在Expressway上為Web、API和CLI訪問配置LDAP

目錄

簡介

本文檔介紹在Expressway伺服器上啟用輕量級目錄訪問協定(LDAP)所需的步驟，以及如何使管理員組能夠通過Web、應用程式程式設計介面(API)和命令列介面(CLI)與您的域使用者一起訪問Expressway。

作者：Jefferson Madriz和Elias Sevilla，思科TAC工程師。

必要條件

需求

- Expressway基礎知識。
- Expressway基本配置已完成。
- 已配置Active Directory(AD)。
- 防火牆規則已準備就緒，允許Expressway和AD伺服器之間的通訊。

採用元件

- Windows Server 2016上安裝了Active Directory。
- X14.0.3版上的Expressway-C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

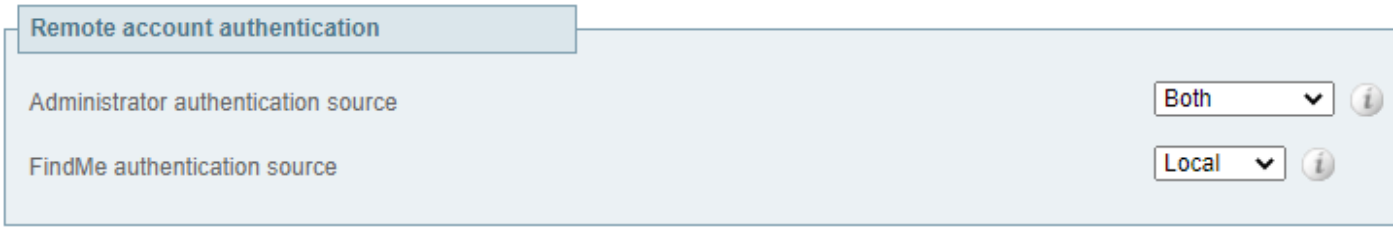
）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

LDAP配置

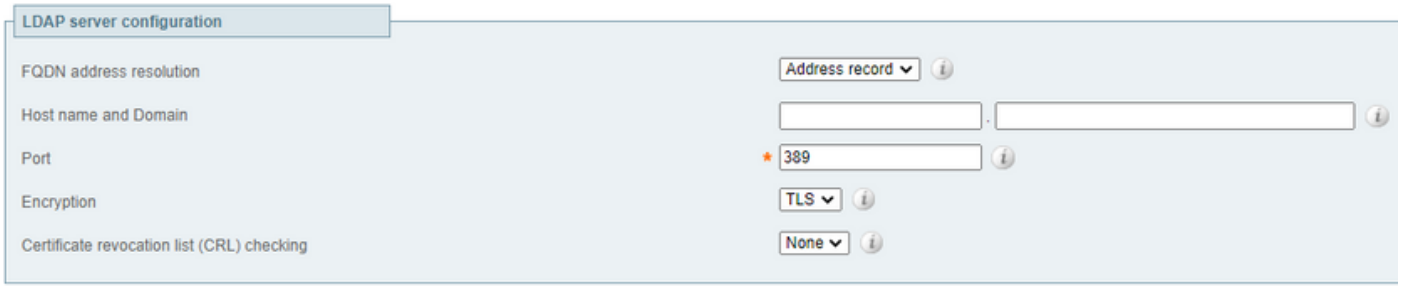
LDAP配置頁面Users > LDAP configuration用於配置到遠端目錄服務的LDAP連線以進行管理員帳戶身份驗證。

- 遠端帳戶身份驗證：本節允許您啟用或禁用使用LDAP進行遠端帳戶身份驗證。



- 僅本地：對儲存在系統中的本地資料庫驗證憑據。
- 僅遠端：憑證會根據外部憑證目錄進行驗證。
- Both:首先根據儲存在系統中的本地資料庫驗證憑據，然後如果帳戶沒有匹配項，則使用外部憑據目錄。

- LDAP伺服器配置：此部分指定到LDAP伺服器的連線詳細資訊。



FQDN地址解析：

- SRV記錄：域名服務(DNS)服務記錄(SRV)查詢。
- 地址記錄：DNS A或AAAA記錄查詢。
- IP 位址:直接輸入為IP地址。

附註：如果使用SRV記錄，請確保_ldap._tcp。記錄使用標準LDAP埠389。Expressway不支援LDAP的其他埠號。

主機名和域：

- SRV記錄：僅需要伺服器地址的域部分。
- 地址記錄：輸入主機名和域。然後，將這些地址組合起來，為DNS地址記錄查詢提供完整的伺服器地址。
- IP 位址:伺服器地址直接作為IP地址輸入。

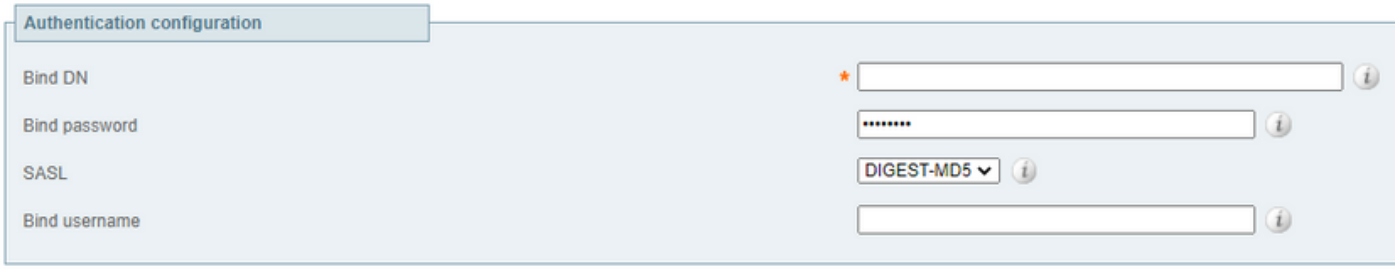
連接埠：

- LDAP伺服器上使用的IP埠。

加密:

- TLS:對與LDAP伺服器的連線使用傳輸層安全(TLS)加密。
- Off:未使用加密。

- 驗證組態:本節指定要用於繫結到LDAP伺服器的Expressway身份驗證憑據。



繫結DN:Expressway用於繫結到LDAP伺服器的區分名稱(DN)（不區分大小寫）。必須按照cn=、ou=、dc=的順序指定DN

附註：繫結帳戶通常是沒有特權的只讀帳戶。

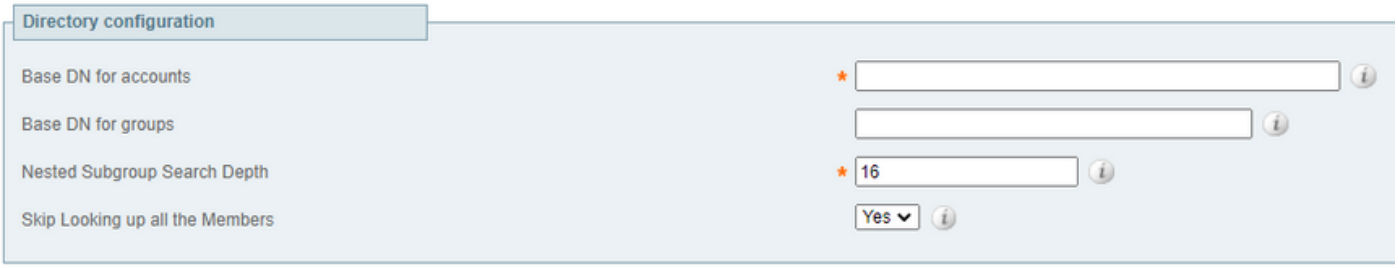
繫結密碼：Expressway用於繫結到LDAP伺服器的密碼（區分大小寫）。

SASL:用於繫結到LDAP伺服器的簡單身份驗證和安全層(SASL)機制

- 無:未使用任何機制。
- DIGEST-MD5:使用DIGEST-MD5機制。

繫結使用者名稱：Expressway用於登入到LDAP伺服器的帳戶的使用者名稱（區分大小寫）。

- 目錄配置：本節指定用於搜尋帳戶和組名稱的基本可分辨名稱。



帳戶的基本DN：組織單位(OU)和域控制器(DC)定義，其中搜尋使用者帳戶以資料庫結構開始（不區分大小寫）。

帳戶和組的基本DN必須處於或低於DC級別（如有必要，包括所有dc=值和ou=值）。LDAP身份驗證不檢視子DC帳戶，只檢視較低的OU和公用節點(CN)級別。

組的基本DN:區別名稱的OU和DC定義，其中搜尋組必須以資料庫結構開始（不區分大小寫）。

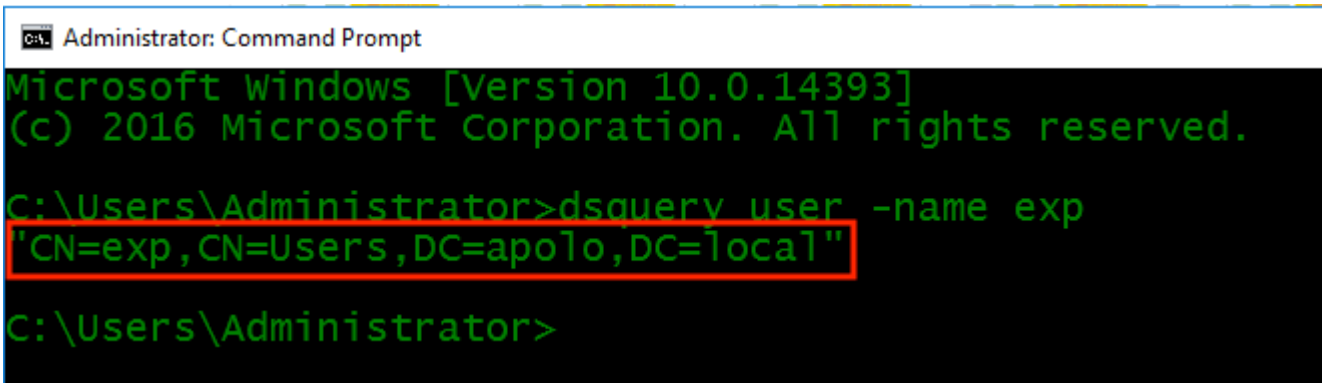
如果未指定組的基礎DN，則帳戶的基礎DN將同時用於組和帳戶。

巢狀子組搜尋深度：用於限制LDAP搜尋的組深度。

跳過查詢所有成員：用於在進行身份驗證搜尋過程時禁用或啟用管理員組的成員查詢。預設值為Yes — 跳過成員查詢。

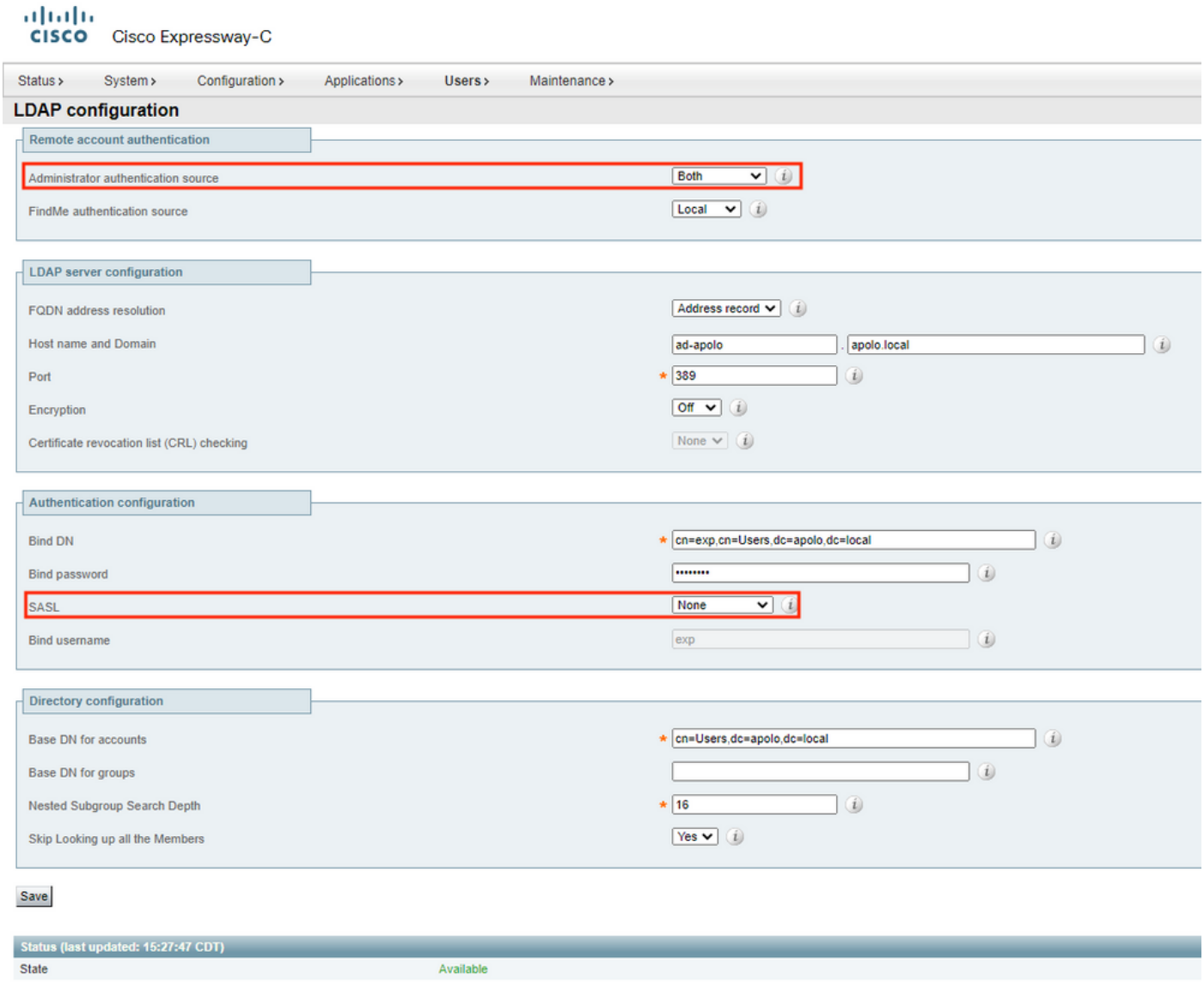
如何查詢基本DN

在AD伺服器上，以管理員身份開啟命令提示符(CMD)並運行命令**dsquery user -name** :。



LDAP配置示例

在本例中，管理員身份驗證源設定為Both,SASL設定為None。



驗證LDAP狀態

驗證LDAP伺服器連線狀態：

- 可使用:未顯示錯誤消息
- 失敗:顯示錯誤消息。LDAP錯誤消息

管理員組配置

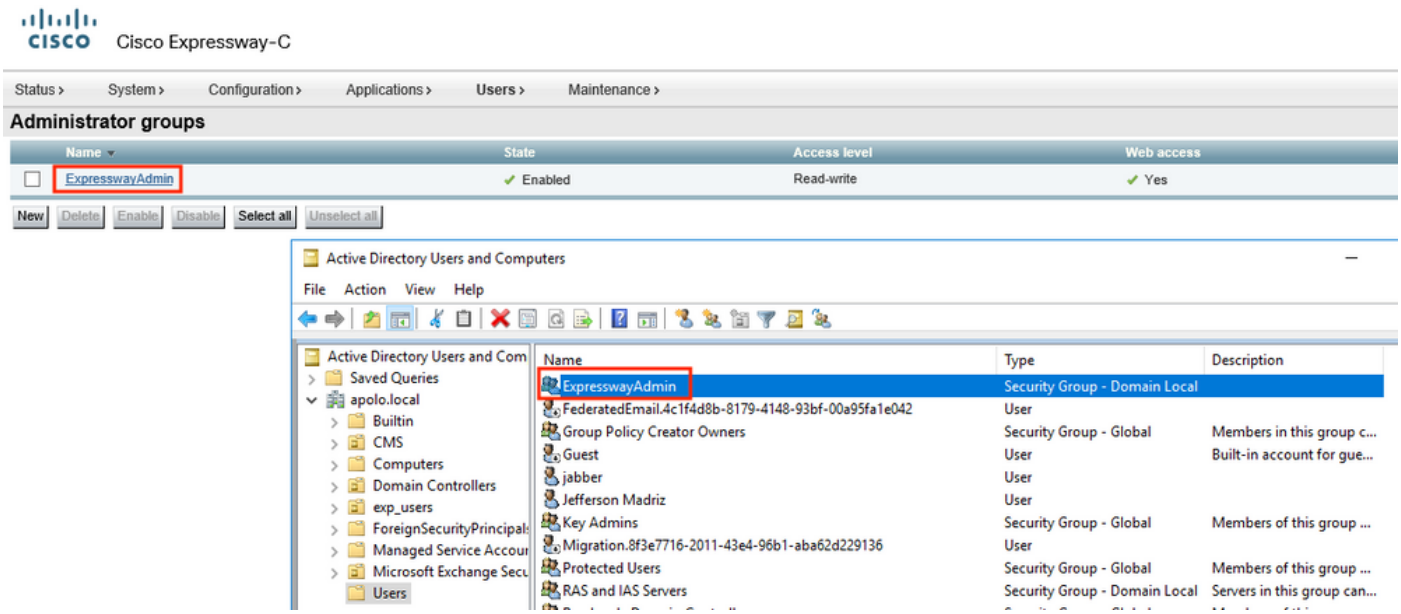
管理員組頁面Users > Administrator groups列出在Expressway上配置的所有管理員組，並允許您新增、編輯和刪除組。

附註：僅當啟用使用LDAP的遠端帳戶身份驗證時，才應用管理員組。

當您登入Expressway Web介面時，您的憑證將根據遠端目錄服務進行身份驗證，並且您被分配與您所屬的組相關聯的訪問許可權。

Expressway上的管理員組配置選項

名稱:管理員組的名稱。在Expressway中定義的組名稱必須與在遠端目錄服務中設定的組名稱相匹配，以便管理對此Expressway的管理員訪問。



訪問級別：

- 讀取/寫入：允許檢視和更改所有配置資訊。這提供了與預設管理員帳戶相同的許可權。
- 唯讀：僅允許檢視和不更改狀態和配置資訊。某些頁面（如Upgrade頁面）被阻止為只讀帳戶。
- 審計員：僅允許訪問「事件日誌」、「配置日誌」、「網路日誌」、「警報」和「概述」頁。
- 無:不允許訪問

Web訪問：確定是否允許此組的成員通過Web介面登入到系統。

API訪問：確定是否允許此組的成員使用API訪問系統的狀態和配置。

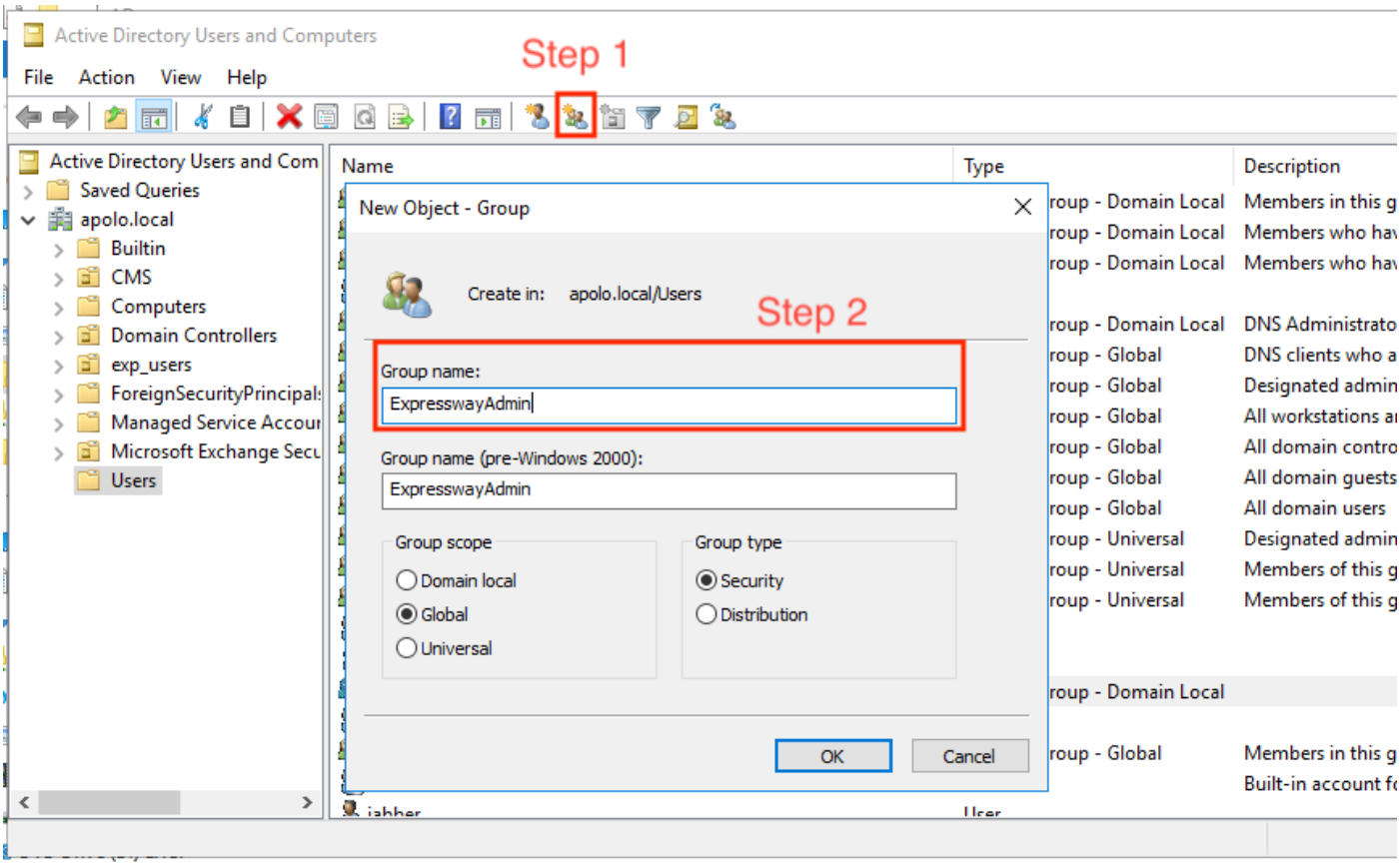
CLI訪問：確定是否允許此組的成員通過CLI訪問系統。

狀態:指示組是處於啟用還是禁用狀態。

AD上的管理員組配置

1.在要儲存使用者的文件夾上建立一個新的對象組。

2.為組名指定名稱。

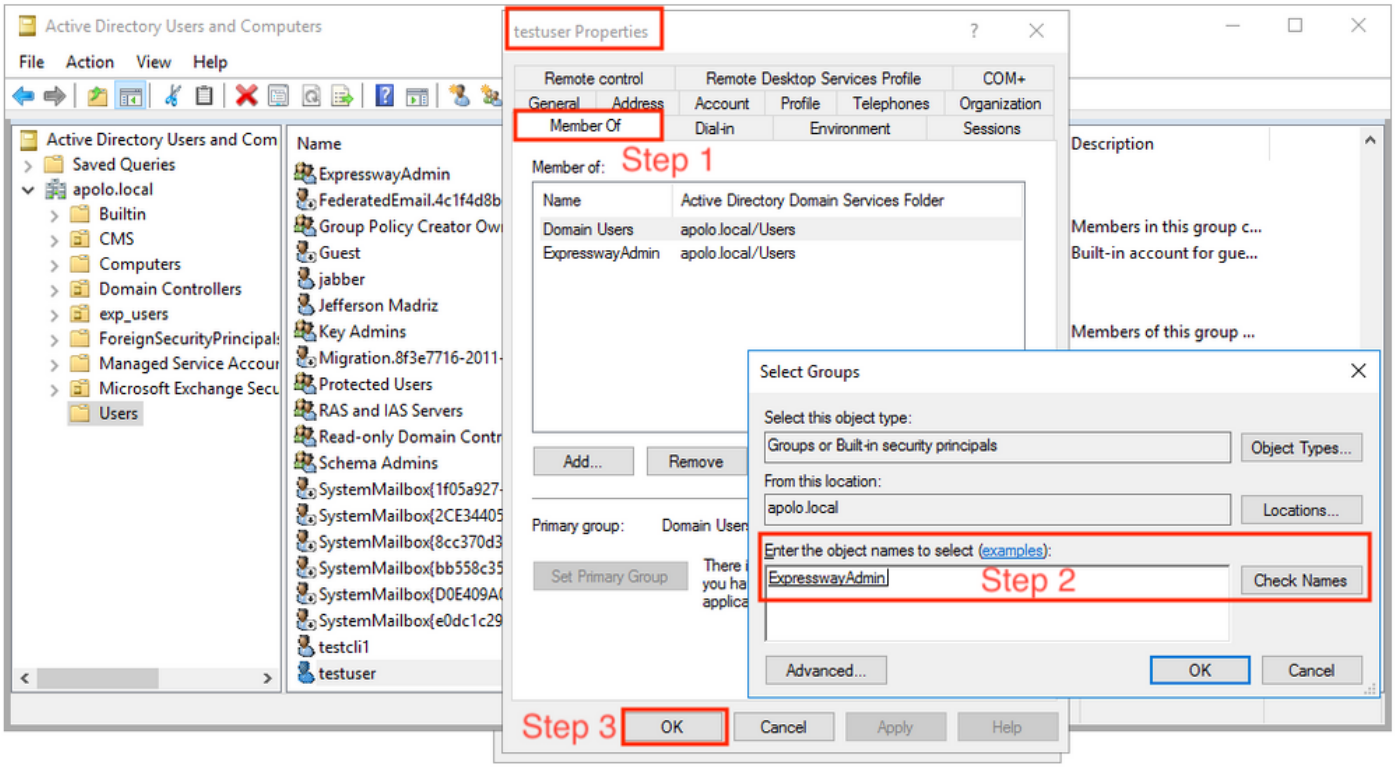


將配置的組分配給需要通過Web、API或CLI訪問Expressway的使用者。在這種情況下，使用者是testuser。

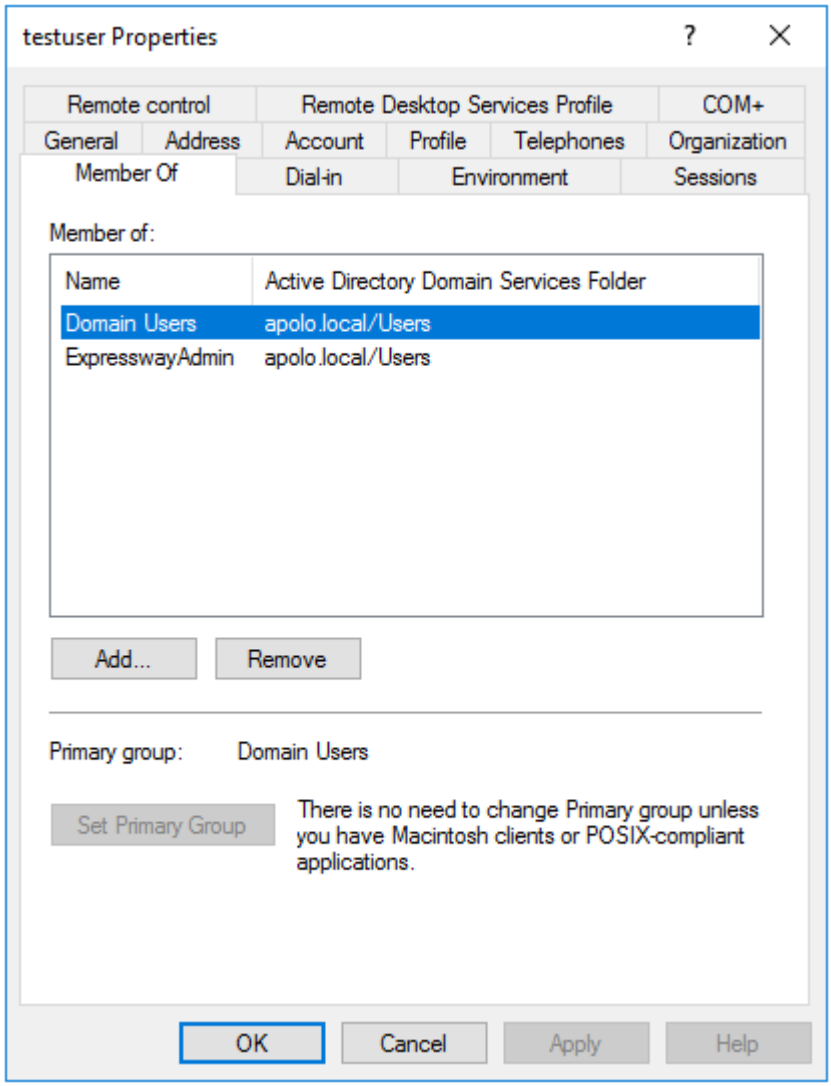
1.開啟使用者屬性，導航到「成員」選項卡，選擇新增

2.搜尋之前創建的組名稱。

3.然後選擇確定。



此時，使用者是Domain Users和ExpresswayAdmin的成員。

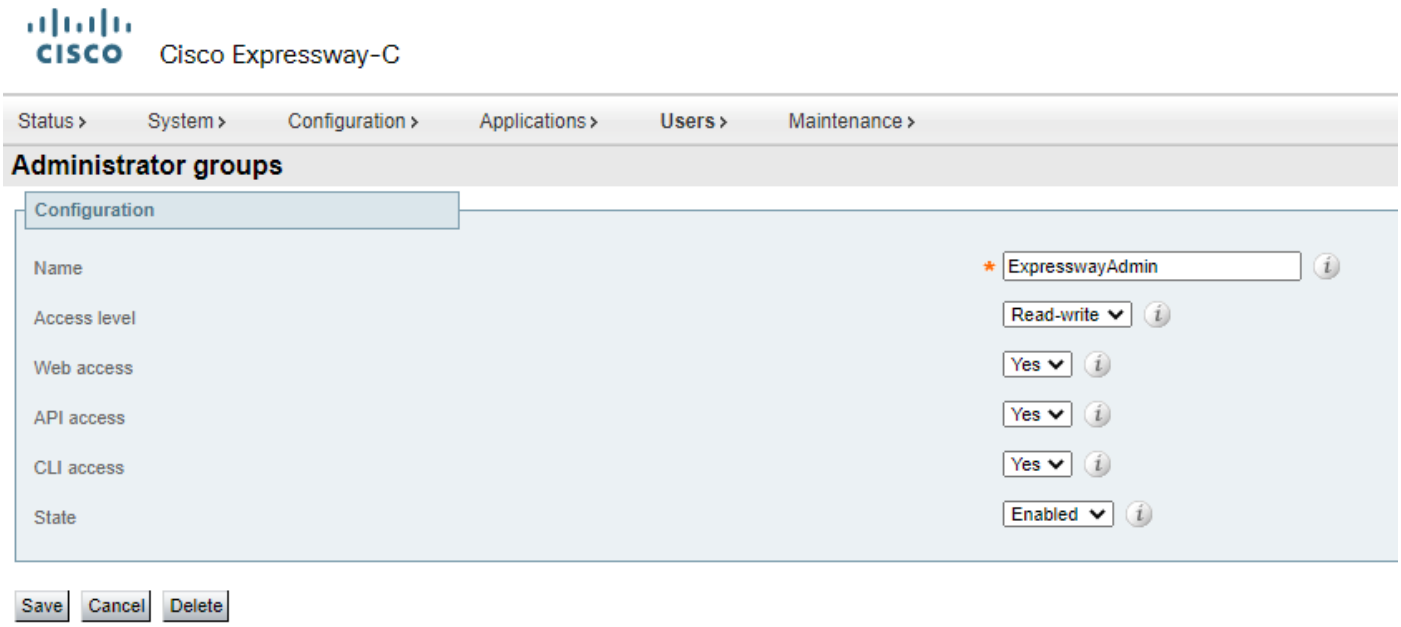


Expressway上的管理員組配置

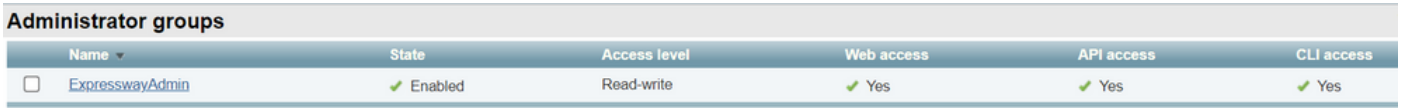
配置完成後，在Expressway上導航到Users > Administrator groups，選擇New

名稱：必須與組名稱配置相匹配，並且與需要訪問Expressway的LDAP使用者相關聯。在本示例中，組名稱為ExpresswayAdmin，因此新的管理員組名稱為ExpresswayAdmin。

此組具有所有可用的許可權和訪問許可權。

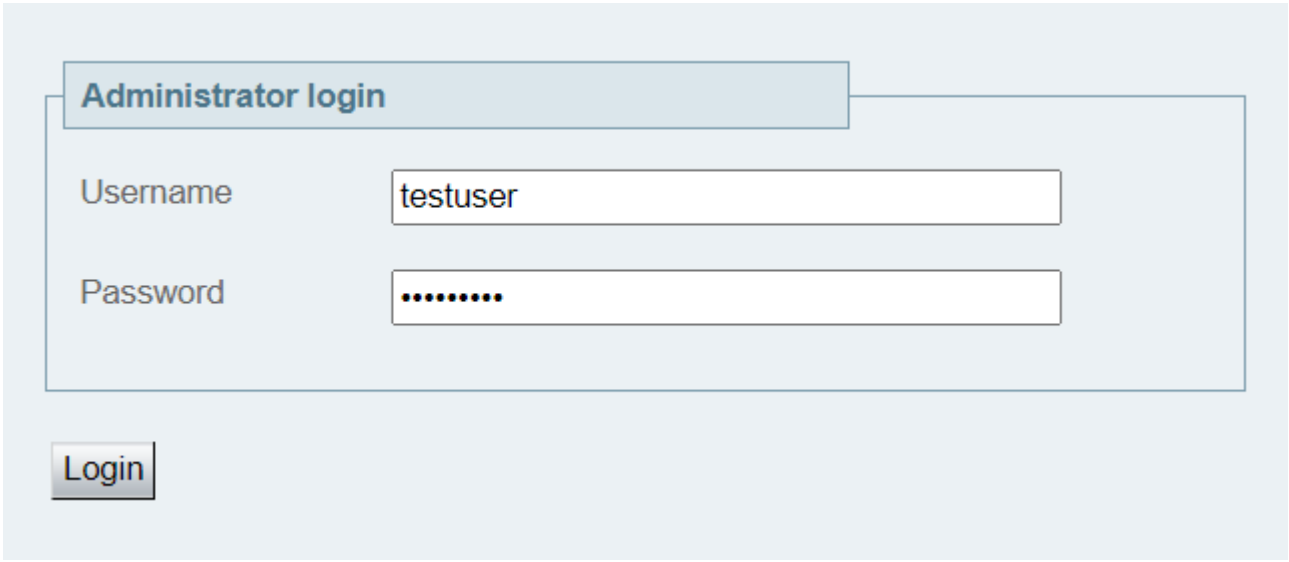


選擇Save。

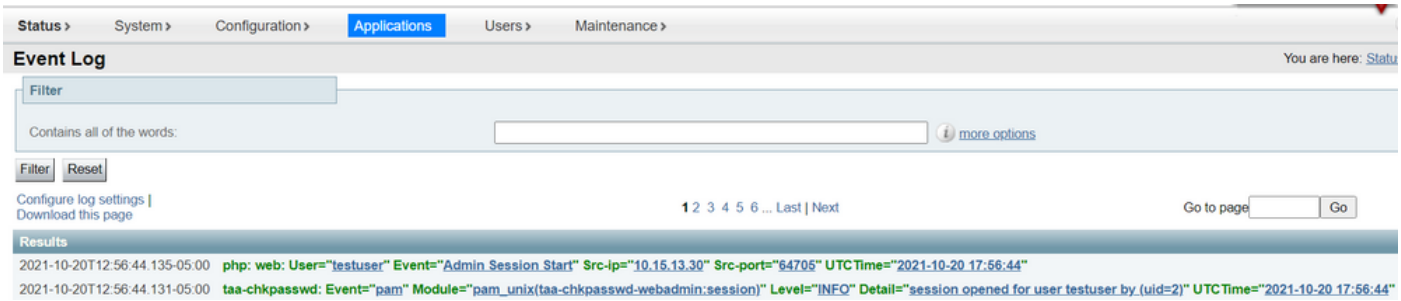


驗證

註銷並嘗試使用與管理員組關聯的LDAP使用者通過Web進行訪問。在本示例中，建立的使用者是testuser。



這可透過Status > Event log確認：



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）。