

为安全LDAP (LDAPS)配置CUCM

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[验证和安装LDAPS证书](#)

[配置Secure LDAP目录](#)

[配置安全LDAP身份验证](#)

[为UC服务配置与AD的安全连接](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文档介绍从非安全LDAP连接更新到安全LDAPS连接的CUCM连接AD的过程。

先决条件

要求

Cisco 建议您了解以下主题：

- AD LDAP服务器
- CUCM LDAP配置
- CUCM IM & Presence服务(IM/P)

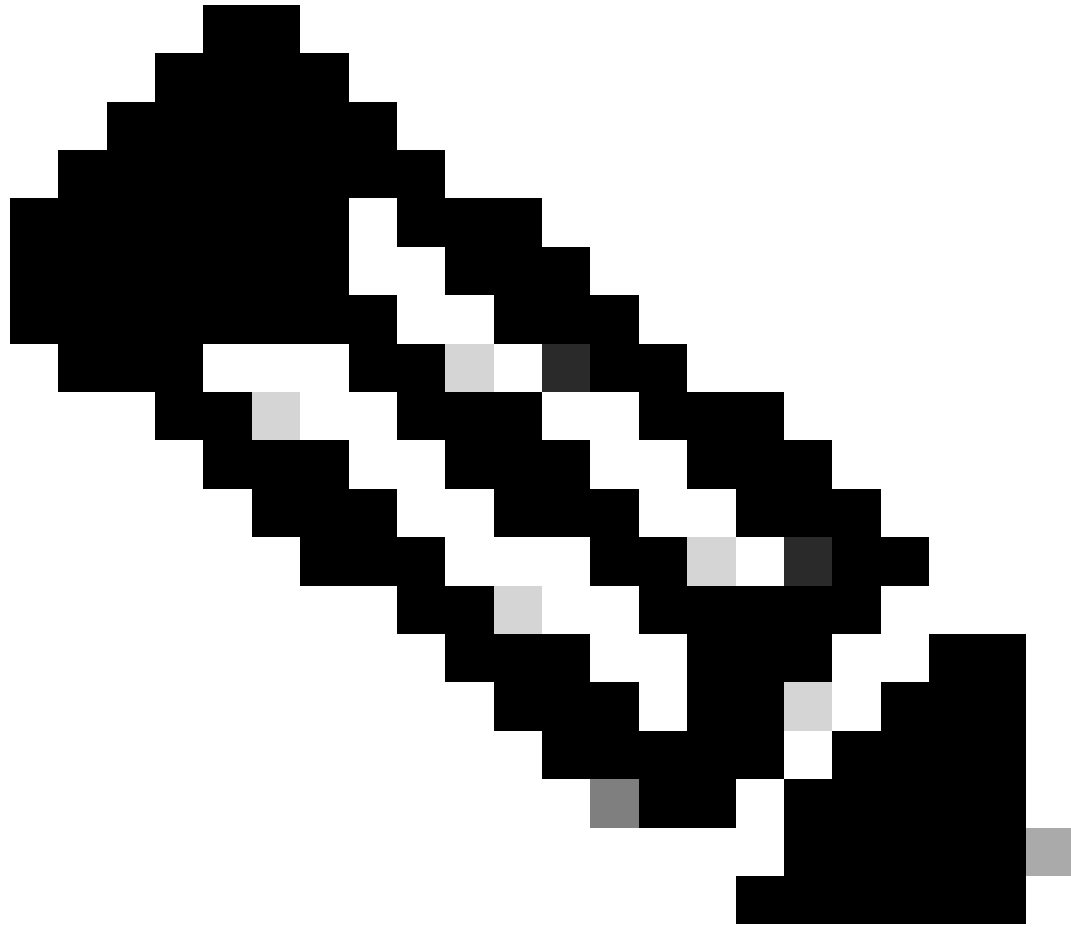
使用的组件

本文档中的信息基于CUCM版本9.x及更高版本。

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。

背景信息

Active Directory (AD)管理员负责为轻型目录访问协议(LDAPS)配置AD轻型目录访问协议(LDAP)。这包括安装符合LDAPS证书要求的CA签名证书。

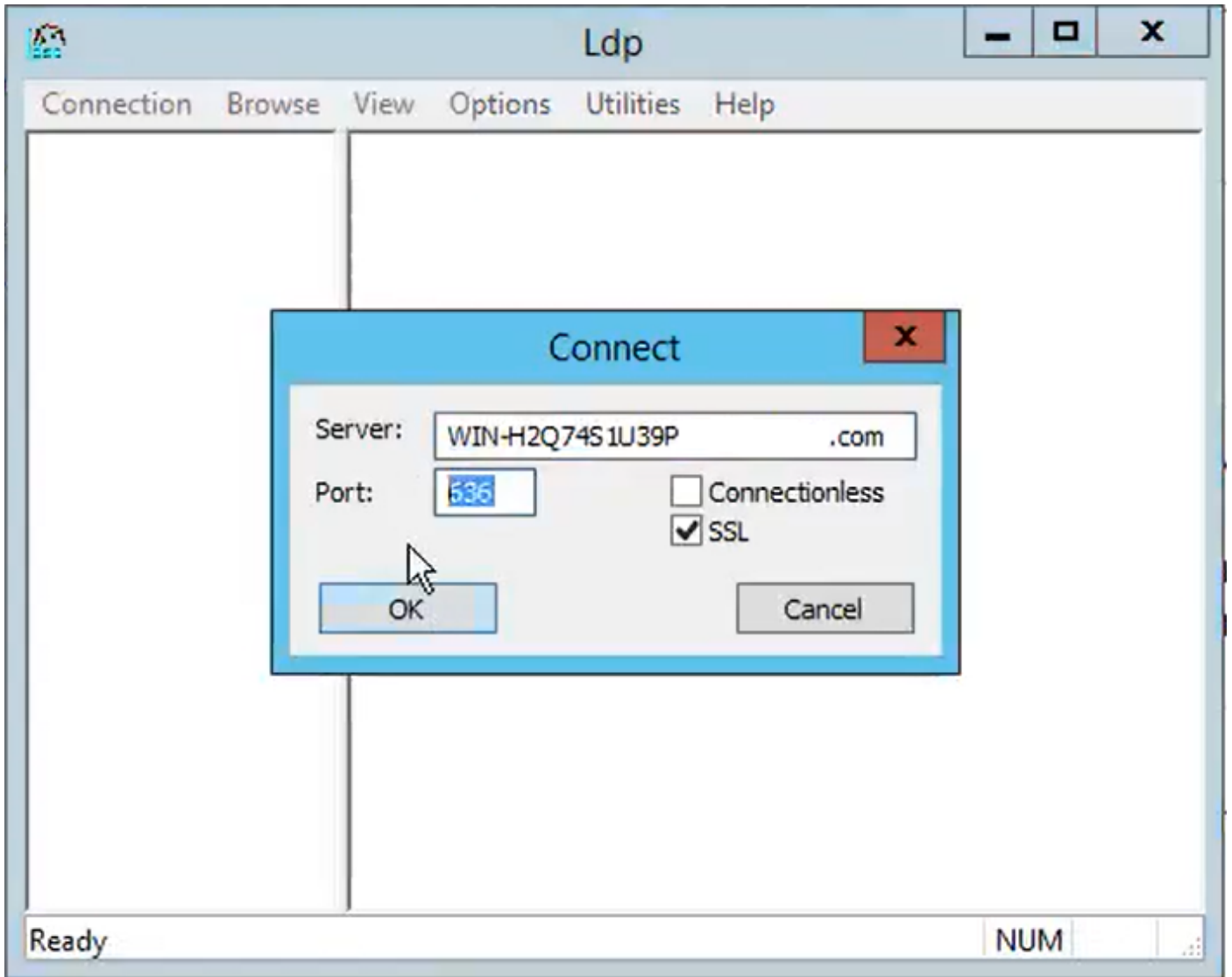


注意：有关从非安全LDAP更新以保护LDAP到AD的连接以用于其他思科协作应用的信息，请参阅以下链接：[软件建议：对于Active Directory连接，安全LDAP是必需的](#)

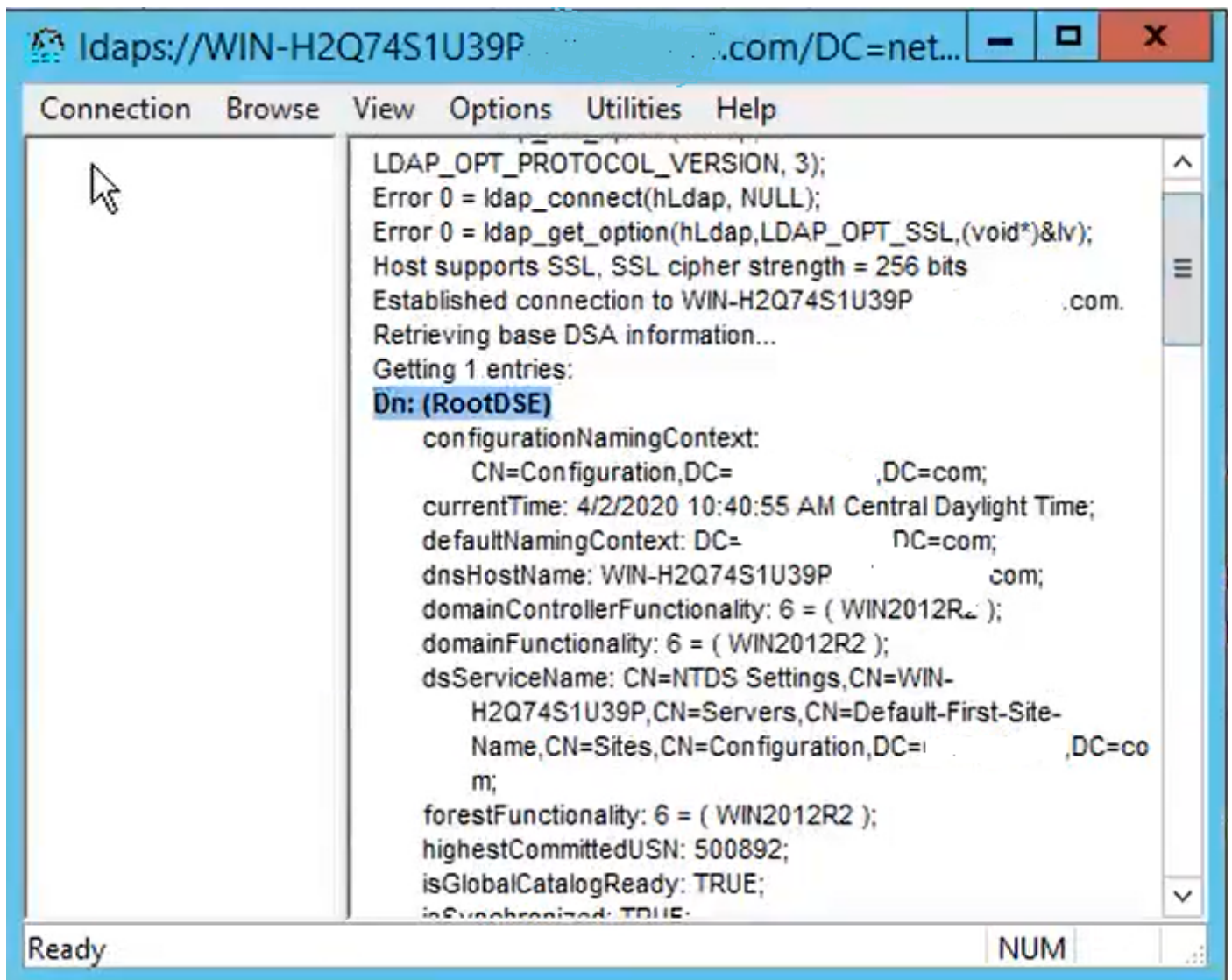
验证和安装LDAPS证书

步骤1:将LDAPS证书上传到AD服务器之后，请使用ldp.exe工具验证是否已在AD服务器上启用LDAPS。

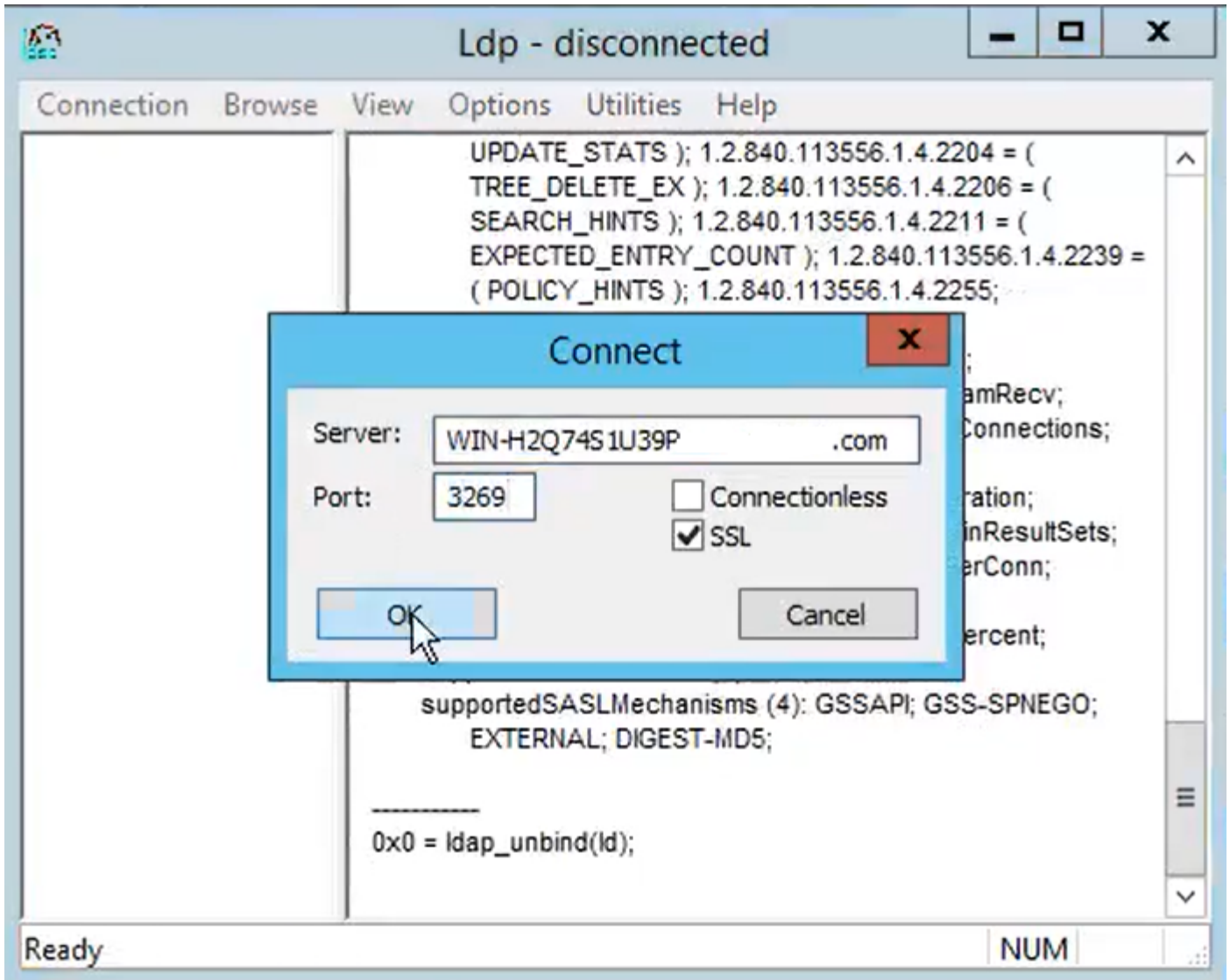
1. 在AD服务器上启动AD管理工具(Ldp.exe)。
2. 在“Connection”菜单上，选择Connect。
3. 输入LDAPS服务器的完全限定域名(FQDN)作为服务器。
4. 输入636作为端口号。
5. 单击OK，如图所示



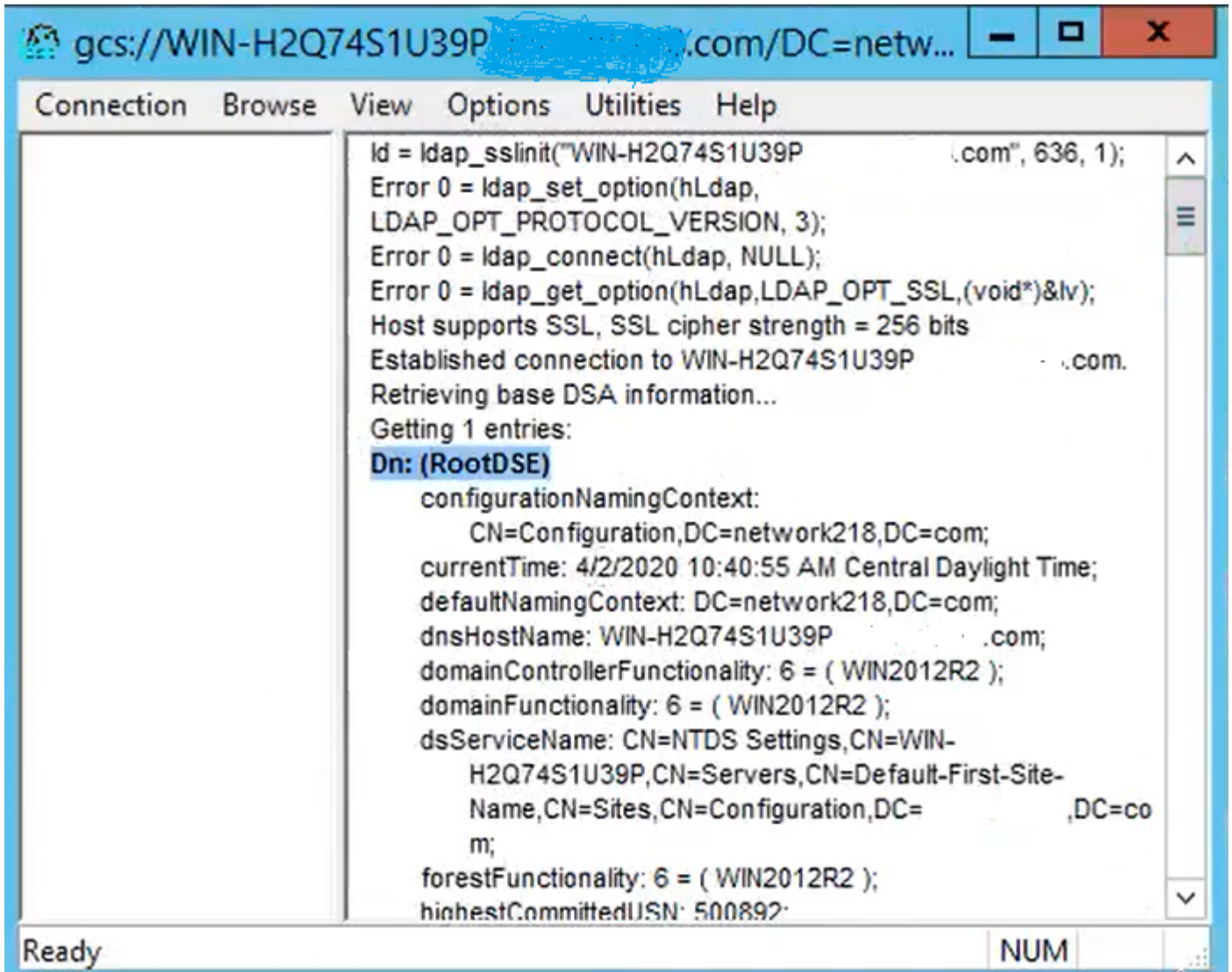
对于端口636上的成功连接，RootDSE信息会打印在右窗格中，如图所示：



对端口3269重复上述步骤，如图所示：

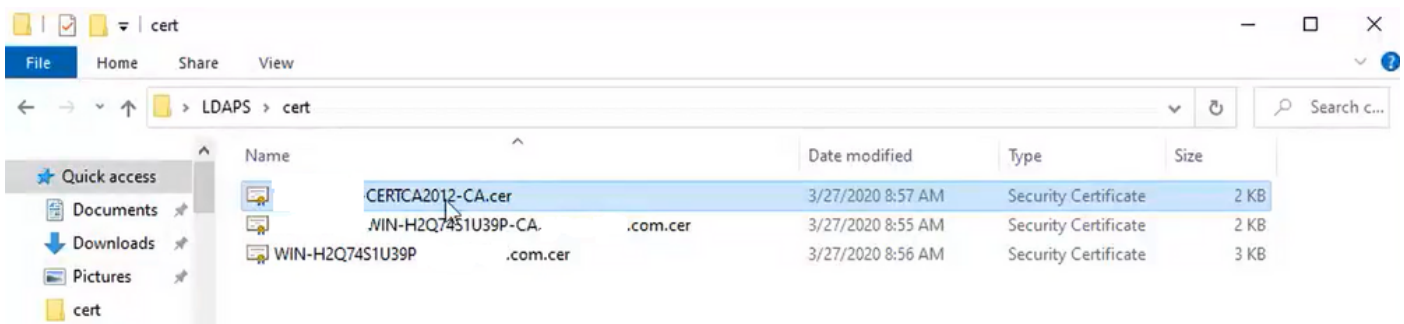


要在端口3269上成功连接，RootDSE信息会打印在右窗格中，如图所示：

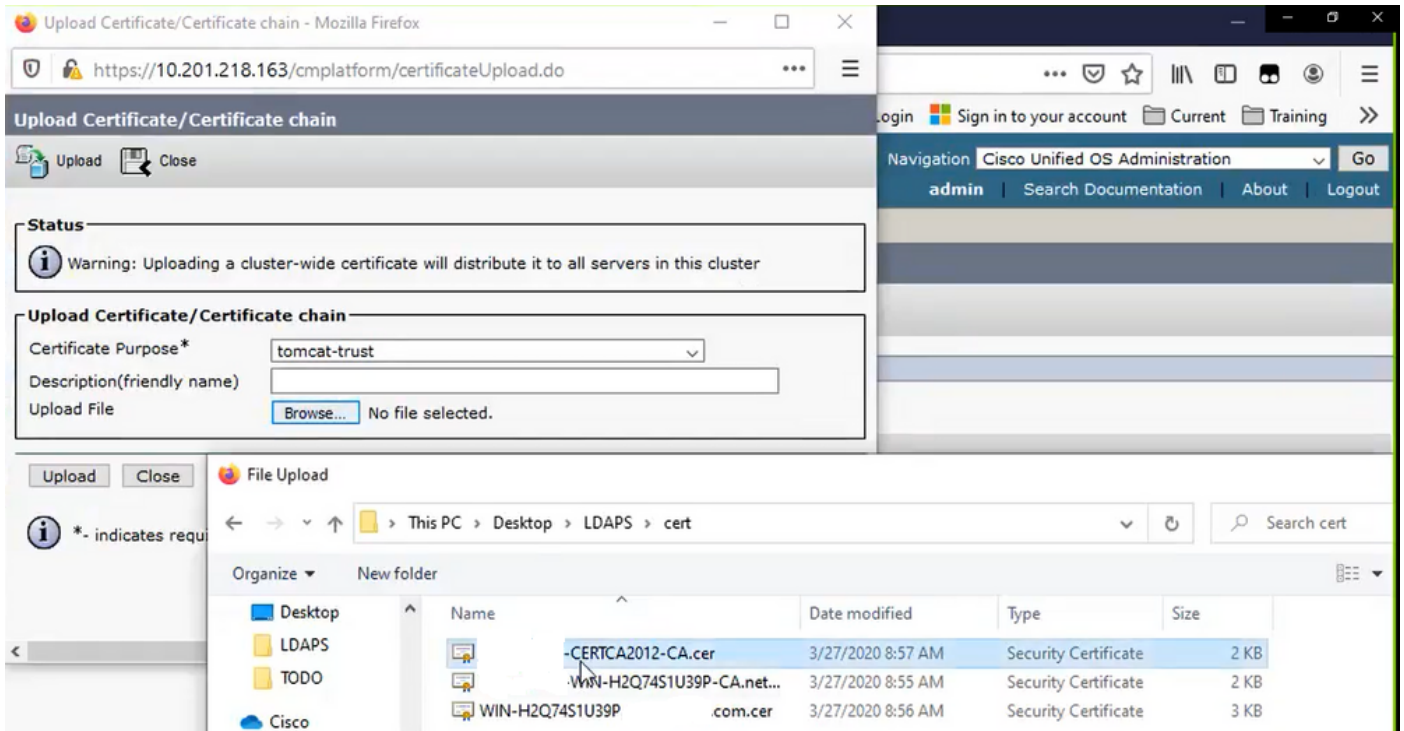


第二步：获取作为LDAPS服务器证书一部分的根证书和任何中间证书，并将这些证书作为tomcat-trust证书安装在每个CUCM和IM/P发布方节点上，作为CallManager-trust安装在CUCM发布方节点上。

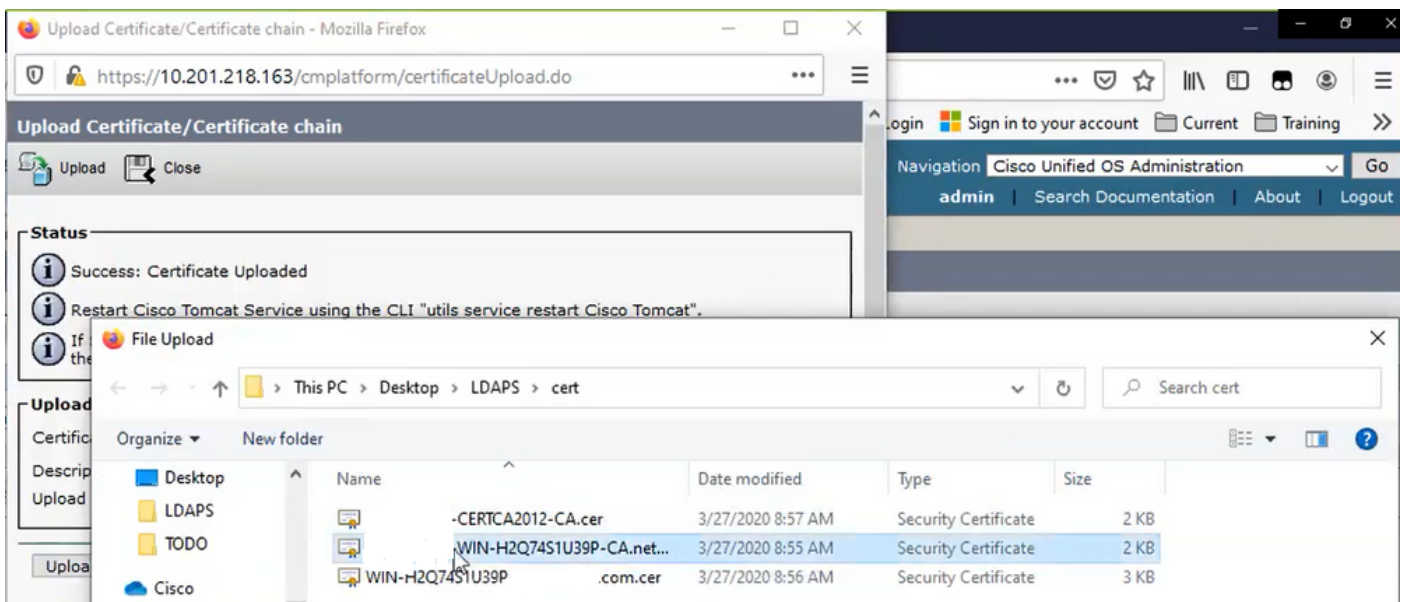
LDAPS服务器证书<hostname>.<Domain>.cer中的根证书和中间证书如下图所示：



导航到CUCM Publisher Cisco Unified OS Administration > Security > Certificate Management。将根桥上传为tomcat-trust（如图所示）和CallManager-trust（未显示）：



将中间上传为tomcat-trust (如图所示) 和CallManager-trust (未显示) :



注意：如果您的IM/P服务器是CUCM集群的一部分，则还需要将这些证书上传到这些IM/P服务器。

注意：作为替代方法，您可以将LDAPS服务器证书安装为tomcat-trust。

第三步：从集群中每个节点 (CUCM和IM/P) 的CLI重新启动Cisco Tomcat。此外，对于CUCM集群，请验证发布方节点上的思科DirSync服务是否已启动。

要重新启动Tomcat服务，您需要为每个节点打开一个CLI会话并运行命令utils service restart Cisco Tomcat，如图所示：

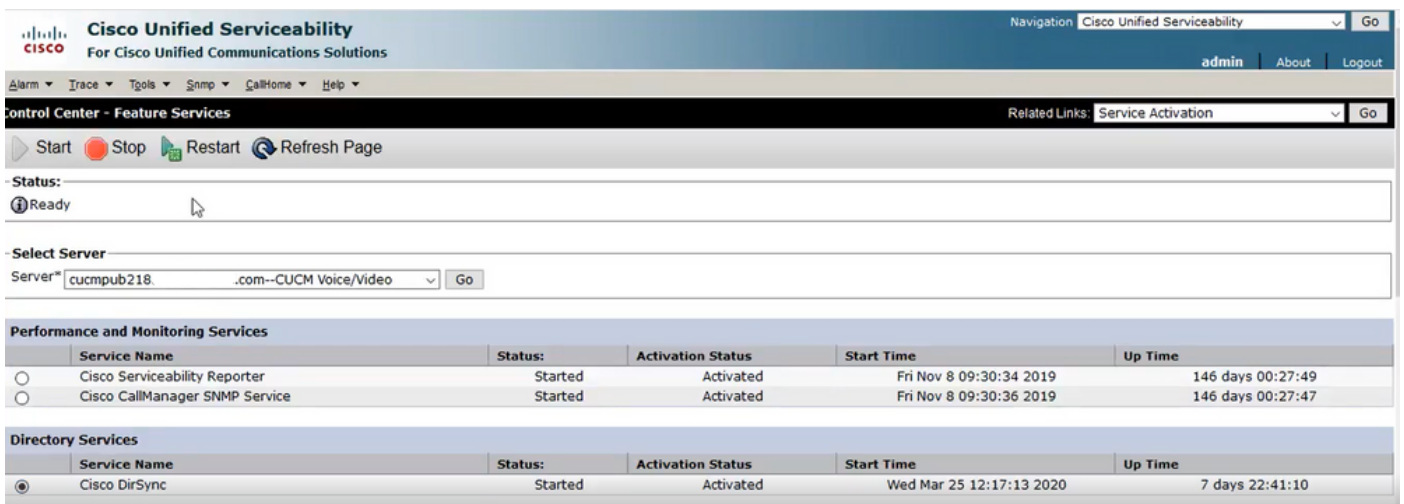
```
10.201.218.163 - PuTTY
login as: admin
admin@10.201.218.163's password:
Command Line Interface is starting up, please wait ...

Welcome to the Platform Command Line Interface

VMware Installation:
  2 vCPU: Intel(R) Xeon(R) CPU E7-2890 v2 @ 2.80GHz
  Disk 1: 80GB, Partitions aligned
  4096 Mbytes RAM

admin:utils service restart Cisco Tomcat
Do not press Ctrl+C while the service is restarting. If the service has not rest
arted properly, execute the same command again.
Service Manager is running
Cisco Tomcat[STOPPING]
Cisco Tomcat[STOPPING]
Cisco Tomcat[STOPPING]
Cisco Tomcat[STOPPING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTED]
admin:█
```

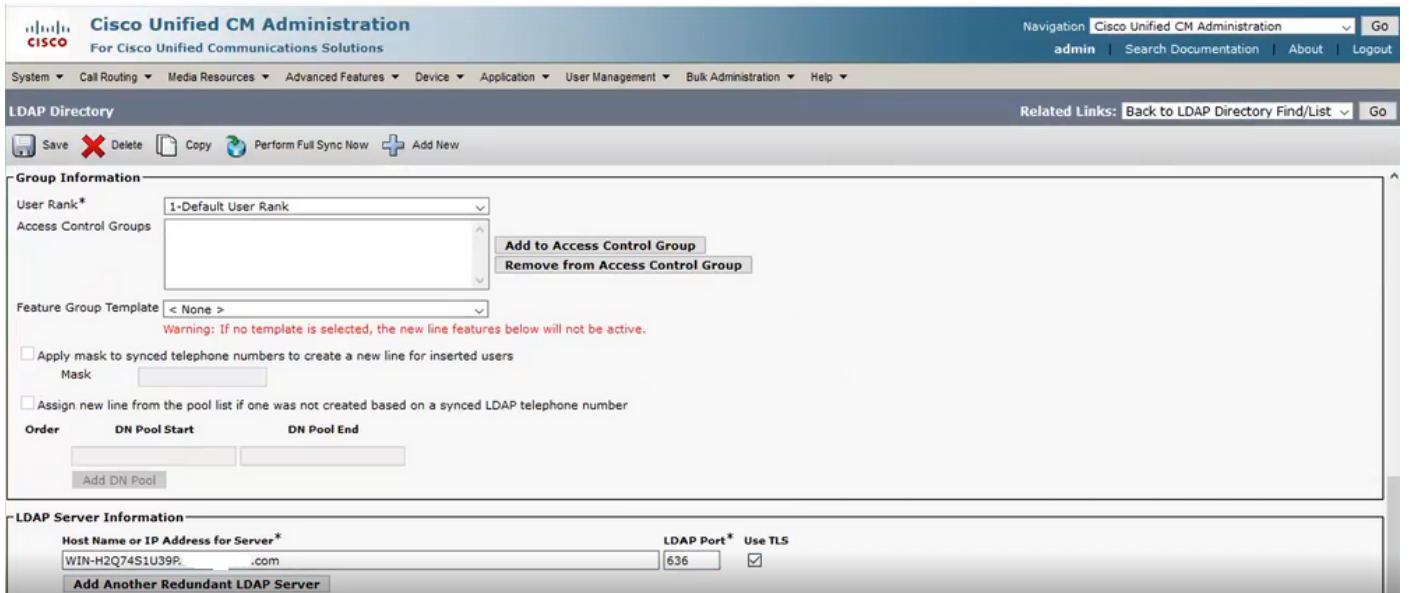
第四步：导航到CUCM发布服务器Cisco Unified Serviceability > Tools > Control Center - Feature Services，验证是否已激活并启动Cisco DirSync服务（如图所示），如果使用此服务（未显示），请在每个节点上重新启动Cisco CTIManager服务：



配置Secure LDAP目录

步骤1:配置CUCM LDAP目录，以便在端口636上利用与AD的LDAPS TLS连接。

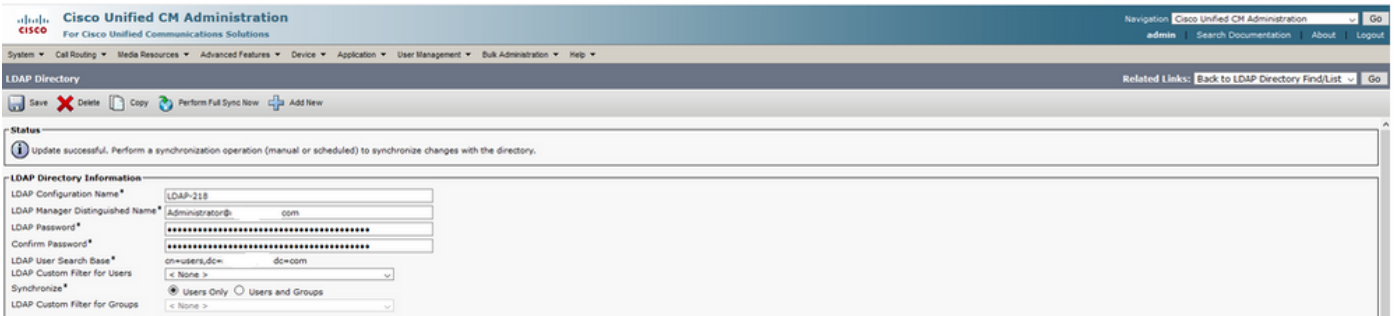
导航到CUCM管理>系统> LDAP目录。键入LDAP服务器信息的FQDN或LDAP服务器的IP地址。指定LDAPS端口636，然后选中Use TLS框，如图所示：



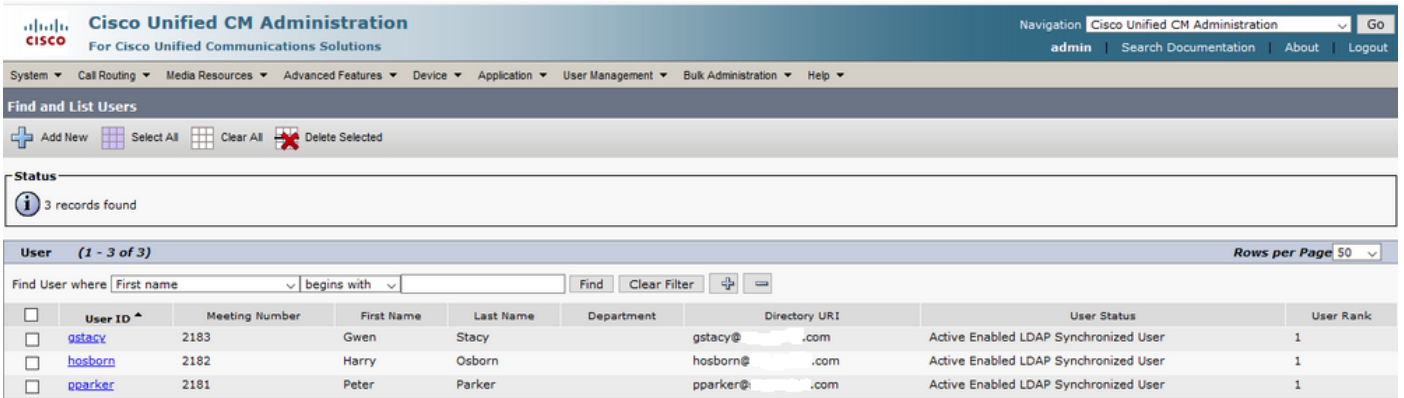
注意：默认情况下，在LDAP服务器信息中配置的10.5(2)SU2和9.1(2)SU3 FQDN版本根据证书的公用名进行检查后，如果使用的是IP地址而不是FQDN，则会发出utils ldap config

ipaddr命令以停止将FQDN实施到CN验证。

第二步：要完成LDAPS的配置更改，请单击Perform Full Sync Now，如图所示：



第三步：导航到CUCM管理>用户管理>最终用户，验证是否存在最终用户，如图所示：



第四步：导航到ccmuser页(https://<cucm pub>的ip地址/ccmuser)验证用户登录是否成功。

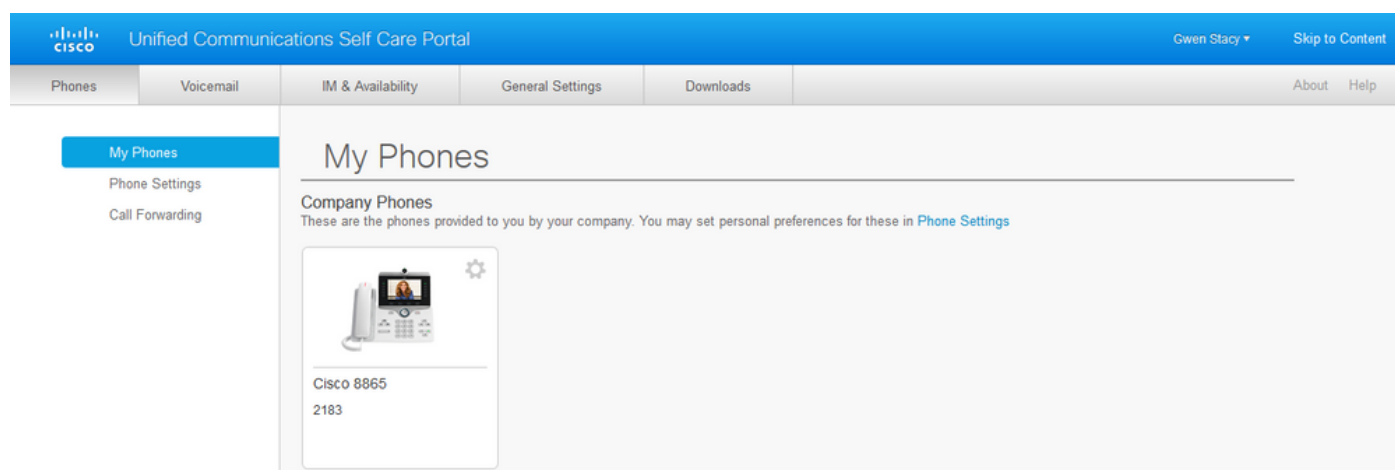
CUCM版本12.0.1的ccmuser页面如下所示：

Cisco Unified Communications Self Care Portal

Username
Password

Sign In

输入LDAP凭证后，用户可以成功登录，如图所示：



配置安全LDAP身份验证

配置CUCM LDAP身份验证以利用到端口3269上的AD的LDAPS TLS连接。

导航到CUCM管理>系统> LDAP身份验证。键入LDAP服务器信息的LDAPS服务器的FQDN。指定LDAPS端口3269，然后选中Use TLS复选框，如图所示：

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration Go
admin | Search Documentation | About | Logout

System | Call Routing | Media Resources | Advanced Features | Device | Application | User Management | Bulk Administration | Help

LDAP Authentication

Save

Status
Update successful

LDAP Authentication for End Users

Use LDAP Authentication for End Users

LDAP Manager Distinguished Name* Administrator@ .com

LDAP Password*

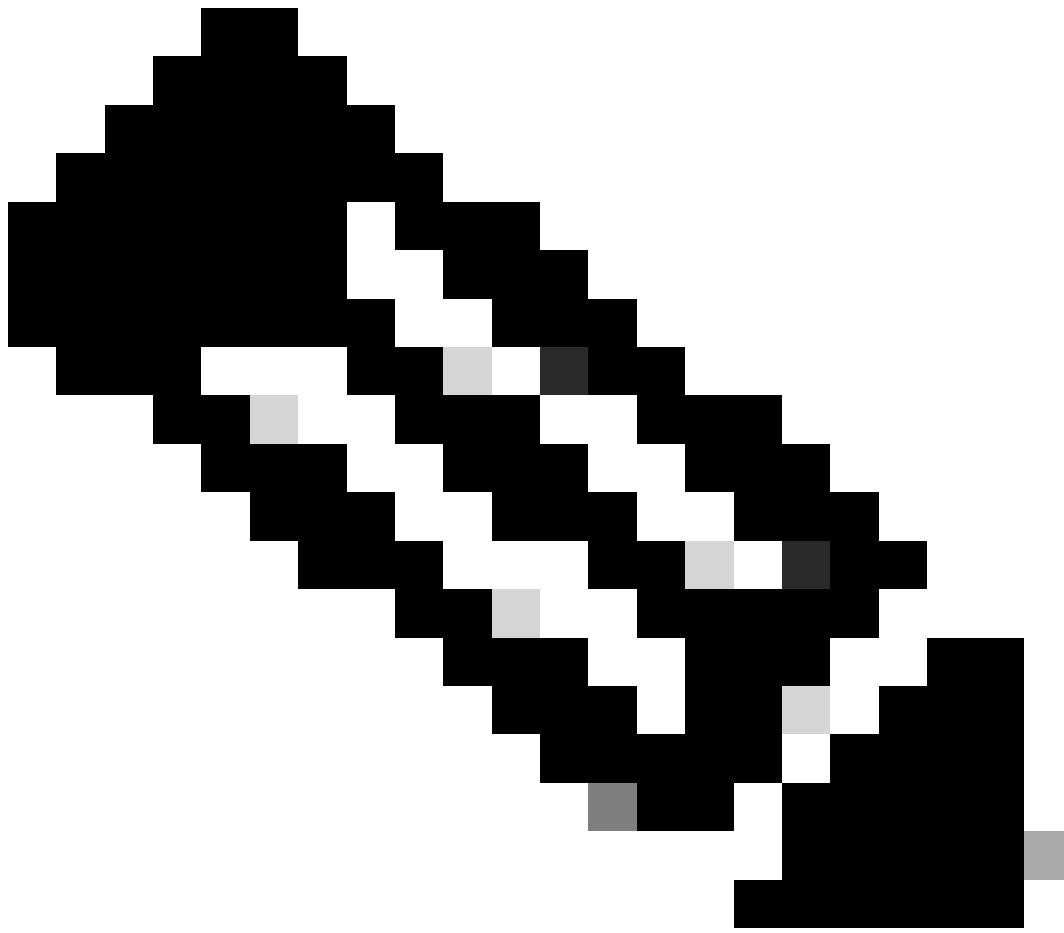
Confirm Password*

LDAP User Search Base* cn=users,dc= dc=com

LDAP Server Information

Host Name or IP Address for Server*	LDAP Port*	Use TLS
WIN-H2Q74S1U39P .com	3269	<input checked="" type="checkbox"/>

Add Another Redundant LDAP Server

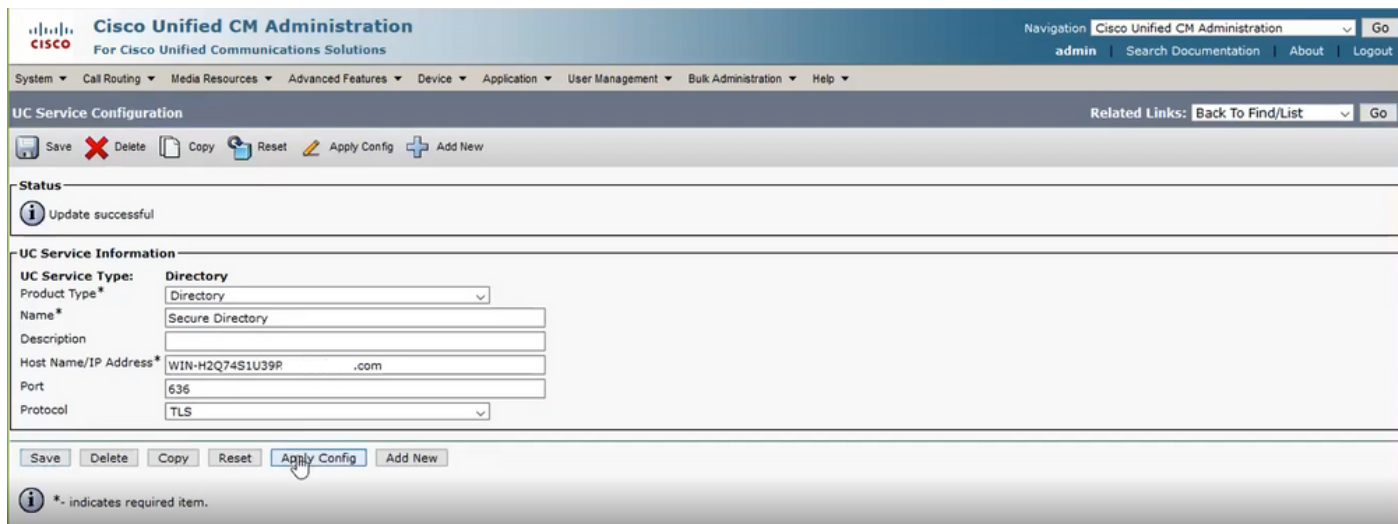


注意：如果您有Jabber客户端，建议使用端口3269进行LDAPS身份验证，因为如果未指定到全局目录服务器的安全连接，则可能会发生登录的Jabber超时。

为UC服务配置与AD的安全连接

如果需要保护利用LDAP的统一通信服务，请配置这些统一通信服务以使用TLS的端口636或3269。

导航到CUCM管理>用户管理>用户设置>统一通信服务。查找指向AD的目录服务。键入LDAPS服务器的FQDN作为主机名/IP地址。将端口指定为636或3269以及协议TLS，如图所示：

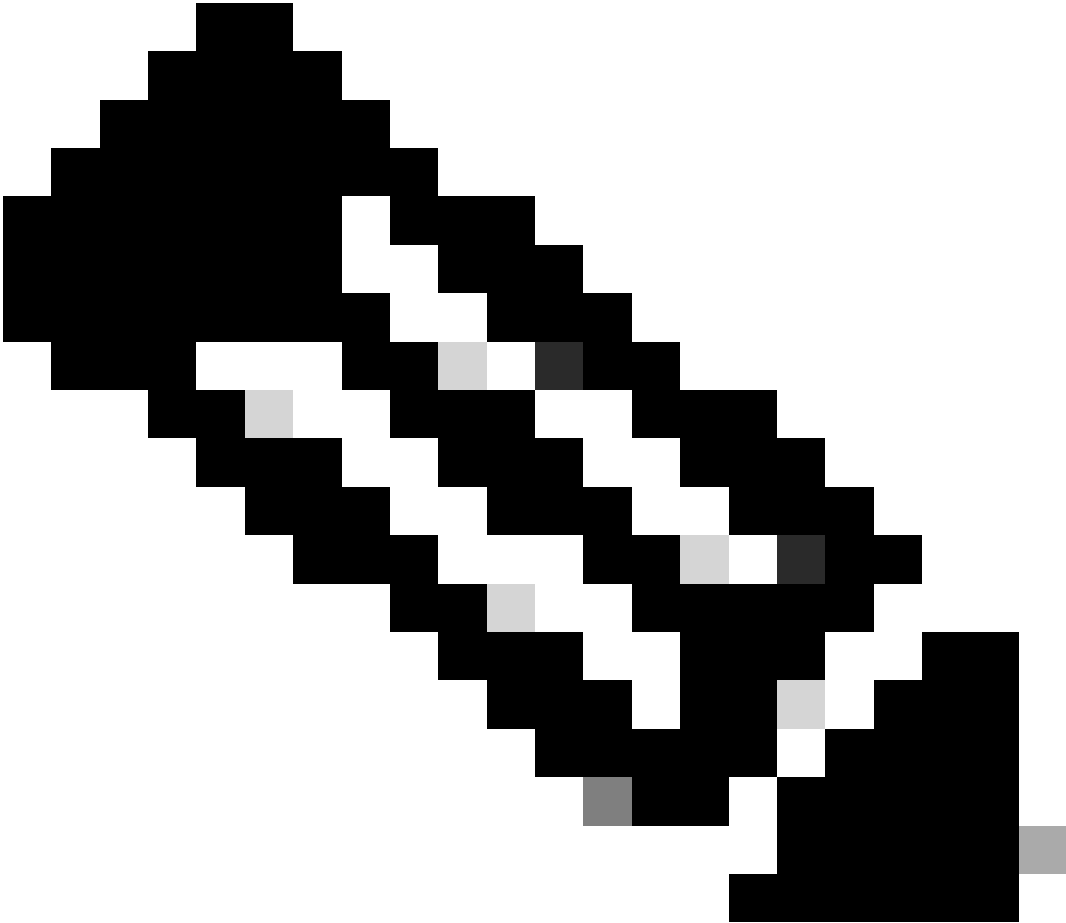


The screenshot displays the Cisco Unified CM Administration web interface. The page title is "UC Service Configuration". The navigation menu includes System, Call Routing, Media Resources, Advanced Features, Device, Application, User Management, Bulk Administration, and Help. The user is logged in as "admin".

The "UC Service Information" section contains the following configuration details:

UC Service Type:	Directory
Product Type*	Directory
Name*	Secure Directory
Description	
Host Name/IP Address*	WIN-H2Q74S1U39R .com
Port	636
Protocol	TLS

At the bottom of the form, there are buttons for Save, Delete, Copy, Reset, Apply Config, and Add New. A note at the bottom left states: "i * indicates required item."



注意：Jabber客户端计算机还需要在Jabber客户端计算机的证书管理信任库中安装CUCM上安装的tomcat-trust LDAPS证书，以允许Jabber客户端建立到AD的LDAPS连接。

验证

使用本部分可确认配置能否正常运行。

要验证从LDAP服务器发送到CUCM的TLS连接的实际LDAPS证书/证书链，请从CUCM数据包捕获中导出LDAPS TLS证书。此链接提供有关如何从CUCM数据包捕获导出TLS证书的信息：[如何从CUCM数据包捕获导出TLS证书](#)

故障排除

当前没有故障排除此配置的特定可用资料。

相关信息

- 此链接提供对穿过LDAPS配置的视频的访问：[安全LDAP目录和身份验证穿透视频](#)
- [技术支持和文档 - Cisco Systems](#)

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）。