在无线局域网控制器(WLCs)上使用LDAP的Web认证配置示例

目录

简介

本文档介绍如何设置无线局域网控制器(WLC)进行Web身份验证。它说明如何将轻量级目录访问协议(LDAP)服务器配置为用于网络身份验证的后端数据库，以检索用户凭证并对用户进行身份验证。

先决条件

要求

Cisco 建议您了解以下主题：

- 了解轻量接入点 (LAP) 和 Cisco WLC 的配置

- 无线接入点协议(CAPWAP)控制和调配知识
- 了解如何设置和配置轻量级目录访问协议(LDAP)、Active Directory和域控制器

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行固件版本 8.2.100.0 的 Cisco 5508 WLC
- Cisco 1142 系列 LAP
- 思科802.11a/b/g无线客户端适配器。
- 执行LDAP服务器角色的Microsoft Windows 2012 Essentials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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

规则

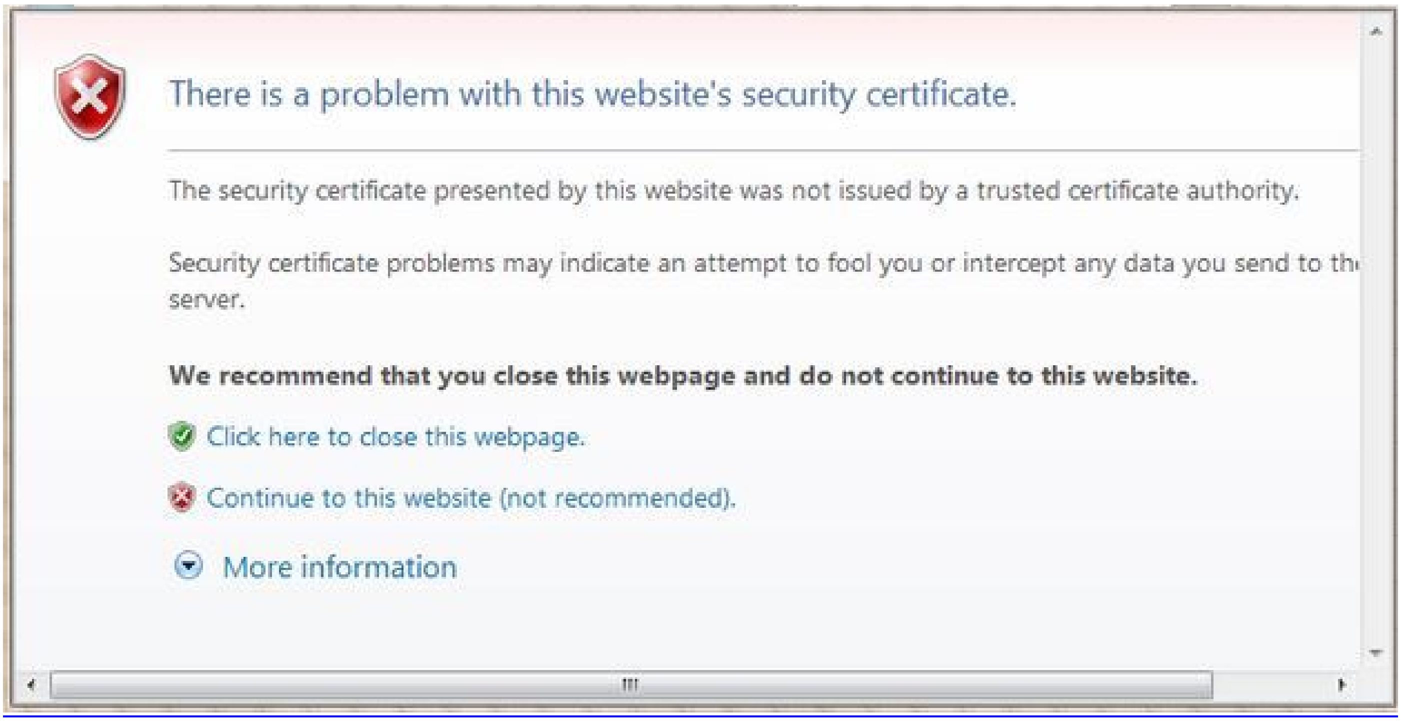
有关文档约定的更多信息，请参考 Cisco 技术提示约定。

Web 身份认证过程

Web身份验证是第3层安全功能，它会导致控制器禁止来自特定客户端的IP流量（DHCP和DNS相关数据包除外），直到该客户端正确提供了有效的用户名和密码。当您使用 Web 身份验证对客户端进行身份验证时，您必须为每个客户端定义一个用户名和口令。然后，当客户端尝试加入无线LAN时，必须在登录页面提示时输入用户名和密码。

当启用Web身份验证时（在第3层安全下），用户在第一次尝试访问URL时偶尔会收到Web浏览器安全警报。

> **提示**：要删除此证书警告，请返回以下有关如何安装第三方受信任证书的指南
> http://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/109597-csr-chained-certificates-wlc-00.html



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to th server.

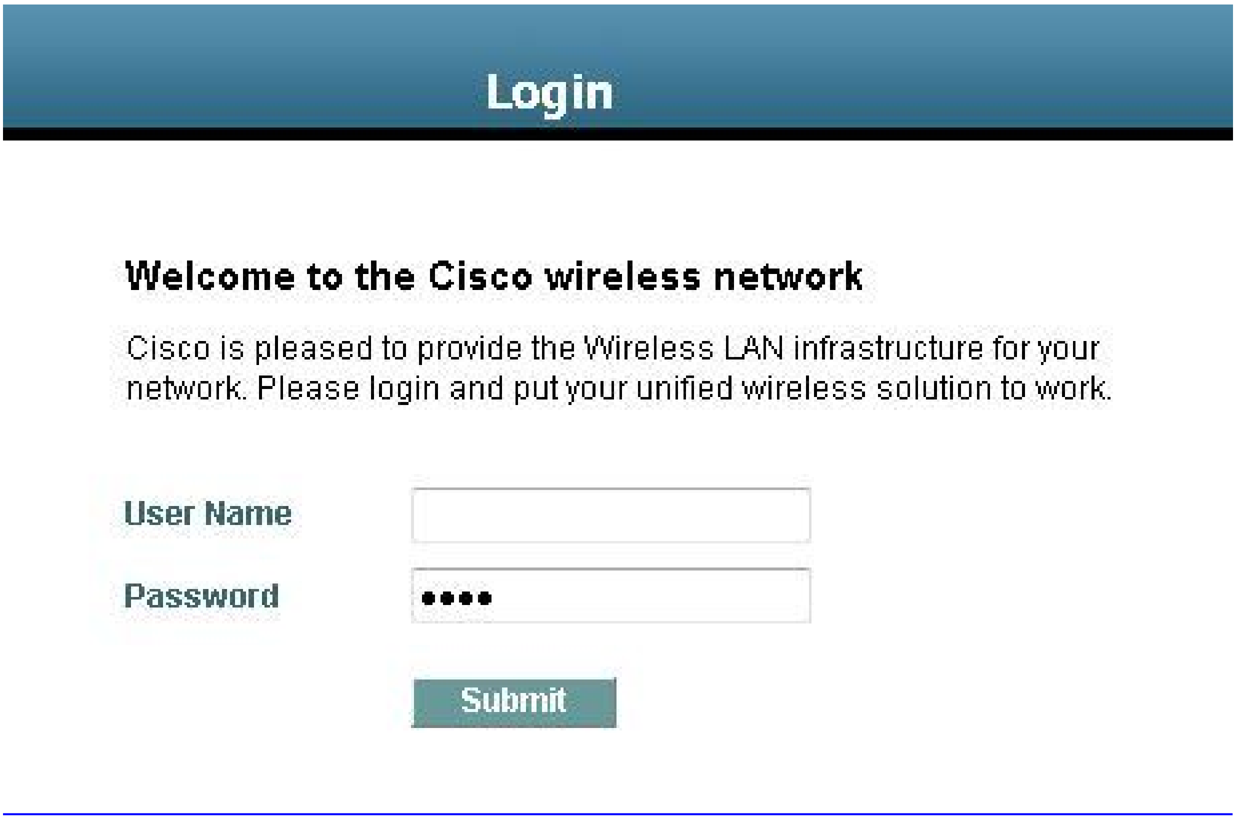
We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

单击**Yes**继续(或更准确地说，**Continue to this website（不推荐）**（例如，对于Firefox浏览器 ）)，或者如果客户端的浏览器不显示安全警报，则Web身份验证系统会将客户端重定向到登录页面 ，如图所示：



Login

Welcome to the Cisco wireless network

Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your unified wireless solution to work.

User Name:

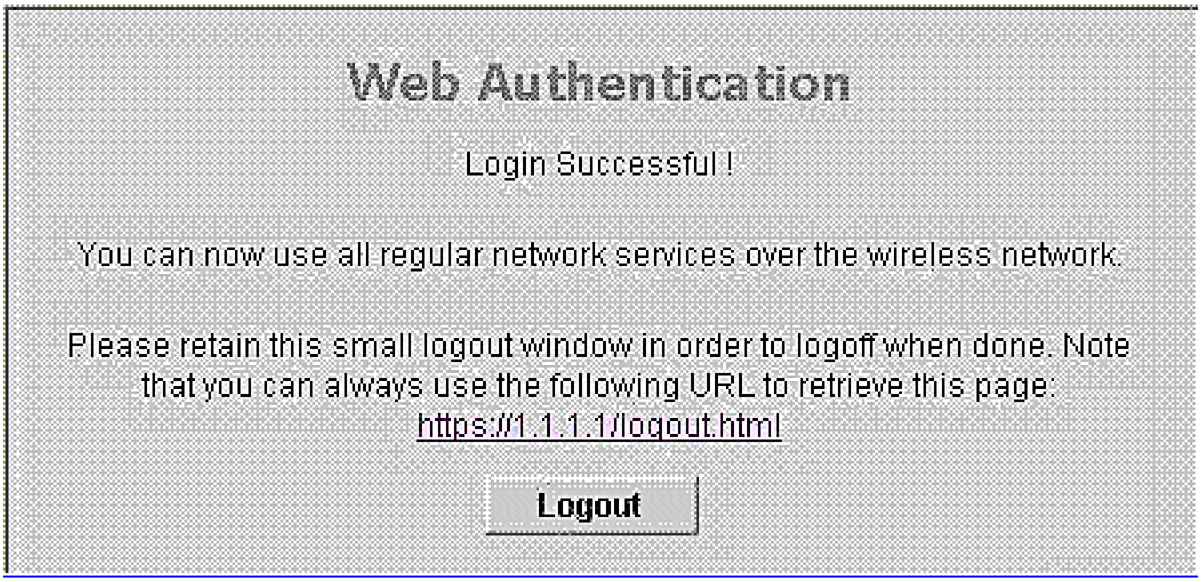
Password: ••••

默认登录页面包含思科徽标和思科特定文本。您可以选择让Web身份验证系统显示以下内容之一：

- 默认登录页
- 默认登录页面的修改版本
- 在外部Web服务器上配置的自定义登录页
- 下载到控制器的自定义登录页面

当您在Web身份验证登录页面上输入有效的用户名和密码并单击**Submit**时，将根据提交的凭证和来

自后端数据库（本例中为LDAP）的成功身份验证进行身份验证。然后，Web身份验证系统显示成功登录页面，并将已身份验证的客户端重定向到请求的URL。



Web Authentication

Login Successful !

You can now use all regular network services over the wireless network.

Please retain this small logout window in order to logoff when done. Note that you can always use the following URL to retrieve this page: https://1.1.1.1/logout.html

默认成功登录页面包含指向虚拟网关地址URL的指针:https://1.1.1.1/logout.html。为控制器虚拟接口设置的IP地址用作登录页的重定向地址。

本文档说明如何使用WLC上的内部网页进行Web身份验证。此示例使用LDAP服务器作为Web身份验证的后端数据库，以检索用户凭据并对用户进行身份验证。

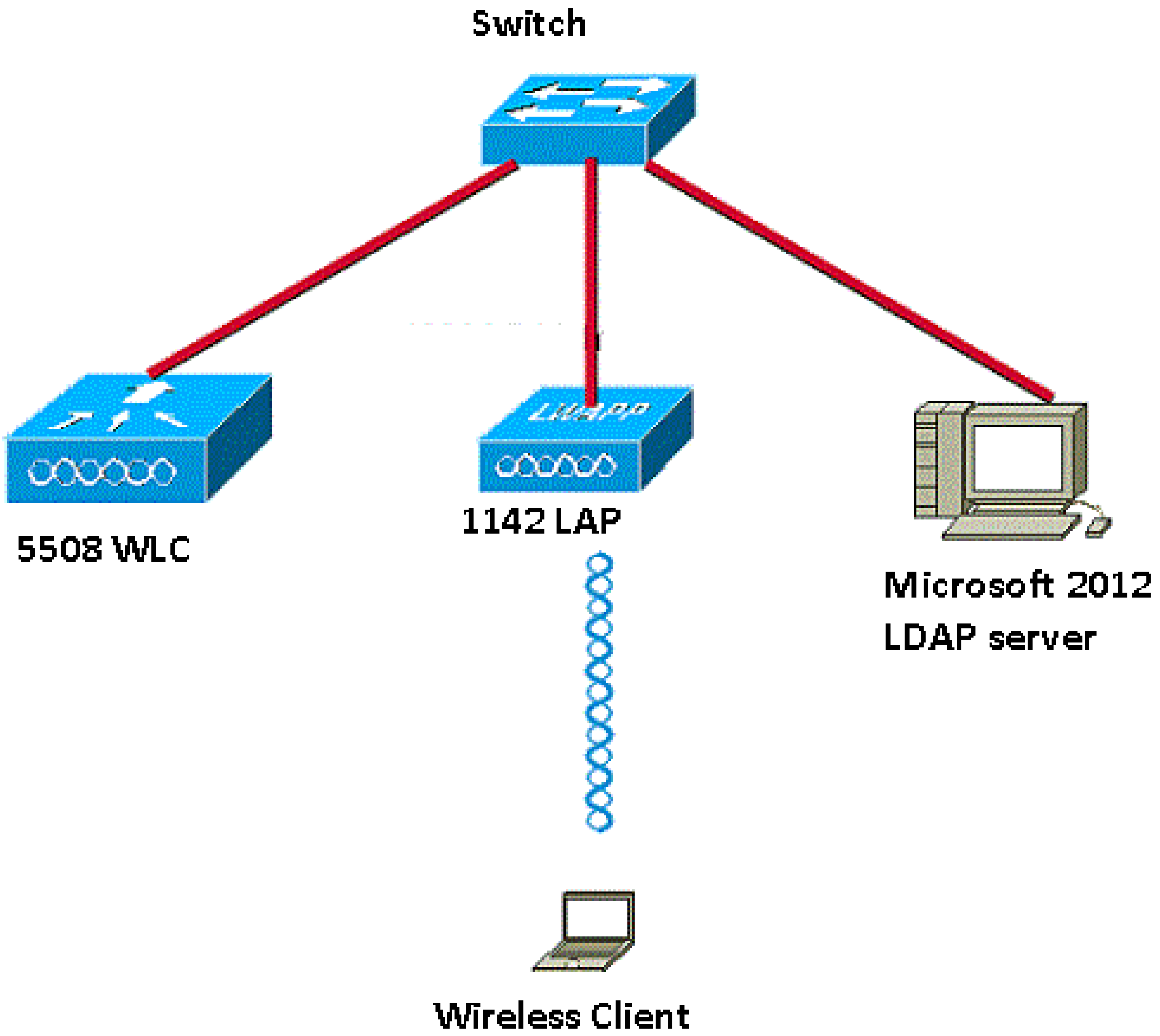
配置

本部分提供有关如何配置本文档所述功能的信息。

注意：要获取此部分中所用命令的更多信息，可使用命令查找工具（仅限已注册客户）。

网络图

本文档使用以下网络设置：



配置

要成功实施此设置，请完成以下步骤：

- 配置 LDAP 服务器.
- 为LDAP服务器配置WLC。
- 配置WLAN进行Web身份验证。

配置 LDAP 服务器

第一步是配置LDAP服务器，该服务器用作后端数据库来存储无线客户端的用户凭证。在本示例中，Microsoft Windows 2012 Essentials服务器用作LDAP服务器。

LDAP服务器配置的第一步是在LDAP服务器上创建用户数据库，以便WLC可以查询此数据库以对用户进行身份验证。

在域控制器上创建用户

组织单位(OU)包含多个组，这些组在PersonProfile中携带对个人条目的引用。人员可以是多个组的成员。所有对象类和属性定义都是LDAP架构默认设置。每个组都包含属于它的每个人的引用(dn)。

在本示例中，将创建一个新的OU LDAP-USERS，并在此OU下创建用户User1。配置此用户进行

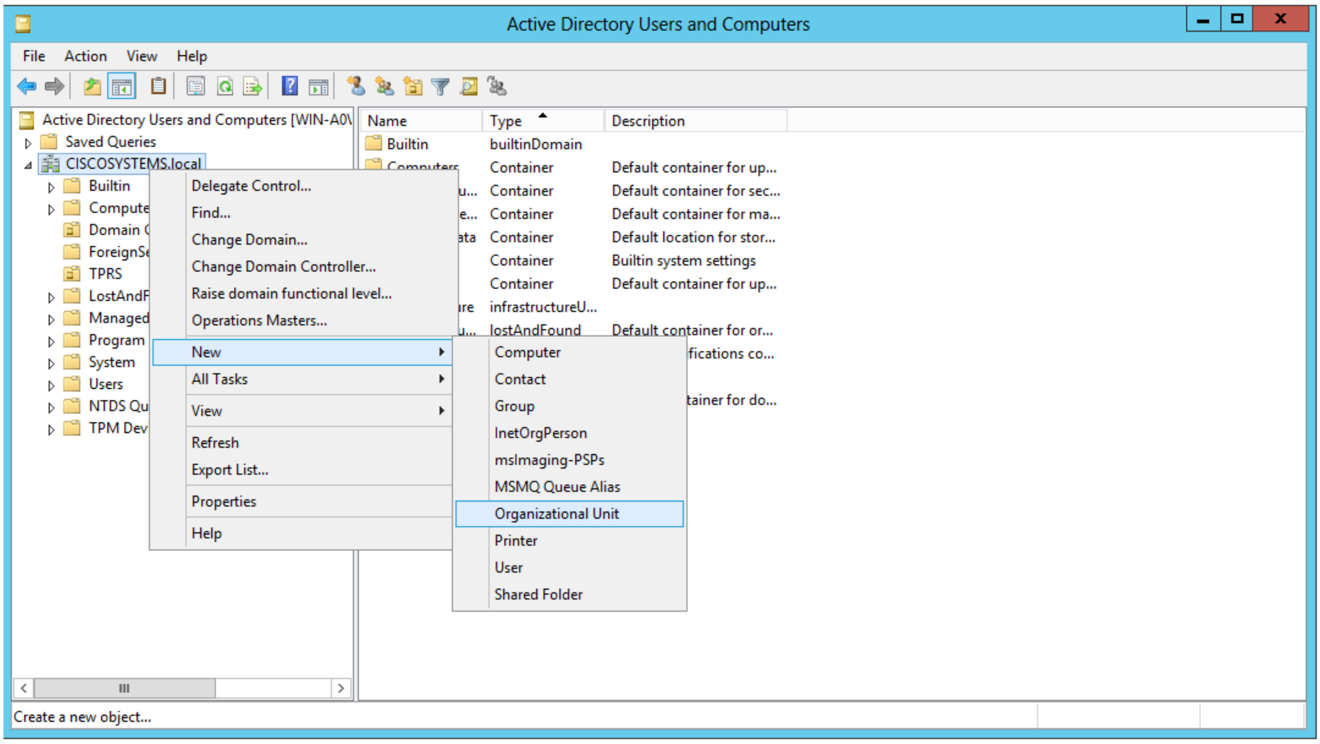
LDAP访问时，WLC可以查询此LDAP数据库以进行用户身份验证。

本示例中使用的域是**CISCOSYSTEMS.local**。

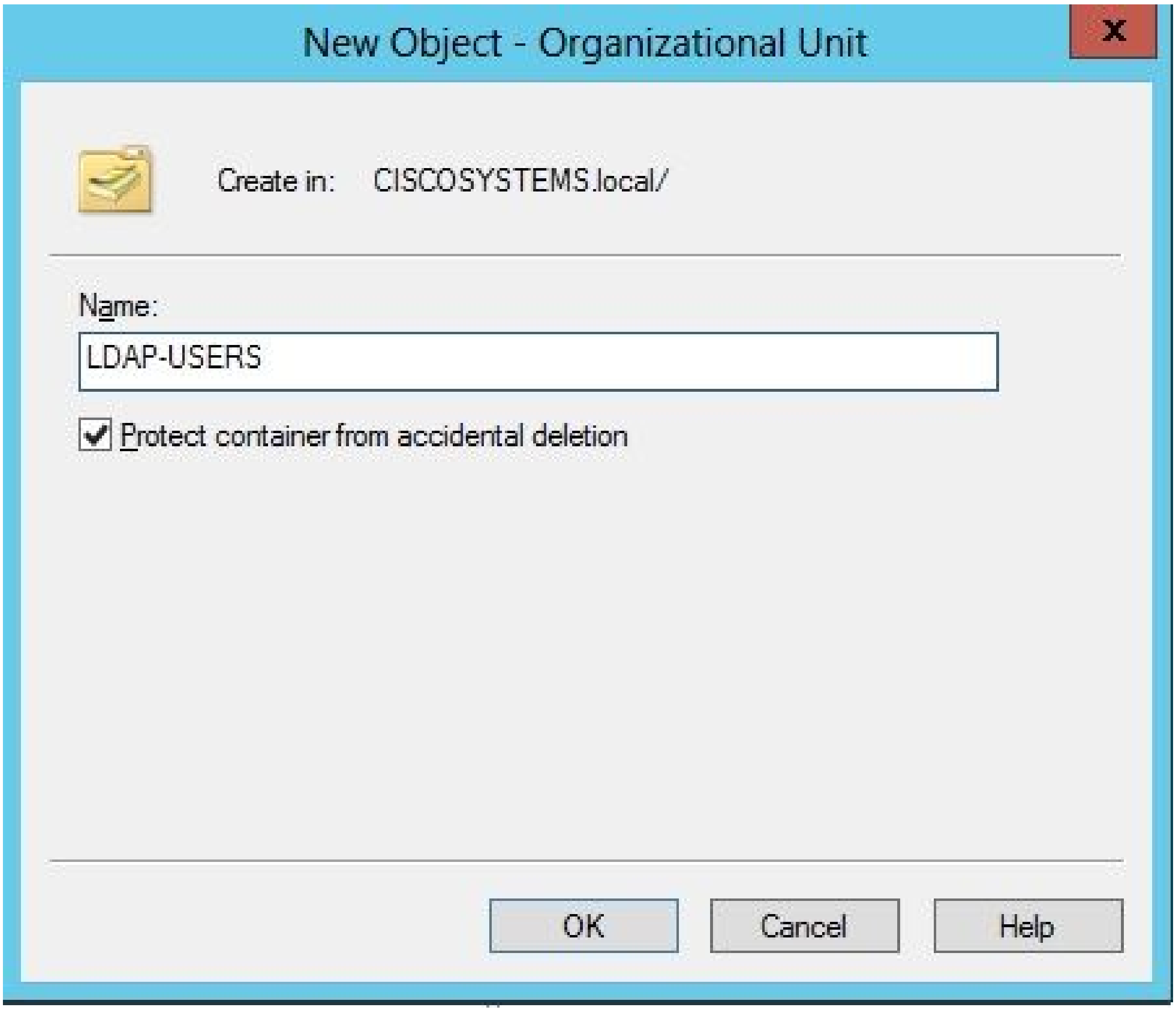
在 OU 下创建用户数据库

本部分解释如何在域中创建新的 OU 以及在此 OU 上创建新用户。

1. 打开Windows PowerShell并键入**servermanager.exe**
2. 在“服务器管理器”窗口中，单击**AD DS**。然后，右键单击服务器名称以选择**Active Directory用户和计算机。**
3. 右键单击您的域名(在本例中为**CISCOSYSTEMS.local**)，然后从上下文菜单导航到**New > Organizational Unit**以创建新的OU。



4. 为此OU分配名称，然后单击**OK**，如图所示：


New Object - Organizational Unit

Create in: CISCOSYSTEMS.local/

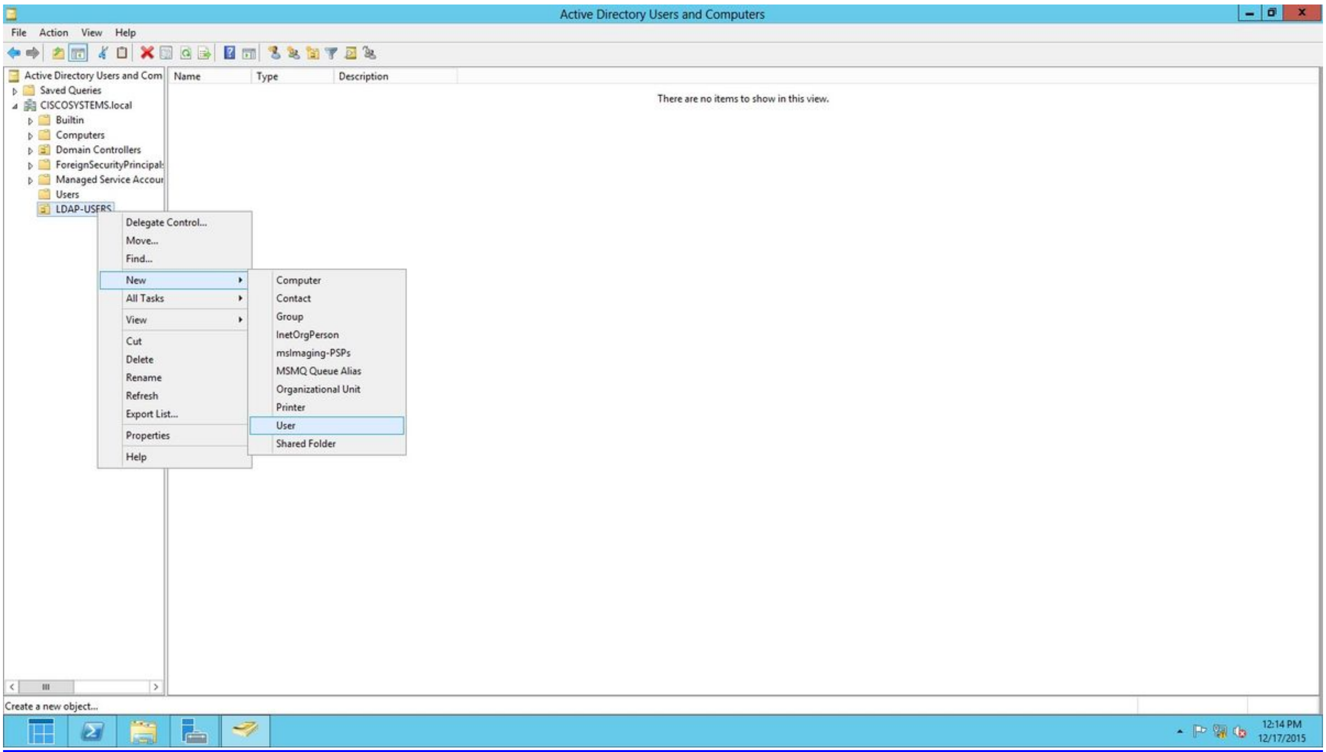
Name:

LDAP-USERS

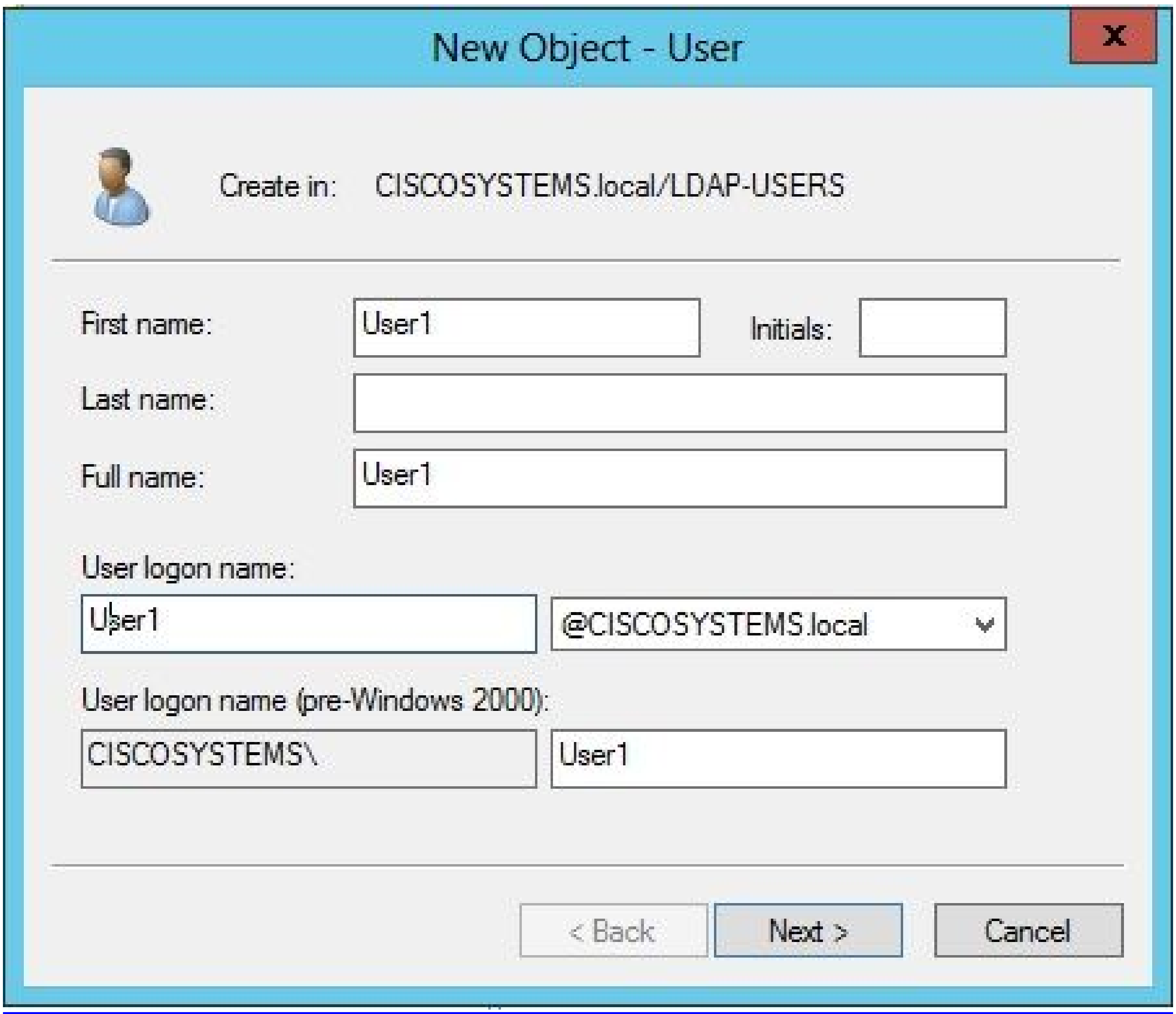
☑ Protect container from accidental deletion

现在在LDAP服务器上创建了新的OU LDAP-USERS，下一步就是在此OU下创建用户**User1**。为此，请完成以下步骤：

1. 右键单击创建的新OU。从生成的上下文菜单导航到**LDAP-USERS> New > User**，以创建新用户，如图所示：



2. 在“用户设置”页中，填写必要的字段，如本示例所示。此示例在**User logon name**字段中包含**User1**。这是在LDAP数据库中验证以对客户端进行身份验证的用户名。此示例在First name和Full Name字段中使用User1。单击 **Next**。



New Object - User

Create in: CISCOSYSTEMS.local/LDAP-USERS

First name: User1

Initials:

Last name:

Full name: User1

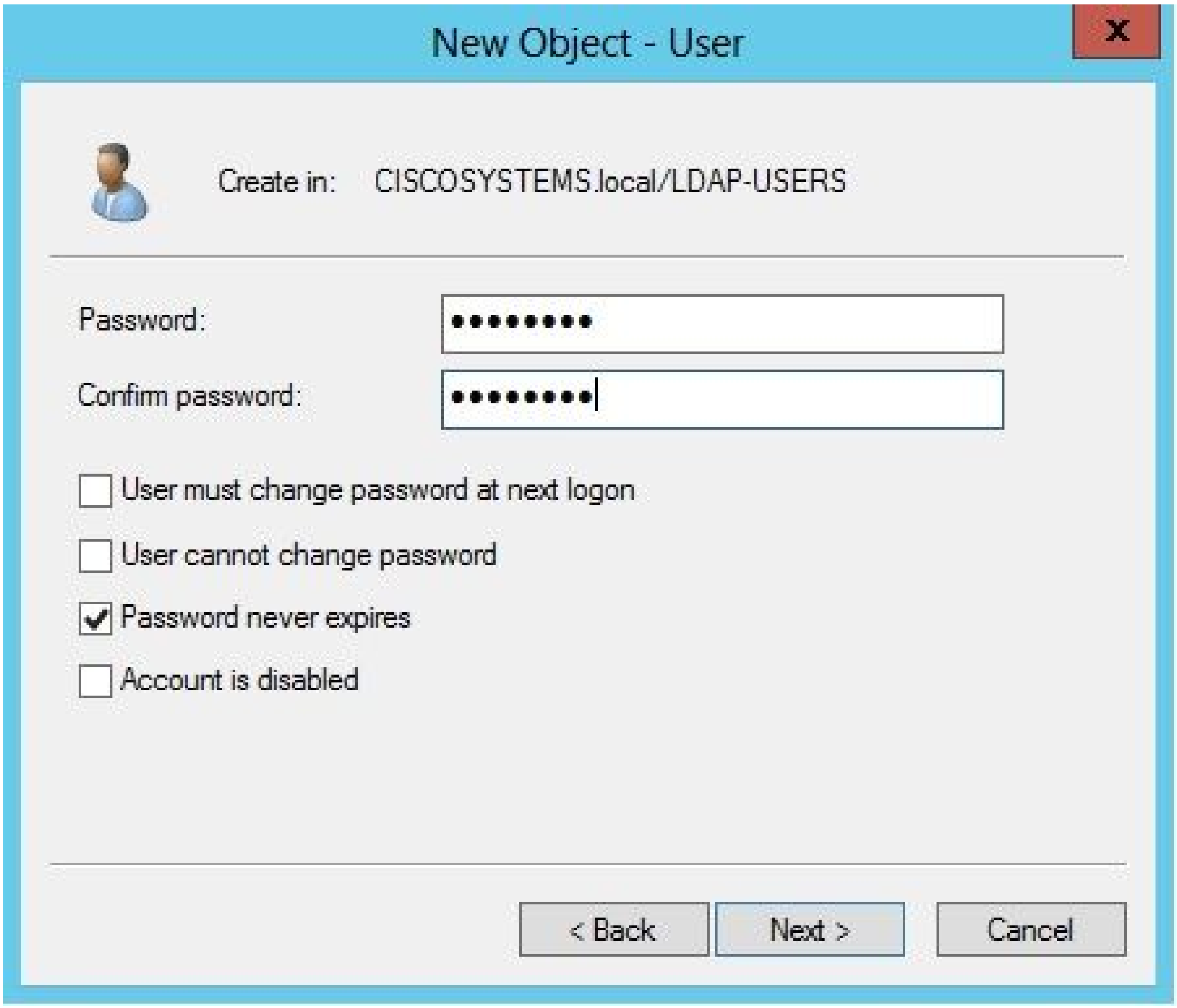
User logon name:

User1 @CISCOSYSTEMS.local

User logon name (pre-Windows 2000):

CISCOSYSTEMS\ User1

3. 输入密码并确认此密码。选中**密码永不过期选项，然后单击“下一步”。**



New Object - User

Create in: CISCOSYSTEMS.local/LDAP-USERS

Password: ●●●●●●●●●

Confirm password: ●●●●●●●●●

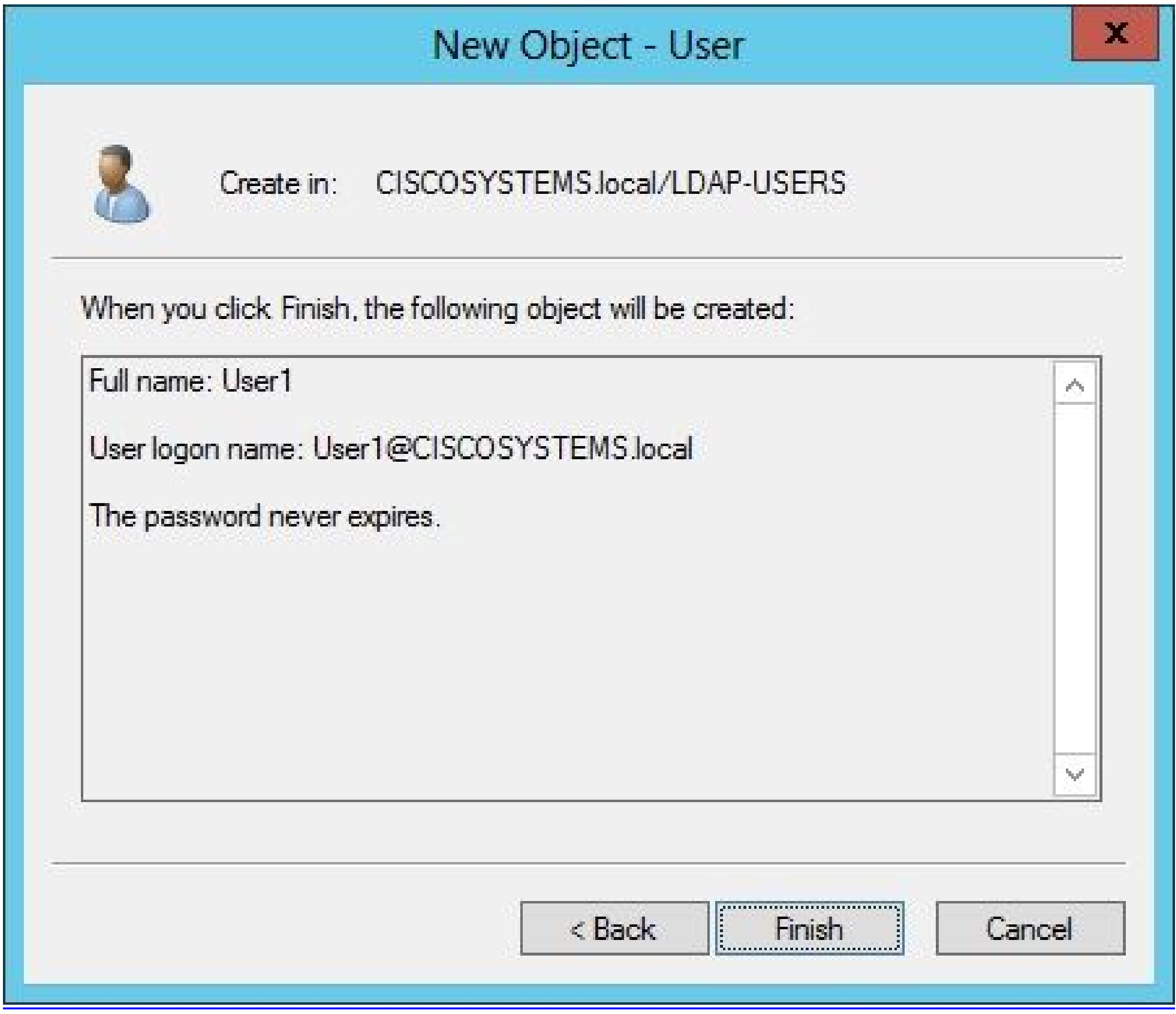
□ User must change password at next logon

□ User cannot change password

☑ Password never expires

□ Account is disabled

4. 单击 **完成**。在OU LDAP-USERS下创建新的用户User1。以下是用户凭证：用户名 **:User1**password： **Laptop123**


New Object - User

Create in: CISCOSYSTEMS.local/LDAP-USERS

When you click Finish, the following object will be created:

Full name: User1

User logon name: User1@CISCOSYSTEMS.local

The password never expires.

现在用户是在OU下创建的，下一步是配置此用户进行LDAP访问。

为 LDAP 访问配置用户

可以选择**Anonymous**或**Authenticated**指定LDAP服务器的本地身份验证绑定方法。Anonymous方法允许匿名访问LDAP服务器。Authenticated方法要求输入用户名和密码才能进行安全访问。默认值是 Anonymous。

本节介绍如何配置匿名方法和身份验证方法。

匿名绑定

注意：不建议使用Anonymous Bind。LDAPLDAP

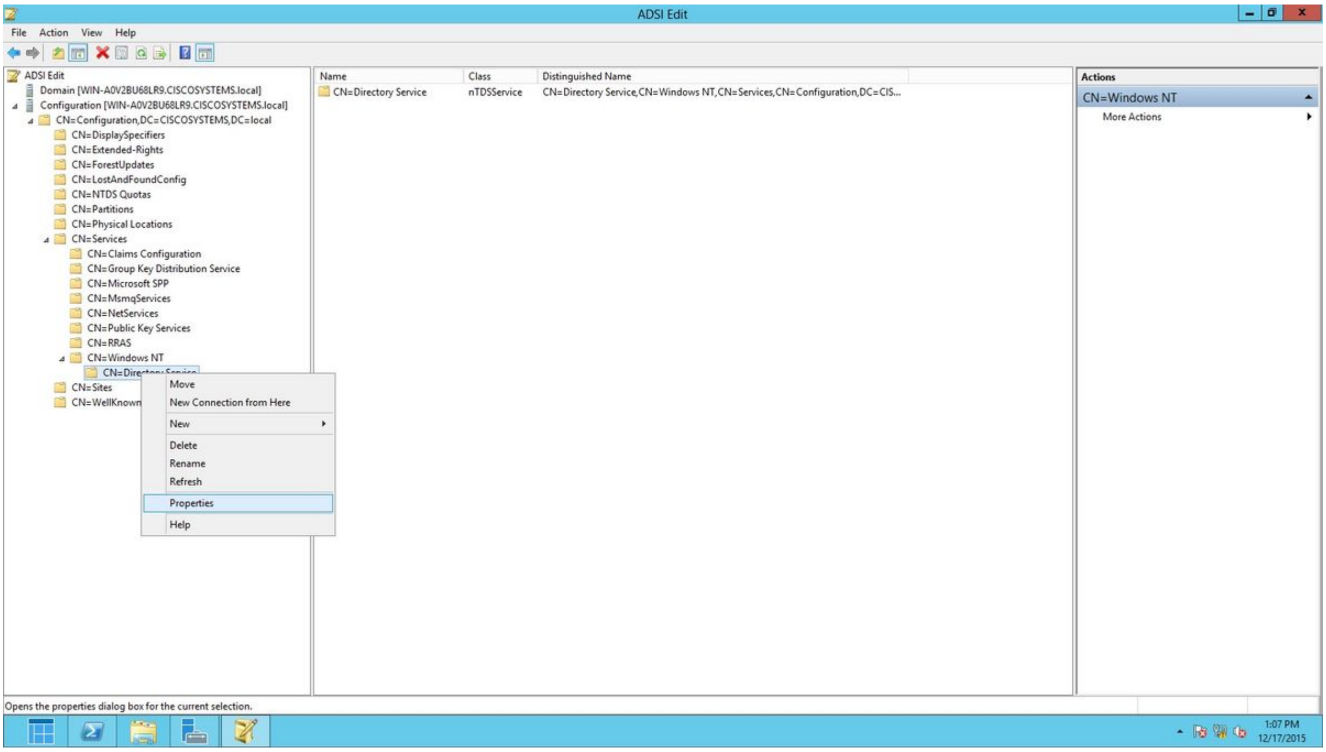
执行本节中的步骤以配置匿名用户进行LDAP访问。

在Windows 2012 Essentials服务器上启用匿名绑定功能

要使任何第三方应用程序（在本例中为WLC）访问LDAP上的Windows 2012 AD，必须在Windows 2012上启用匿名绑定功能。默认情况下，Windows 2012 域控制器上不允许执行匿名 LDAP 操作。要启用匿名绑定功能，请执行以下步骤：

1. 在Windows PowerShell中键入ADSIEdit.msc，**启动**ADSI Edit工具。此工具是Windows 2012支持工具的一部分。

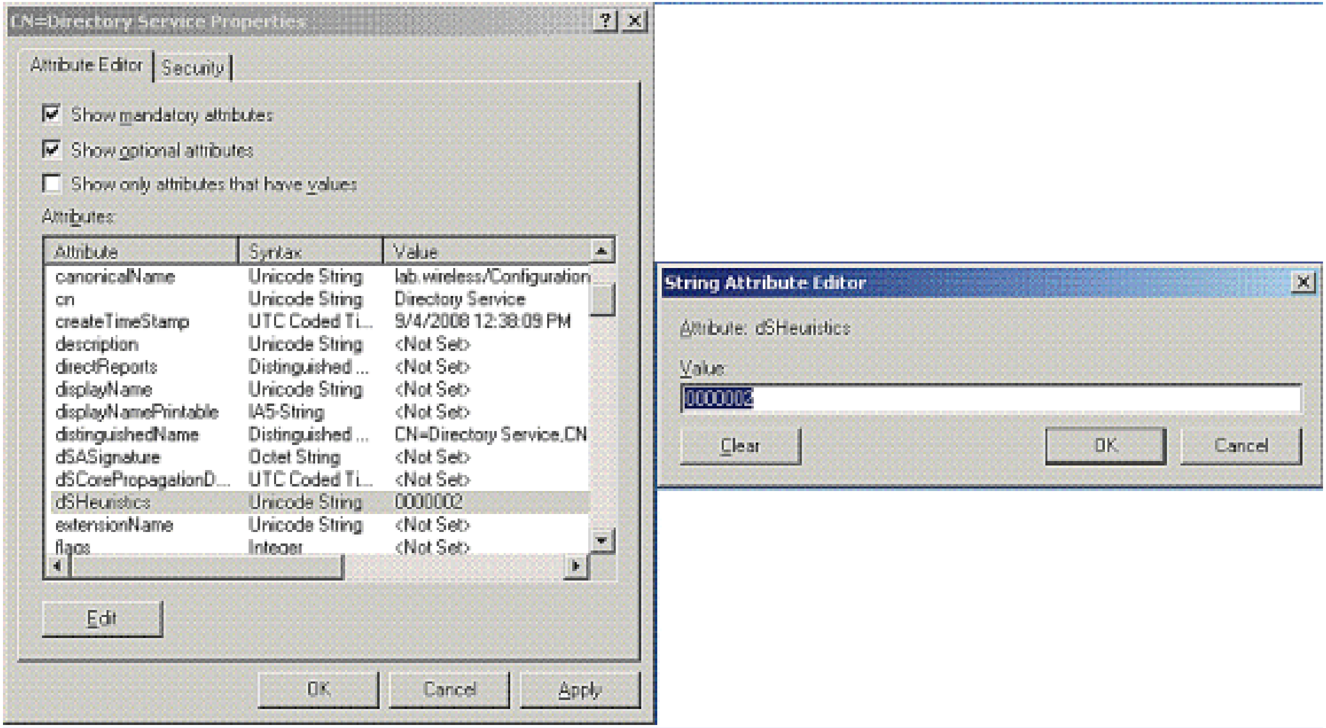
2. 在ADSI Edit窗口中，展开根域(Configuration [WIN-A0V2BU68LR9.CISCOSYSTEMS.local])。导航到**CN=Services > CN=Windows NT > CN=Directory Service**。右键单击**CN=Directory Service**容器，然后从上下文菜单中选择**属性**，如图所示：



Name	Class	Distinguished Name
CN=Directory Service	nTDSService	CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=CIS...

Opens the properties dialog box for the current selection.

3. 在CN=Directory Service Properties窗口的**Attributes**下，单击Attribute字段下的**dsHeuristics**属性，然后选择**Edit**。在此属性的“字符串属性编辑器”窗口中，输入值**000002**；单击**Apply**和**OK**，如图所示。Windows 2012服务器上启用了匿名绑定功能。**注**：最后（第七）个字符用于控制可以绑定到LDAP服务的方式。0（零）或无第七个字符表示禁用匿名LDAP操作。如果将第七个字符设置为2，则会启用匿名绑定功能。



☑ Show mandatory attributes
☑ Show optional attributes
□ Show only attributes that have values

Attributes:

Attribute	Syntax	Value
canonicalName	Unicode String	lab.wireless/Configuration
cn	Unicode String	Directory Service
createTimeStamp	UTC Coded Ti...	9/4/2008 12:38:09 PM
description	Unicode String	<Not Set>
directReports	Distinguished ...	<Not Set>
displayName	Unicode String	<Not Set>
displayNamePrintable	IA5-String	<Not Set>
distinguishedName	Distinguished ...	CN=Directory Service,CN
dSASignature	Octet String	<Not Set>
dSCorePropagationD...	UTC Coded Ti...	<Not Set>
dSHeuristics	Unicode String	0000002
extensionName	Unicode String	<Not Set>
flags	Integer	<Not Set>

Attribute: dSHeuristics

Value:
0000002

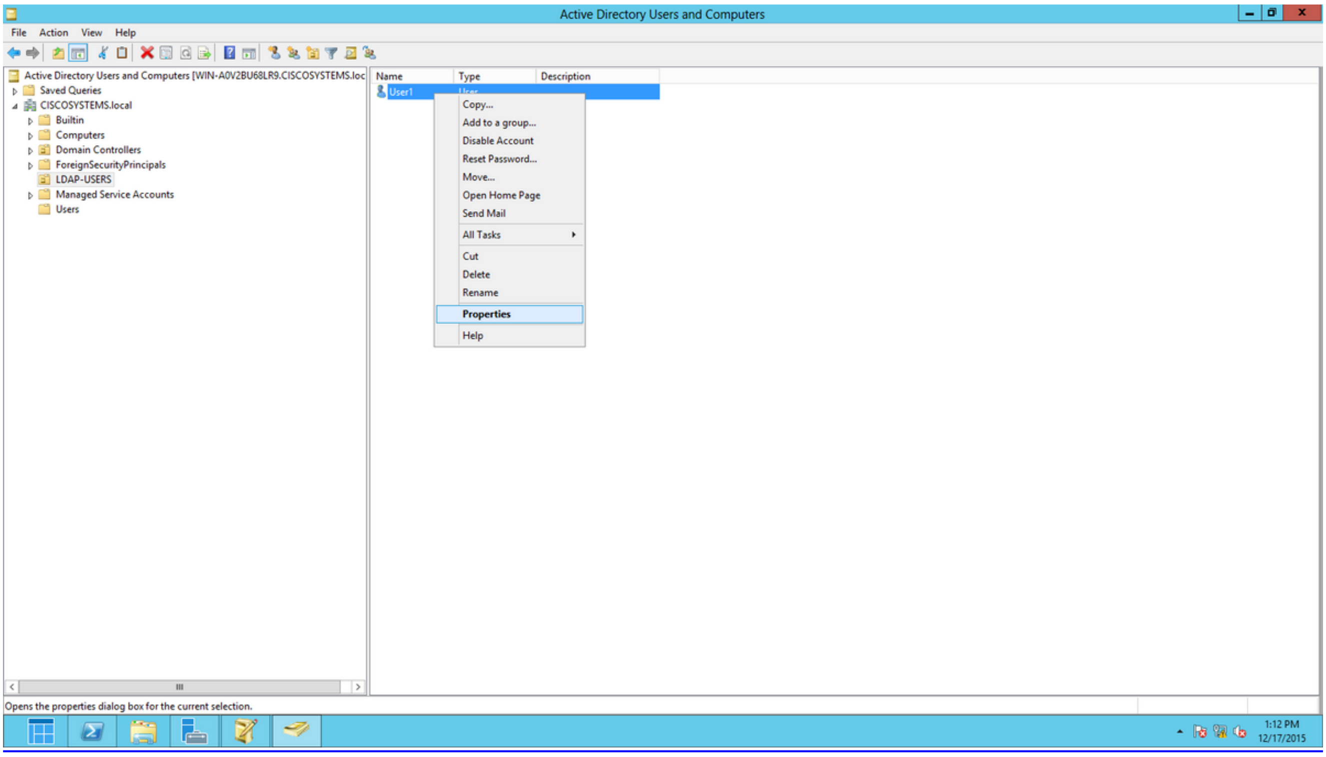
向用户授予ANONYMOUS登录访问权限

下一步是向用户User1授予ANONYMOUS LOGON访问权限。为此，请完成以下步骤：

1. 打开 **Active Directory 用户和计算机。**

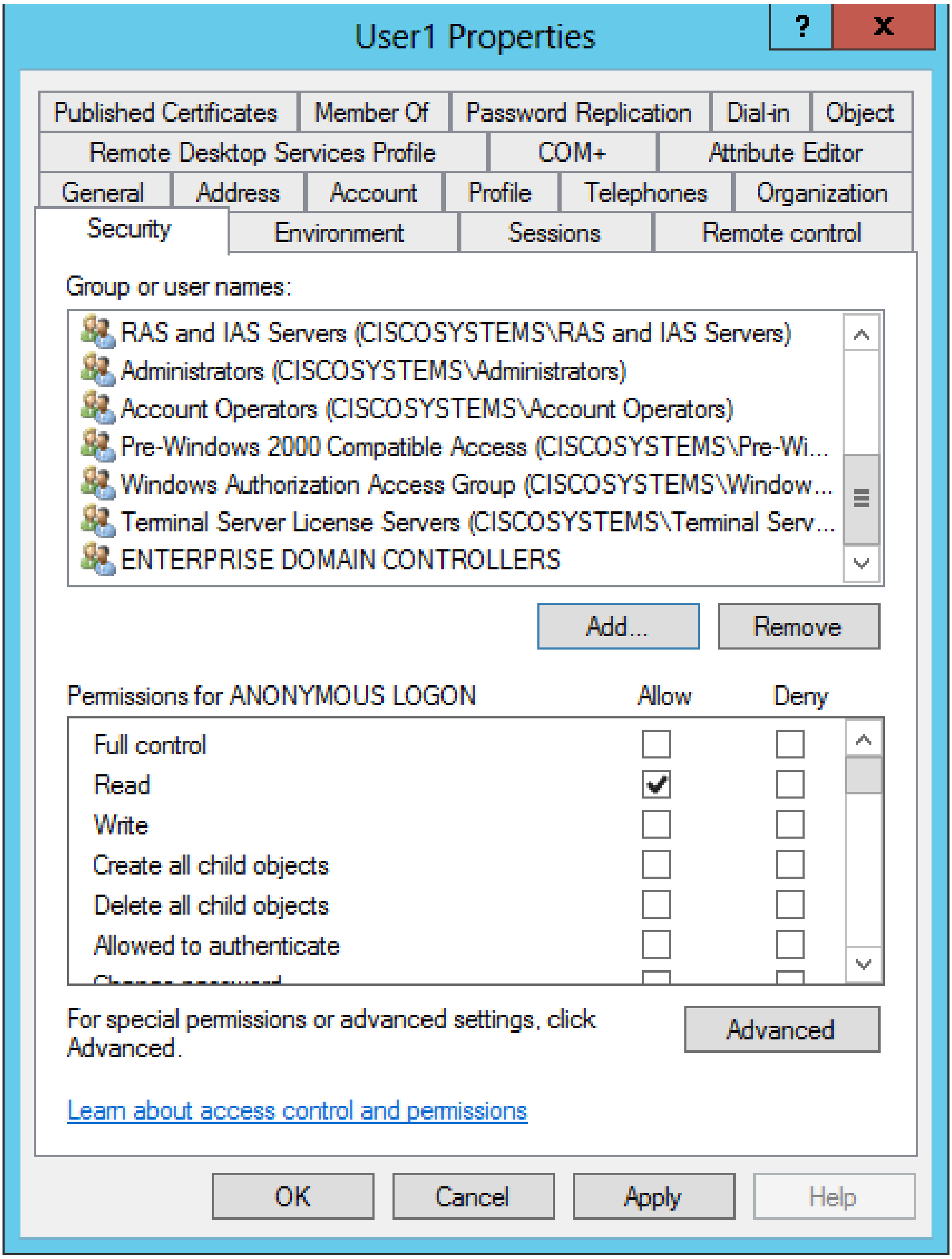
2. 确保选中**View Advanced Features**。

3. 导航到用户User1，然后右键单击该用户。从上下文菜单中选择**属性**。此用户以名字User1标识。



Opens the properties dialog box for the current selection.

4. 单击**Security**选项卡，如图所示：



Group or user names:

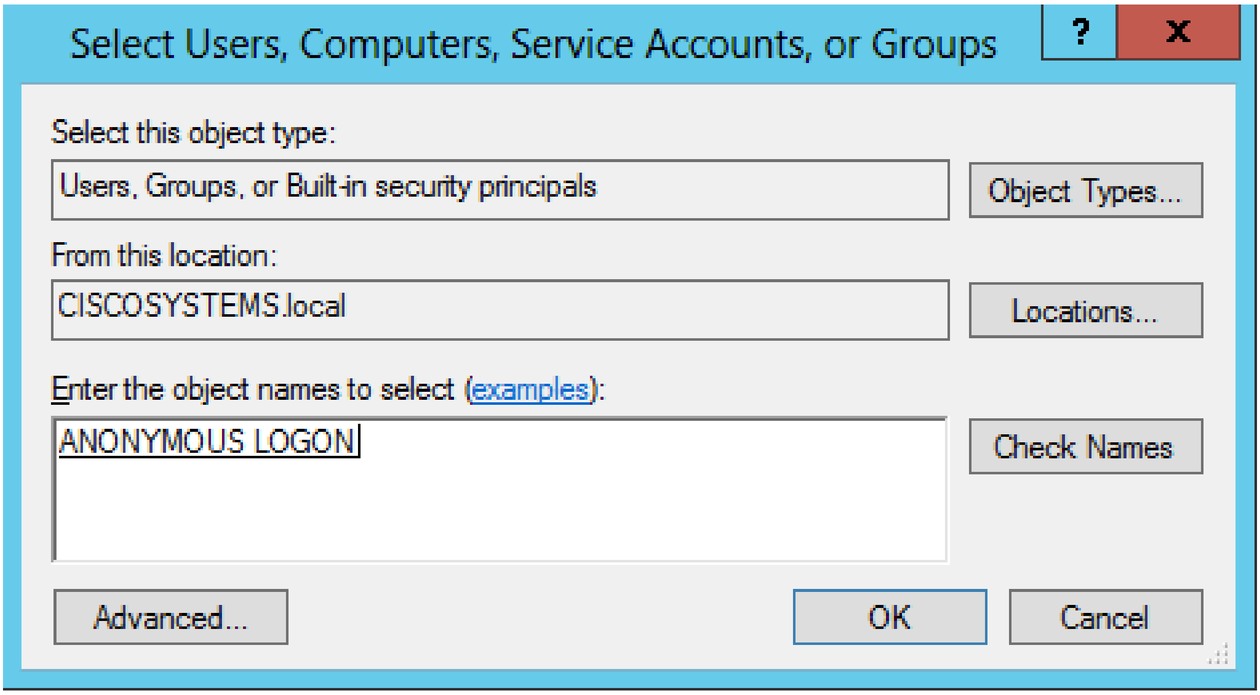
- RAS and IAS Servers (CISCOSYSTEMS\RAS and IAS Servers)
- Administrators (CISCOSYSTEMS\Administrators)
- Account Operators (CISCOSYSTEMS\Account Operators)
- Pre-Windows 2000 Compatible Access (CISCOSYSTEMS\Pre-Wi...
- Windows Authorization Access Group (CISCOSYSTEMS\Window...
- Terminal Server License Servers (CISCOSYSTEMS\Terminal Serv...
- ENTERPRISE DOMAIN CONTROLLERS

Permissions for ANONYMOUS LOGON	Allow	Deny
Full control	□	□
Read	☑	□
Write	□	□
Create all child objects	□	□
Delete all child objects	□	□
Allowed to authenticate	□	□
Change password	□	□

For special permissions or advanced settings, click Advanced.

5. 在所显示的窗口中单击**添加。**

6. 在*Enter the object names to select*框下输入**ANONYMOUS LOGON**并确认对话框，如图所示：



Select Users, Computers, Service Accounts, or Groups

Select this object type:

Users, Groups, or Built-in security principals

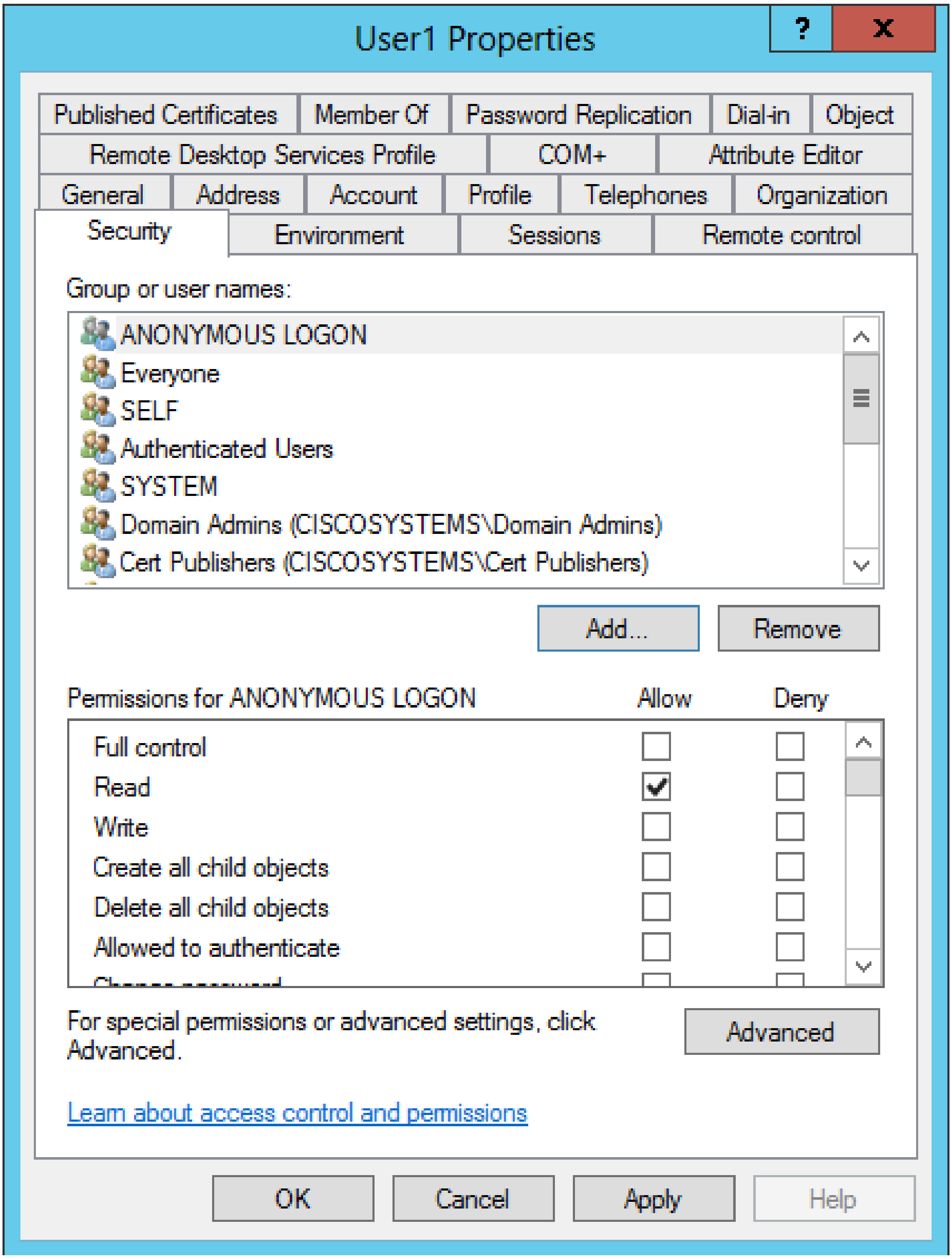
From this location:

CISCOSYSTEMS.local

Enter the object names to select (examples):

ANONYMOUS LOGON

7. 在ACL中，请注意ANONYMOUS LOGON有权访问用户的一些属性集。Click **OK**.ANONYMOUS LOGON访问权限被授予此用户，如图所示：



Group or user names:

- ANONYMOUS LOGON
- Everyone
- SELF
- Authenticated Users
- SYSTEM
- Domain Admins (CISCOSYSTEMS\Domain Admins)
- Cert Publishers (CISCOSYSTEMS\Cert Publishers)

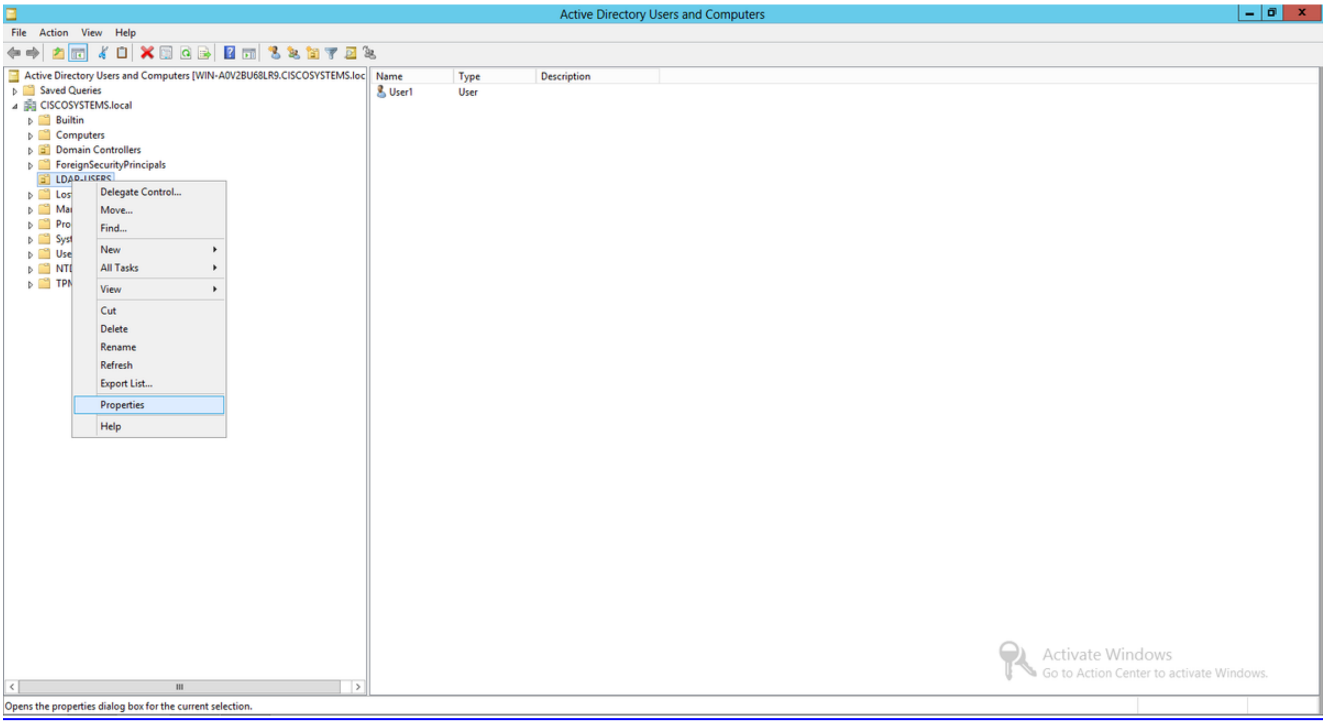
Permissions for ANONYMOUS LOGON	Allow	Deny
Full control	□	□
Read	☑	□
Write	□	□
Create all child objects	□	□
Delete all child objects	□	□
Allowed to authenticate	□	□

For special permissions or advanced settings, click Advanced.

对OU授予列表内容权限

下一步是至少向用户所在的OU上的ANONYMOUS LOGON授予List Contents权限。在本示例中，User1位于OU LDAP-USERS上。为此，请完成以下步骤：

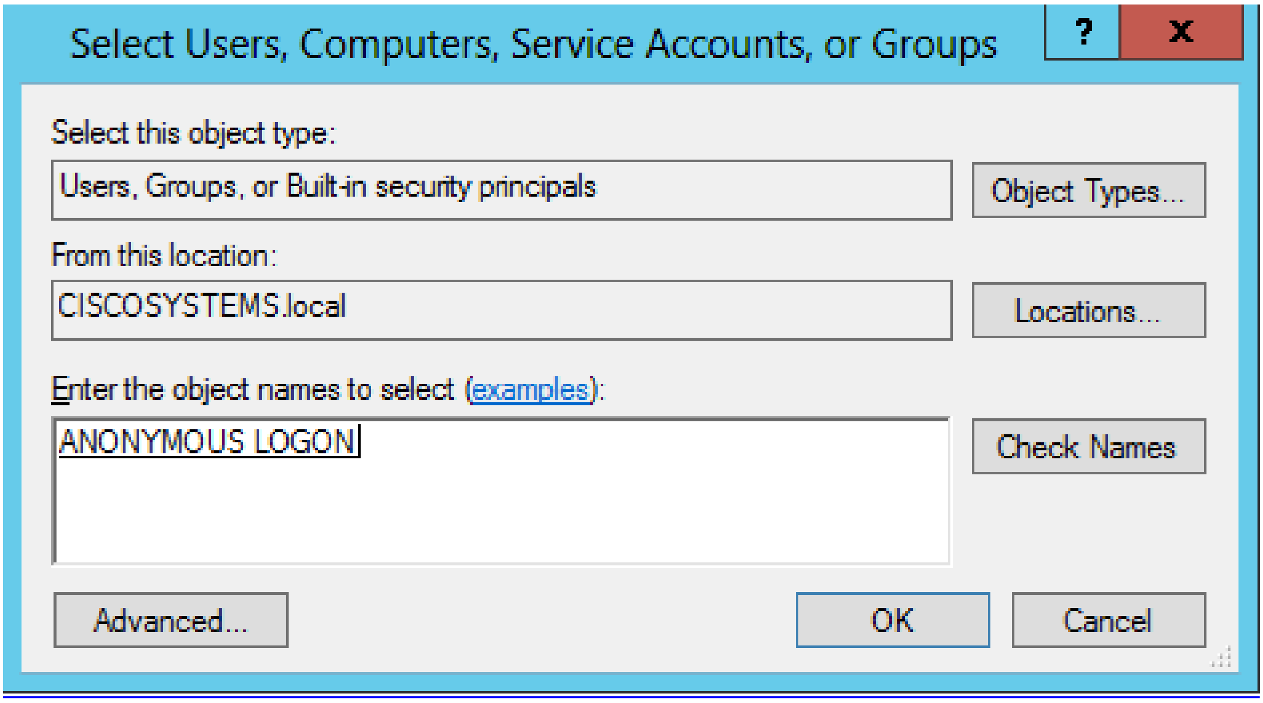
1. 在**Active Directory Users and Computers**中，右键单击**OU LDAP-USERS**，然后选择**Properties**，如图所示：



Opens the properties dialog box for the current selection.

2. 单击 **Security**。

3. 单击 **Add**。在打开的对话框中，输入**ANONYMOUS LOGON**并确认对话框，如图所示：



Select Users, Computers, Service Accounts, or Groups

Select this object type:
Users, Groups, or Built-in security principals

From this location:
CISCOSYSTEMS.local

Enter the object names to select (examples):
ANONYMOUS LOGON

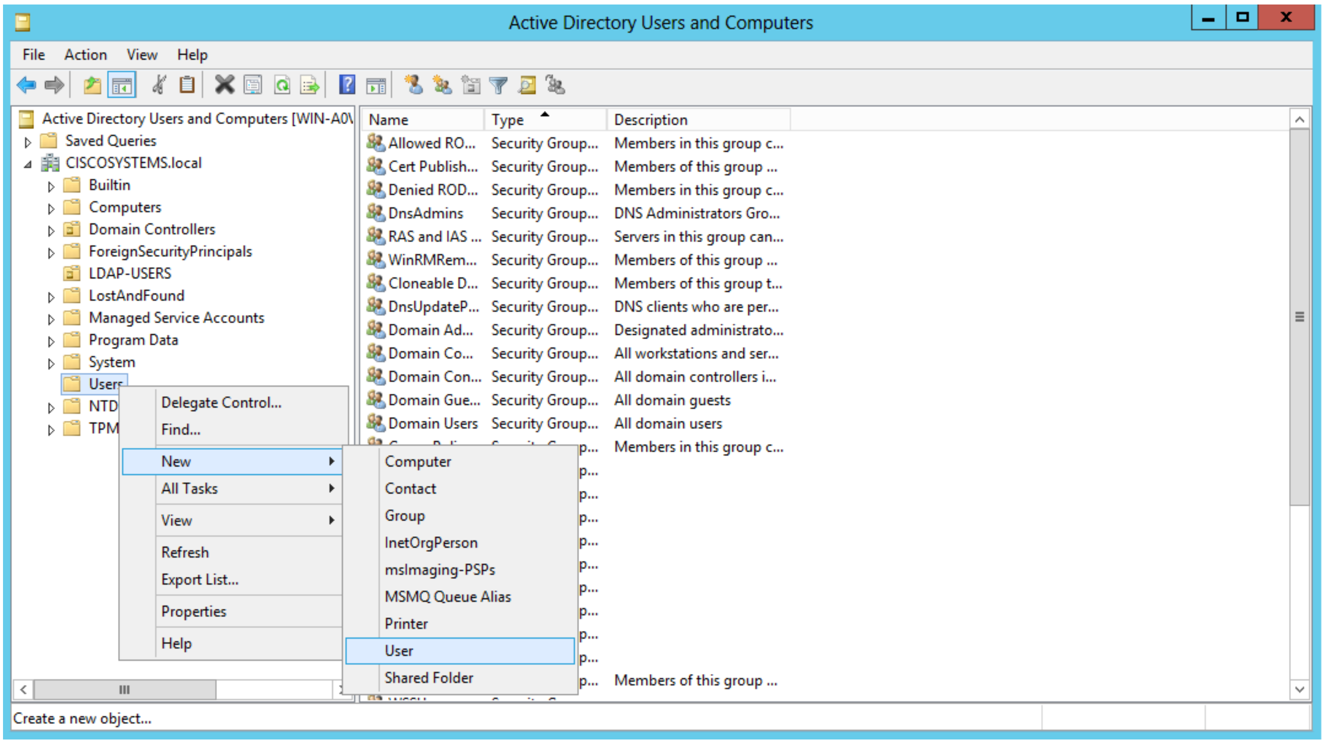
经过身份验证的绑定

执行本节中的步骤以配置对LDAP服务器进行本地身份验证的用户。

1. 打开Windows PowerShell并键入 **servermanager.exe**

2. 在“服务器管理器”窗口中，单击**AD DS**。然后右键单击您的服务器名称以选择 **Active Directory用户和计算机。**

3. 右键单击**Users**。从生成的上下文菜单导航到**New** > **User**，以创建新用户。



Name	Type	Description
Allowed RO...	Security Group...	Members in this group c...
Cert Publish...	Security Group...	Members of this group ...
Denied ROD...	Security Group...	Members in this group c...
DnsAdmins	Security Group...	DNS Administrators Gro...
RAS and IAS ...	Security Group...	Servers in this group can...
WinRMRem...	Security Group...	Members of this group ...
Cloneable D...	Security Group...	Members of this group t...
DnsUpdateP...	Security Group...	DNS clients who are per...
Domain Ad...	Security Group...	Designated administrato...
Domain Co...	Security Group...	All workstations and ser...
Domain Con...	Security Group...	All domain controllers i...
Domain Gue...	Security Group...	All domain guests
Domain Users	Security Group...	All domain users

4. 在“用户设置”页中，填写必要的字段，如本示例所示。此示例在**User logon name**字段中包含**WLC-admin**。这是用于对LDAP服务器进行本地身份验证的用户名。单击 **Next**。

5. 输入密码并确认此密码。选中**密码永不过期选项，然后单击“下一步”。**

6. 单击 **完成**。在**Users**容器下创建新的用户WLC-admin。以下是用户凭证：用户名:**WLC-admin**密码：**Admin123**

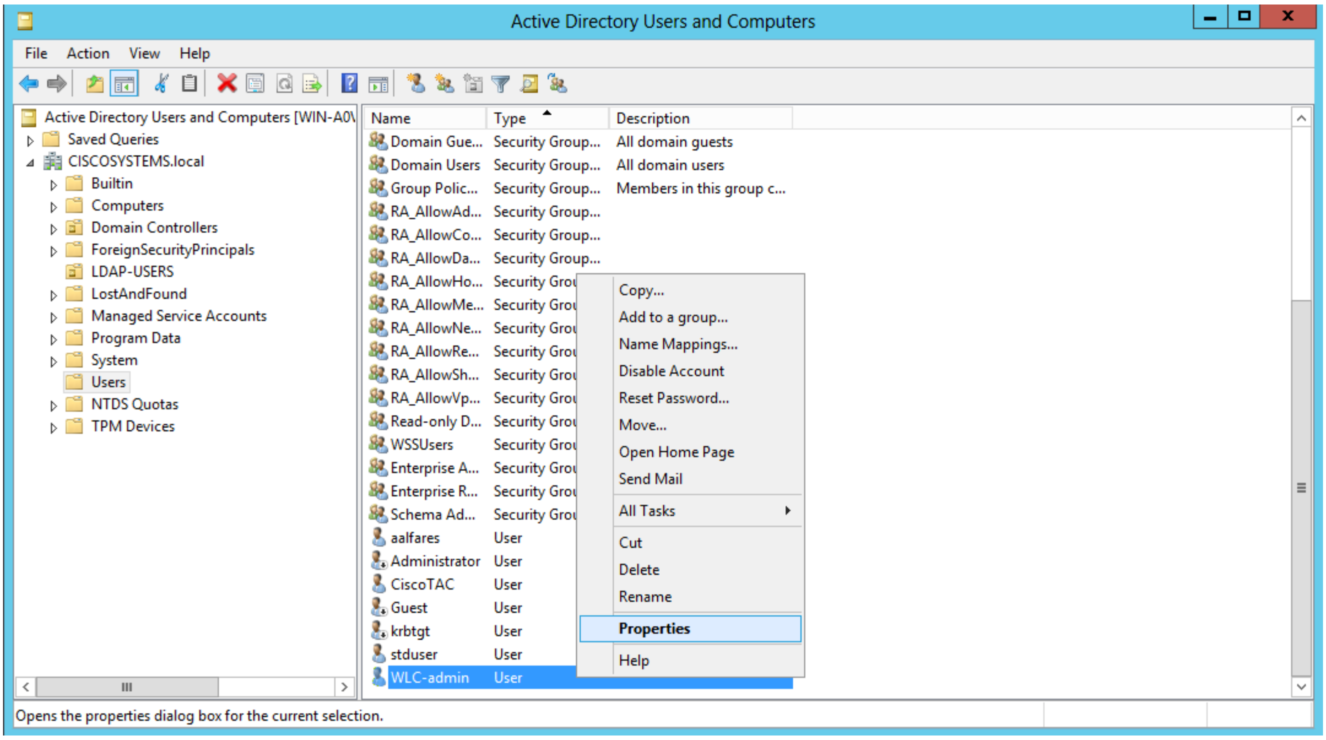
向WLC-admin授予管理员权限

创建本地身份验证用户后，我们需要授予其管理员权限。为此，请完成以下步骤：

1. 打开 **Active Directory 用户和计算机。**

2. 确保选中**View Advanced Features**。

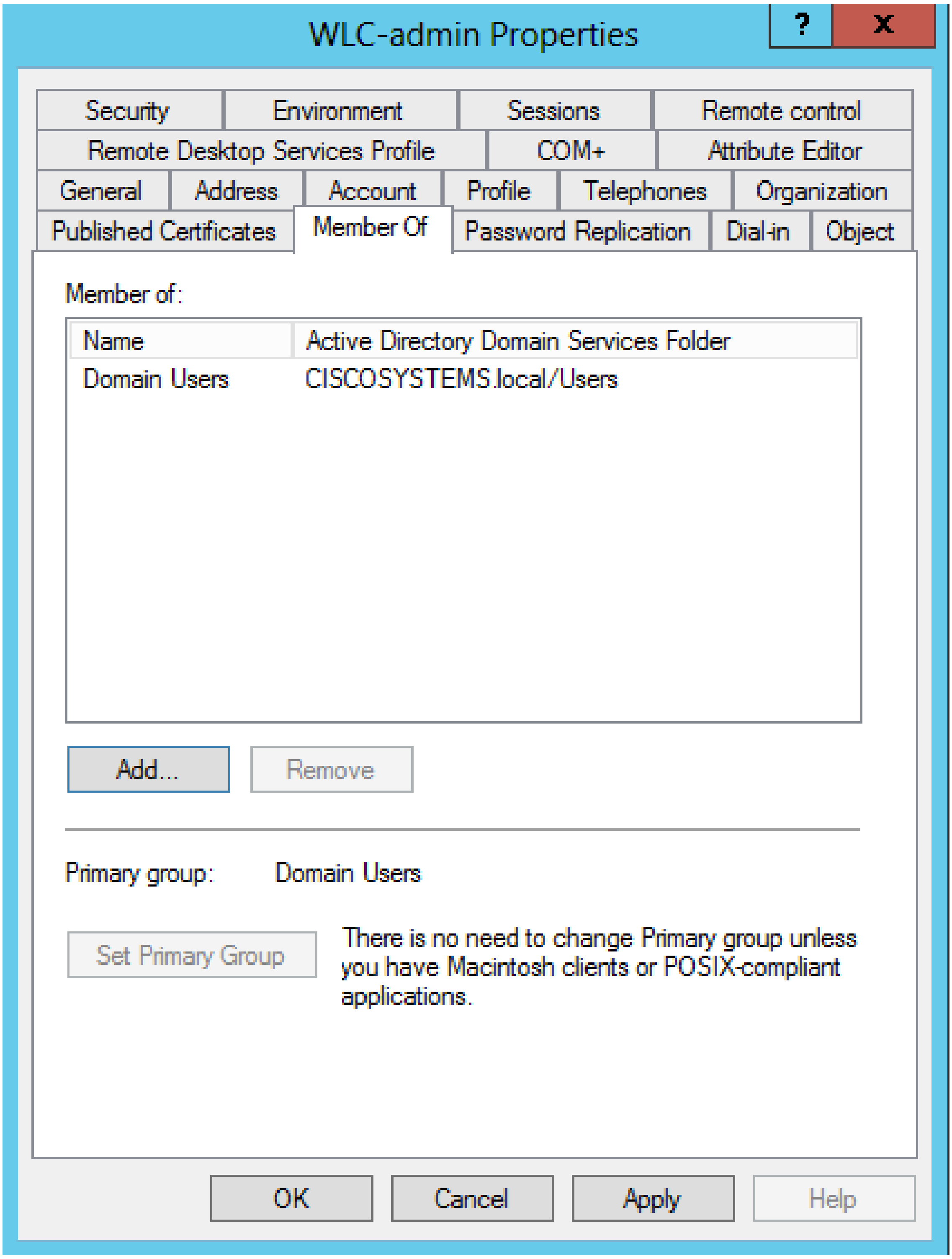
3. 导航到用户**WLC-admin**，然后右键单击该用户。从上下文菜单中选择**属性**，如图所示。此用户使用名字WLC-admin进行标识。



Name	Type	Description
Domain Gue...	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Group Polic...	Security Group...	Members in this group c...
RA_AllowAd...	Security Group...	
RA_AllowCo...	Security Group...	
RA_AllowDa...	Security Group...	
RA_AllowHo...	Security Grou	
RA_AllowMe...	Security Grou	
RA_AllowNe...	Security Grou	
RA_AllowRe...	Security Grou	
RA_AllowSh...	Security Grou	
RA_AllowVp...	Security Grou	
Read-only D...	Security Grou	
WSSUsers	Security Grou	
Enterprise A...	Security Grou	
Enterprise R...	Security Grou	
Schema Ad...	Security Grou	
aalfares	User	
Administrator	User	
CiscoTAC	User	
Guest	User	
krbtgt	User	
stduser	User	
WLC-admin	User	

Opens the properties dialog box for the current selection.

4. 单击**Member Of**选项卡，如图所示：



WLC-admin Properties

Member of:

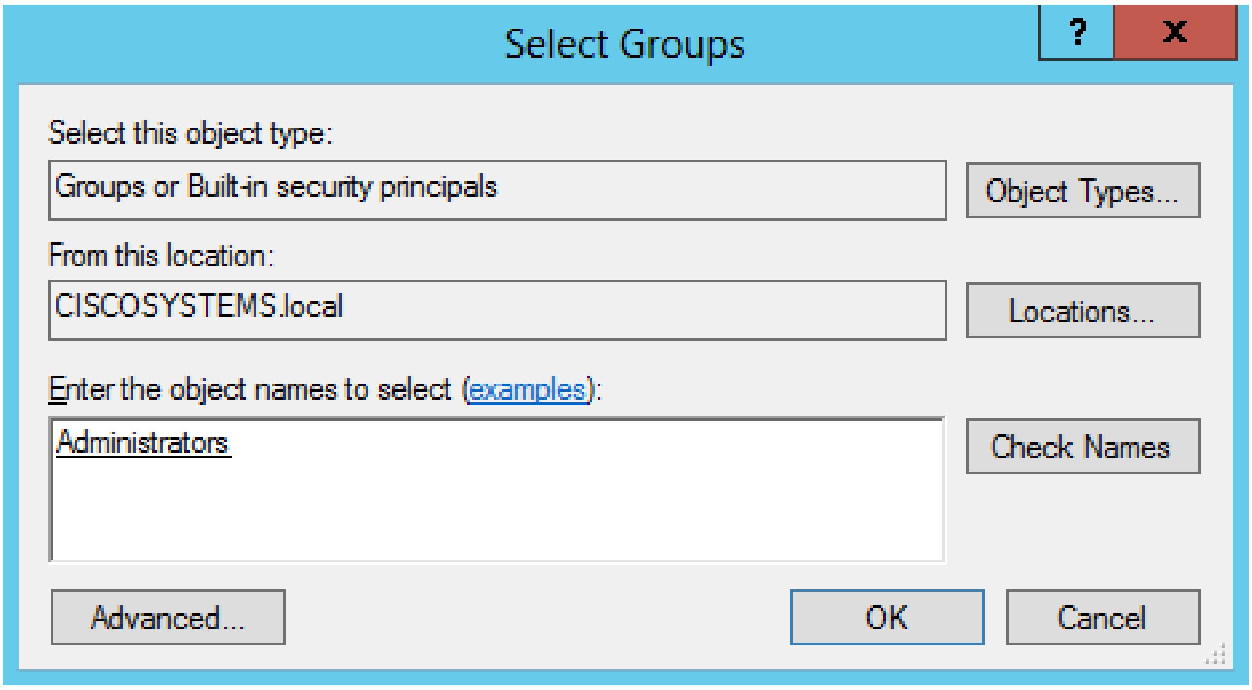
Name	Active Directory Domain Services Folder
Domain Users	CISCOSYSTEMS.local/Users

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

::

5. 单击 **Add**。在打开的对话框中，输入**Administrators**，然后单击**OK**，如图所示：



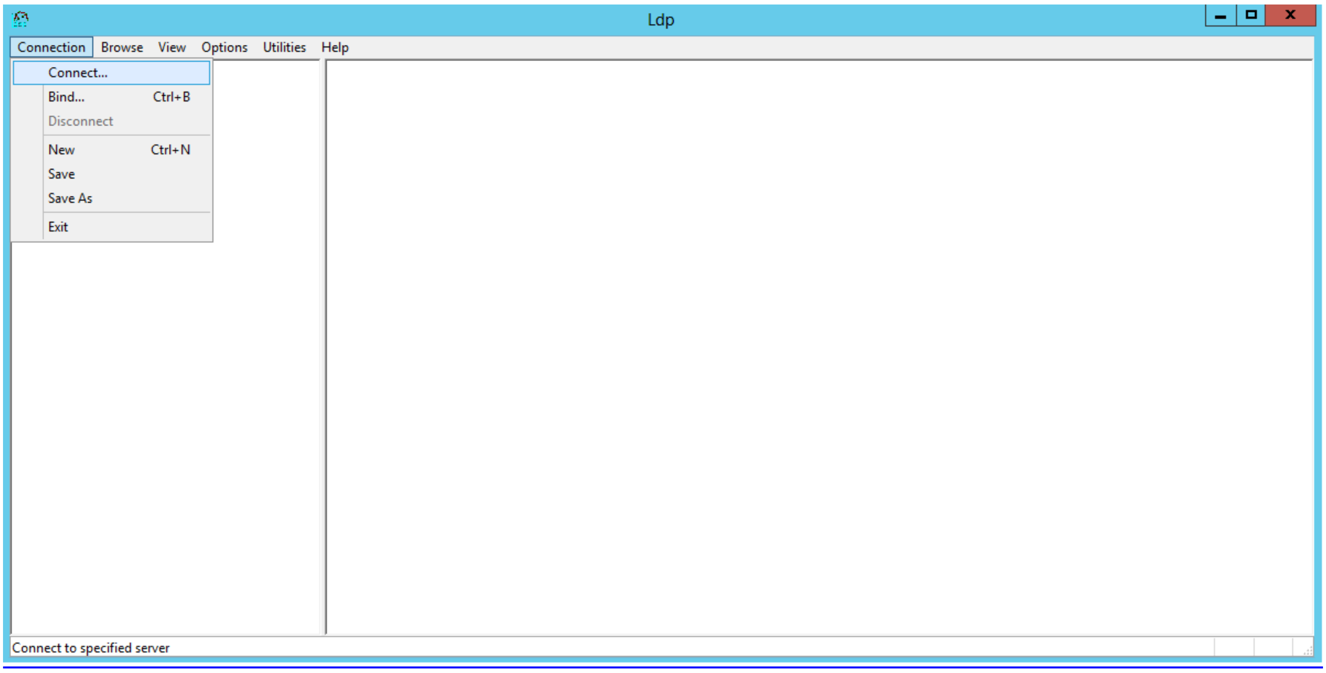
使用LDP标识用户属性

此GUI工具是一个LDAP客户端，允许用户针对任何与LDAP兼容的目录（如Active Directory）执行操作，如连接、绑定、搜索、修改、添加或删除。LDP用于查看Active Directory中存储的对象及其元数据，例如安全描述符和复制元数据。

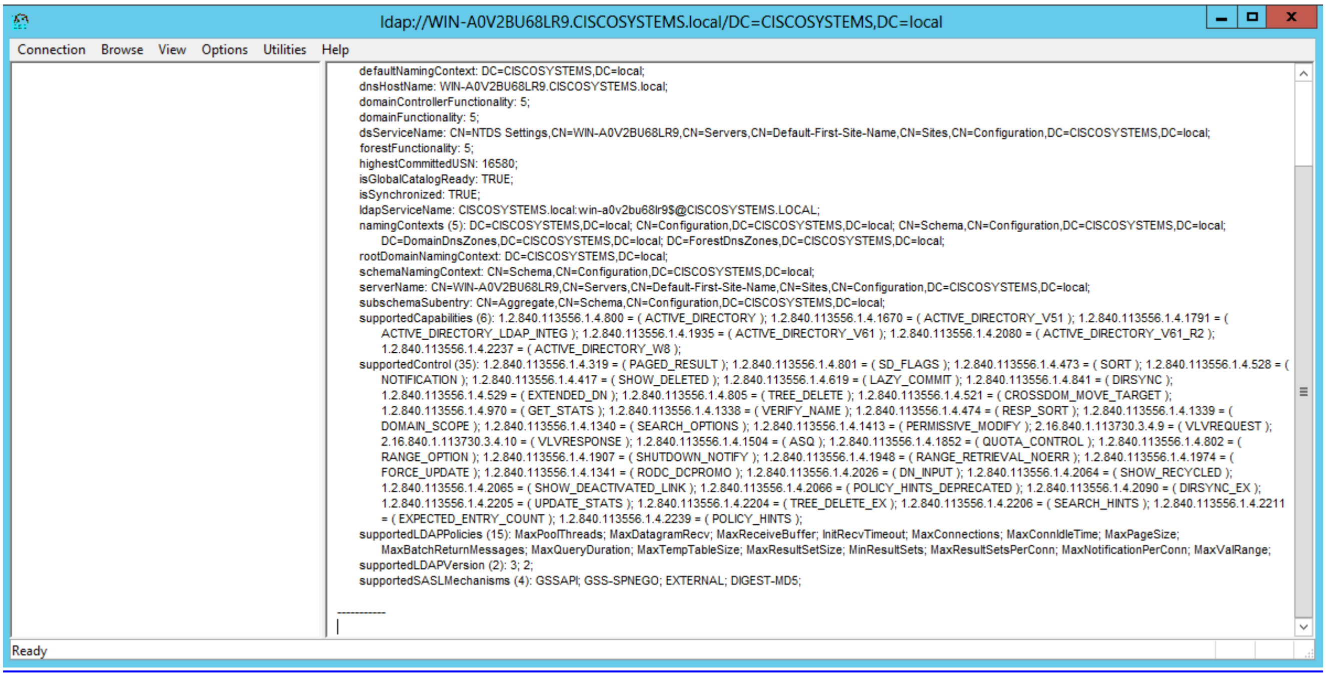
从产品CD安装Windows Server 2003支持工具时，会包括LDP GUI工具。本节介绍如何使用LDP实用程序标识与用户User1关联的特定属性。其中有些属性用于填充 WLC 上的 LDAP 服务器配置参数，例如“用户属性”类型和“用户对象”类型。

1. 在Windows 2012服务器上（即使在同一LDAP服务器上），打开Windows PowerShell并输入**LDP**以访问LDP浏览器.

2. 在LDP主窗口中，导航到**Connection > Connect**，并在输入LDAP服务器的IP地址时连接到LDAP服务器，如图所示。



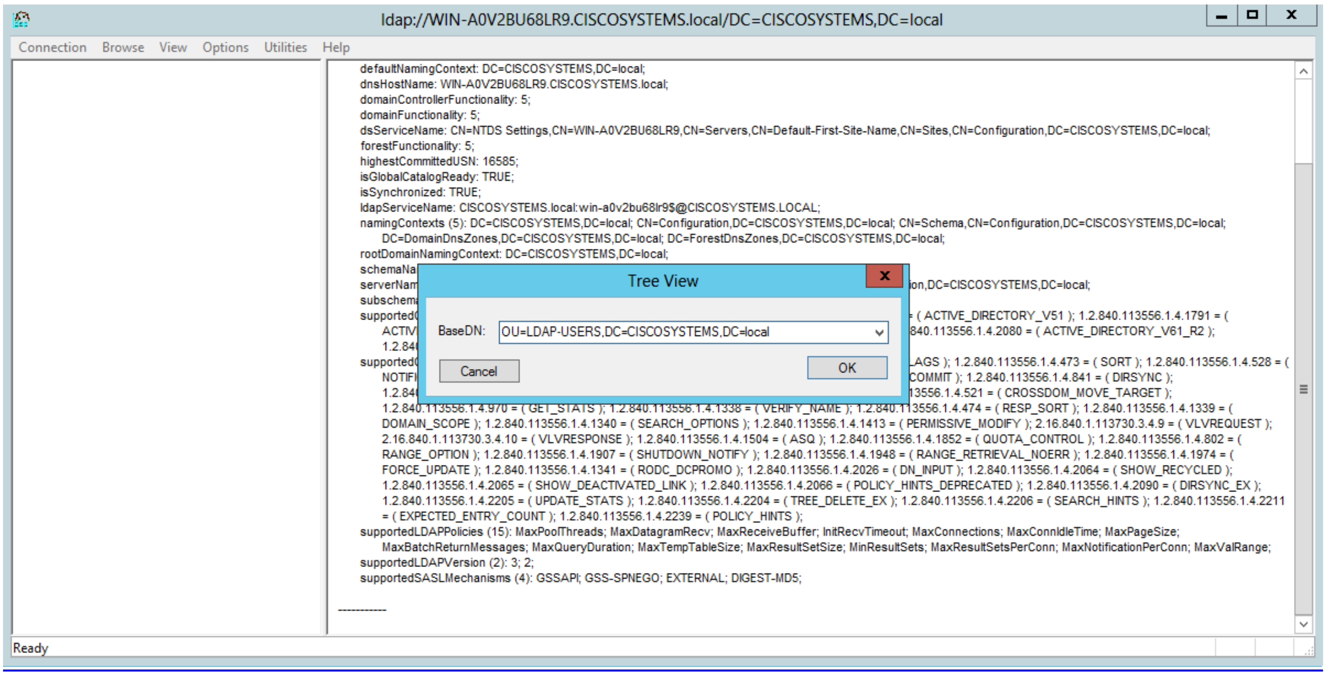
3. 连接到LDAP服务器后，从主菜单中选择**View**，然后单击**Tree**，如图所示：


ldap://WIN-A0V2BU68LR9.CISCOSYSTEMS.local/DC=CISCOSYSTEMS,DC=local
Connection
Browse
View
Options
Utilities
Help
Ready

```
defaultNamingContext: DC=CISCOSYSTEMS,DC=local;
dnsHostName: WIN-A0V2BU68LR9.CISCOSYSTEMS.local;
domainControllerFunctionality: 5;
domainFunctionality: 5;
dsServiceName: CN=NTDS Settings,CN=WIN-A0V2BU68LR9,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=CISCOSYSTEMS,DC=local;
forestFunctionality: 5;
highestCommittedUSN: 16580;
isGlobalCatalogReady: TRUE;
isSynchronized: TRUE;
ldapServiceName: CISCOSYSTEMS.local:win-a0v2bu68lr9$@CISCOSYSTEMS.LOCAL;
namingContexts (5): DC=CISCOSYSTEMS,DC=local; CN=Configuration,DC=CISCOSYSTEMS,DC=local; CN=Schema,CN=Configuration,DC=CISCOSYSTEMS,DC=local;
    DC=DomainDnsZones,DC=CISCOSYSTEMS,DC=local; DC=ForestDnsZones,DC=CISCOSYSTEMS,DC=local;
rootDomainNamingContext: DC=CISCOSYSTEMS,DC=local;
schemaNamingContext: CN=Schema,CN=Configuration,DC=CISCOSYSTEMS,DC=local;
serverName: CN=WIN-A0V2BU68LR9,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=CISCOSYSTEMS,DC=local;
subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=CISCOSYSTEMS,DC=local;
supportedCapabilities (6): 1.2.840.113556.1.4.800 = ( ACTIVE_DIRECTORY ); 1.2.840.113556.1.4.1670 = ( ACTIVE_DIRECTORY_V51 ); 1.2.840.113556.1.4.1791 = (
    ACTIVE_DIRECTORY_LDAP_INTEG ); 1.2.840.113556.1.4.1935 = ( ACTIVE_DIRECTORY_V61 ); 1.2.840.113556.1.4.2080 = ( ACTIVE_DIRECTORY_V61_R2 );
    1.2.840.113556.1.4.2237 = ( ACTIVE_DIRECTORY_W8 );
supportedControl (35): 1.2.840.113556.1.4.319 = ( PAGED_RESULT ); 1.2.840.113556.1.4.801 = ( SD_FLAGS ); 1.2.840.113556.1.4.473 = ( SORT ); 1.2.840.113556.1.4.528 = (
    NOTIFICATION ); 1.2.840.113556.1.4.417 = ( SHOW_DELETED ); 1.2.840.113556.1.4.619 = ( LAZY_COMMIT ); 1.2.840.113556.1.4.841 = ( DIRSYNC );
    1.2.840.113556.1.4.529 = ( EXTENDED_DN ); 1.2.840.113556.1.4.805 = ( TREE_DELETE ); 1.2.840.113556.1.4.521 = ( CROSSDOM_MOVE_TARGET );
    1.2.840.113556.1.4.970 = ( GET_STATS ); 1.2.840.113556.1.4.1338 = ( VERIFY_NAME ); 1.2.840.113556.1.4.474 = ( RESP_SORT ); 1.2.840.113556.1.4.1339 = (
    DOMAIN_SCOPE ); 1.2.840.113556.1.4.1340 = ( SEARCH_OPTIONS ); 1.2.840.113556.1.4.1413 = ( PERMISSIVE_MODIFY ); 2.16.840.1.113730.3.4.9 = ( VLVREQUEST );
    2.16.840.1.113730.3.4.10 = ( VLVRESPONSE ); 1.2.840.113556.1.4.1504 = ( ASQ ); 1.2.840.113556.1.4.1852 = ( QUOTA_CONTROL ); 1.2.840.113556.1.4.802 = (
    RANGE_OPTION ); 1.2.840.113556.1.4.1907 = ( SHUTDOWN_NOTIFY ); 1.2.840.113556.1.4.1948 = ( RANGE_RETRIEVAL_NOERR ); 1.2.840.113556.1.4.1974 = (
    FORCE_UPDATE ); 1.2.840.113556.1.4.1341 = ( RODC_DCPROMO ); 1.2.840.113556.1.4.2026 = ( DN_INPUT ); 1.2.840.113556.1.4.2064 = ( SHOW_RECYCLED );
    1.2.840.113556.1.4.2065 = ( SHOW_DEACTIVATED_LINK ); 1.2.840.113556.1.4.2066 = ( POLICY_HINTS_DEPRECATED ); 1.2.840.113556.1.4.2090 = ( DIRSYNC_EX );
    1.2.840.113556.1.4.2205 = ( UPDATE_STATS ); 1.2.840.113556.1.4.2204 = ( TREE_DELETE_EX ); 1.2.840.113556.1.4.2206 = ( SEARCH_HINTS ); 1.2.840.113556.1.4.2211
    = ( EXPECTED_ENTRY_COUNT ); 1.2.840.113556.1.4.2239 = ( POLICY_HINTS );
supportedLDAPPolicies (15): MaxPoolThreads; MaxDatagramRecv; MaxReceiveBuffer; InitRecvTimeout; MaxConnections; MaxConnIdleTime; MaxPageSize;
    MaxBatchReturnMessages; MaxQueryDuration; MaxTempTableSize; MaxResultSetSize; MinResultSets; MaxResultSetsPerConn; MaxNotificationPerConn; MaxValRange;
supportedLDAPVersion (2): 3; 2;
supportedSASLMechanisms (4): GSSAPI; GSS-SPNEGO; EXTERNAL; DIGEST-MD5;

-----------
```

4. 在所显示的树视图窗口中，输入用户的 BaseDN。在本示例中，User1位于域CISCOSYSTEMS.local下的OU "LDAP-USERS"下。单击**OK**，如图所示：

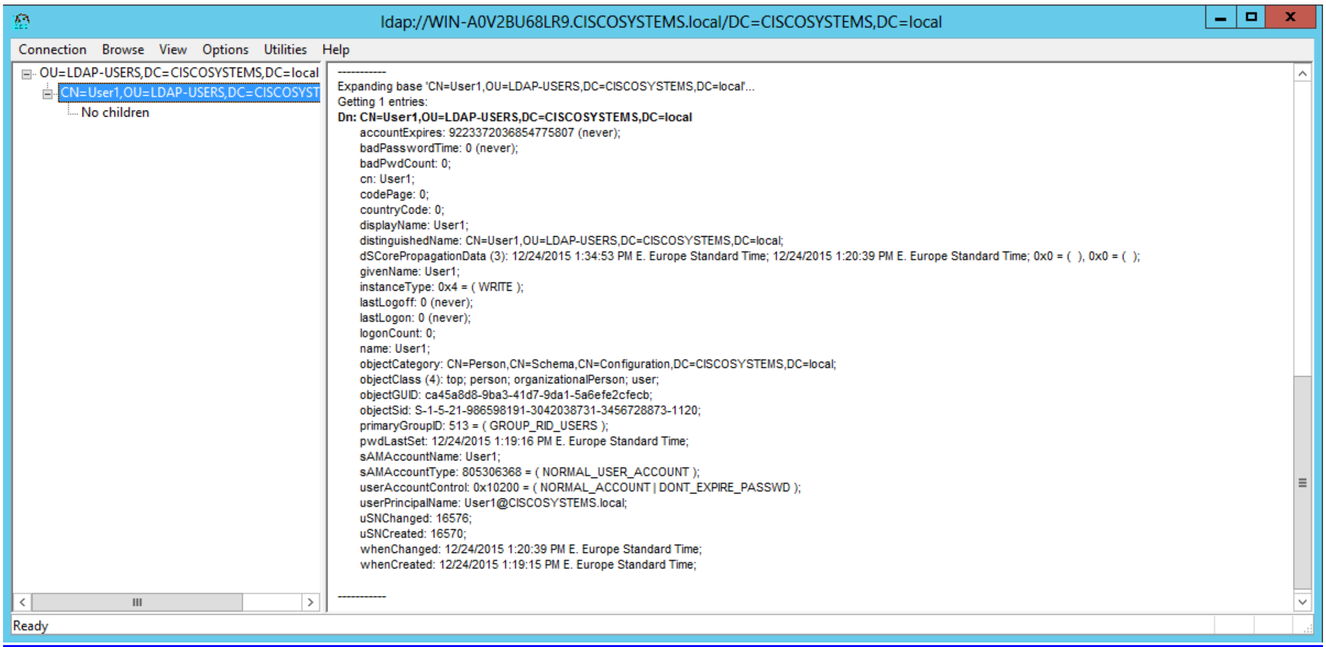

ldap://WIN-A0V2BU68LR9.CISCOSYSTEMS.local/DC=CISCOSYSTEMS,DC=local
Connection
Browse
View
Options
Utilities
Help
Tree View
Cancel
OK
Ready

BaseDN: OU=LDAP-USERS,DC=CISCOSYSTEMS,DC=local

```
defaultNamingContext: DC=CISCOSYSTEMS,DC=local;
dnsHostName: WIN-A0V2BU68LR9.CISCOSYSTEMS.local;
domainControllerFunctionality: 5;
domainFunctionality: 5;
dsServiceName: CN=NTDS Settings,CN=WIN-A0V2BU68LR9,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=CISCOSYSTEMS,DC=local;
forestFunctionality: 5;
highestCommittedUSN: 16585;
isGlobalCatalogReady: TRUE;
isSynchronized: TRUE;
ldapServiceName: CISCOSYSTEMS.local:win-a0v2bu68lr9$@CISCOSYSTEMS.LOCAL;
namingContexts (5): DC=CISCOSYSTEMS,DC=local; CN=Configuration,DC=CISCOSYSTEMS,DC=local; CN=Schema,CN=Configuration,DC=CISCOSYSTEMS,DC=local;
    DC=DomainDnsZones,DC=CISCOSYSTEMS,DC=local; DC=ForestDnsZones,DC=CISCOSYSTEMS,DC=local;
rootDomainNamingContext: DC=CISCOSYSTEMS,DC=local;
schemaNa
serverNam                                             ion,DC=CISCOSYSTEMS,DC=local;
subschem
supported                                             = ( ACTIVE_DIRECTORY_V51 ); 1.2.840.113556.1.4.1791 = (
    ACTIV                                             840.113556.1.4.2080 = ( ACTIVE_DIRECTORY_V61_R2 );
    1.2.84
supported                                             AGS ); 1.2.840.113556.1.4.473 = ( SORT ); 1.2.840.113556.1.4.528 = (
    NOTIFI                                            COMMIT ); 1.2.840.113556.1.4.841 = ( DIRSYNC );
    1.2.84                                            13556.1.4.521 = ( CROSSDOM_MOVE_TARGET );
    1.2.840.113556.1.4.970 = ( GET_STATS ); 1.2.840.113556.1.4.1338 = ( VERIFY_NAME ); 1.2.840.113556.1.4.474 = ( RESP_SORT ); 1.2.840.113556.1.4.1339 = (
    DOMAIN_SCOPE ); 1.2.840.113556.1.4.1340 = ( SEARCH_OPTIONS ); 1.2.840.113556.1.4.1413 = ( PERMISSIVE_MODIFY ); 2.16.840.1.113730.3.4.9 = ( VLVREQUEST );
    2.16.840.1.113730.3.4.10 = ( VLVRESPONSE ); 1.2.840.113556.1.4.1504 = ( ASQ ); 1.2.840.113556.1.4.1852 = ( QUOTA_CONTROL ); 1.2.840.113556.1.4.802 = (
    RANGE_OPTION ); 1.2.840.113556.1.4.1907 = ( SHUTDOWN_NOTIFY ); 1.2.840.113556.1.4.1948 = ( RANGE_RETRIEVAL_NOERR ); 1.2.840.113556.1.4.1974 = (
    FORCE_UPDATE ); 1.2.840.113556.1.4.1341 = ( RODC_DCPROMO ); 1.2.840.113556.1.4.2026 = ( DN_INPUT ); 1.2.840.113556.1.4.2064 = ( SHOW_RECYCLED );
    1.2.840.113556.1.4.2065 = ( SHOW_DEACTIVATED_LINK ); 1.2.840.113556.1.4.2066 = ( POLICY_HINTS_DEPRECATED ); 1.2.840.113556.1.4.2090 = ( DIRSYNC_EX );
    1.2.840.113556.1.4.2205 = ( UPDATE_STATS ); 1.2.840.113556.1.4.2204 = ( TREE_DELETE_EX ); 1.2.840.113556.1.4.2206 = ( SEARCH_HINTS ); 1.2.840.113556.1.4.2211
    = ( EXPECTED_ENTRY_COUNT ); 1.2.840.113556.1.4.2239 = ( POLICY_HINTS );
supportedLDAPPolicies (15): MaxPoolThreads; MaxDatagramRecv; MaxReceiveBuffer; InitRecvTimeout; MaxConnections; MaxConnIdleTime; MaxPageSize;
    MaxBatchReturnMessages; MaxQueryDuration; MaxTempTableSize; MaxResultSetSize; MinResultSets; MaxResultSetsPerConn; MaxNotificationPerConn; MaxValRange;
supportedLDAPVersion (2): 3; 2;
supportedSASLMechanisms (4): GSSAPI; GSS-SPNEGO; EXTERNAL; DIGEST-MD5;

-----------
```

5. LDP浏览器的左侧显示出现在指定BaseDN下的整个树(OU=LDAP-USERS，dc=CISCOSYSTEMS， dc=local)。展开树查找用户User1。此用户可以用代表用户名字的CN 值表示。在本示例中，它是CN=User1。双击**CN=User1**。在LDP浏览器的右侧窗格中，LDP显示与User1关联的所有属性，如图所示：


ldap://WIN-A0V2BU68LR9.CISCOSYSTEMS.local/DC=CISCOSYSTEMS,DC=local
Connection Browse View Options Utilities Help
OU=LDAP-USERS,DC=CISCOSYSTEMS,DC=local
CN=User1,OU=LDAP-USERS,DC=CISCOSYST
No children
Ready

```
-----------
Expanding base 'CN=User1,OU=LDAP-USERS,DC=CISCOSYSTEMS,DC=local'...
Getting 1 entries:
Dn: CN=User1,OU=LDAP-USERS,DC=CISCOSYSTEMS,DC=local
    accountExpires: 9223372036854775807 (never);
    badPasswordTime: 0 (never);
    badPwdCount: 0;
    cn: User1;
    codePage: 0;
    countryCode: 0;
    displayName: User1;
    distinguishedName: CN=User1,OU=LDAP-USERS,DC=CISCOSYSTEMS,DC=local;
    dSCorePropagationData (3): 12/24/2015 1:34:53 PM E. Europe Standard Time; 12/24/2015 1:20:39 PM E. Europe Standard Time; 0x0 = ( ), 0x0 = ( );
    givenName: User1;
    instanceType: 0x4 = ( WRITE );
    lastLogoff: 0 (never);
    lastLogon: 0 (never);
    logonCount: 0;
    name: User1;
    objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=CISCOSYSTEMS,DC=local;
    objectClass (4): top; person; organizationalPerson; user;
    objectGUID: ca45a8d8-9ba3-41d7-9da1-5a6efe2cfecb;
    objectSid: S-1-5-21-986598191-3042038731-3456728873-1120;
    primaryGroupID: 513 = ( GROUP_RID_USERS );
    pwdLastSet: 12/24/2015 1:19:16 PM E. Europe Standard Time;
    sAMAccountName: User1;
    sAMAccountType: 805306368 = ( NORMAL_USER_ACCOUNT );
    userAccountControl: 0x10200 = ( NORMAL_ACCOUNT | DONT_EXPIRE_PASSWD );
    userPrincipalName: User1@CISCOSYSTEMS.local;
    uSNChanged: 16576;
    uSNCreated: 16570;
    whenChanged: 12/24/2015 1:20:39 PM E. Europe Standard Time;
    whenCreated: 12/24/2015 1:19:15 PM E. Europe Standard Time;

-----------
```

6. 为LDAP服务器配置WLC时，在*User Attribute*字段中，在包含用户名的用户记录中输入属性的名称。从此LDP输出中，您可以看到sAMAccountName是包含用户名“User1”的一个属性，因此请输入与WLC上的User Attribute字段对应的sAMAccountName属性。

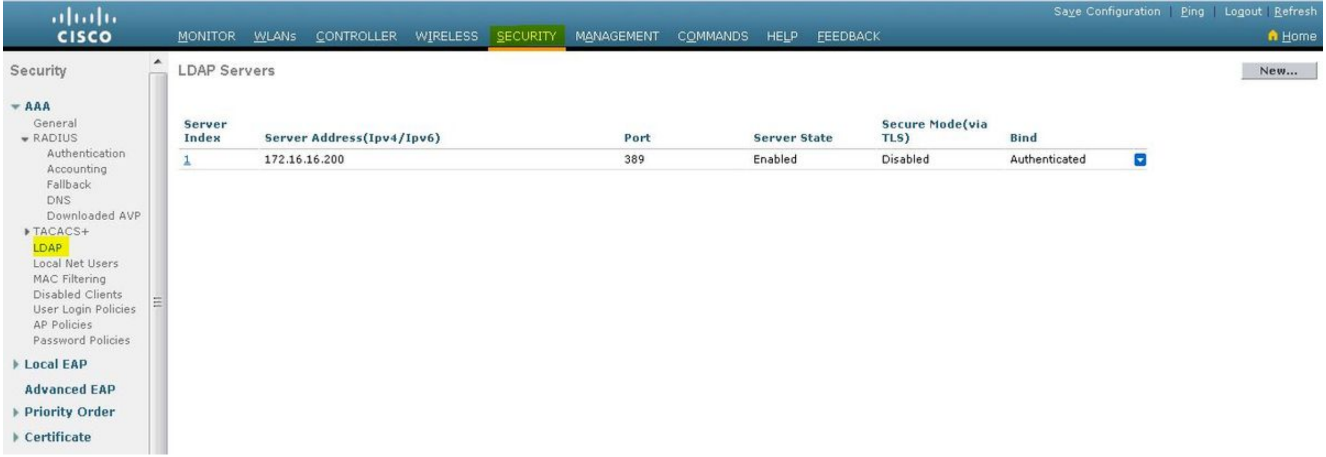
7. 为LDAP服务器配置WLC时，在*User Object Type*字段中，输入将记录标识为用户的LDAP objectType属性的值。通常，用户记录具有多个 objectType 属性值，其中有些对用户是唯一的，而另一些则与其他对象类型共享。在LDP输出中，CN=Person是将记录标识为用户的值，因此在WLC上将**Person**指定为User Object Type属性。下一步是为LDAP服务器配置WLC。

为LDAP服务器配置WLC

现在已配置LDAP服务器，下一步是使用LDAP服务器的详细信息配置WLC。在WLC GUI上完成以下步骤：

> **注**：本文档假设WLC已配置为基本操作，并且LAP已注册到WLC。如果您是希望设置WLC以便使用LAP执行基本操作的新用户，请参阅向无线局域网控制器(WLC)注册轻量AP(LAP)。

1. 在WLC的Security页面中，从左侧任务窗格中选择**AAA > LDAP**以转到LDAP服务器配置页面。



LDAP Servers

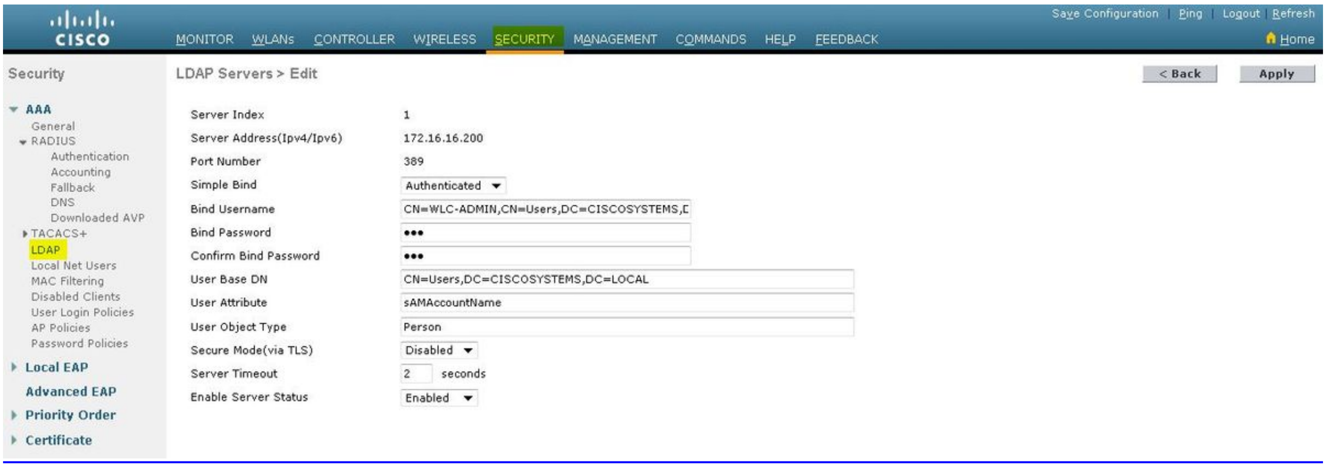
Server Index	Server Address(Ipv4/Ipv6)	Port	Server State	Secure Mode(via TLS)	Bind
1	172.16.16.200	389	Enabled	Disabled	Authenticated

要添加 LDAP 服务器，请单击 **New**。这会显示 LDAP Servers > New 页。

2. 在LDAP Servers Edit页中，指定LDAP服务器的详细信息，例如LDAP服务器的IP地址、端口号、启用服务器状态等。从 Server Index (Priority) 下拉框中选择一个数字，以便指定此服务器相对于其他任何已配置的 LDAP 服务器的优先顺序。最多可以配置 17 个服务器。如果控制

器不能到达第一个服务器，则尝试列表中的第二个服务器，依此类推。在 Server IP Address 字段中输入 LDAP 服务器的 IP 地址。在Port Number字段中输入LDAP服务器的**TCP端口号。**有效范围是 1 到 65535，默认值是 389。对于Simple bind，我们使用Authenticated作为绑定用户名，它是用于访问LDAP服务器及其密码的WLC管理员用户的位置在“User Base DN”字段中，请输入包含所有用户列表的 LDAP 服务器中的子树的可分辨名称 (DN)。例如，ou=组织单位，.ou=下一个组织单位，o=corporation.com。如果包含用户的树是基本DN，请输入o=corporation.com或dc=corporation，dc=com。在本示例中，用户位于组织单位(OU)LDAP-USERS下，而组织单位(OU)LDAP-USERS又作为lab.wireless域的一部分创建。用户基础DN必须指向用户信息（根据EAP-FAST身份验证方法的用户凭证）所在的完整路径。在本示例中，用户位于基础DN OU=LDAP-USERS， DC=CISCOSYSTEMS， DC=local下。在 User Attribute 字段中，输入包含用户名的用户记录中的属性名称。在 User Object Type 字段中，输入将记录标识为用户的 LDAP objectType 属性的值。通常，用户记录具有多个objectType属性值，其中一些值对于用户是唯一的，还有一些值与其他对象类型共享您可以使用Windows 2012支持工具中的LDAP浏览器实用程序从目录服务器获取这两个字段的值。此 Microsoft LDAP 浏览器工具称为 LDP。在此工具的帮助下，您可以了解此用户的用户基准DN、用户属性和用户对象类型字段。有关如何使用LDP了解这些用户特定属性的详细信息，请参阅本文档的*使用LDP识别用户属性*部分。在 Server Timeout 字段中，输入重新传输之间相隔的秒数。有效范围是 2 到 30 秒，默认值是 2 秒。选中 **Enable Server Status 复选框以启用此 LDAP 服务器，或者取消选中以禁用。**默认值是禁用。单击**适用做您的更改。**以下是已使用此信息配置的示例

：



LDAP Servers > Edit

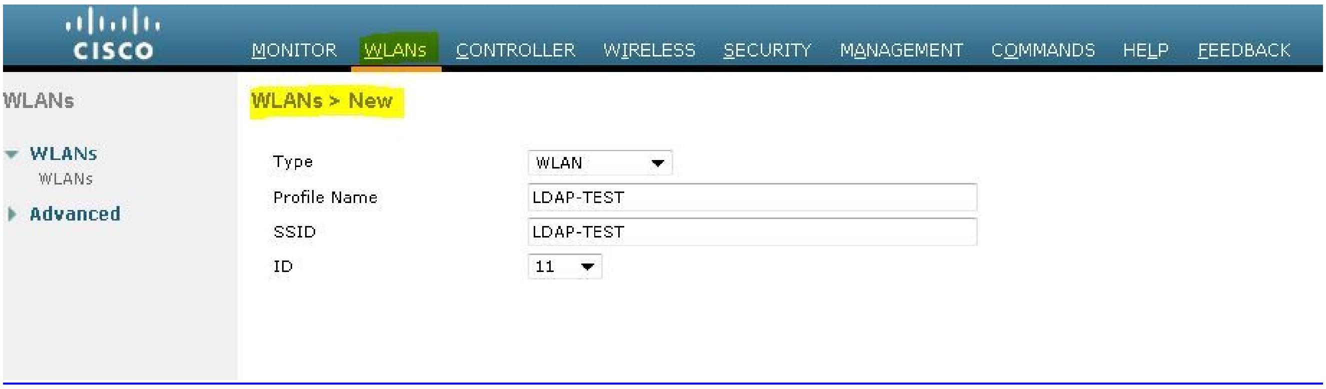
Server Index	1
Server Address(Ipv4/Ipv6)	172.16.16.200
Port Number	389
Simple Bind	Authenticated ▾
Bind Username	CN=WLC-ADMIN,CN=Users,DC=CISCOSYSTEMS,D
Bind Password	•••
Confirm Bind Password	•••
User Base DN	CN=Users,DC=CISCOSYSTEMS,DC=LOCAL
User Attribute	sAMAccountName
User Object Type	Person
Secure Mode(via TLS)	Disabled ▾
Server Timeout	2 seconds
Enable Server Status	Enabled ▾

3. 现在已在WLC上配置有关LDAP服务器的详细信息，下一步是配置用于Web身份验证的WLAN。

配置用于Web身份验证的WLAN

第一步是为用户创建WLAN。请完成以下步骤：

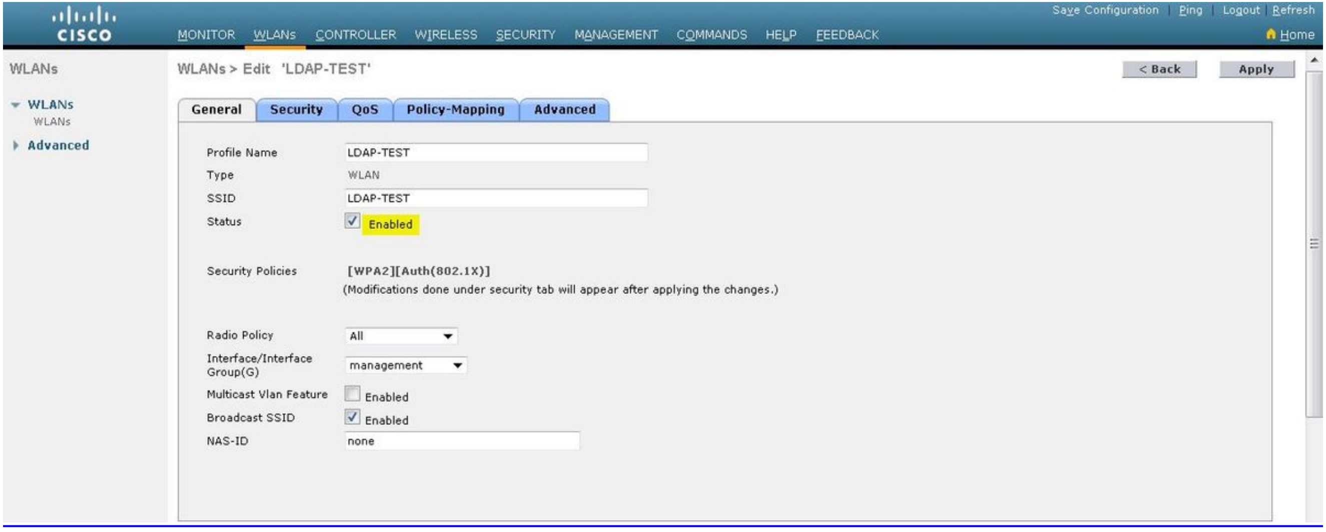
1. 要创建 WLAN，请从控制器 GUI 中单击 **WLANs。**随即显示 WLAN 窗口。该窗口列出了控制器中配置的 WLAN。
2. 要配置新的 WLAN，请单击 **New。**在本示例中，WLAN命名为Web-Auth。



WLANs > New

Type: WLAN
Profile Name: LDAP-TEST
SSID: LDAP-TEST
ID: 11

3. 单击 **Apply**。
4. 在“WLAN”>“Edit”窗口中，定义特定于该 WLAN 的参数。



WLANs > Edit 'LDAP-TEST'

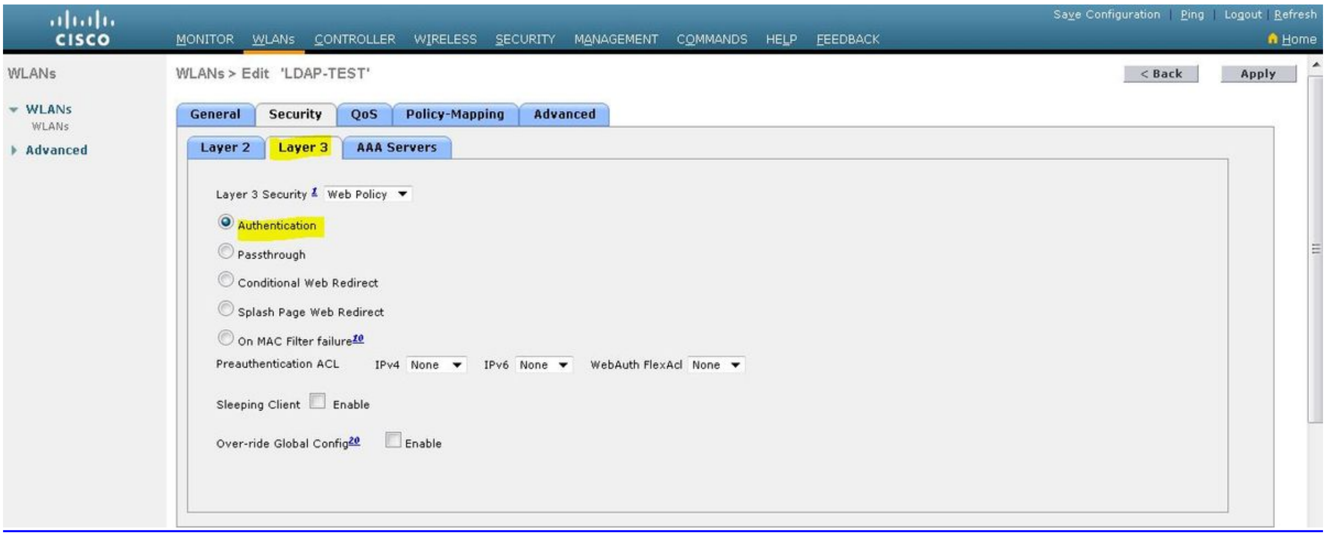
Profile Name: LDAP-TEST
Type: WLAN
SSID: LDAP-TEST
Status: ☑ Enabled

Security Policies: [WPA2][Auth(802.1X)]
(Modifications done under security tab will appear after applying the changes.)

Radio Policy: All
Interface/Interface Group(G): management
Multicast Vlan Feature: □ Enabled
Broadcast SSID: ☑ Enabled
NAS-ID: none

选中Status复选框以启用WLAN。对于 WLAN，请从“Interface Name”字段中选择相应的接口。此示例映射连接到WLAN Web-Auth的管理接口。

5. 单击“Security”选项卡。在Layer 3 Security字段中，选中**Web Policy**复选框，然后选择**Authentication**选项。

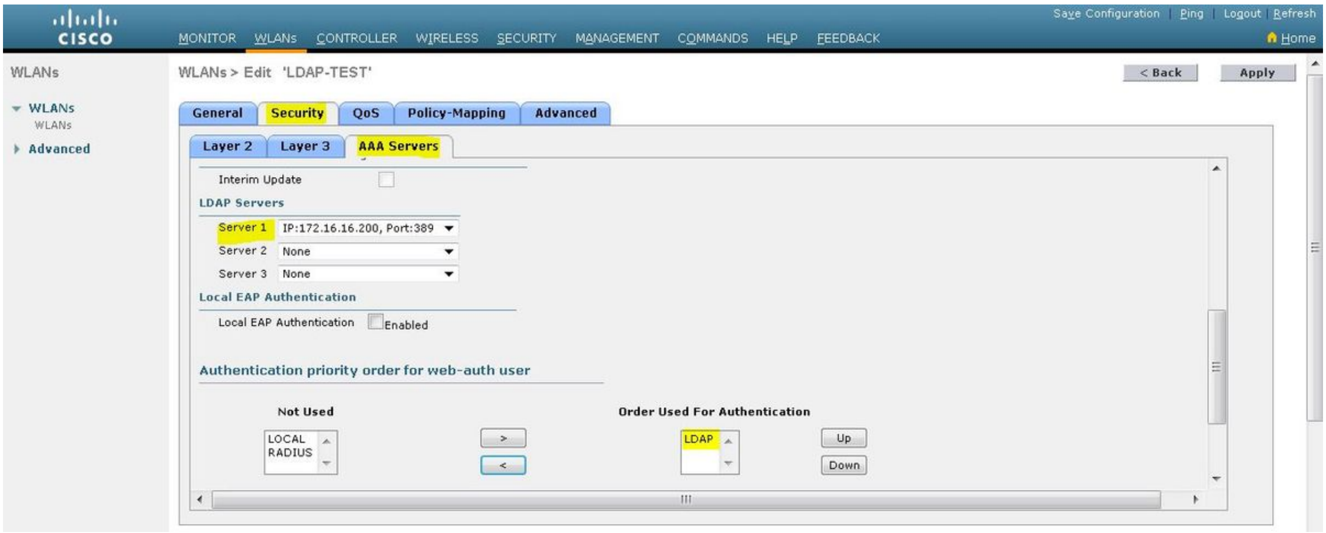


WLANs > Edit 'LDAP-TEST'

Layer 3 Security 1 Web Policy
● Authentication
○ Passthrough
○ Conditional Web Redirect
○ Splash Page Web Redirect
○ On MAC Filter failure10
Preauthentication ACL IPv4 None IPv6 None WebAuth FlexAcl None
Sleeping Client □ Enable
Over-ride Global Config20 □ Enable

之所以选择此选项，是因为使用Web身份验证对无线客户端进行身份验证。选中**Override Global Config**复选框以根据WLAN Web身份验证配置启用。从Web Auth type下拉菜单中选择相应的Web身份验证类型。此示例使用内部Web身份验证。**注意**：802.1x身份验证不支持Web身份验证。这意味着在使用 Web 身份验证时，您不能选择 802.1x 或使用 802.1x 的 WPA/WPA2 作为第 2 层安全方法。支持 Web 身份验证使用所有其他的第 2 层安全参数。

6. 单击 **AAA Servers 选项卡。**从LDAP服务器下拉菜单中选择配置的LDAP服务器。如果使用本地数据库或RADIUS服务器，可以在*Authentication priority order for web-auth userfield*下设置身份验证优先级。



WLANs > Edit 'LDAP-TEST'

Interim Update □

LDAP Servers

Server 1 IP:172.16.16.200, Port:389

Server 2 None

Server 3 None

Local EAP Authentication

Local EAP Authentication □Enabled

Authentication priority order for web-auth user

Not Used: LOCAL, RADIUS

Order Used For Authentication: LDAP

7. 单击 **Apply**。**注意**：在本示例中，未使用第2层安全方法对用户进行身份验证，因此在第2层安全(Layer 2 Security)字段中选择**无(None)。**

验证

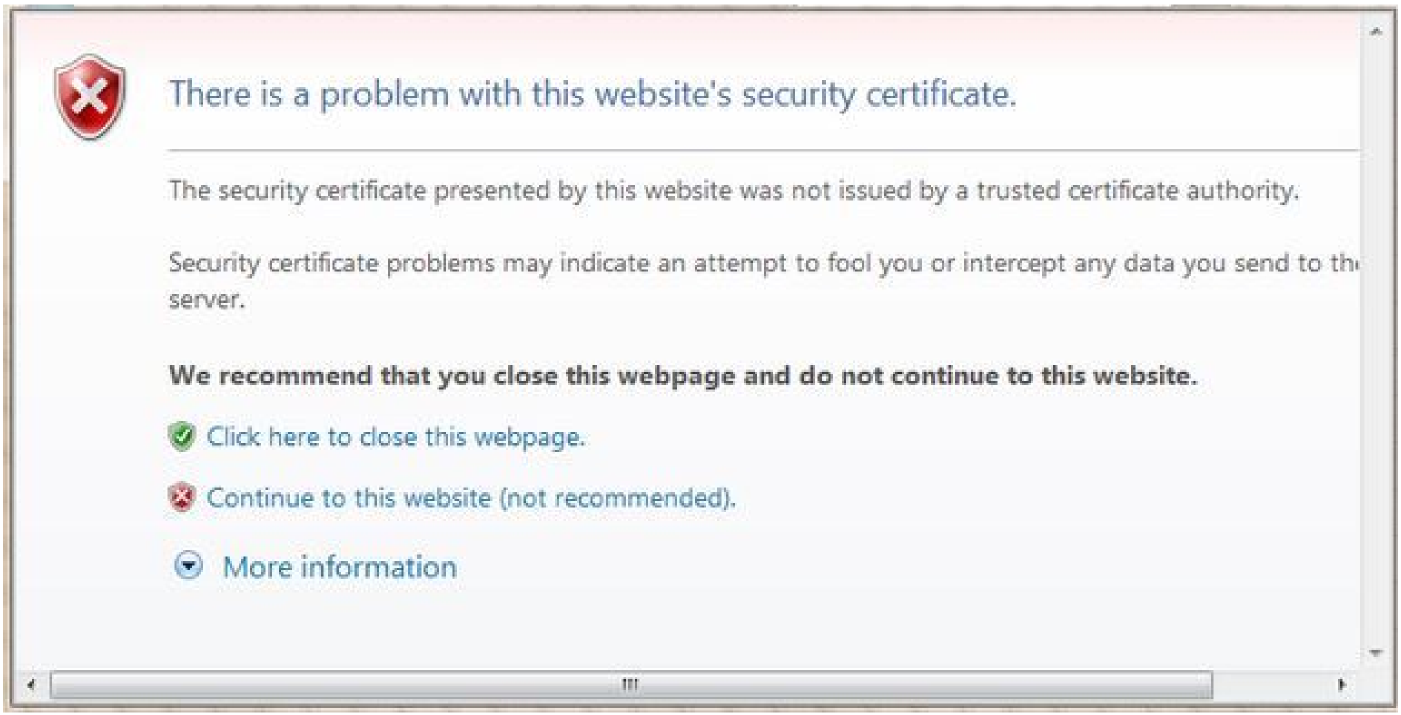
使用本部分可确认配置能否正常运行。

要验证此设置，请连接无线客户端并检查配置是否按预期工作。

无线客户端打开，用户在Web浏览器中输入www.yahoo.com等URL。由于用户尚未通过身份验证，因此WLC会将用户重定向到内部Web登录URL。

将会提示用户输入用户凭证。用户提交用户名和密码后，登录页面将接受用户凭证输入，并在提交后将请求发送回WLC Web服务器的action_URL示例http://1.1.1.1/login.html。它以输入参数形式提供给客户重定向 URL，其中 1.1.1.1 是交换机上的虚拟接口地址。

WLC根据LDAP用户数据库对用户进行身份验证。身份验证成功后，WLC Web服务器会将用户转发到配置的重定向URL或客户端启动时使用的URL，例如 www.yahoo.com。



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

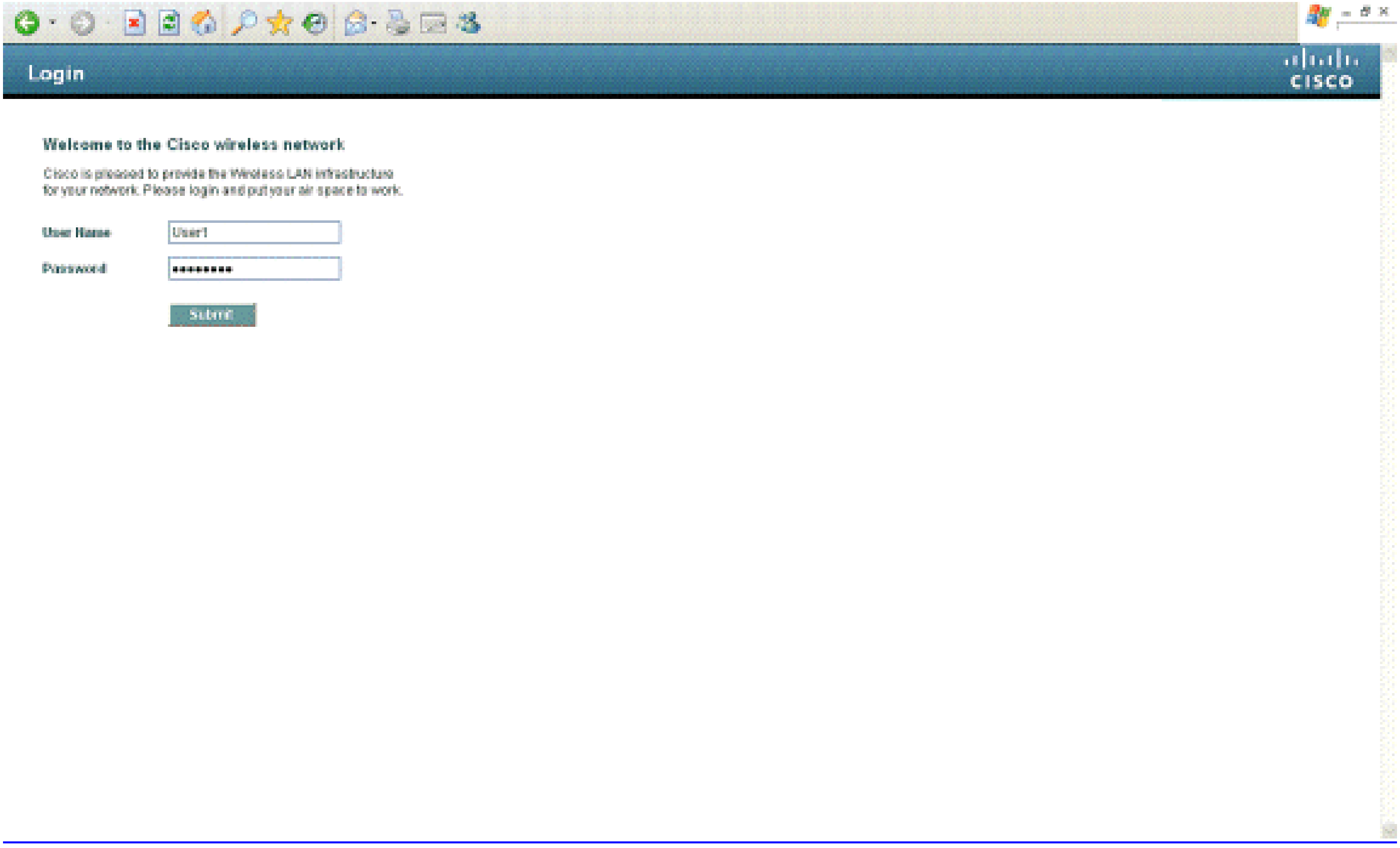
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

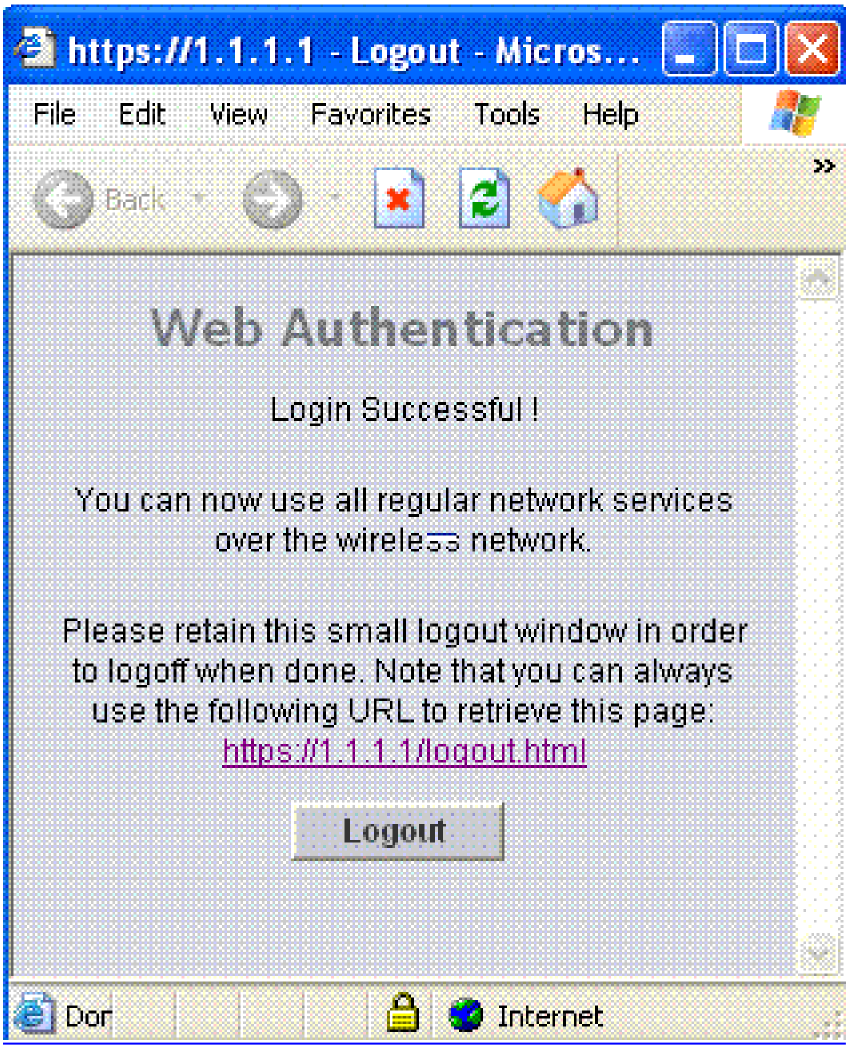


Welcome to the Cisco wireless network

Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your air space to work.

User Name: User1

Password: *********



Web Authentication

Login Successful !

You can now use all regular network services over the wireless network.

Please retain this small logout window in order to logoff when done. Note that you can always use the following URL to retrieve this page:

https://1.1.1.1/logout.html

故障排除

本部分提供的信息可用于对配置进行故障排除。

使用以下命令排除配置故障：

- **debug mac addr** <client-MAC-address xx:xx:xx:xx:xx:xx>
- **debug aaa all enable**
- **debug pem state enable**
- **debug pem events enable**
- **debug dhcp message enable**
- **debug dhcp packet enable**

以下是**debug mac addr cc:fa:00:f7:32:35**命令的输出示例

debug aaa ldap enable

```
(Cisco_Controller) >*pemReceiveTask: Dec 24 03:45:23.089: cc:fa:00:f7:32:35 Sent an XID frame
*apfMsConnTask_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 Processing assoc-req
station:cc:fa:00:f7:32:35 AP:00:23:eb:e5:04:10-01 thread:18ec9330
*apfMsConnTask_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 Association received from mobile on
BSSID 00:23:eb:e5:04:1f AP AP1142-1
*apfMsConnTask_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 Global 200 Clients are allowed to AP
radio

*apfMsConnTask_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 Max Client Trap Threshold: 0  cur: 1

*apfMsConnTask_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 Rf profile 600 Clients are allowed to
AP wlan

*apfMsConnTask_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 override for default ap group, marking
intgrp NULL
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Applying Interface policy on Mobile,
role Local. Ms NAC State 2 Quarantine Vlan 0 Access Vlan 16

*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Re-applying interface policy for client

*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Changing
IPv4 ACL 'none' (ACL ID 255) ===> 'none' (ACL ID 255) --- (caller apf_policy.c:2699)
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Changing
IPv6 ACL 'none' (ACL ID 255) ===> 'none' (ACL ID 255) --- (caller apf_policy.c:2720)
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 apfApplyWlanPolicy: Apply WLAN Policy
over PMIPv6 Client Mobility Type, Tunnel User - 0
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 In processSsidIE:6246 setting Central
switched to TRUE
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 In processSsidIE:6249 apVapId = 1 and
Split Acl Id = 65535
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Applying site-specific Local Bridging
override for station cc:fa:00:f7:32:35 - vapId 1, site 'default-group', interface 'management'
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Applying Local Bridging Interface
Policy for station cc:fa:00:f7:32:35 - vlan 16, interface id 0, interface 'management'
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 processSsidIE  statusCode is 0 and
status is 0
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 processSsidIE  ssid_done_flag is 0
finish_flag is 0
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 STA - rates (3): 24 164 48 0 0 0 0 0 0
0 0 0 0 0 0 0
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 suppRates  statusCode is 0 and
```

```
gotSuppRatesElement is 1
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 AID 2 in Assoc Req from flex AP
00:23:eb:e5:04:10 is same as in mscb cc:fa:00:f7:32:35
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 apfMs1xStateDec
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Change
state to START (0) last state WEBAUTH_REQD (8)

*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 pemApfAddMobileStation2:
APF_MS_PEM_WAIT_L2_AUTH_COMPLETE = 0.
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 START (0) Initializing
policy
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 START (0) Change state to
AUTHCHECK (2) last state START (0)

*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 AUTHCHECK (2) Change
state to L2AUTHCOMPLETE (4) last state AUTHCHECK (2)

*pemReceiveTask: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 Removed NPU entry.
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Not Using WMM Compliance code qosCap 00
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 L2AUTHCOMPLETE (4)
Plumbed mobile LWAPP rule on AP 00:23:eb:e5:04:10 vapId 1 apVapId 1 flex-acl-name:
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 L2AUTHCOMPLETE (4) Change
state to WEBAUTH_REQD (8) last state L2AUTHCOMPLETE (4)

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8)
pemApfAddMobileStation2 3802, Adding TMP rule
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Adding
Fast Path rule
 type = Airespace AP Client - ACL passthru
 on AP 00:23:eb:e5:04:10, slot 1, interface = 1, QOS = 0
 IPv4 ACL I
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast
Path rule (contd...) 802.1P = 0, DSCP = 0, TokenID = 15206, IntfId = 0  Local Bridging Vlan =
16, Local Bridging intf id = 0
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast
Path rule (contd...) AVC Ratelimit:  AppID = 0 ,AppAction = 4, AppToken = 15206  AverageRate =
0, BurstRate = 0

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast
Path rule (contd...) AVC Ratelimit:  AppID = 0 ,AppAction = 4, AppToken = 15206  AverageRate =
0, BurstRate = 0

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast
Path rule (contd...) AVC Ratelimit:  AppID = 0 ,AppAction = 4, AppToken = 15206  AverageRate =
0, BurstRate = 0

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8)
Successfully plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8)
pemApfAddMobileStation2 3911, Adding TMP rule
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8)
Replacing Fast Path rule
 type = Airespace AP Client - ACL passthru
 on AP 00:23:eb:e5:04:10, slot 1, interface = 1, QOS = 0
 IPv4 AC
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast
Path rule (contd...) 802.1P = 0, DSCP = 0, TokenID = 15206, IntfId = 0  Local Bridging Vlan =
16, Local Bridging intf id = 0
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast
Path rule (contd...) AVC Ratelimit:  AppID = 0 ,AppAction = 4, AppToken = 15206  AverageRate =
0, BurstRate = 0

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast
Path rule (contd...) AVC Ratelimit:  AppID = 0 ,AppAction = 4, AppToken = 15206  AverageRate =
0, BurstRate = 0

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast
Path rule (contd...) AVC Ratelimit:  AppID = 0 ,AppAction = 4, AppToken = 15206  AverageRate =
0, BurstRate = 0

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8)
Successfully plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 apfPemAddUser2 (apf_policy.c:359)
Changing state for mobile cc:fa:00:f7:32:35 on AP 00:23:eb:e5:04:10 from Associated to
Associated

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 apfPemAddUser2:session timeout
forstation cc:fa:00:f7:32:35 - Session Tout 1800, apfMsTimeOut '1800' and sessionTimerRunning
flag is  1
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 Scheduling deletion of Mobile Station:
(callerId: 49) in 1800 seconds
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 Func: apfPemAddUser2, Ms Timeout =
1800, Session Timeout = 1800

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 Sending assoc-resp with status 0
station:cc:fa:00:f7:32:35 AP:00:23:eb:e5:04:10-01 on apVapId 1
*apfMsConnTask_1: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 Sending Assoc Response to station on
BSSID 00:23:eb:e5:04:1f (status 0) ApVapId 1 Slot 1
*apfMsConnTask_1: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 apfProcessAssocReq (apf_80211.c:10187)
Changing state for mobile cc:fa:00:f7:32:35 on AP 00:23:eb:e5:04:10 from Associated to
Associated

*pemReceiveTask: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 172.16.16.122 Added NPU entry of type 2,
dtlFlags 0x0
*pemReceiveTask: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 Sent an XID frame
*pemReceiveTask: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 172.16.16.122 Added NPU entry of type 2,
dtlFlags 0x0
*pemReceiveTask: Dec 24 03:45:43.558: cc:fa:00:f7:32:35 Sent an XID frame
*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP received op BOOTREQUEST (1) (len
322,vlan 16, port 1, encap 0xec03, xid 0x62743488)
*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP (encap type 0xec03) mstype
0ff:ff:ff:ff:ff:ff
*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP selecting relay 1 - control block
settings:
                       dhcpServer: 172.16.16.25, dhcpNetmask: 255.255.254.0,
                       dhcpGateway: 172.16.16.1, dhcpRelay: 172.16.16.25  VLAN: 16
*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP mscbVapLocalAddr=172.16.16.25
mscbVapLocalNetMask= 255.255.254.0 mscbdhcpRelay=172.16.16.25
*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP selected relay 1 - 172.16.16.25
(local address 172.16.16.25, gateway 172.16.16.25, VLAN 16, port 1)
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selecting relay 2 - control block
settings:
                       dhcpServer: 172.16.16.25, dhcpNetmask: 255.255.254.0,
                       dhcpGateway: 172.16.16.1, dhcpRelay: 172.16.16.25  VLAN: 16
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selected relay 2 - NONE
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selecting relay 1 - control block
settings:
                       dhcpServer: 172.16.16.25, dhcpNetmask: 0.0.0.0,
                       dhcpGateway: 0.0.0.0, dhcpRelay: 172.16.16.25  VLAN: 16
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP mscbVapLocalAddr=172.16.16.25
mscbVapLocalNetMask= 255.255.254.0 mscbdhcpRelay=172.16.16.25
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selected relay 1 - 172.16.16.25
(local address 172.16.16.25, gateway 172.16.16.25, VLAN 16, port 1)
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP transmitting DHCP DISCOVER (1)
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP   op: BOOTREQUEST, htype:
Ethernet, hlen: 6, hops: 1
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP   xid: 0x62743488 (1651782792),
secs: 0, flags: 0
```

```
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP   chaddr: cc:fa:00:f7:32:35
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP   ciaddr: 0.0.0.0,  yiaddr:
0.0.0.0
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP   siaddr: 0.0.0.0,  giaddr:
172.16.16.25
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selecting relay 2 - control block
settings:
                       dhcpServer: 172.16.16.25, dhcpNetmask: 0.0.0.0,
                       dhcpGateway: 0.0.0.0, dhcpRelay: 172.16.16.25  VLAN: 16
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selected relay 2 - NONE
*DHCP Proxy Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP received op BOOTREPLY (2) (len
572,vlan 0, port 0, encap 0x0, xid 0x62743488)
*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP sending REPLY to STA (len 418,
port 1, vlan 16)
*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP transmitting DHCP OFFER (2)
*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP   op: BOOTREPLY, htype: Ethernet,
hlen: 6, hops: 0
*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP   xid: 0x62743488 (1651782792),
secs: 0, flags: 0
*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP   chaddr: cc:fa:00:f7:32:35
*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP   ciaddr: 0.0.0.0,  yiaddr:
172.16.16.122
*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP   siaddr: 0.0.0.0,  giaddr:
0.0.0.0
*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP   server id: 1.1.1.1  rcvd server
id: 172.16.16.25
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP received op BOOTREQUEST (1) (len
334,vlan 16, port 1, encap 0xec03, xid 0x62743488)
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP (encap type 0xec03) mstype
0ff:ff:ff:ff:ff:ff
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP selecting relay 1 - control block
settings:
                       dhcpServer: 172.16.16.25, dhcpNetmask: 0.0.0.0,
                       dhcpGateway: 0.0.0.0, dhcpRelay: 172.16.16.25  VLAN: 16
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP mscbVapLocalAddr=172.16.16.25
mscbVapLocalNetMask= 255.255.254.0 mscbdhcpRelay=172.16.16.25
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP selected relay 1 - 172.16.16.25
(local address 172.16.16.25, gateway 172.16.16.25, VLAN 16, port 1)
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP transmitting DHCP REQUEST (3)
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP   op: BOOTREQUEST, htype:
Ethernet, hlen: 6, hops: 1
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP   xid: 0x62743488 (1651782792),
secs: 0, flags: 0
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP   chaddr: cc:fa:00:f7:32:35
*DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP   ciaddr: 0.0.0.0,  yiaddr:
0.0.0.0
*DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP   siaddr: 0.0.0.0,  giaddr:
172.16.16.25
*DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP   requested ip: 172.16.16.122
*DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP   server id: 172.16.16.25  rcvd
server id: 1.1.1.1
*DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP selecting relay 2 - control block
settings:
                       dhcpServer: 172.16.16.25, dhcpNetmask: 0.0.0.0,
                       dhcpGateway: 0.0.0.0, dhcpRelay: 172.16.16.25  VLAN: 16
*DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP selected relay 2 - NONE
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP received op BOOTREPLY (2) (len
572,vlan 0, port 0, encap 0x0, xid 0x62743488)
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP setting server from ACK
(mscb=0x40e64b88 ip=0xac10107a)(server 172.16.16.25, yiaddr 172.16.16.122)
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP sending REPLY to STA (len 418,
port 1, vlan 16)
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP transmitting DHCP ACK (5)
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP   op: BOOTREPLY, htype: Ethernet,
hlen: 6, hops: 0
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP   xid: 0x62743488 (1651782792),
secs: 0, flags: 0
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP   chaddr: cc:fa:00:f7:32:35
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP   ciaddr: 0.0.0.0,  yiaddr:
172.16.16.122
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP   siaddr: 0.0.0.0,  giaddr:
0.0.0.0
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP   server id: 1.1.1.1  rcvd server
id: 172.16.16.25
*ewmwebWebauth1: Dec 24 03:46:01.222: cc:fa:00:f7:32:35 Username entry (User1) created for
mobile, length = 7
*ewmwebWebauth1: Dec 24 03:46:01.222: cc:fa:00:f7:32:35 Username entry (User1) created in mscb
for mobile, length = 7
*aaaQueueReader: Dec 24 03:46:01.222: AuthenticationRequest: 0x2b6bdc3c


*aaaQueueReader: Dec 24 03:46:01.222:   Callback....................................0x12088c50

*aaaQueueReader: Dec 24 03:46:01.222:   protocolType................................0x00000002

*aaaQueueReader: Dec 24 03:46:01.222:
proxyState..................................CC:FA:00:F7:32:35-00:00

*aaaQueueReader: Dec 24 03:46:01.222:   Packet contains 15 AVPs (not shown)

*LDAP DB Task 1: Dec 24 03:46:01.222: ldapTask [1] received msg 'REQUEST' (2) in state 'IDLE'
(1)
*LDAP DB Task 1: Dec 24 03:46:01.222: LDAP server 1 changed state to INIT
*LDAP DB Task 1: Dec 24 03:46:01.223: LDAP_OPT_REFERRALS = -1

*LDAP DB Task 1: Dec 24 03:46:01.223: ldapInitAndBind [1] called lcapi_init (rc = 0 - Success)
*LDAP DB Task 1: Dec 24 03:46:01.225: ldapInitAndBind [1] configured Method Authenticated
lcapi_bind (rc = 0 - Success)
*LDAP DB Task 1: Dec 24 03:46:01.225: LDAP server 1 changed state to CONNECTED
*LDAP DB Task 1: Dec 24 03:46:01.225: disabled LDAP_OPT_REFERRALS

*LDAP DB Task 1: Dec 24 03:46:01.225: LDAP_CLIENT: UID Search
(base=CN=Users,DC=CISCOSYSTEMS,DC=local, pattern=(&(objectclass=Person)(sAMAccountName=User1)))
*LDAP DB Task 1: Dec 24 03:46:01.226: LDAP_CLIENT: ldap_search_ext_s returns 0 -5
*LDAP DB Task 1: Dec 24 03:46:01.226: LDAP_CLIENT: Returned 2 msgs including 0 references
*LDAP DB Task 1: Dec 24 03:46:01.226: LDAP_CLIENT: Returned msg 1 type 0x64
*LDAP DB Task 1: Dec 24 03:46:01.226: LDAP_CLIENT: Received 1 attributes in search entry msg
*LDAP DB Task 1: Dec 24 03:46:01.226: LDAP_CLIENT: Returned msg 2 type 0x65
*LDAP DB Task 1: Dec 24 03:46:01.226: LDAP_CLIENT : No matched DN
*LDAP DB Task 1: Dec 24 03:46:01.226: LDAP_CLIENT : Check result error 0 rc 1013
*LDAP DB Task 1: Dec 24 03:46:01.226: LDAP_CLIENT: Received no referrals in search result msg
*LDAP DB Task 1: Dec 24 03:46:01.226: ldapAuthRequest [1] 172.16.16.200 - 389 called lcapi_query
base="CN=Users,DC=CISCOSYSTEMS,DC=local" type="Person" attr="sAMAccountName" user="User1" (rc =
0 - Success)
*LDAP DB Task 1: Dec 24 03:46:01.226: Attempting user bind with username
CN=User1,CN=Users,DC=CISCOSYSTEMS,DC=local
*LDAP DB Task 1: Dec 24 03:46:01.228: LDAP ATTR> dn = CN=User1,CN=Users,DC=CISCOSYSTEMS,DC=local
(size 45)
*LDAP DB Task 1: Dec 24 03:46:01.228: Handling LDAP response Success
*LDAP DB Task 1: Dec 24 03:46:01.228: Authenticated bind : Closing the binded session

*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Change
state to WEBAUTH_NOL3SEC (14) last state WEBAUTH_REQD (8)

*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 apfMsRunStateInc
*LDAP DB Task 1: Dec 24 03:46:01.228: ldapClose [1] called lcapi_close (rc = 0 - Success)
*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_NOL3SEC (14)
Change state to RUN (20) last state WEBAUTH_NOL3SEC (14)
```

```
*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 Stopping deletion of Mobile Station:
(callerId: 74)
*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 Setting Session Timeout to 1800 sec -
starting session timer for the mobile
*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Reached
PLUMBFASTPATH: from line 6972
*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Replacing Fast
Path rule
 type = Airespace AP Client
 on AP 00:23:eb:e5:04:10, slot 1, interface = 1, QOS = 0
 IPv4 ACL ID = 255, IPv6 ACL ID
*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Fast Path rule
(contd...) 802.1P = 0, DSCP = 0, TokenID = 15206, IntfId = 0  Local Bridging Vlan = 16, Local
Bridging intf id = 0
*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Fast Path rule
(contd...) AVC Ratelimit:  AppID = 0 ,AppAction = 4, AppToken = 15206  AverageRate = 0,
BurstRate = 0

*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Fast Path rule
(contd...) AVC Ratelimit:  AppID = 0 ,AppAction = 4, AppToken = 15206  AverageRate = 0,
BurstRate = 0

*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Fast Path rule
(contd...) AVC Ratelimit:  AppID = 0 ,AppAction = 4, AppToken = 15206  AverageRate = 0,
BurstRate = 0

*ewmwebWebauth1: Dec 24 03:46:01.229: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Successfully
plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
*pemReceiveTask: Dec 24 03:46:01.229: cc:fa:00:f7:32:35 172.16.16.122 Added NPU entry of type 1,
dtlFlags 0x0


(Cisco_Controller) >show client detail cc:fa:00:f7:32:35
Client MAC Address............................... cc:fa:00:f7:32:35
Client Username ................................. User1
AP MAC Address................................... 00:23:eb:e5:04:10
AP Name.......................................... AP1142-1
AP radio slot Id................................. 1
Client State..................................... Associated
Client User Group................................ User1
Client NAC OOB State............................. Access
Wireless LAN Id.................................. 1
Wireless LAN Network Name (SSID)................. LDAP-TEST
Wireless LAN Profile Name........................ LDAP-TEST
Hotspot (802.11u)................................ Not Supported
BSSID............................................ 00:23:eb:e5:04:1f
Connected For ................................... 37 secs
Channel.......................................... 36
IP Address....................................... 172.16.16.122
Gateway Address.................................. 172.16.16.1
Netmask.......................................... 255.255.254.0
Association Id................................... 2
Authentication Algorithm......................... Open System
Reason Code...................................... 1
Status Code...................................... 0

--More or (q)uit current module or <ctrl-z> to abort
Session Timeout.................................. 1800
Client CCX version............................... No CCX support
QoS Level........................................ Silver
Avg data Rate.................................... 0
Burst data Rate.................................. 0
Avg Real time data Rate.......................... 0
```

```
Burst Real Time data Rate........................ 0
802.1P Priority Tag.............................. disabled
CTS Security Group Tag........................... Not Applicable
KTS CAC Capability............................... No
Qos Map Capability............................... No
WMM Support...................................... Enabled
 APSD ACs.......................................  BK  BE  VI  VO
Current Rate..................................... m7
Supported Rates.................................. 12.0,18.0,24.0
Mobility State................................... Local
Mobility Move Count.............................. 0
Security Policy Completed........................ Yes
Policy Manager State............................. RUN
Audit Session ID................................. ac10101900000005567b69f8
AAA Role Type.................................... none
Local Policy Applied............................. none
IPv4 ACL Name.................................... none

--More or (q)uit current module or <ctrl-z> to abort
FlexConnect ACL Applied Status................... Unavailable
IPv4 ACL Applied Status.......................... Unavailable
IPv6 ACL Name.................................... none
IPv6 ACL Applied Status.......................... Unavailable
Layer2 ACL Name.................................. none
Layer2 ACL Applied Status........................ Unavailable
Client Type...................................... SimpleIP
mDNS Status...................................... Enabled
mDNS Profile Name................................ default-mdns-profile
No. of mDNS Services Advertised.................. 0
Policy Type...................................... N/A
Encryption Cipher................................ None
Protected Management Frame ...................... No
Management Frame Protection...................... No
EAP Type......................................... Unknown
FlexConnect Data Switching....................... Central
FlexConnect Dhcp Status.......................... Central
FlexConnect Vlan Based Central Switching......... No
FlexConnect Authentication....................... Central
FlexConnect Central Association.................. No
Interface........................................ management
VLAN............................................. 16
Quarantine VLAN.................................. 0

--More or (q)uit current module or <ctrl-z> to abort
Access VLAN...................................... 16
Local Bridging VLAN.............................. 16
Client Capabilities:
     CF Pollable................................ Not implemented
     CF Poll Request............................ Not implemented
     Short Preamble............................. Not implemented
     PBCC....................................... Not implemented
     Channel Agility............................ Not implemented
     Listen Interval............................ 10
     Fast BSS Transition........................ Not implemented
     11v BSS Transition......................... Not implemented
Client Wifi Direct Capabilities:
     WFD capable................................ No
     Manged WFD capable......................... No
     Cross Connection Capable................... No
     Support Concurrent Operation............... No
Fast BSS Transition Details:
Client Statistics:
     Number of Bytes Received................... 16853
     Number of Bytes Sent....................... 31839
     Total Number of Bytes Sent................ 31839
     Total Number of Bytes Recv................ 16853
     Number of Bytes Sent (last 90s)........... 31839

--More or (q)uit current module or <ctrl-z> to abort
     Number of Bytes Recv (last 90s)........... 16853
     Number of Packets Received................ 146
     Number of Packets Sent.................... 92
     Number of Interim-Update Sent............. 0
     Number of EAP Id Request Msg Timeouts...... 0
     Number of EAP Id Request Msg Failures...... 0
     Number of EAP Request Msg Timeouts......... 0
     Number of EAP Request Msg Failures......... 0
     Number of EAP Key Msg Timeouts............. 0
     Number of EAP Key Msg Failures............. 0
     Number of Data Retries.................... 2
     Number of RTS Retries..................... 0
     Number of Duplicate Received Packets....... 0
     Number of Decrypt Failed Packets........... 0
     Number of Mic Failured Packets............. 0
     Number of Mic Missing Packets.............. 0
     Number of RA Packets Dropped............... 0
     Number of Policy Errors.................... 0
     Radio Signal Strength Indicator............ -48 dBm
     Signal to Noise Ratio..................... 41 dB
Client Rate Limiting Statistics:
     Number of Data Packets Received........... 0
     Number of Data Rx Packets Dropped.......... 0

--More or (q)uit current module or <ctrl-z> to abort
     Number of Data Bytes Received............. 0
     Number of Data Rx Bytes Dropped........... 0
     Number of Realtime Packets Received........ 0
     Number of Realtime Rx Packets Dropped...... 0
     Number of Realtime Bytes Received.......... 0
     Number of Realtime Rx Bytes Dropped........ 0
     Number of Data Packets Sent............... 0
     Number of Data Tx Packets Dropped.......... 0
     Number of Data Bytes Sent................. 0
     Number of Data Tx Bytes Dropped........... 0
     Number of Realtime Packets Sent........... 0
     Number of Realtime Tx Packets Dropped...... 0
     Number of Realtime Bytes Sent............. 0
     Number of Realtime Tx Bytes Dropped........ 0
Nearby AP Statistics:
     AP1142-1(slot 0)
       antenna0: 25 secs ago.................... -37 dBm
       antenna1: 25 secs ago.................... -37 dBm
     AP1142-1(slot 1)
       antenna0: 25 secs ago.................... -44 dBm
       antenna1: 25 secs ago.................... -57 dBm
DNS Server details:
     DNS server IP ............................ 0.0.0.0

--More or (q)uit current module or <ctrl-z> to abort
     DNS server IP ............................ 0.0.0.0
Assisted Roaming Prediction List details:



Client Dhcp Required:     False
```

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）。