在Expressway上配置LDAP以进行Web、API和CLI访问

目录

简介

本文档介绍在Expressway服务器上启用轻量级目录访问协议(LDAP)所需的步骤，以及如何使管理员组能够通过Web、应用编程接口(API)和命令行界面(CLI)与域用户访问Expressway。

作者：Jefferson Madriz和Elias Sevilla，Cisco TAC工程师。

先决条件

要求

- Expressway基础知识。
- Expressway基本配置已完成。
- Active Directory(AD)已配置。
- 防火墙规则就绪，允许Expressway和AD服务器之间的通信。

使用的组件

- Windows Server 2016上安装的Active Directory。
- 版本X14.0.3上的Expressway-C服务器。

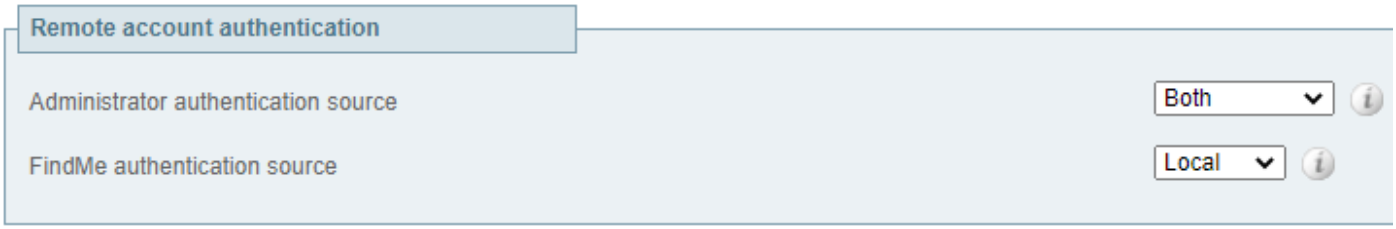
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

LDAP配置

LDAP配置页面Users > LDAP configuration用于配置到远程目录服务的LDAP连接，以进行管理员帐户身份验证。

- 远程帐户身份验证：此部分允许您启用或禁用使用LDAP进行远程帐户身份验证。



-仅限本地:根据系统上存储的本地数据库验证凭证。
— 仅远程：根据外部凭证目录验证凭证。
-两者：首先根据系统上存储的本地数据库验证凭证，如果与帐户不匹配，则使用外部凭证目录。

- LDAP服务器配置：此部分指定到LDAP服务器的连接详细信息。

FQDN地址解析：

- SRV记录：域名服务(DNS)服务记录(SRV)查找。
- 地址记录：DNS A或AAAA记录查找。
- IP 地址：直接输入为IP地址。

注意：如果使用SRV记录，请确保_ldap._tcp。记录使用标准LDAP端口389。Expressway不支持LDAP的其他端口号。

主机名和域：

- SRV 记录:仅需要服务器地址的域部分。
- 地址记录：输入主机名和域。然后，将这些地址组合起来，为DNS地址记录查找提供完整的服务器地址。
- IP 地址：服务器地址直接作为IP地址输入。

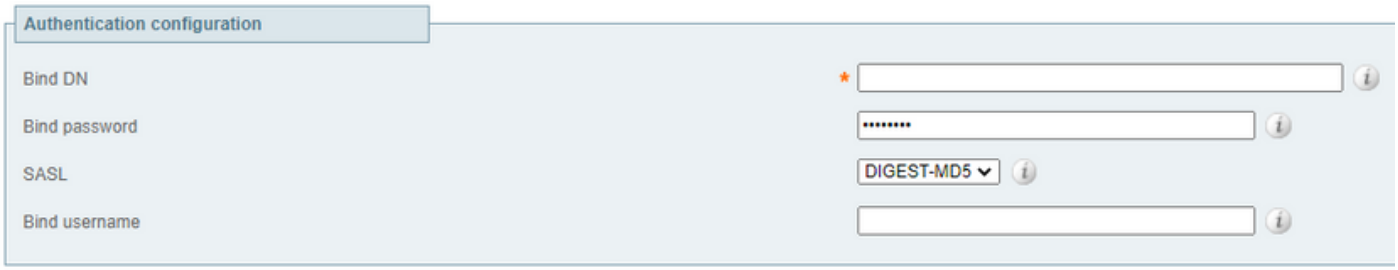
端口：

- LDAP服务器上使用的IP端口。

加密：

- TLS:对与LDAP服务器的连接使用传输层安全(TLS)加密。
- 关闭:未使用加密。

- 身份验证配置：本节指定用于绑定到LDAP服务器的Expressway身份验证凭证。



绑定DN:Expressway用于绑定到LDAP服务器的可分辨名称(DN)（不区分大小写）。必须按照cn=、ou=、dc=的顺序指定DN

注意：绑定帐户通常是没有特权的只读帐户。

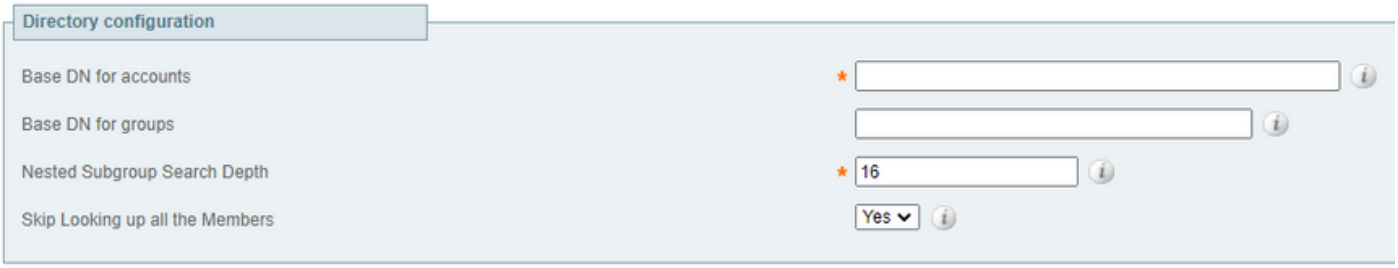
绑定密码：Expressway用于绑定到LDAP服务器的密码（区分大小写）。

SASL:用于绑定到LDAP服务器的简单身份验证和安全层(SASL)机制

- 无:未使用任何机制。
- DIGEST-MD5:使用DIGEST-MD5机制。

绑定用户名：Expressway用于登录到LDAP服务器的帐户的用户名（区分大小写）。

- 目录配置:本节指定用于搜索帐户和组名称的基本可分辨名称。



帐户的基本DN：可分辨名称的组织单位(OU)和域控制器(DC)定义，其中搜索用户帐户以数据库结构开始（不区分大小写）。

帐户和组的基础DN必须处于或低于DC级别（如有必要，包括所有dc=值和ou=值）。LDAP身份验证不检查子DC帐户，只检查较低的OU和公用名称(CN)级别。

组的基本DN:可分辨名称的OU和DC定义，其中必须在数据库结构中开始搜索组（不区分大小写）。

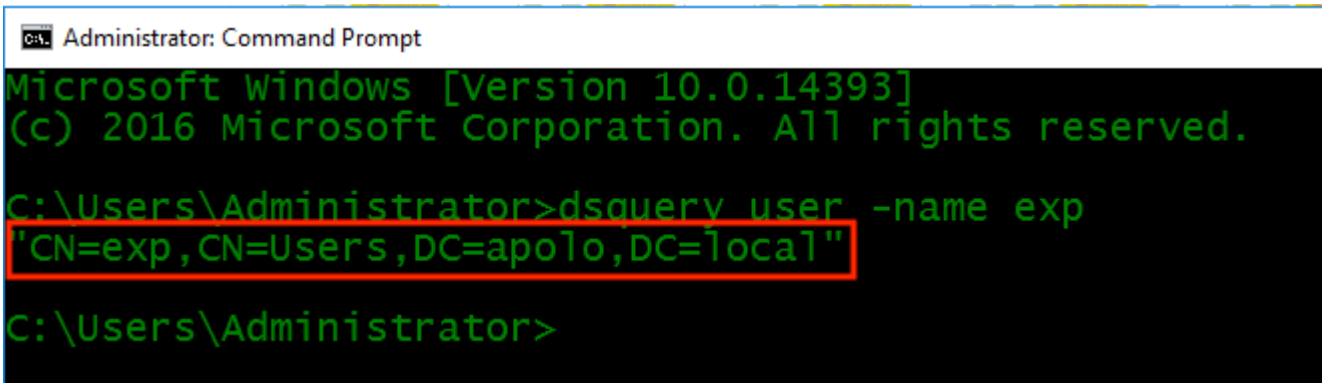
如果未指定组的基础DN，则帐户的基础DN用于组和帐户。

嵌套子组搜索深度：用于限制LDAP搜索的组深度。

跳过查找所有成员：用于在进行身份验证搜索过程时禁用或启用管理员组的成员查找。默认值为Yes — 跳过成员查找。

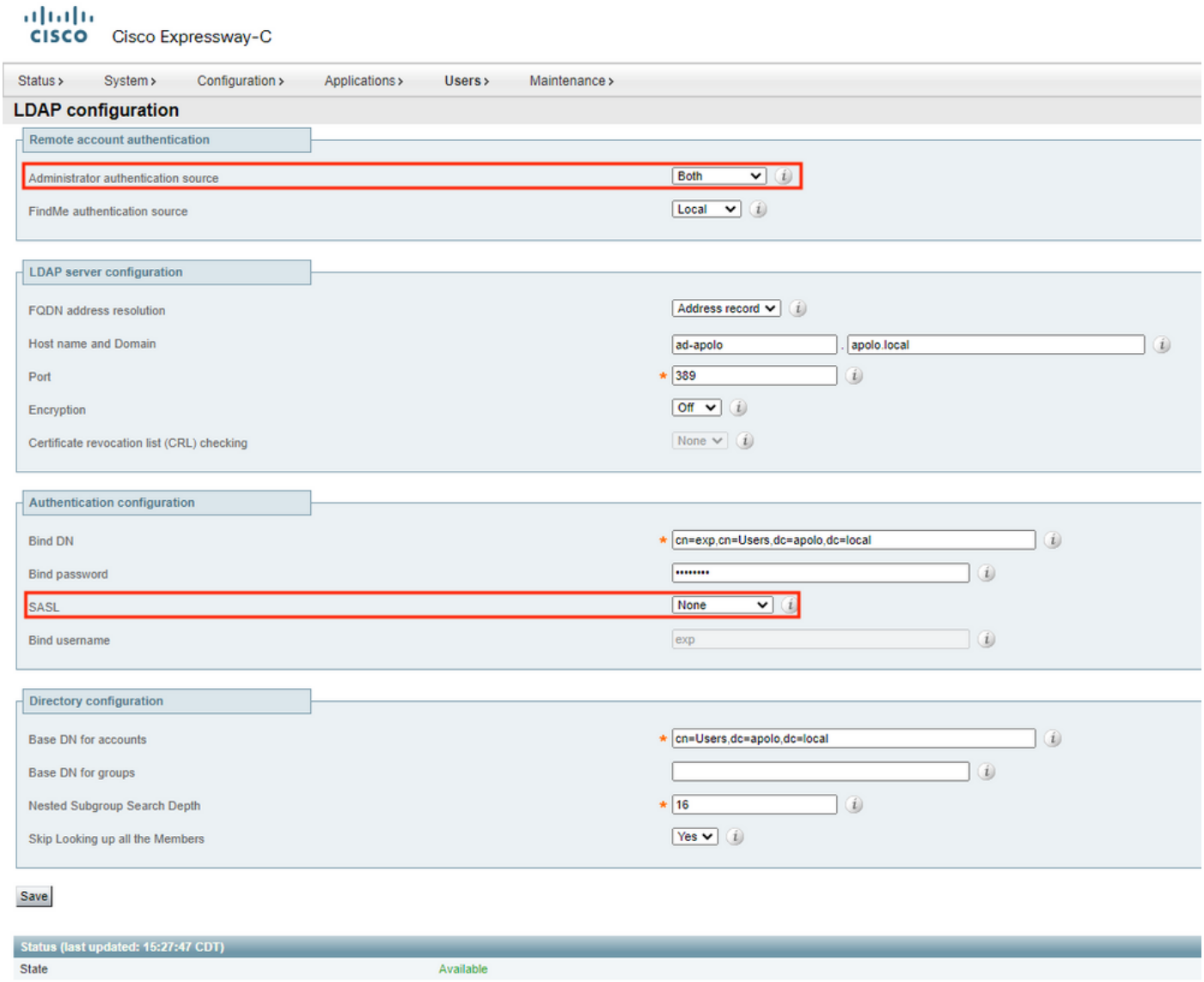
如何查找基础DN

在AD服务器上，以管理员身份打开命令提示符(CMD)并运行命令**dsquery user -name** :。



LDAP配置示例

在本例中，管理员身份验证源设置为Both,SASL设置为None。



验证LDAP状态

验证LDAP服务器连接状态：

- 线上:未显示错误消息
- 失败:显示错误消息。LDAP错误消息

管理员组配置

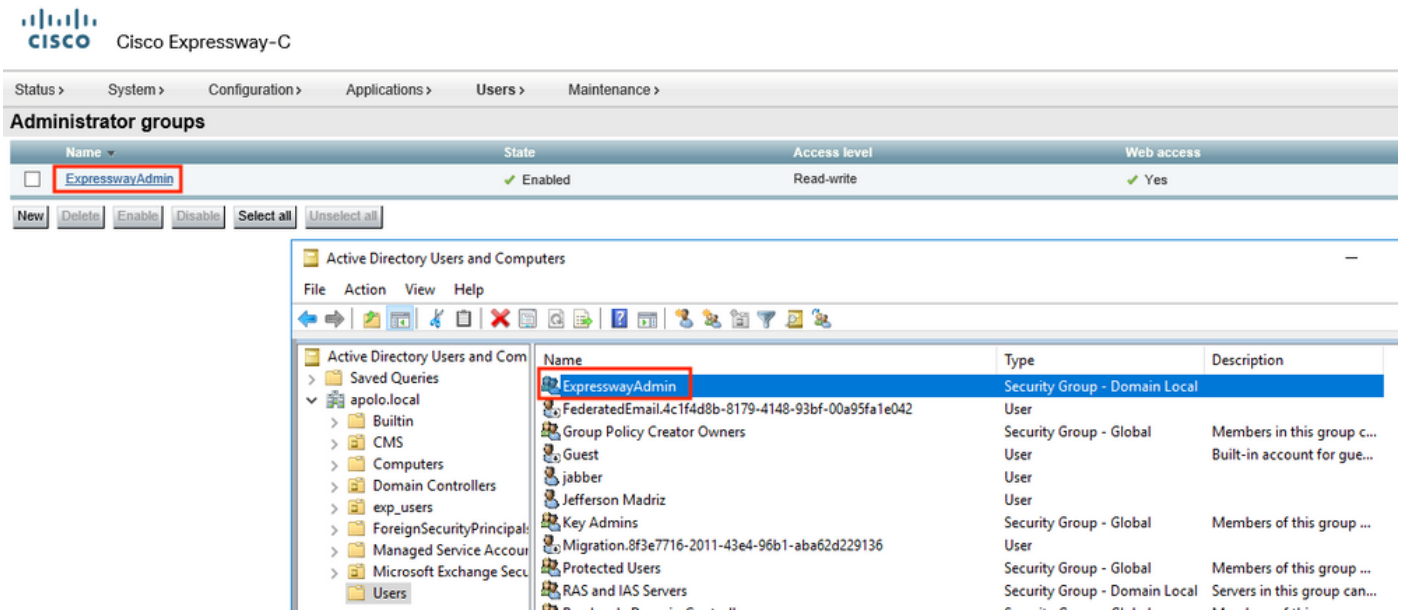
管理员组页面Users > Administrator groups列出在Expressway上配置的所有管理员组，并允许您添加、编辑和删除组。

注意：仅当启用使用LDAP的远程帐户身份验证时，管理员组才适用。

当您登录Expressway Web界面时，系统会根据远程目录服务对您的凭证进行身份验证，并且会为您分配与您所属的组相关联的访问权限。

Expressway上的管理员组配置选项

名称：管理员组的名称。在Expressway中定义的组名称必须与在远程目录服务中设置的组名称匹配，以便管理对此Expressway的管理员访问。



访问级别:

- 读写：允许查看和更改所有配置信息。这提供了与默认管理员帐户相同的权限。
- 只读：仅允许查看和不更改状态和配置信息。某些页面（如Upgrade页面）被阻止为只读帐户。
- 审计员：仅允许访问“事件日志”(Event Log)、“配置日志”(Configuration Log)、“网络日志”(Network Log)、“警报”(Alarms)和“概述”(Overview)页面。
- 无:不允许访问

Web 访问:确定是否允许此组的成员通过Web界面登录到系统。

API访问：确定是否允许此组的成员使用API访问系统的状态和配置。

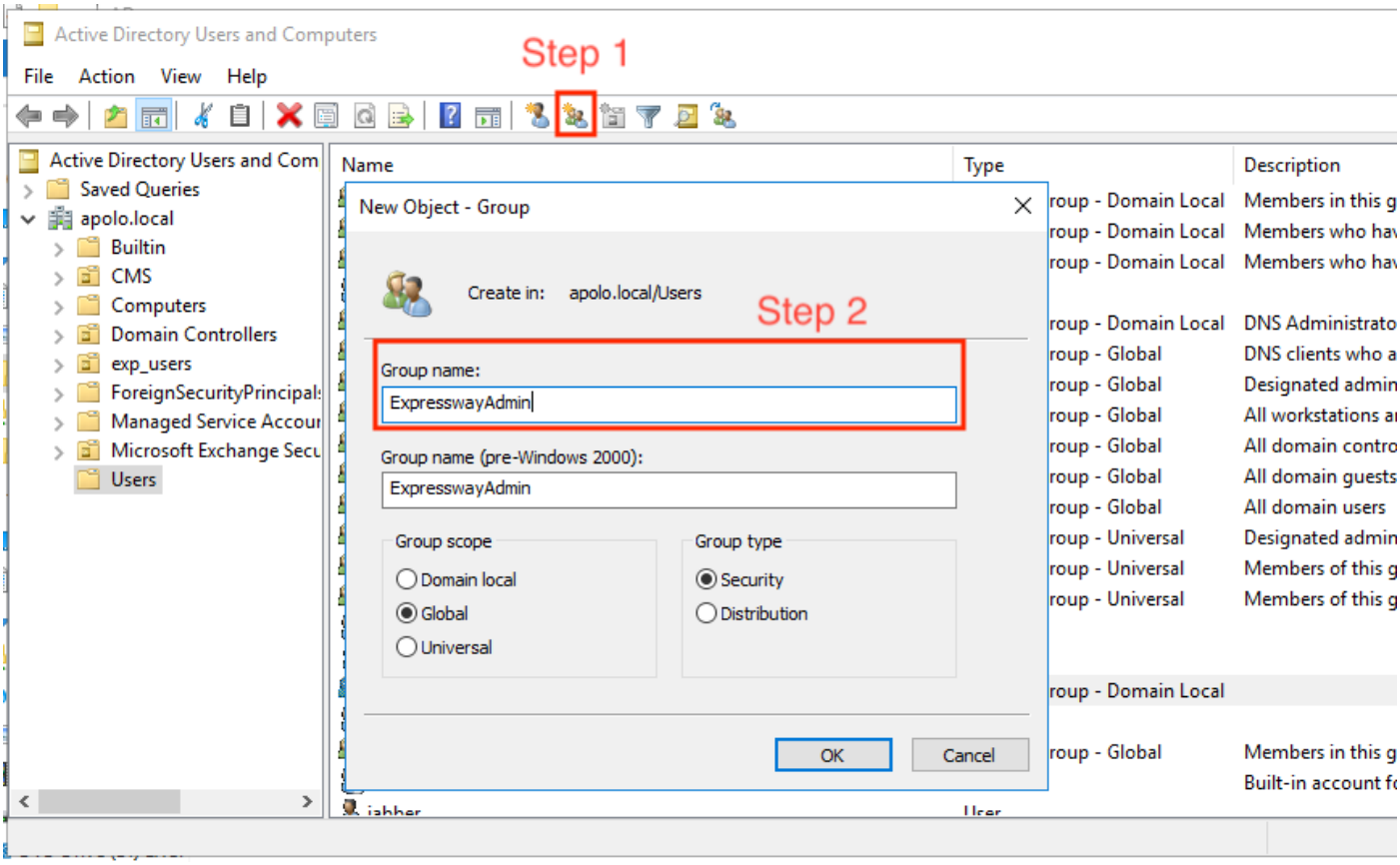
CLI访问：确定是否允许此组的成员通过CLI访问系统。

状态:指示组是处于启用状态还是禁用状态。

AD上的管理员组配置

1.在要存储用户的文件夹上创建一个新的对象组。

2.为组名指定名称。

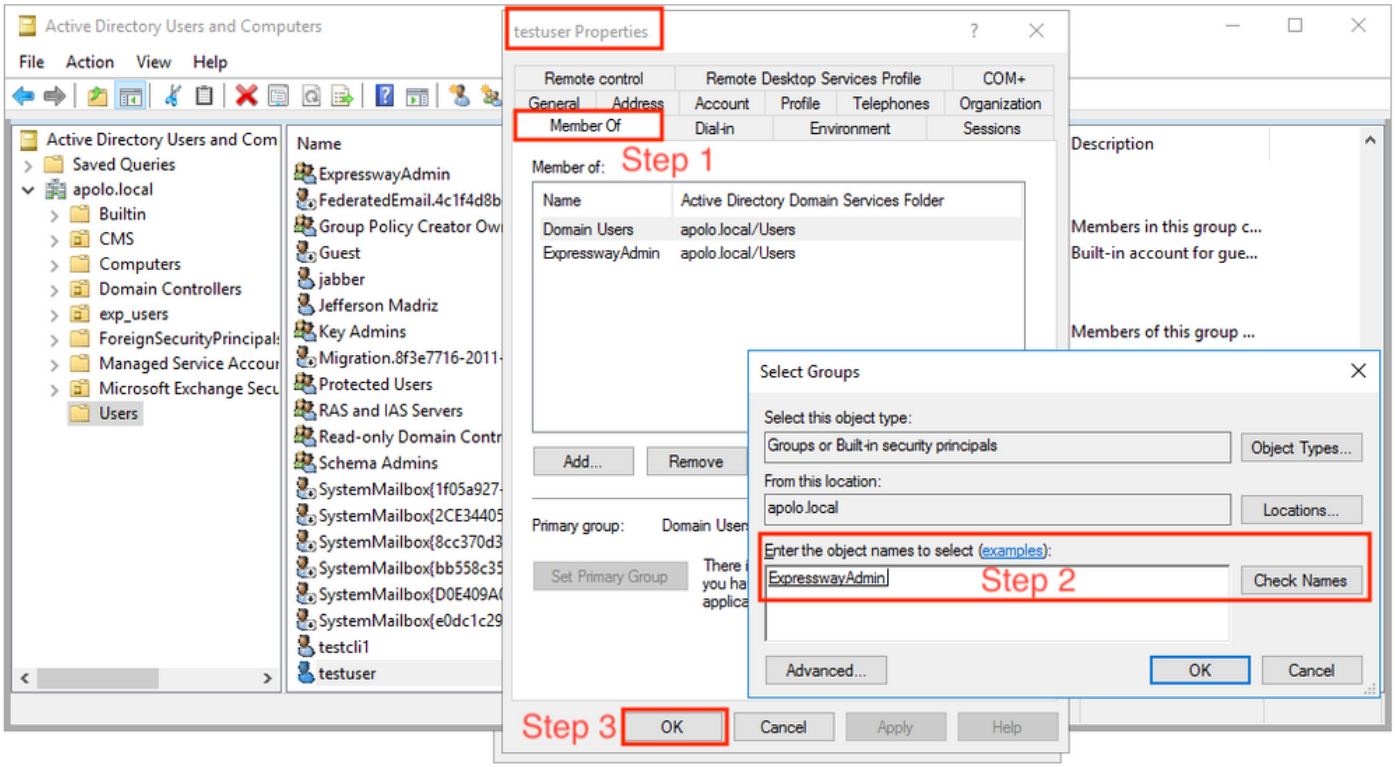


将配置的组分配给需要通过Web、API或CLI访问Expressway的用户。在本例中，用户是testuser。

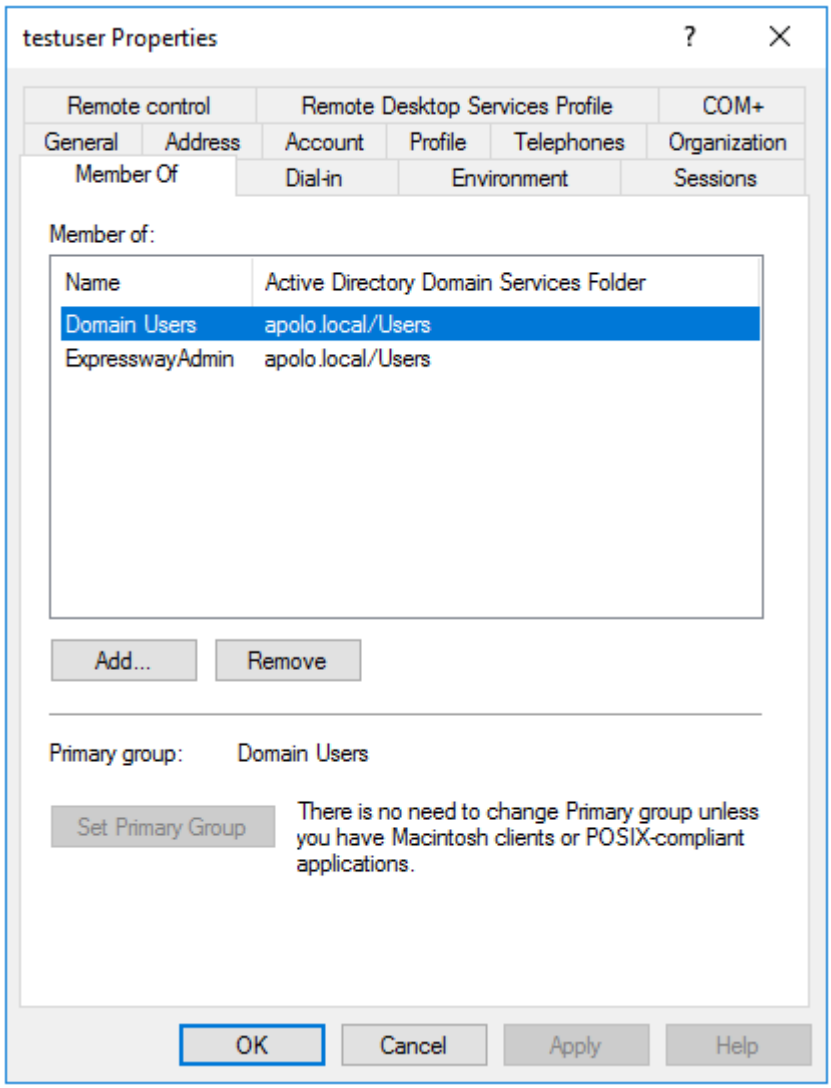
1.打开用户属性，定位至“成员”选项卡，选择添加

2.搜索之前创建的组名称。

3.然后选择确定。



此时，用户是Domain Users和ExpresswayAdmin的成员。

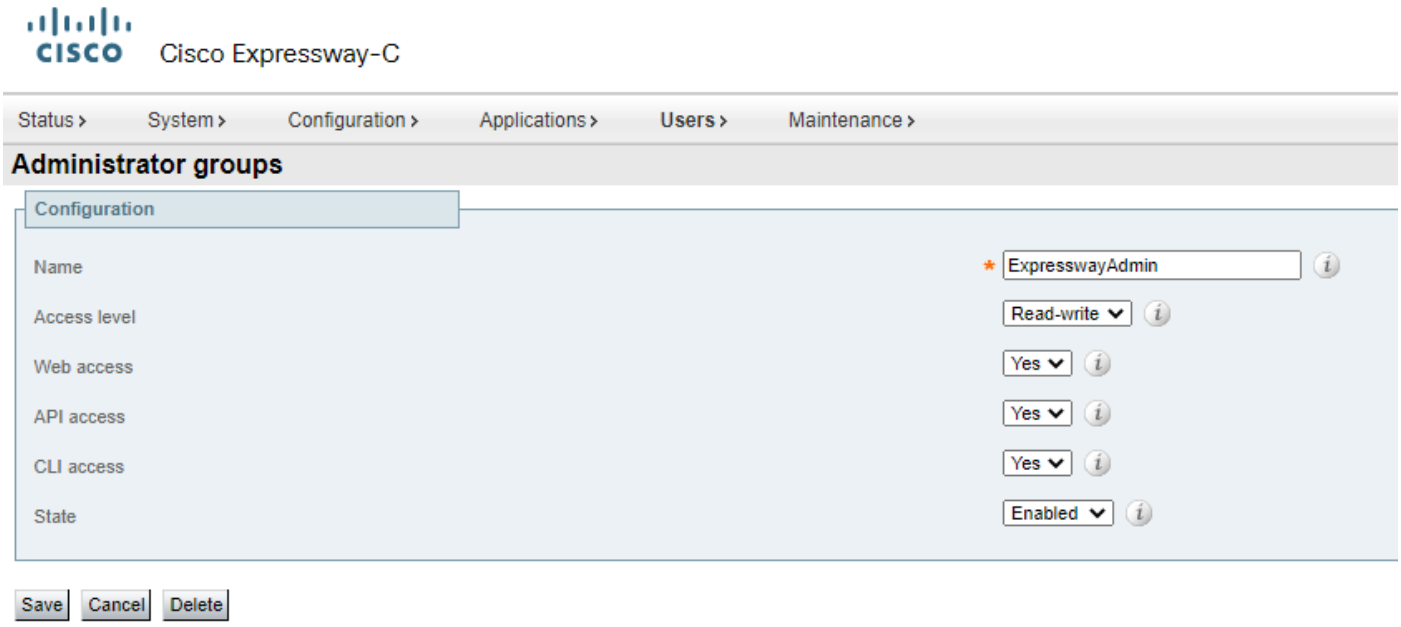


Expressway上的管理员组配置

完成配置后，在Expressway上导航到Users > Administrator groups，选择New

Name：必须与组名配置相匹配，并且与需要访问Expressway的LDAP用户相关联。在本示例中，组名称为ExpresswayAdmin，因此新的管理员组名称为ExpresswayAdmin。

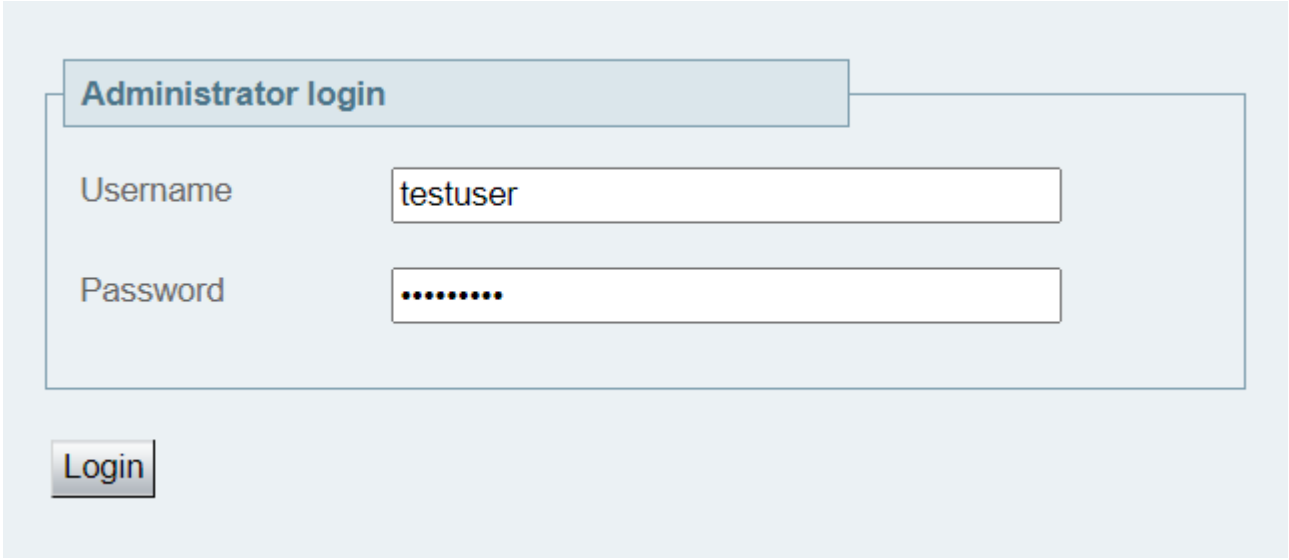
此组具有所有可用的权限和访问权限。



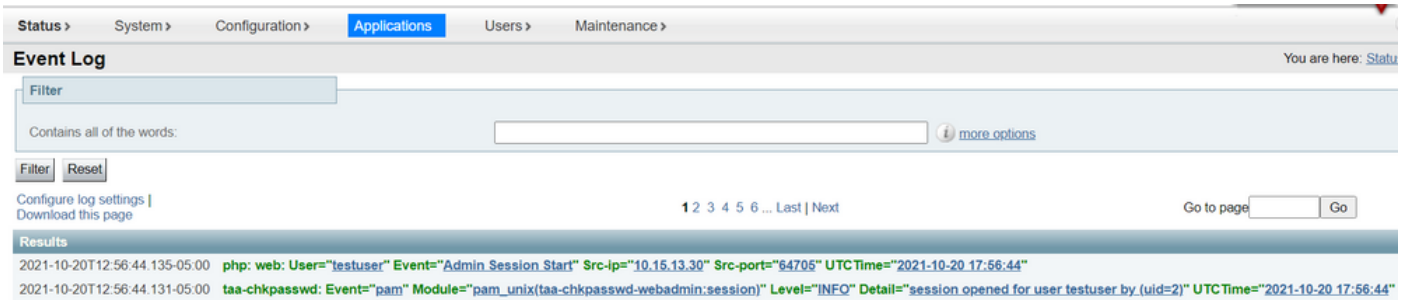
选择Save。

验证

注销并尝试使用与管理员组关联的LDAP用户通过Web进行访问。在本示例中，创建的用户是testuser。



这可以通过Status > Event log进行确认：


Status › System › Configuration › Applications Users › Maintenance ›
Event Log
You are here: Statu
Filter
Contains all of the words:
more options
Filter Reset
Configure log settings |
Download this page
1 2 3 4 5 6 ... Last | Next
Go to page Go
Results
2021-10-20T12:56:44.135-05:00 php: web: User="testuser" Event="Admin Session Start" Src-ip="10.15.13.30" Src-port="64705" UTCTime="2021-10-20 17:56:44"
2021-10-20T12:56:44.131-05:00 taa-chkpasswd: Event="pam" Module="pam_unix(taa-chkpasswd-webadmin:session)" Level="INFO" Detail="session opened for user testuser by (uid=2)" UTCTime="2021-10-20 17:56:44"

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）。