为安全LDAP(LDAP)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

配置安全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

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

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 9.x版及更高版本。

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

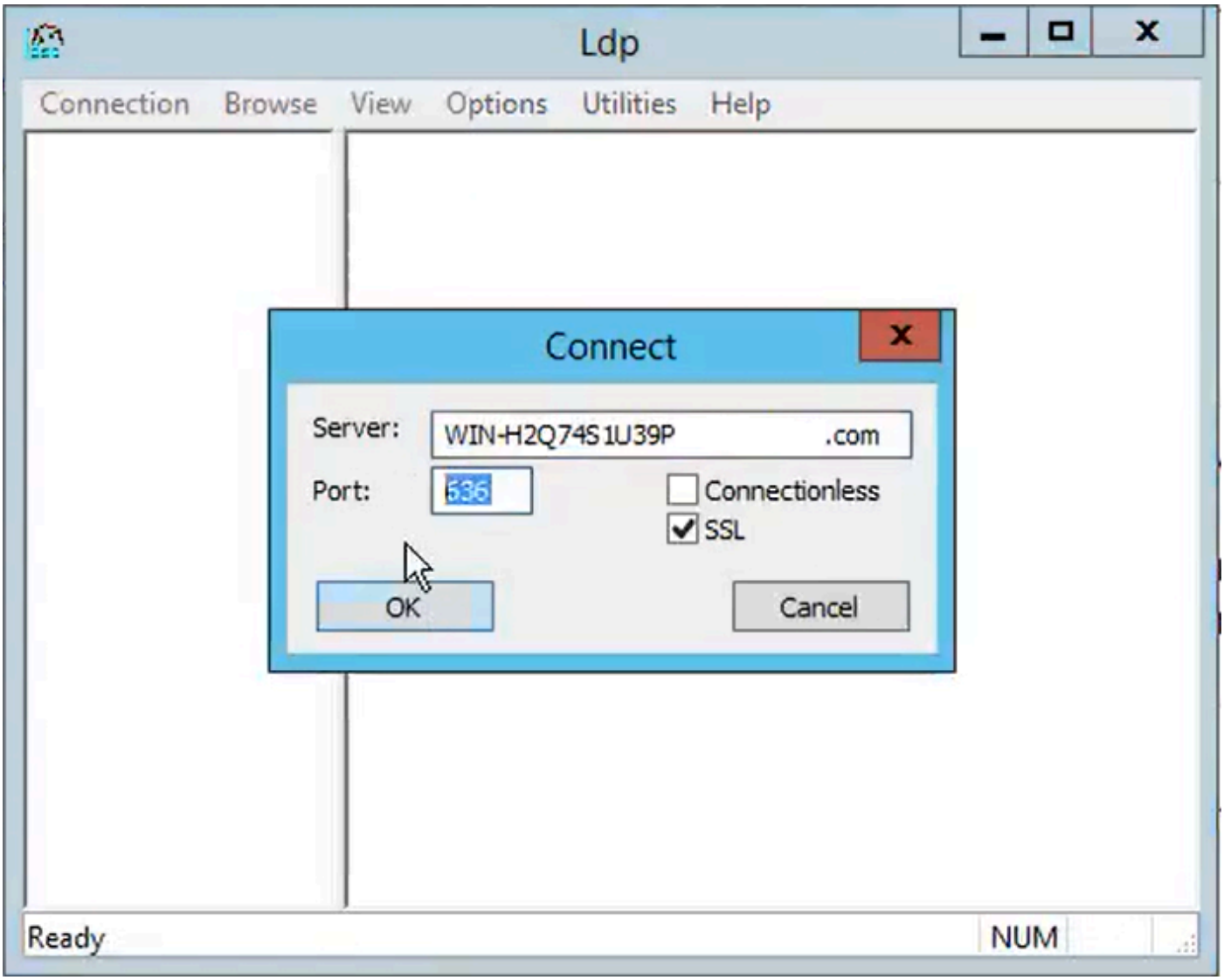
Active Directory(AD)管理员负责为轻量级目录访问协议(LDAPS)配置AD轻量级目录访问协议(LDAP)。 这包括安装符合LDAPS证书要求的CA签名证书。

注意：有关从非安全LDAP更新以保护LDAP到AD连接的其他思科协作应用的信息，请参阅以下链接：软件建议：Active Directory连接必需Secure LDAP

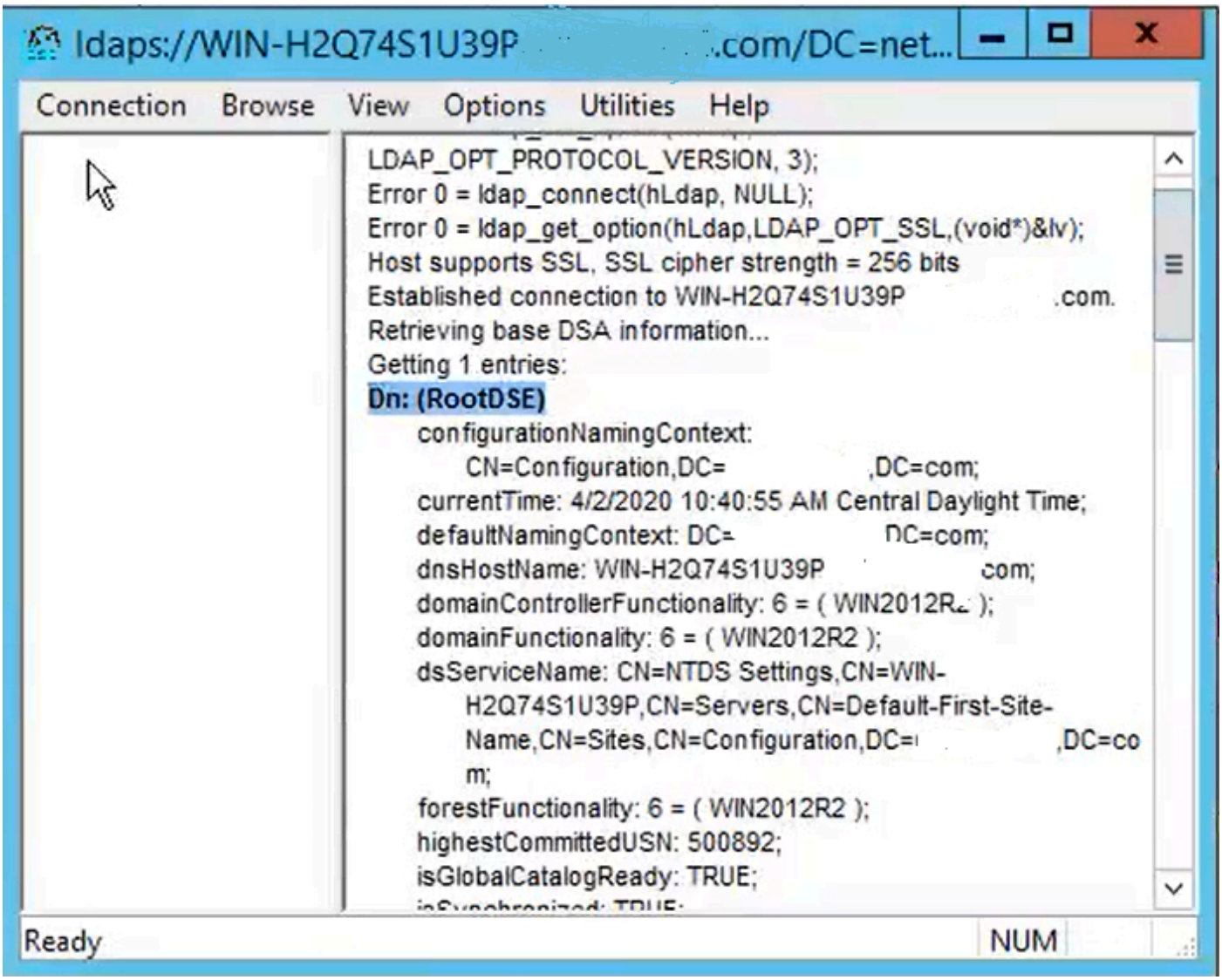
验证和安装LDAPS证书

步骤1.将LDAPS证书上传到AD服务器后，使用ldp.exe工具验证AD服务器上是否已启用LDAPS。

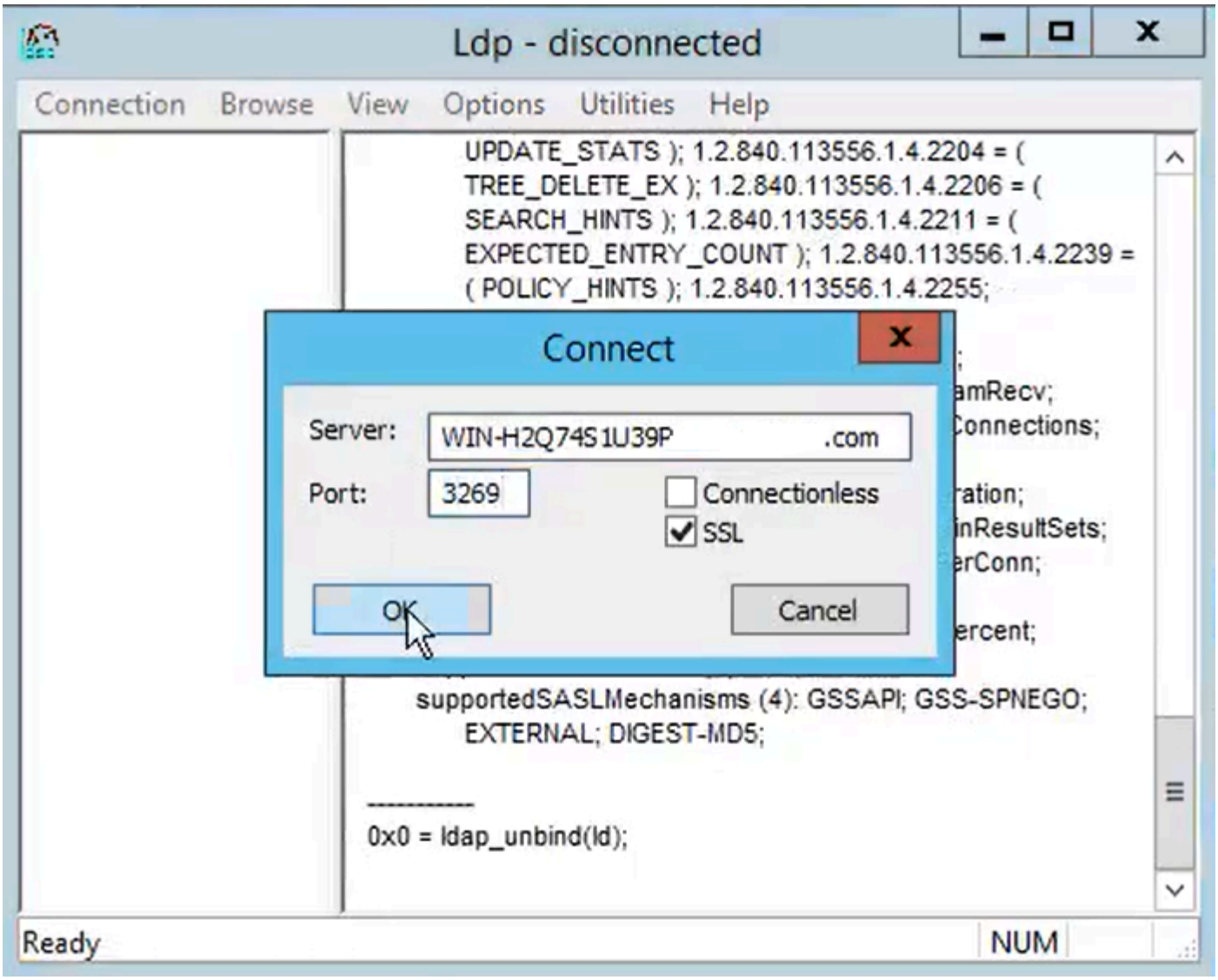
1. 在AD服务器上启动AD管理工具(Ldp.exe)。
2. 在Connection菜单中，选择Connect。
3. 输入LDAPS服务器的Fully Qualified Domain Name(FQDN)作为服务器。
4. 输入636作为端口号。
5. 单击OK，如图所示



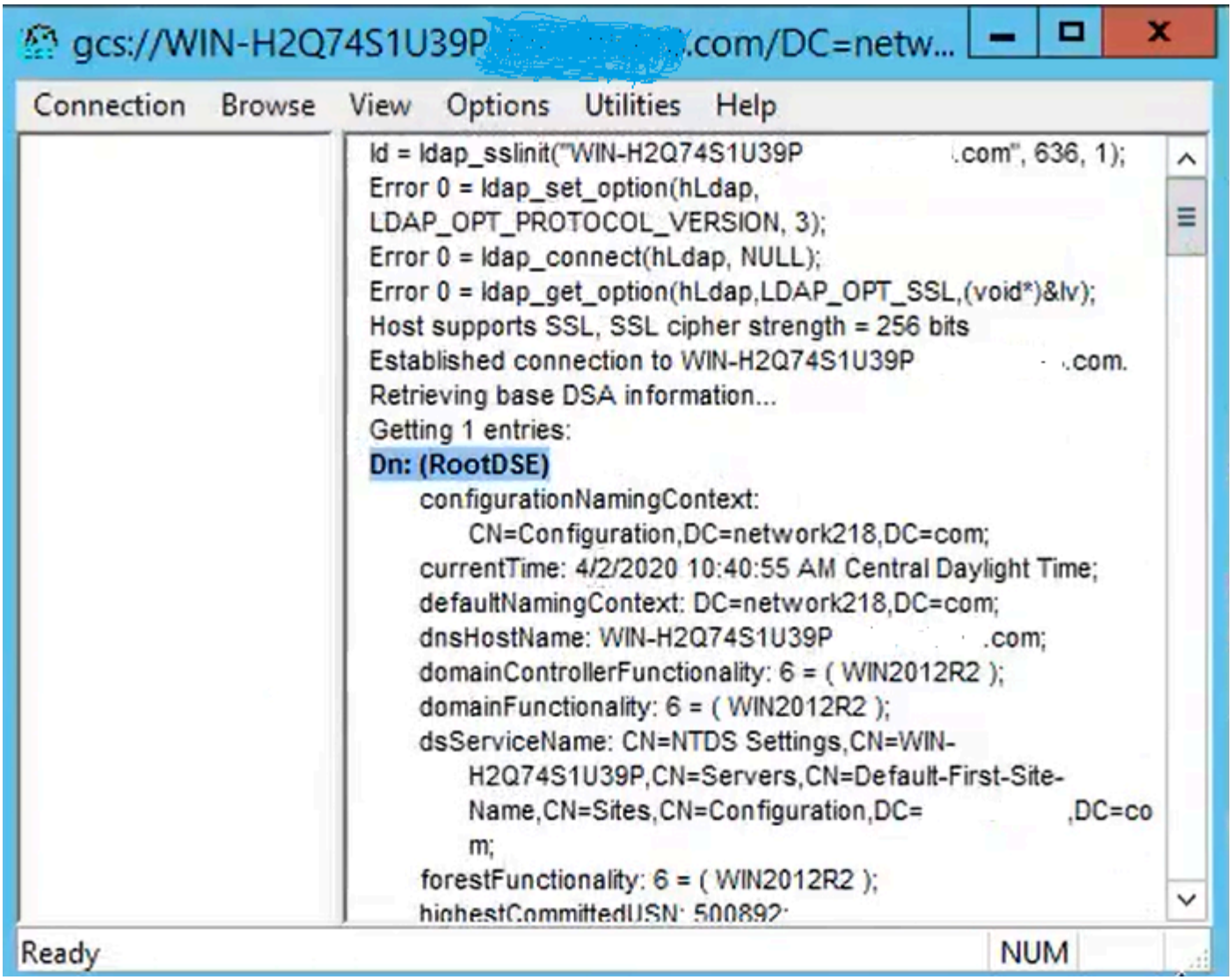
对于端口636上的成功连接，RootDSE信息会打印在右窗格中，如图所示：



对端口3269重复此过程，如图所示：

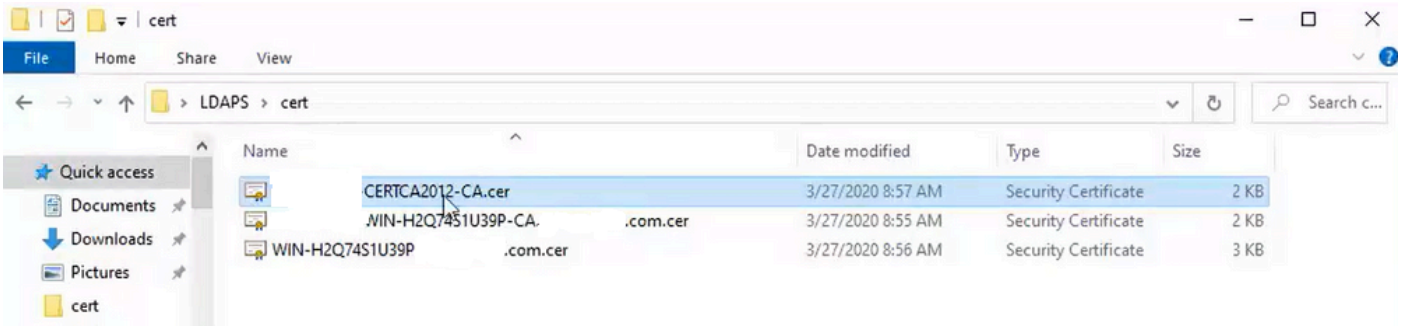


要在端口3269上成功连接，RootDSE信息会打印在右窗格中，如图所示：

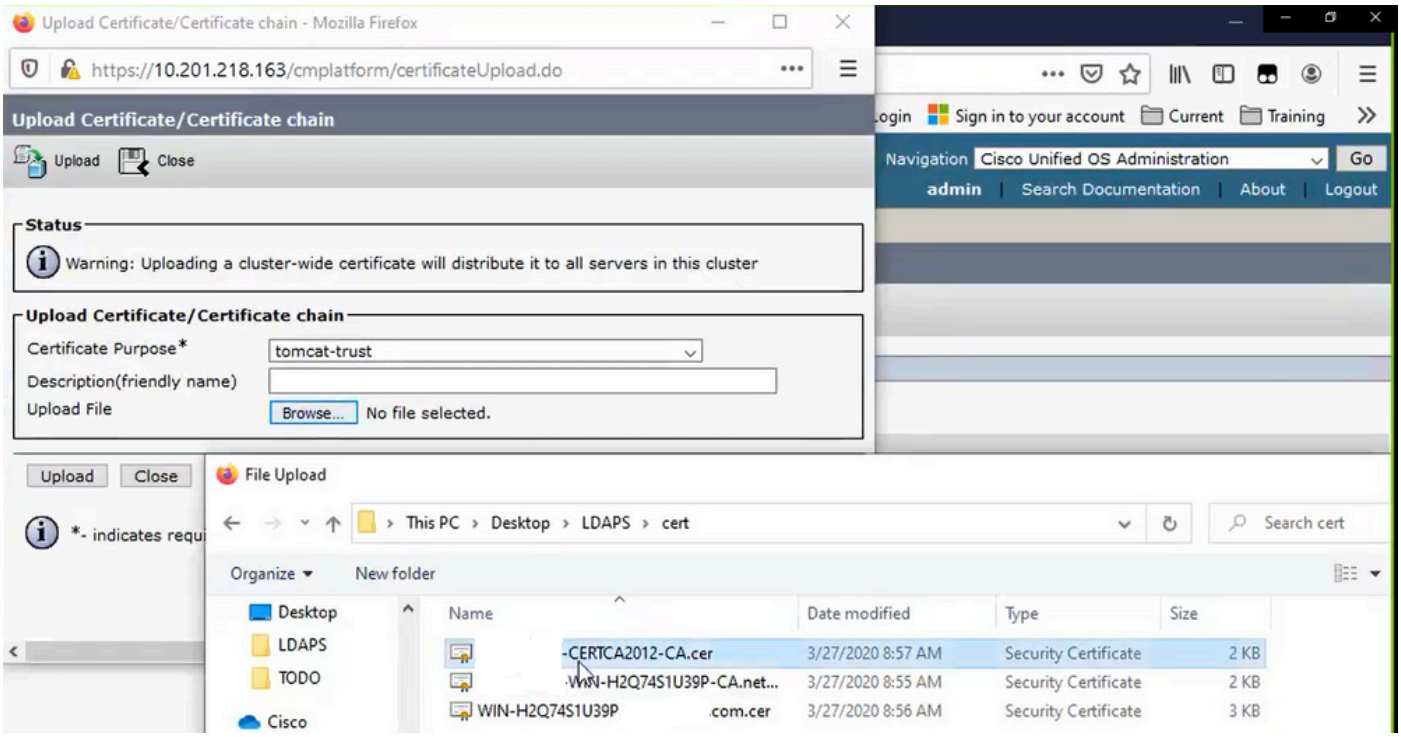


步骤2.获取根证书和作为LDAPS服务器证书一部分的任何中间证书，并将这些证书作为tomcat-trust证书安装在每个CUCM和IM/P发布方节点上，作为CallManager-trust安装在CUCM发布方上。

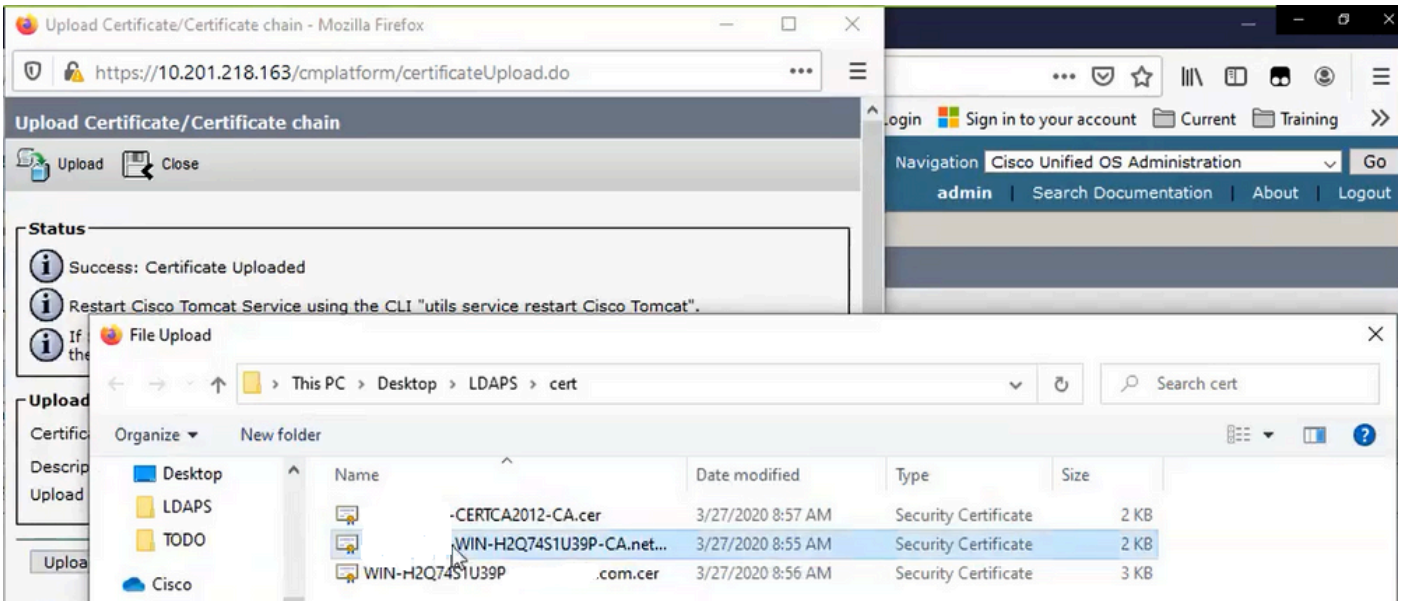
作为LDAPS服务器证书一部分的根证书和中间证书<hostname>.<Domain>.cer如图所示：



导航到CUCM publisher Cisco Unified OS Administration > Security > Certificate Management。将根上传为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）：

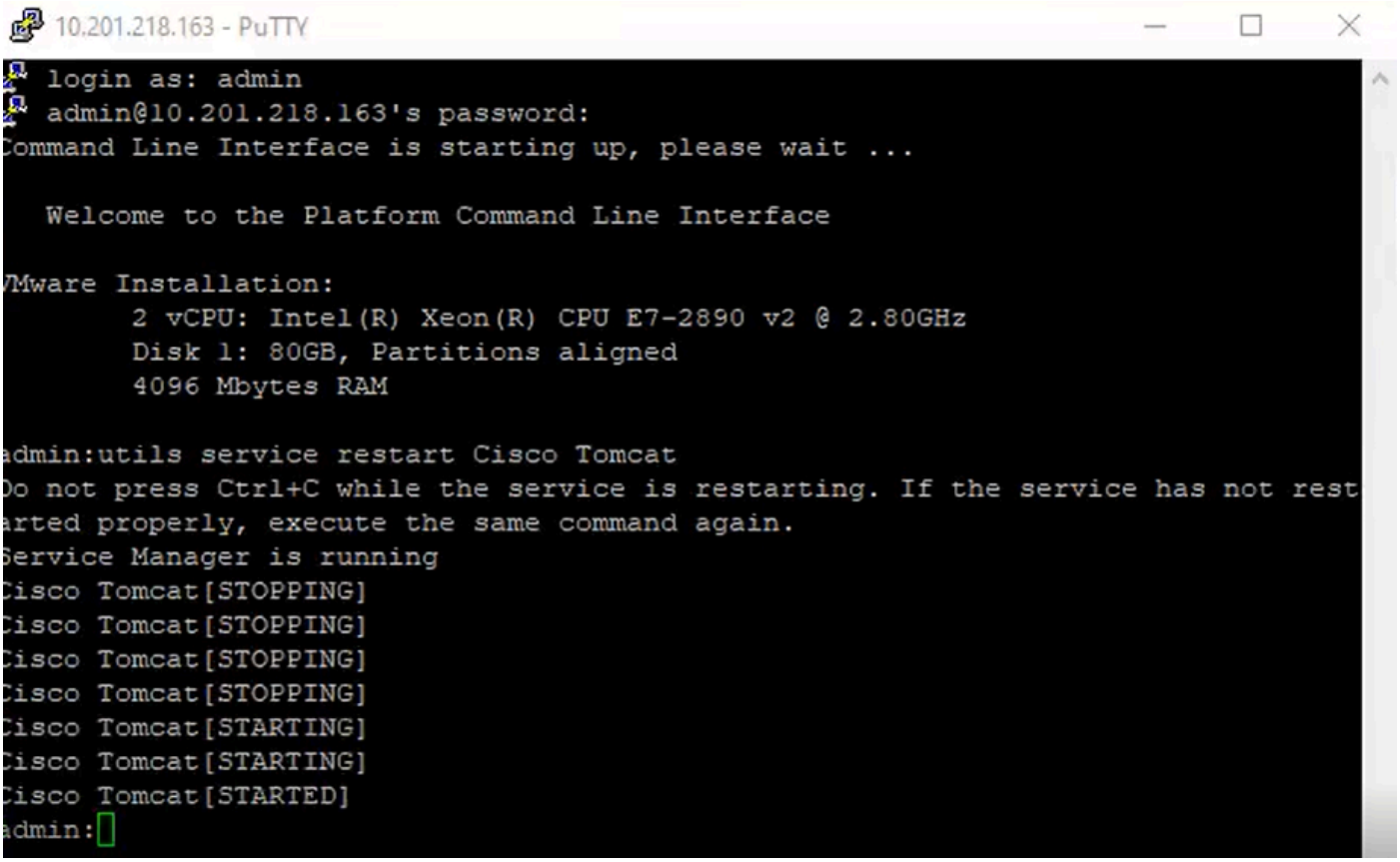


注意：如果您有属于CUCM集群的IM/P服务器，则还需要将这些证书上传到这些IM/P服务器。

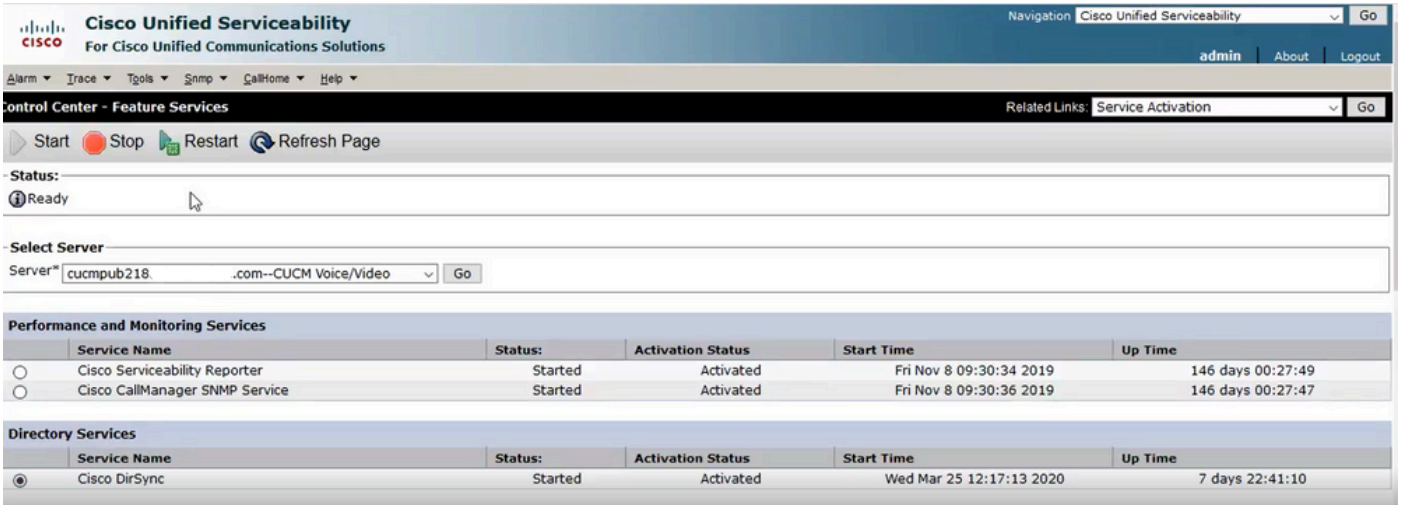
注意：或者，可以将LDAPS服务器证书安装为tomcat-trust。

步骤3.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Cisco 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CLI会话并运行命令utils service restart Cisco Tomcat，如图所示：



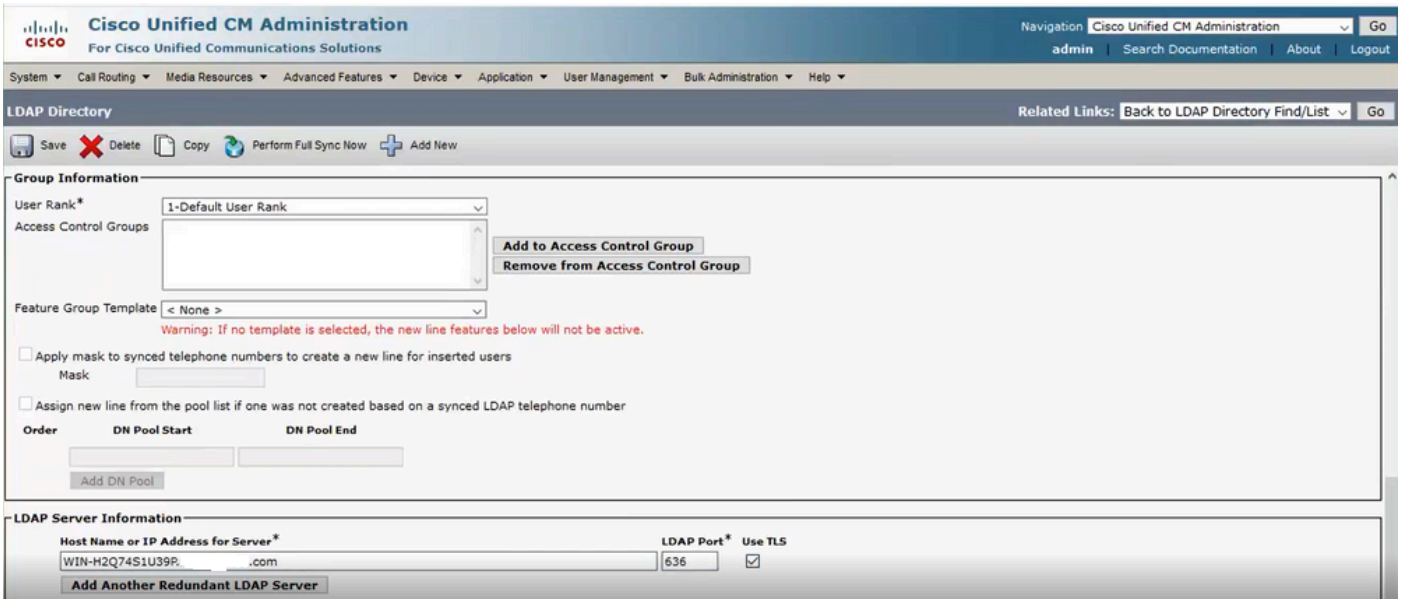
第4步：导航到CUCM发布服务器Cisco Unified Serviceability > Tools > Control Center - Feature Services，验证是否已激活和启动Cisco DirSync服务（如图所示），并在每个节点上重新启动Cisco CTIManager服务（如图所示）（未显示）：



配置安全LDAP目录

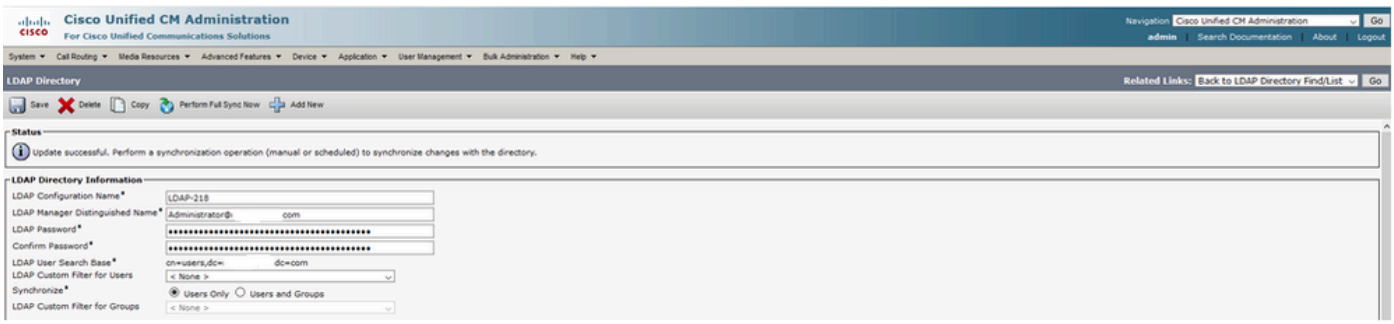
步骤1.配置CUCM LDAP目录，以便在端口636上利用到AD的LDAPS TLS连接。

导航到CUCM Administration > System > LDAP Directory。为LDAP服务器信息键入FQDN或LDAP服务器的IP地址。指定LDAPS端口636，并选中使用TLS复选框，如图所示：

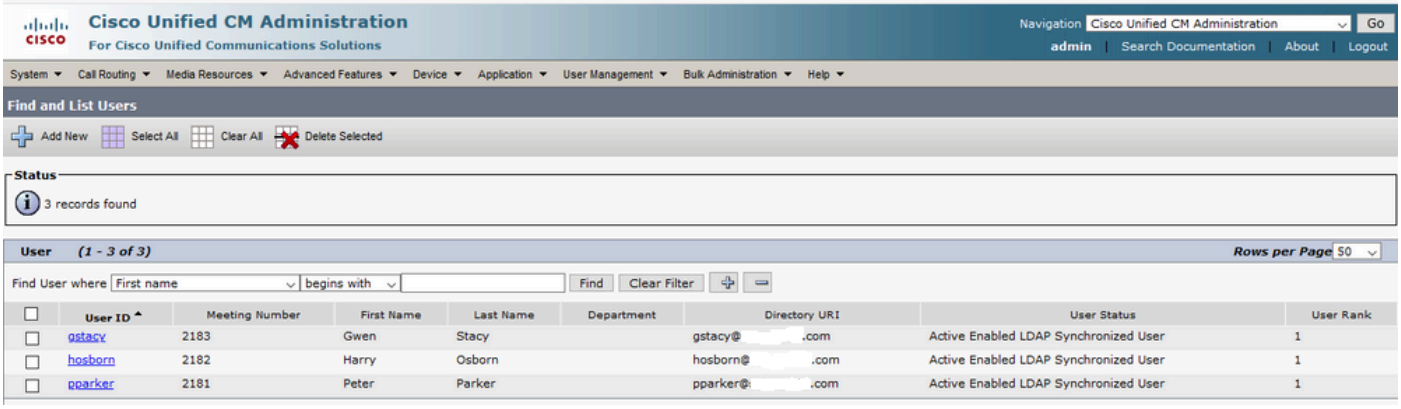


注意：默认情况下，在LDAP服务器信息中配置的10.5(2)SU2和9.1(2)SU3 FQDN版本根据证书的公用名进行检查后，如果使用的是IP地址而不是FQDN，则发出命令utils ldap config ipaddr以停止FQDN到CN验证的实施。

步骤2.要完成对LDAPS的配置更改，请单击Perform Full Sync Now，如图所示：

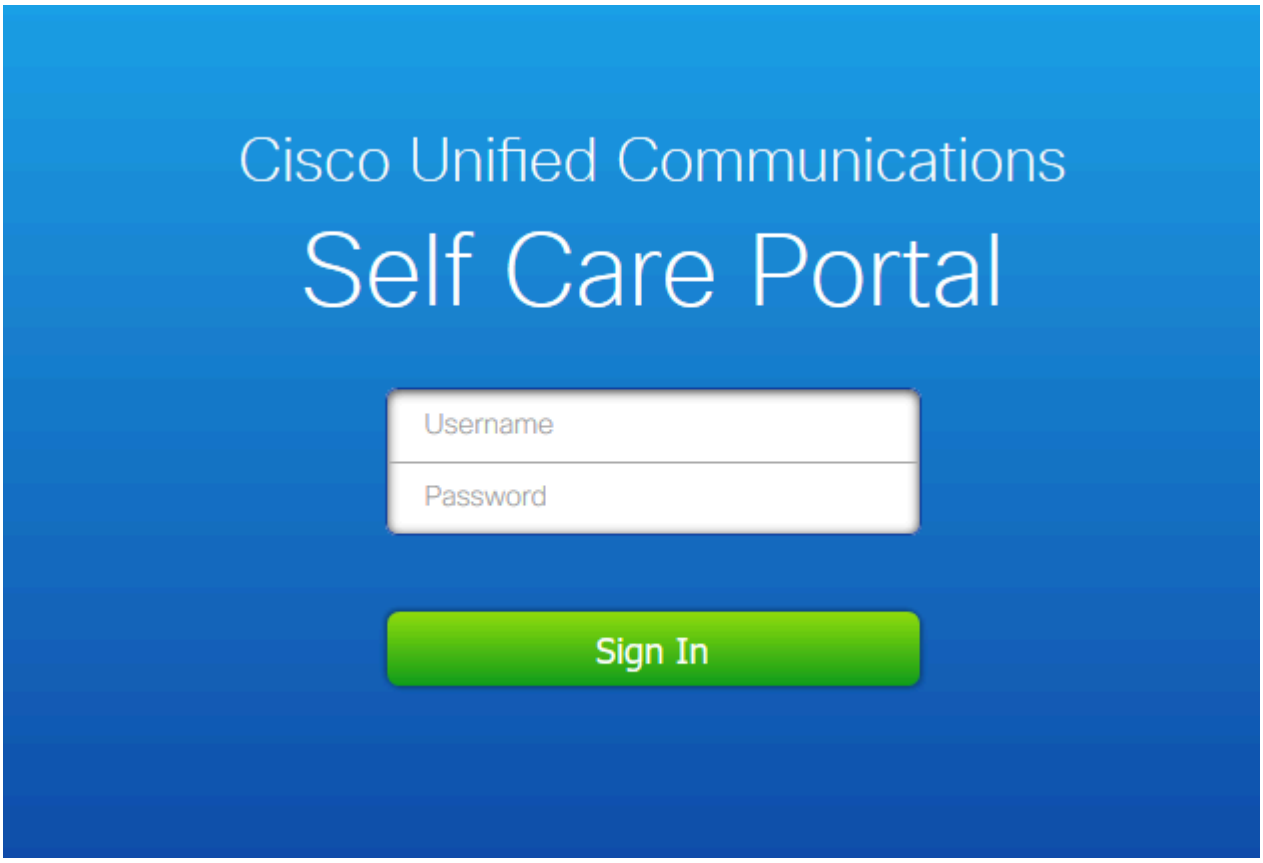


第3步：导航到CUCM Administration > User Management > End User，验证最终用户是否存在，如图所示：

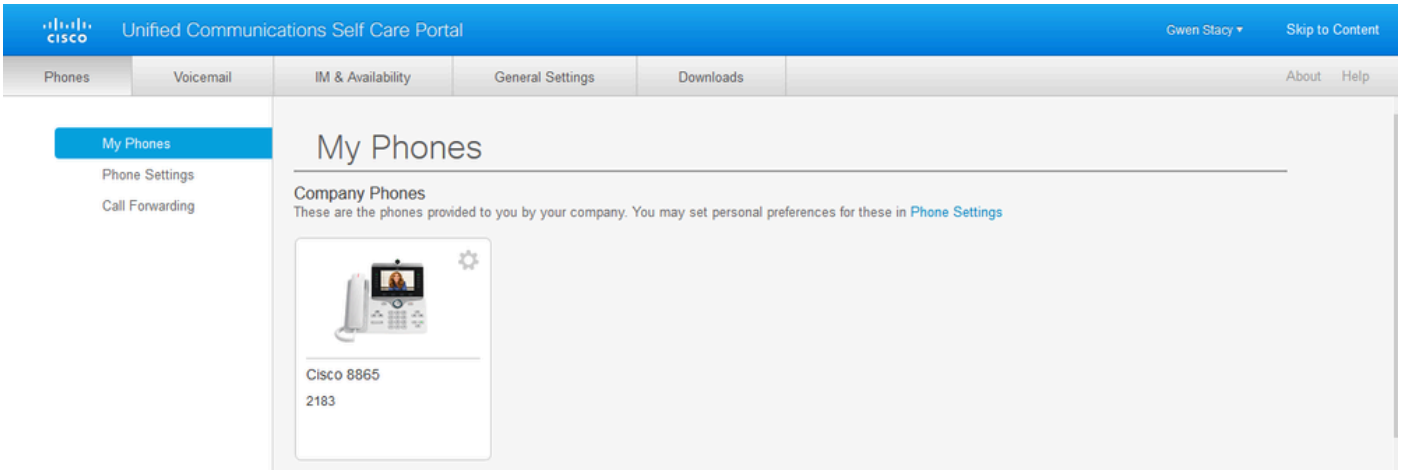


步骤4.导航到ccmuser页(https://<cucm pub>/ccmuser)以验证用户登录是否成功。

CUCM版本12.0.1的ccmuser页面如下所示：



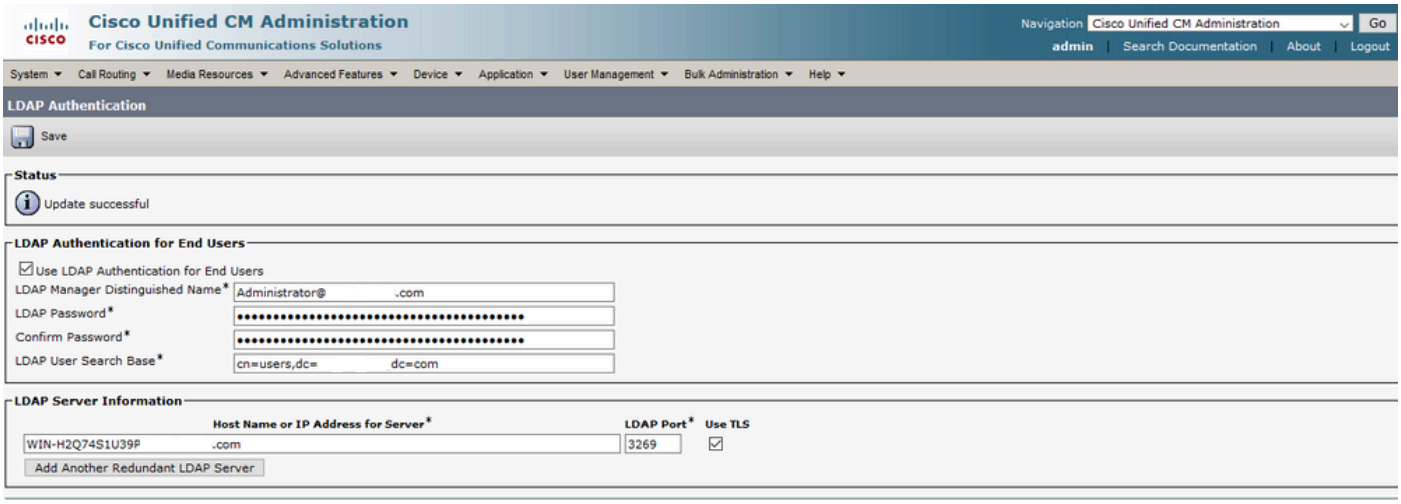
用户可以在输入LDAP凭证后成功登录，如图所示：



配置安全LDAP身份验证

配置CUCM LDAP身份验证，以便在端口3269上利用到AD的LDAPS TLS连接。

导航到CUCM Administration > System > LDAP Authentication。键入LDAP服务器信息的LDAPS服务器的FQDN。指定LDAPS端口3269，并选中Use TLS复选框，如图所示：

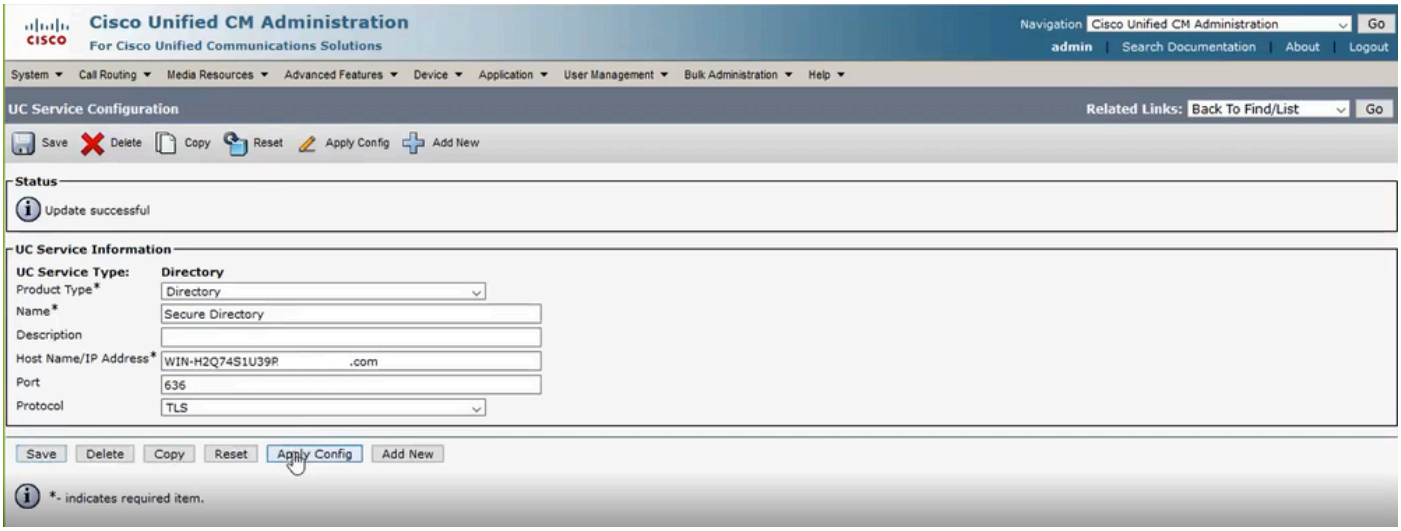


注意：如果您有Jabber客户端，建议使用端口3269进行LDAPS身份验证，因为如果未指定到全局目录服务器的安全连接，可能会发生登录的Jabber超时。

为UC服务配置与AD的安全连接

如果您需要保护使用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> UC服务。查找指向AD的目录服务。键入LDAPS server的FQDN作为主机名/IP地址。将端口指定为636或3269和协议TLS，如图所示：



注意：Jabber客户端计算机还需要将CUCM上安装的tomcat-trust LDAPS证书安装在Jabber客户端计算机的证书管理信任库中，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用于TLS连接的实际LDAPS证书/证书链，请从CUCM数据包捕获导出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

- 此链接提供对通过LDAPS配置的视频的访问：安全LDAP目录和身份验证漫游视频
- 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）。