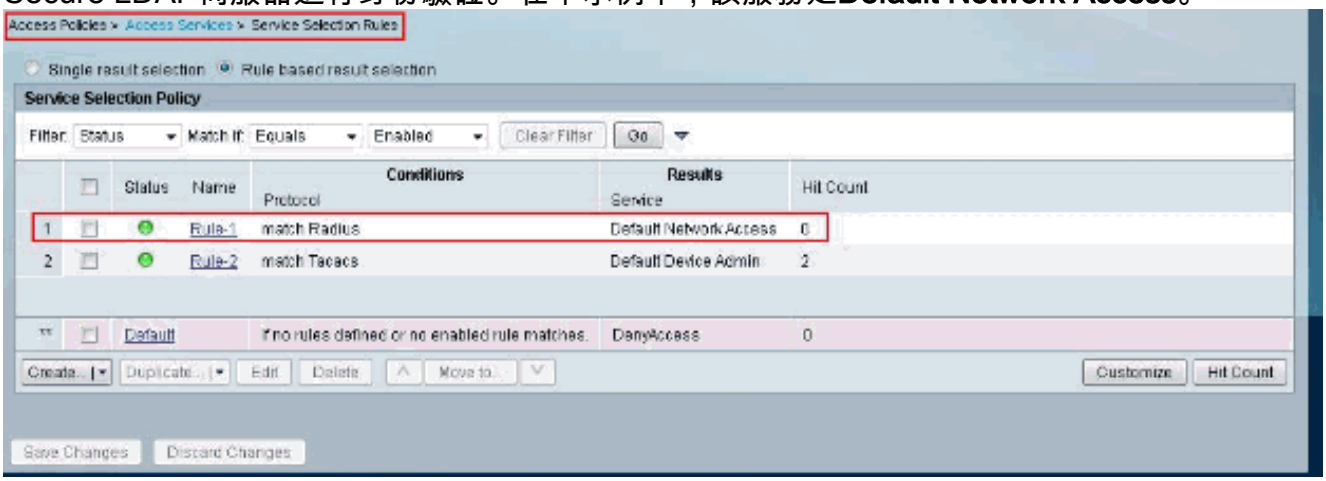
LDAP伺服器已成功建立。



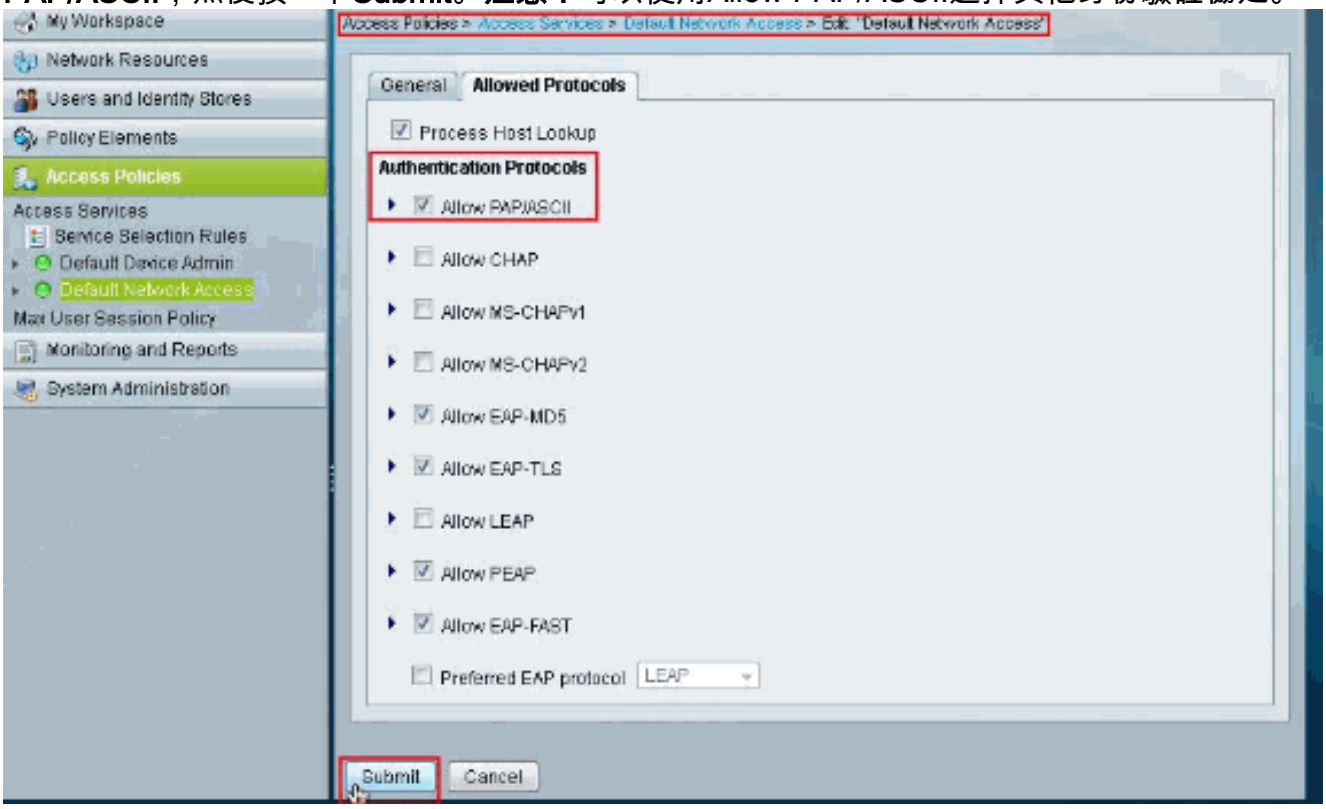
配置身份庫

完成以下步驟以配置身份庫：

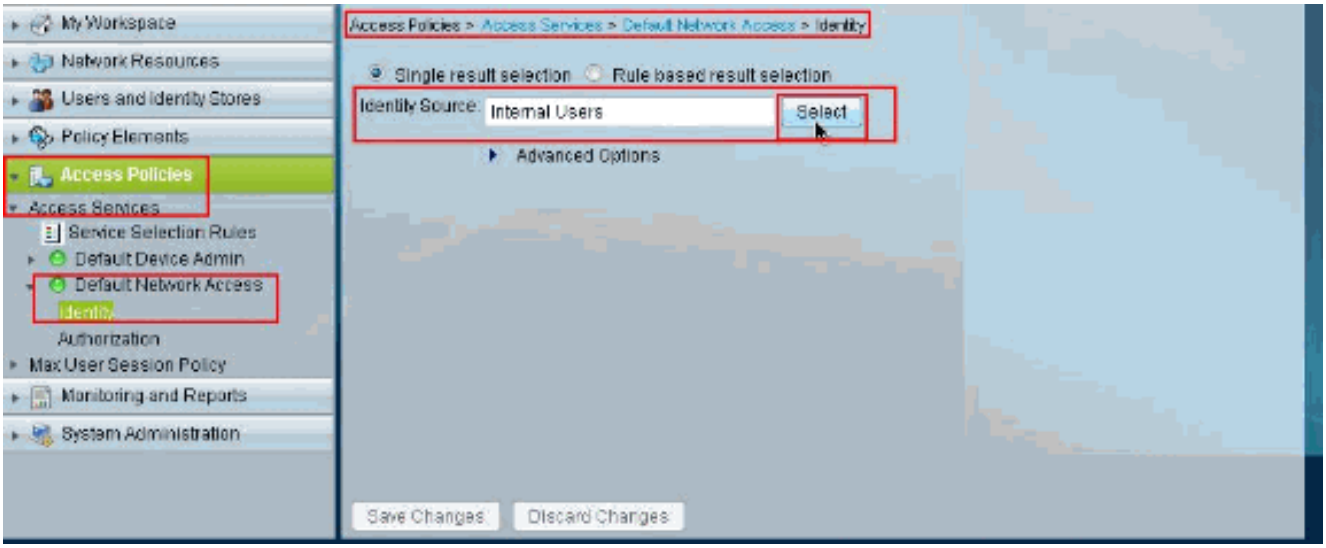
1. 選擇**Access Policies > Access Services > Service Selection Rules**，並驗證哪個服務將使用Secure LDAP伺服器進行身份驗證。在本示例中，該服務是**Default Network Access**。



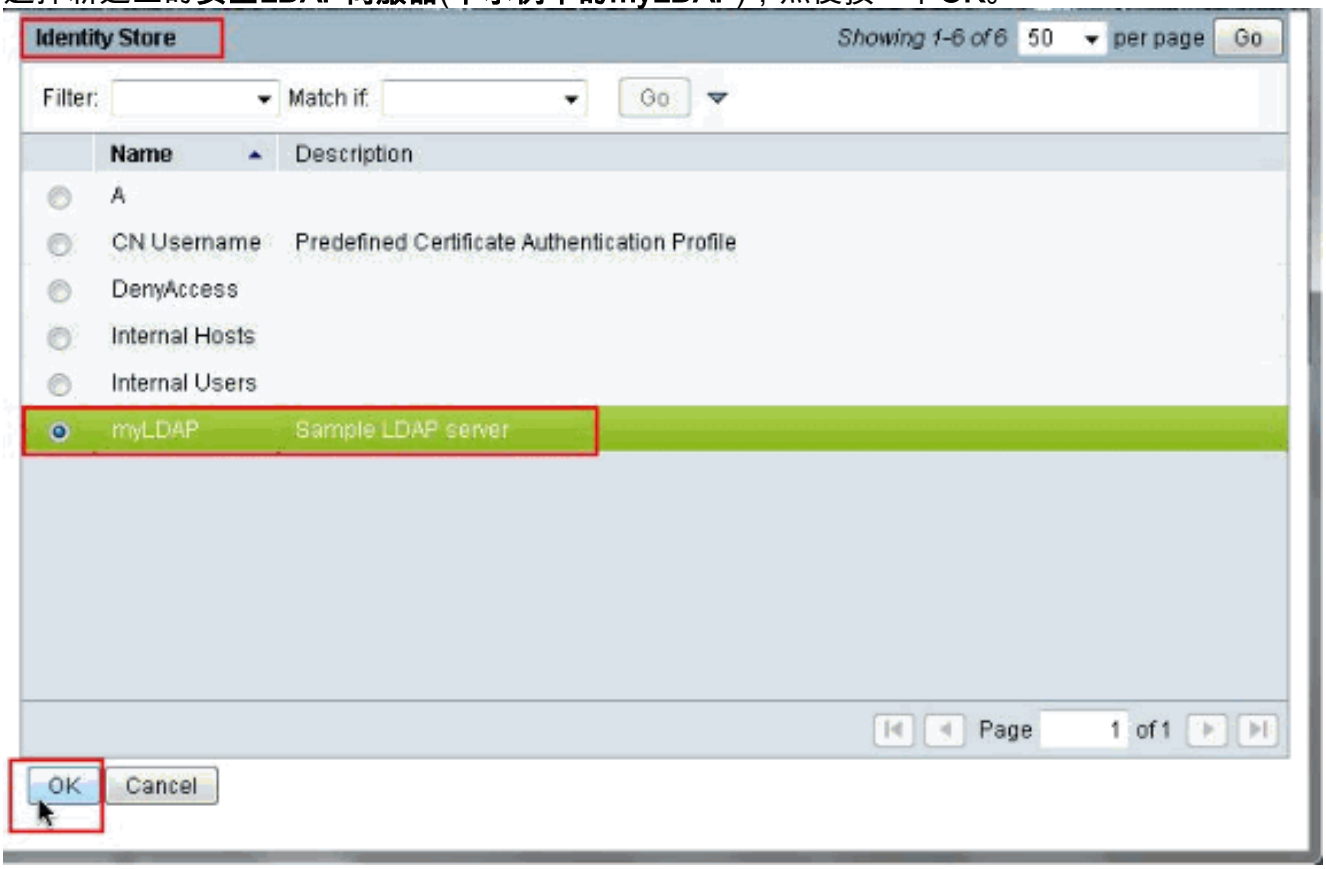
2. 在步驟1中驗證該服務後，請轉至該特定服務，然後按一下**Allowed Protocols**。確保選中**Allow PAP/ASCII**，然後按一下**Submit**。**注意**：可以使用Allow PAP/ASCII選擇其他身份驗證協定。



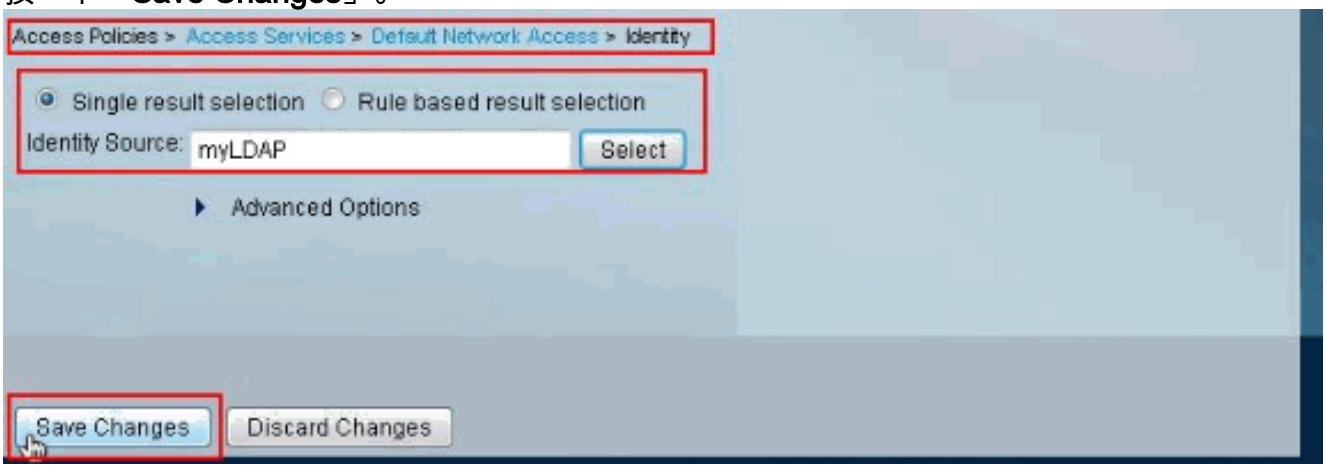
3. 按一下步驟1中標識的服務，然後按一下**Identity**。按一下**Identity Source**旁邊的**Select**。



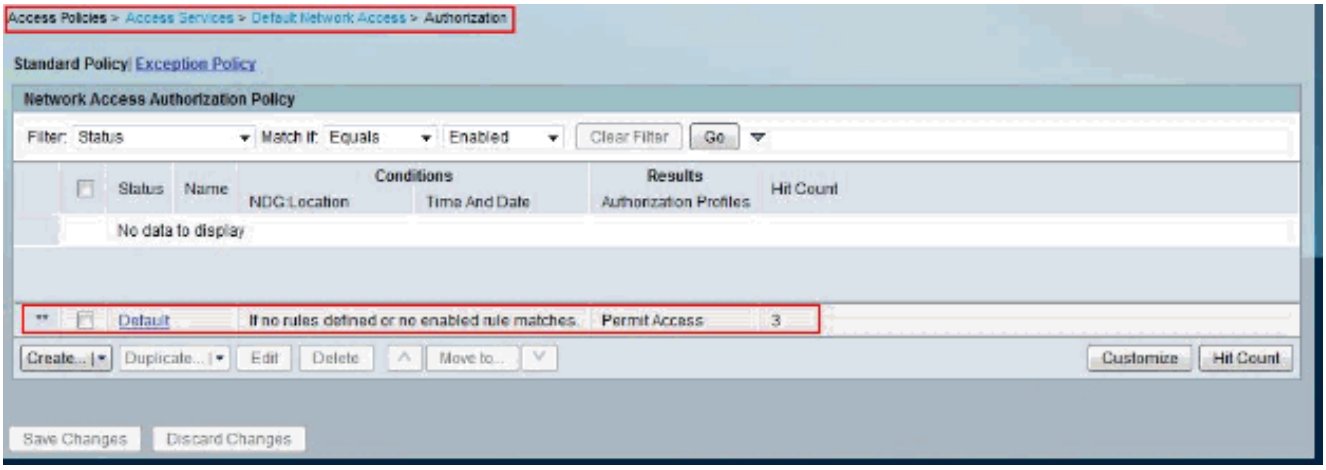
4. 選擇新建立的**安全LDAP伺服器(本示例中的myLDAP)**，然後按一下**OK**。



5. 按一下「**Save Changes**」。



6. 轉到**步驟1**中識別的服務的**Authorization**部分，並確保至少有一個規則允許**Authentication**。



疑難排解

ACS傳送繫結請求，以根據LDAP伺服器對使用者進行身份驗證。繫結請求以明文形式包含使用者的DN和使用者密碼。當使用者的DN和密碼與LDAP目錄中的使用者名稱和密碼匹配時，即對使用者進行身份驗證。

- **驗證錯誤**— ACS在ACS日誌檔案中記錄驗證錯誤。
- **初始化錯誤** — 使用LDAP伺服器超時設定配置ACS在確定LDAP伺服器上的連線或身份驗證失敗之前等待來自LDAP伺服器的響應的秒數。LDAP伺服器返回初始化錯誤的可能原因如下：不支援LDAP伺服器已關閉伺服器記憶體不足使用者沒有許可權配置的管理員憑據不正確
- **繫結錯誤**— LDAP伺服器返回繫結（身份驗證）錯誤的可能原因如下：篩選錯誤使用篩選條件的搜尋失敗引數錯誤輸入的引數無效使用者帳戶受到限制（禁用、鎖定、過期、密碼過期等）

這些錯誤被記錄為外部資源錯誤，這表明LDAP伺服器可能存在問題：

- 發生連線錯誤
- 超時已過期
- 伺服器已關閉
- 伺服器記憶體不足

此錯誤記錄為「未知使用者」錯誤：。

此錯誤記錄為「無效密碼」錯誤，其中使用者存在，但傳送的密碼無效：。

相關資訊

- 思科安全存取控制系統
- 要求建議 (RFC)
- 技術支援與文件 - Cisco Systems