為安全LDAP (LDAPS)配置CUCM

目錄

簡介

本文檔介紹從非安全LDAP連線更新到安全LDAPS連線的CUCM與AD連線的過程。

必要條件

需求

思科建議您瞭解以下主題：

· AD LDAP伺服器
· CUCM LDAP配置

· CUCM IM和線上狀態服務(IM/P)

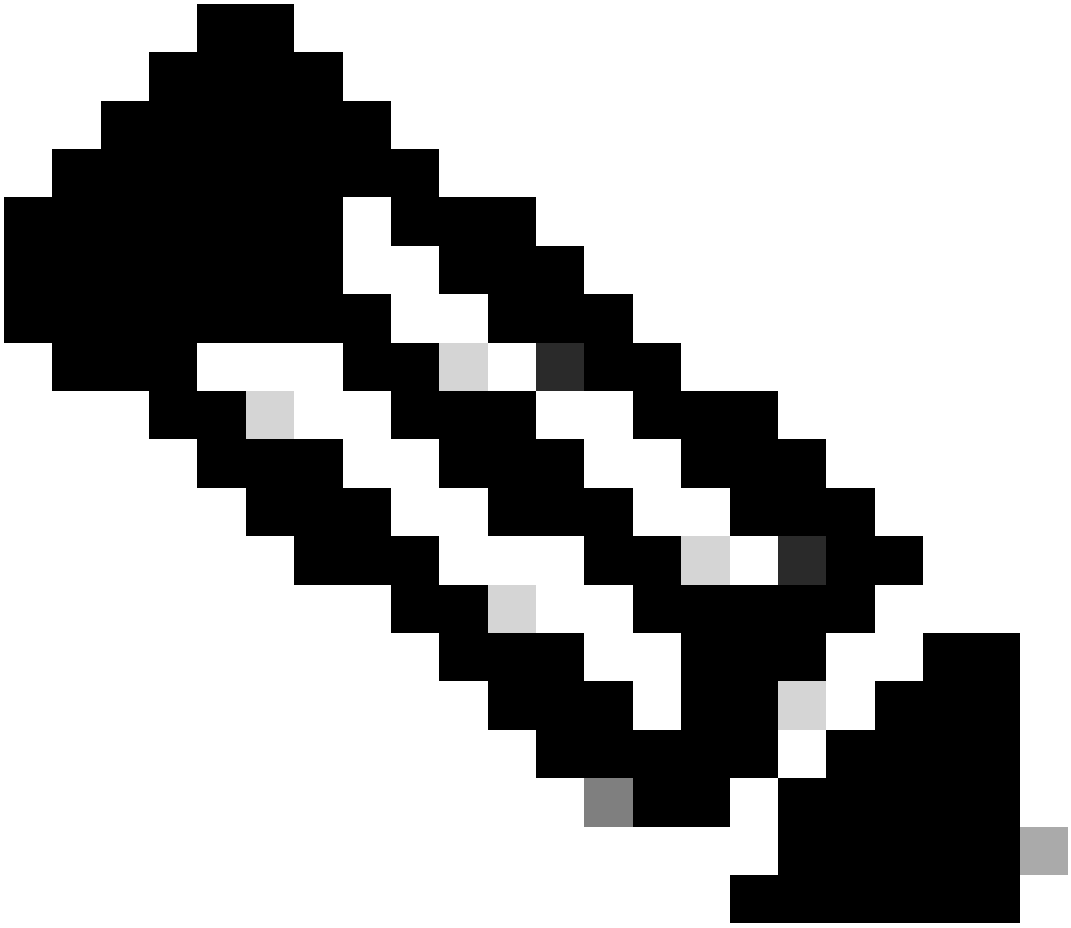
採用元件

本文檔中的資訊基於CUCM版本9.x及更高版本。

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。

背景資訊

Active Directory (AD)管理員負責為輕型目錄訪問協定(LDAPS)配置AD輕型目錄訪問協定(LDAP)。這包括安裝符合LDAPS證書要求的CA簽名證書。

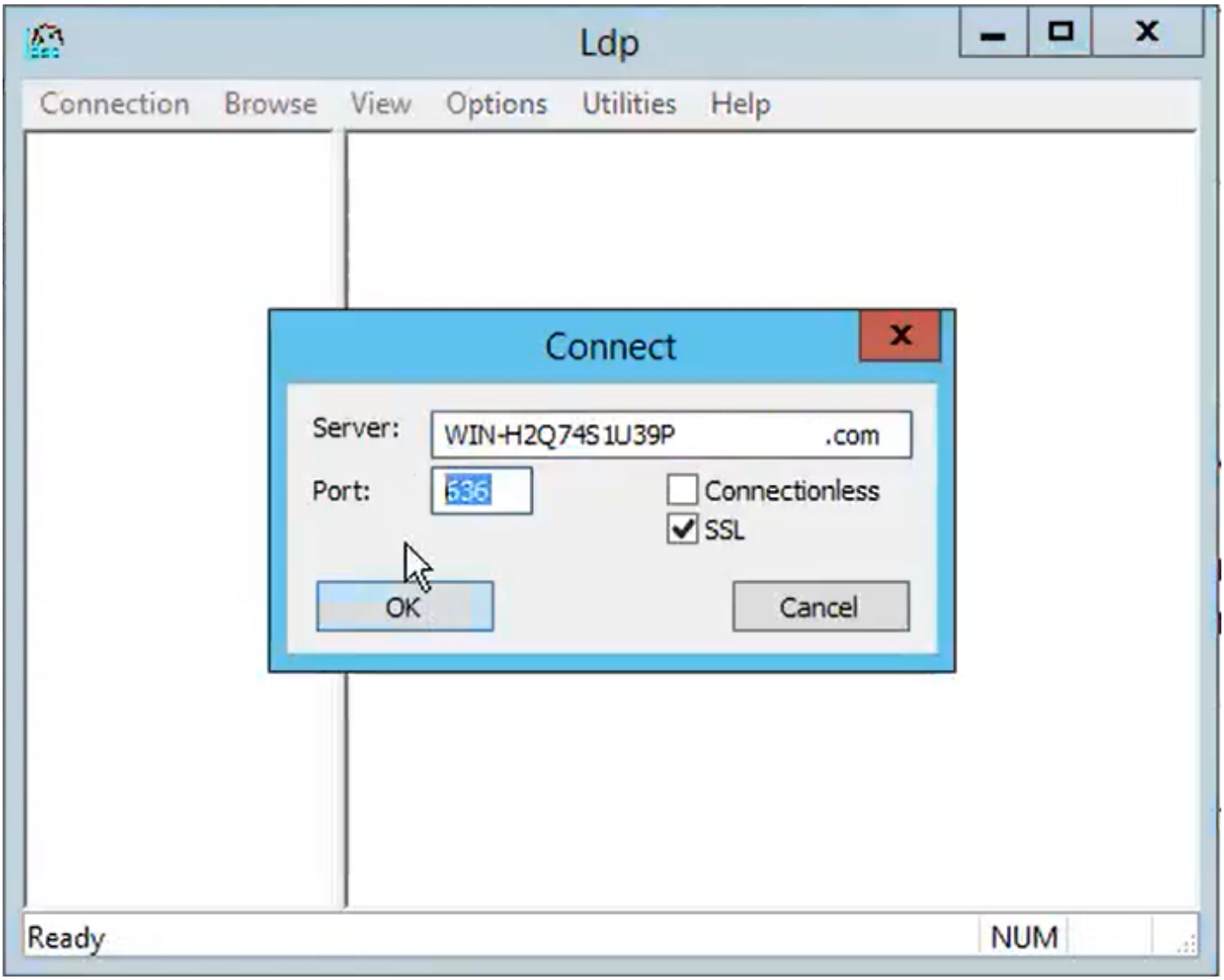


注意：如需從非安全LDAP更新以保護LDAPS連線至AD的其他思科協同合作應用程式的資訊，請參閱此連結：軟體建議：Active Directory連線必須使用Secure LDAP

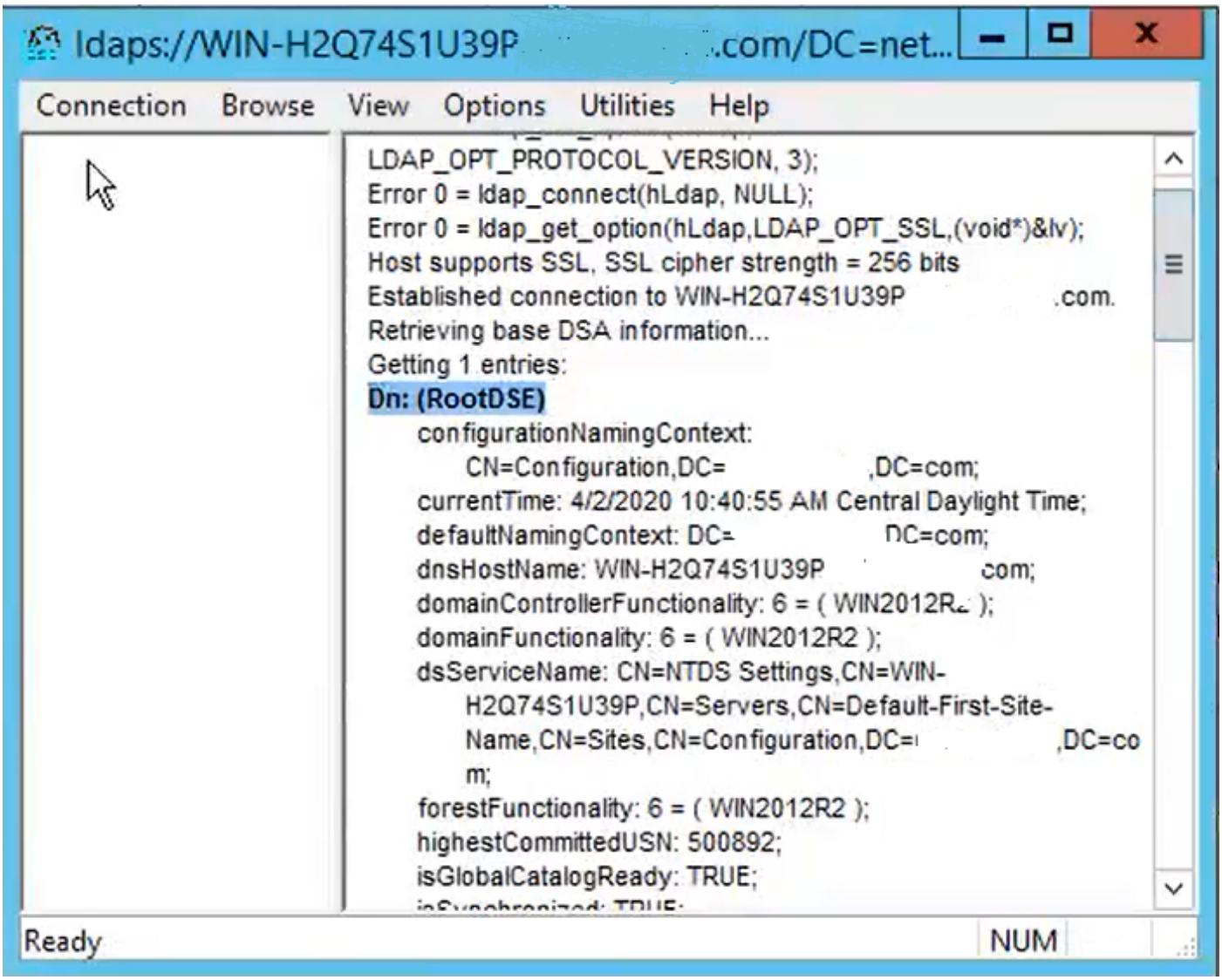
驗證和安裝LDAPS證書

步驟 1.將LDAPS證書上傳到AD伺服器後，請使用ldp.exe工具驗證是否已在AD伺服器上啟用LDAPS。

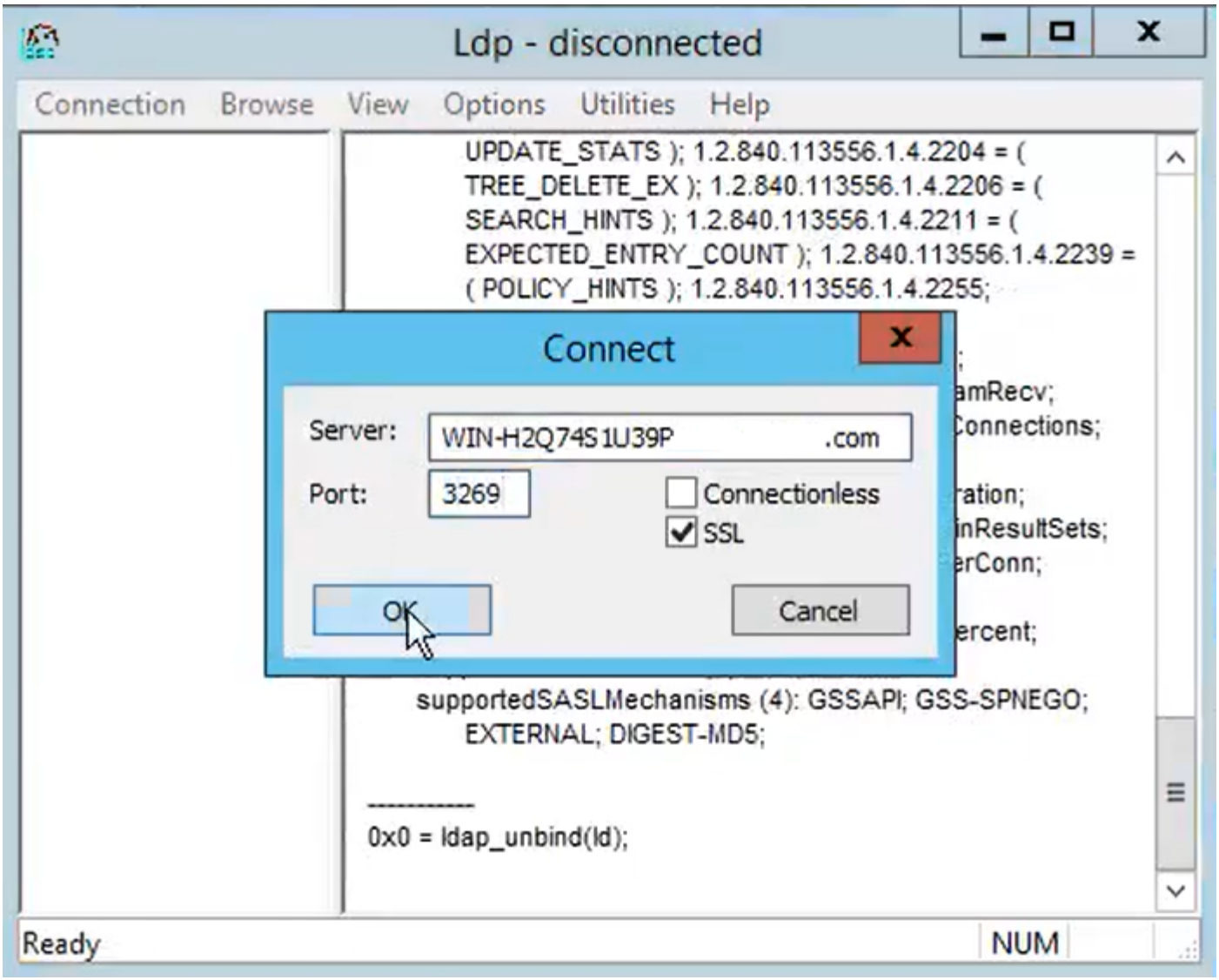
1. 在AD伺服器上啟動AD管理工具(Ldp.exe)。
2. 在「連線」選單上，選擇連線。
3. 輸入LDAPS伺服器作為伺服器的完整網域名稱(FQDN)。
4. 輸入636作為埠號。
5. 按一下OK（如圖所示）



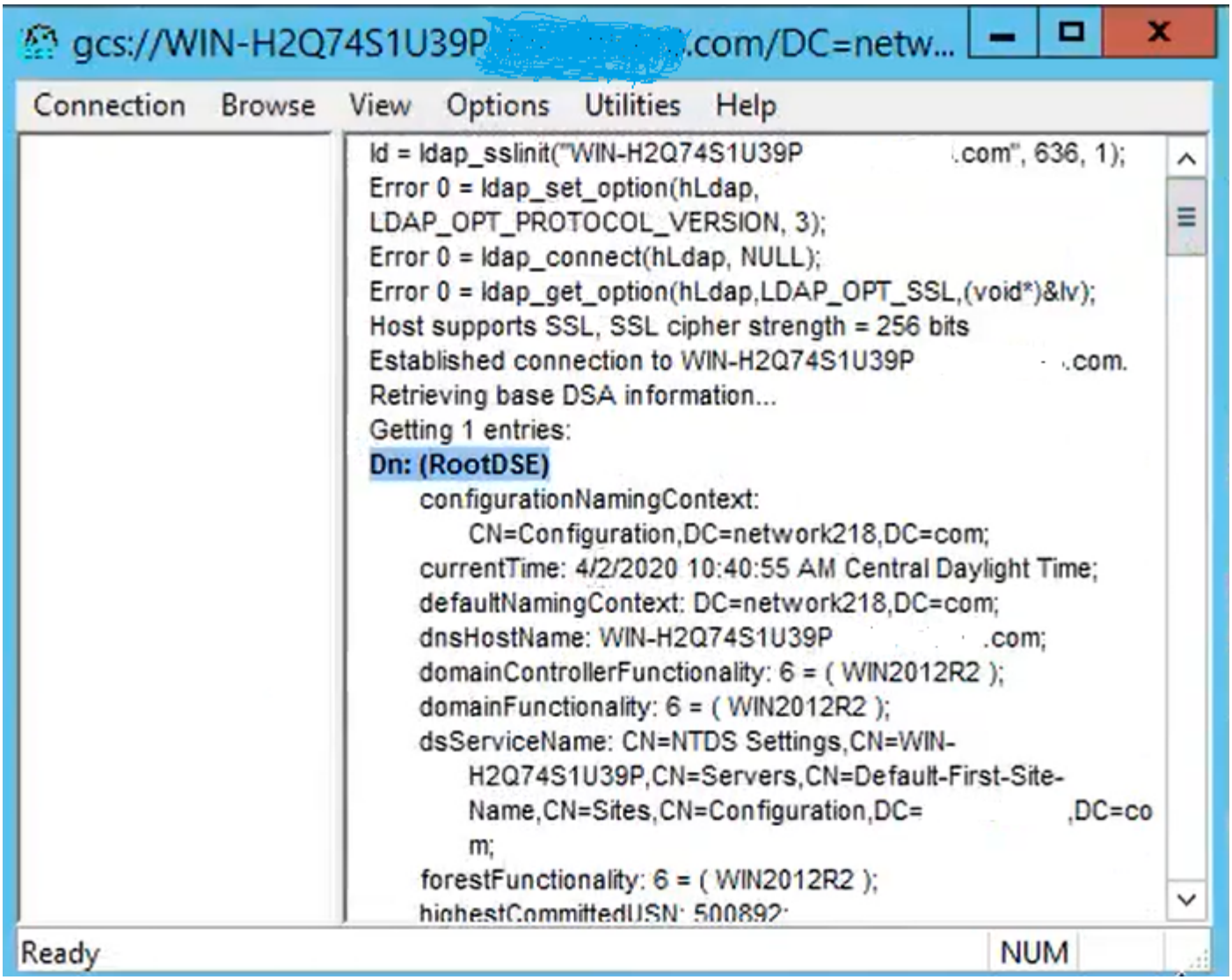
要在埠636上成功連線，RootDSE資訊會列印在右窗格中，如圖所示：



對埠3269重複該過程，如圖所示：

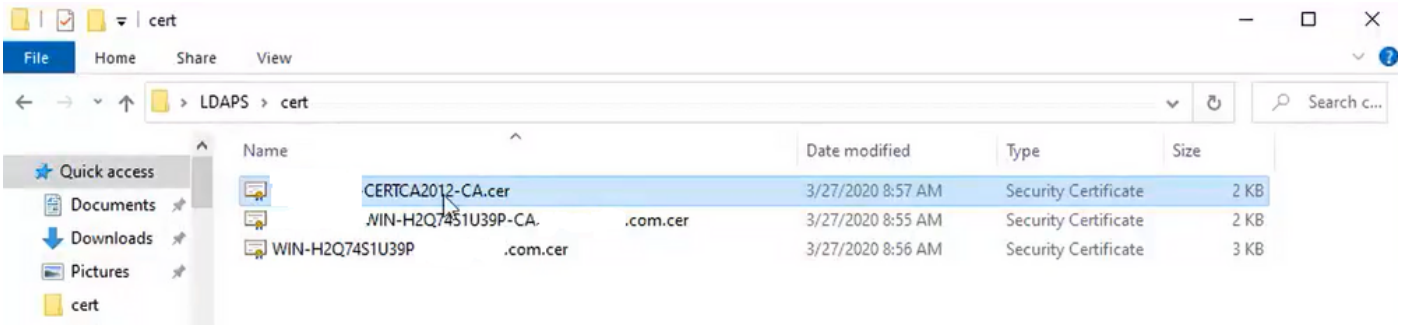


要在埠3269上成功連線，RootDSE資訊會列印在右窗格中，如圖所示：

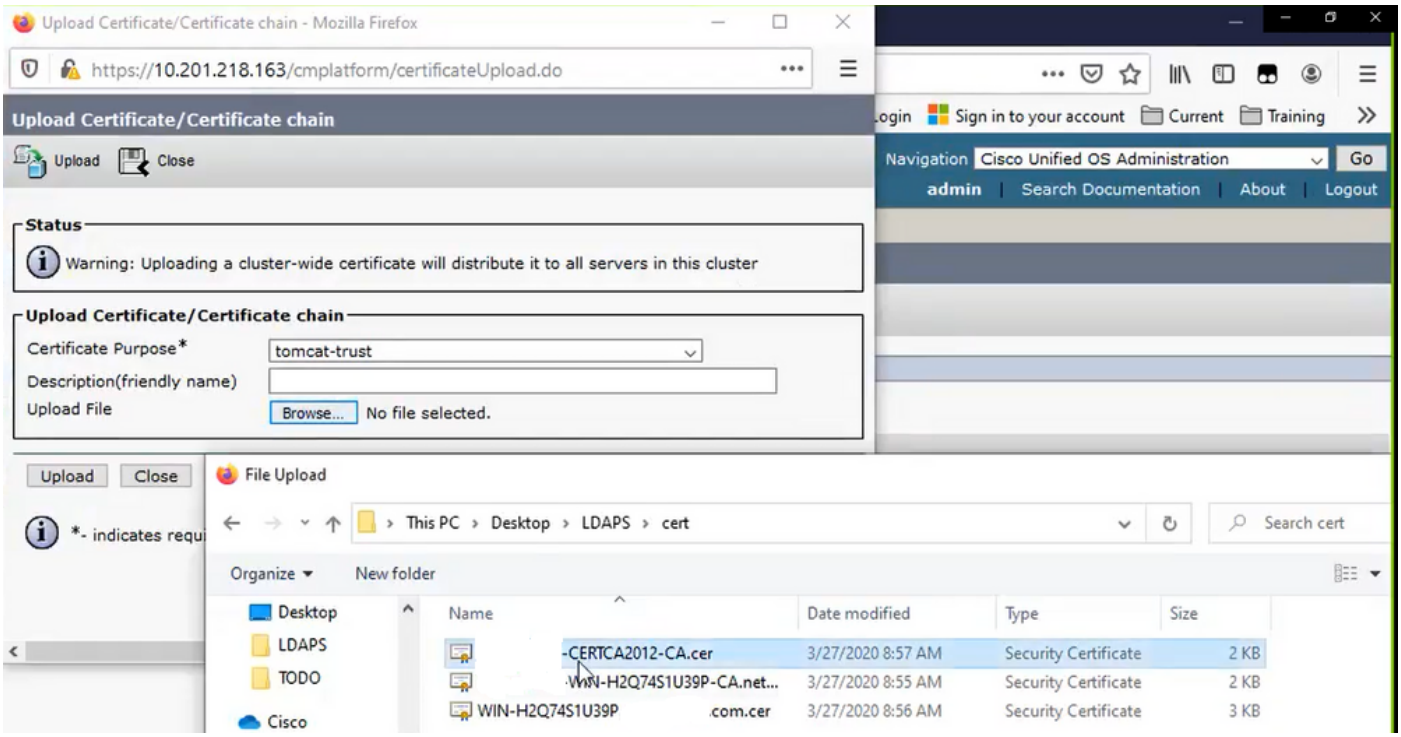


步驟 2.獲取根證書和屬於LDAPS伺服器證書一部分的任何中間證書，並將這些證書作為tomcat-trust證書安裝在CUCM和IM/P發佈伺服器節點上，作為CallManager-trust安裝在CUCM發佈伺服器上。

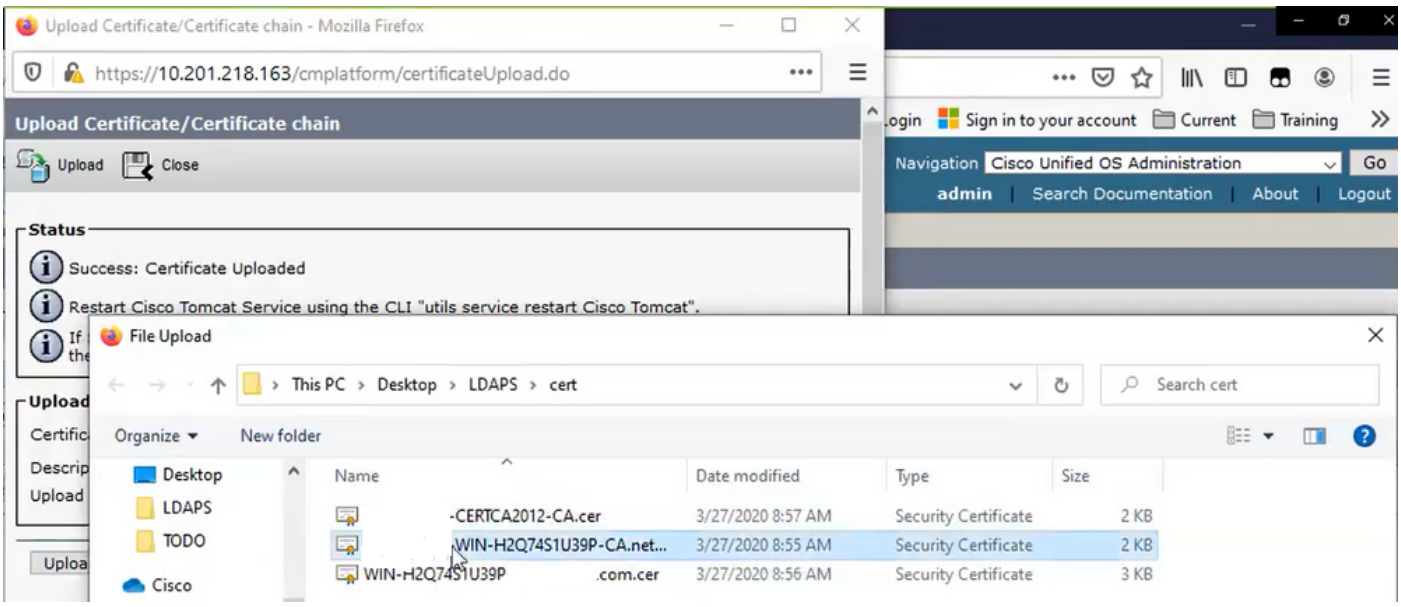
LDAPS伺服器證書<hostname>.<Domain>.cer中的根證書和中間證書如下圖所示：



導航到CUCM發佈伺服器思科統一作業系統管理>安全>證書管理。將根上傳為tomcat-trust （如圖所示）和CallManager-trust（未顯示）：



將intermediate上傳為tomcat-trust （如圖所示）和CallManager-trust（未顯示）：

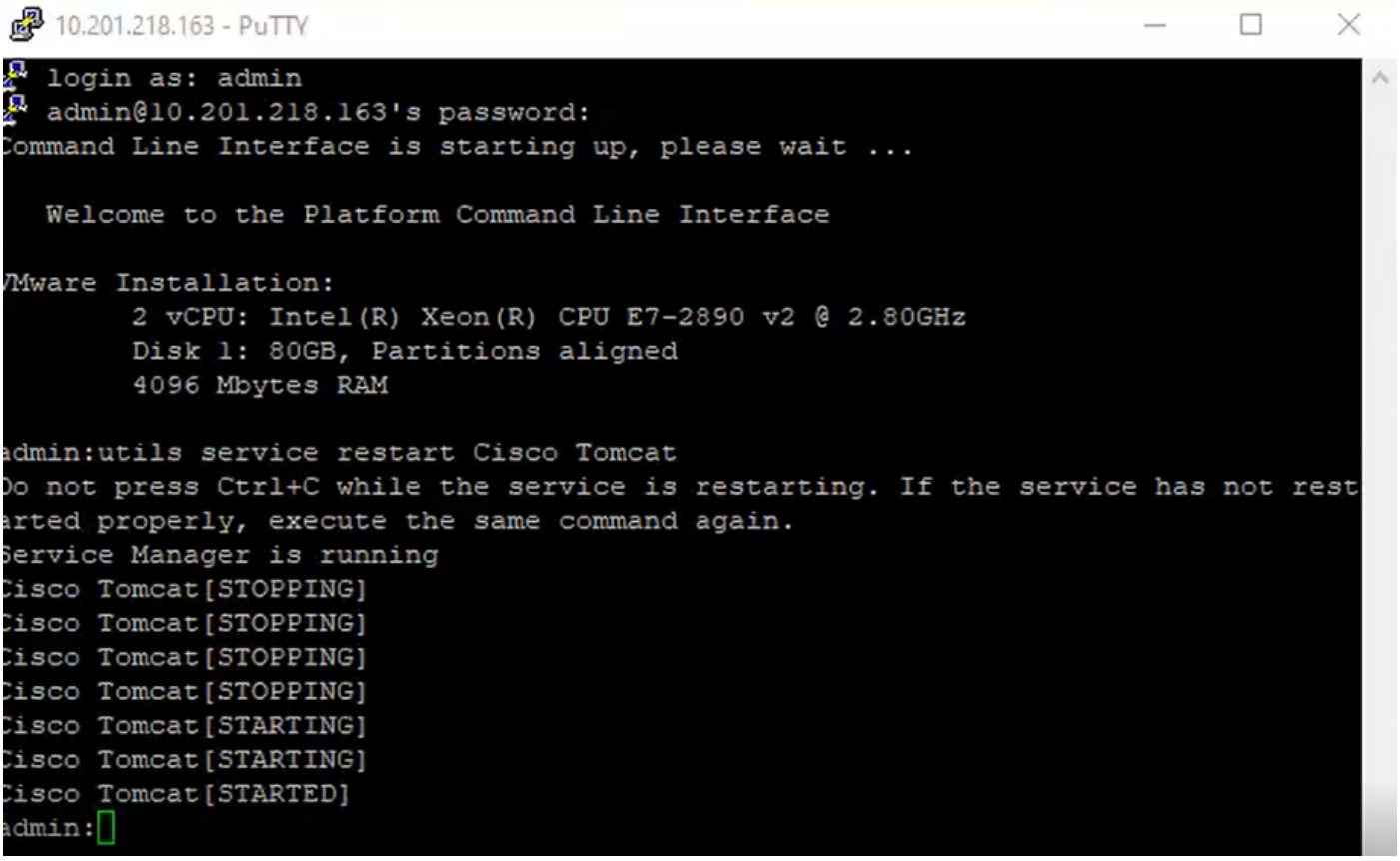


注意：如果您的IM/P伺服器是CUCM集群的一部分，則還需要將這些證書上傳到這些IM/P伺服器。

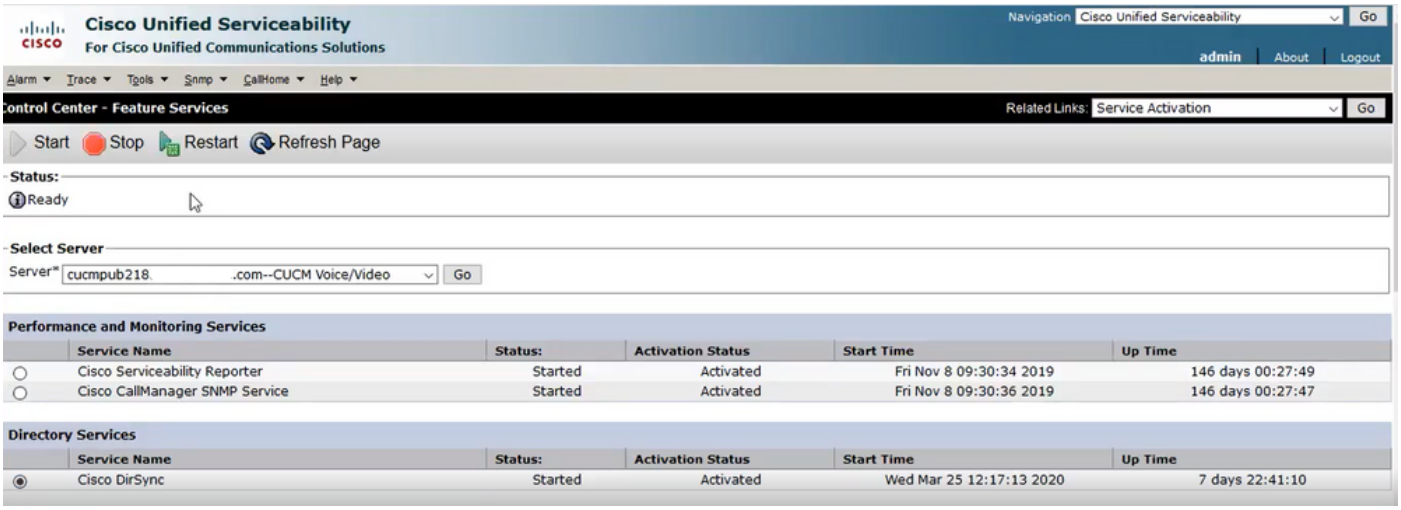
注意：您也可以將LDAPS伺服器憑證安裝為tomcat-trust。

步驟 3.從集群中每個節點（CUCM和IM/P）的CLI重新啟動Cisco Tomcat。此外，對於CUCM集群，驗證發佈伺服器節點上的Cisco DirSync服務是否已啟動。

要重新啟動Tomcat服務，需要為每個節點打開一個CLI會話並運行utils service restart Cisco Tomcat命令，如下圖所示：



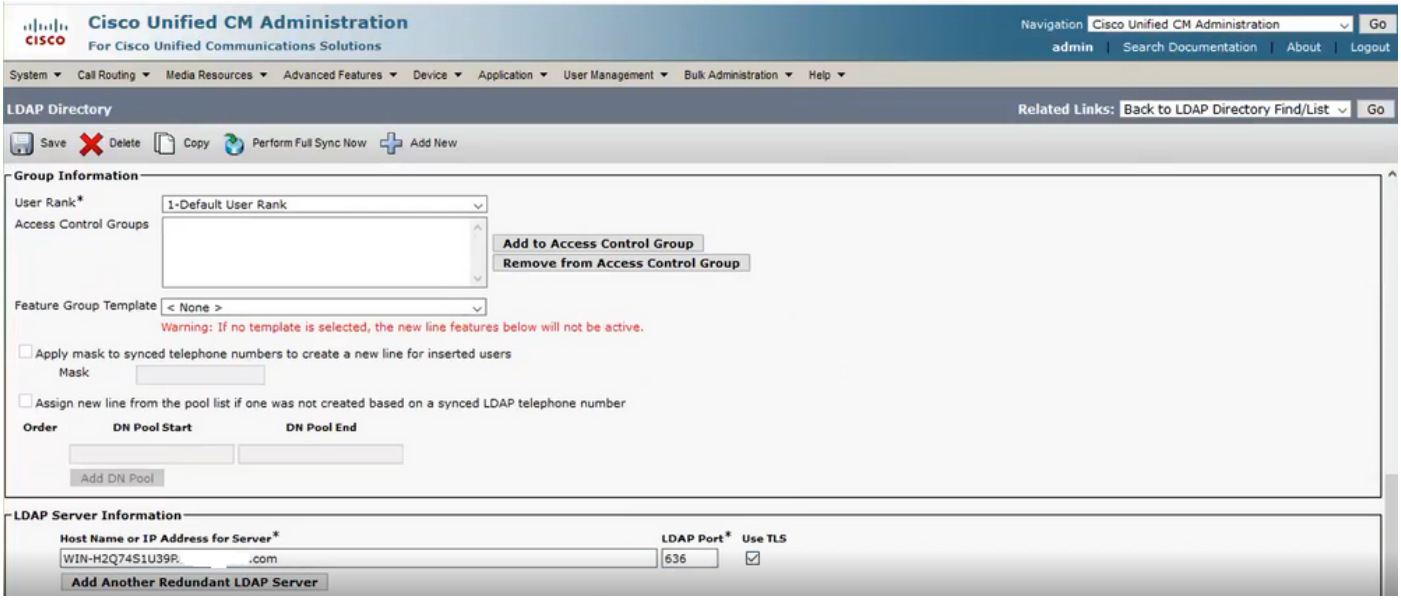
步驟 4.導航到CUCM發佈伺服器Cisco Unified Serviceability > Tools > Control Center - Feature Services，驗證Cisco DirSync服務是否已啟用和啟動（如圖所示），如果使用了Cisco CTIManager服務（未顯示），請在每個節點上重新啟動該服務：

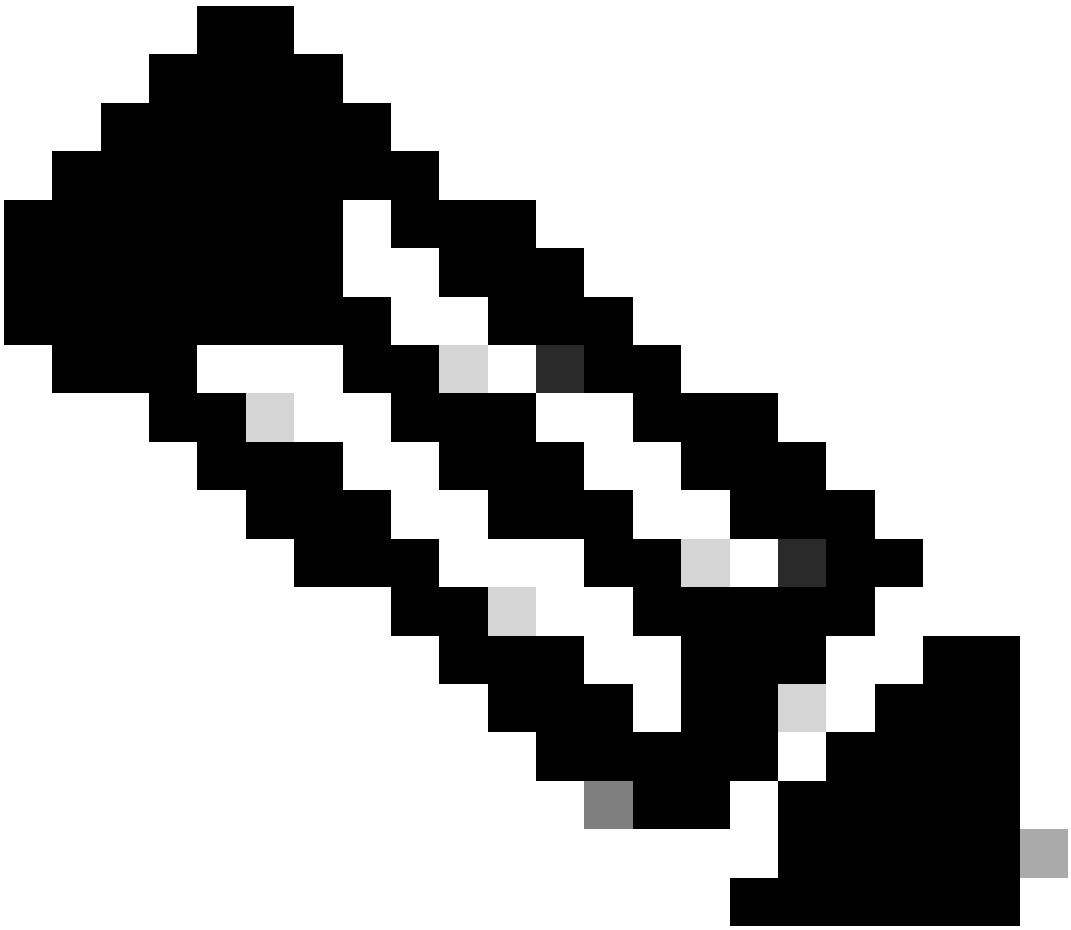


配置Secure LDAP目錄

步驟 1.配置CUCM LDAP目錄，以便在埠636上利用LDAPS TLS與AD的連線。

導航到CUCM管理>系統> LDAP目錄。鍵入LDAP伺服器資訊的FQDN或LDAP伺服器的IP地址。指定LDAPS埠636，並選中Use TLS框，如下圖所示：

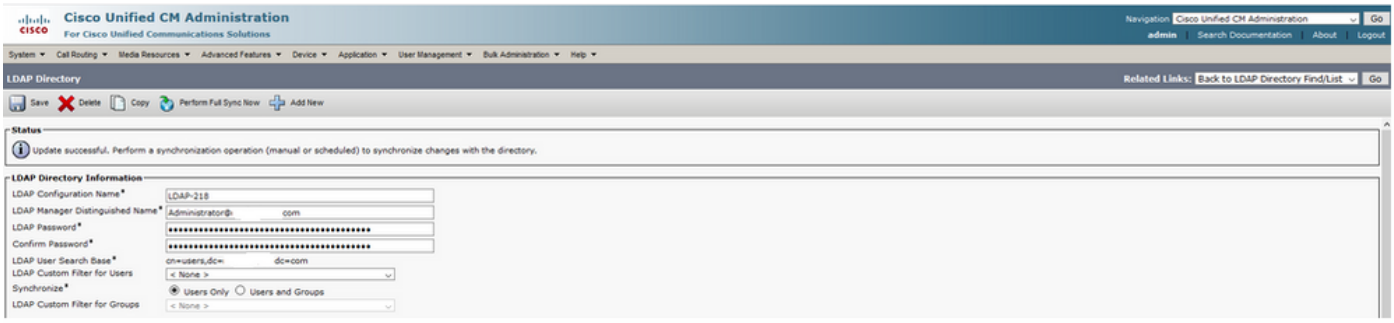




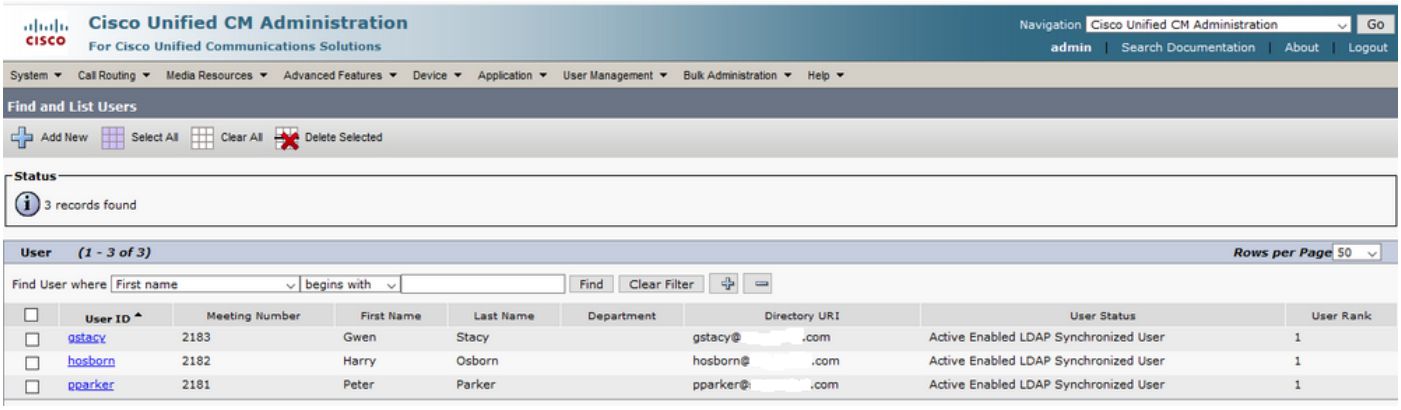
注意：預設情況下，在LDAP伺服器資訊中配置的10.5(2)SU2和9.1(2)SU3 FQDN版本根據證書的公用名進行檢查後，如果使用的是IP地址而不是FQDN，則會發出utils ldap config

ipaddr命令停止將FQDN強制實施到CN驗證。

步驟 2.要完成對LDAPS的配置更改，請按一下Perform Full Sync，如圖所示：

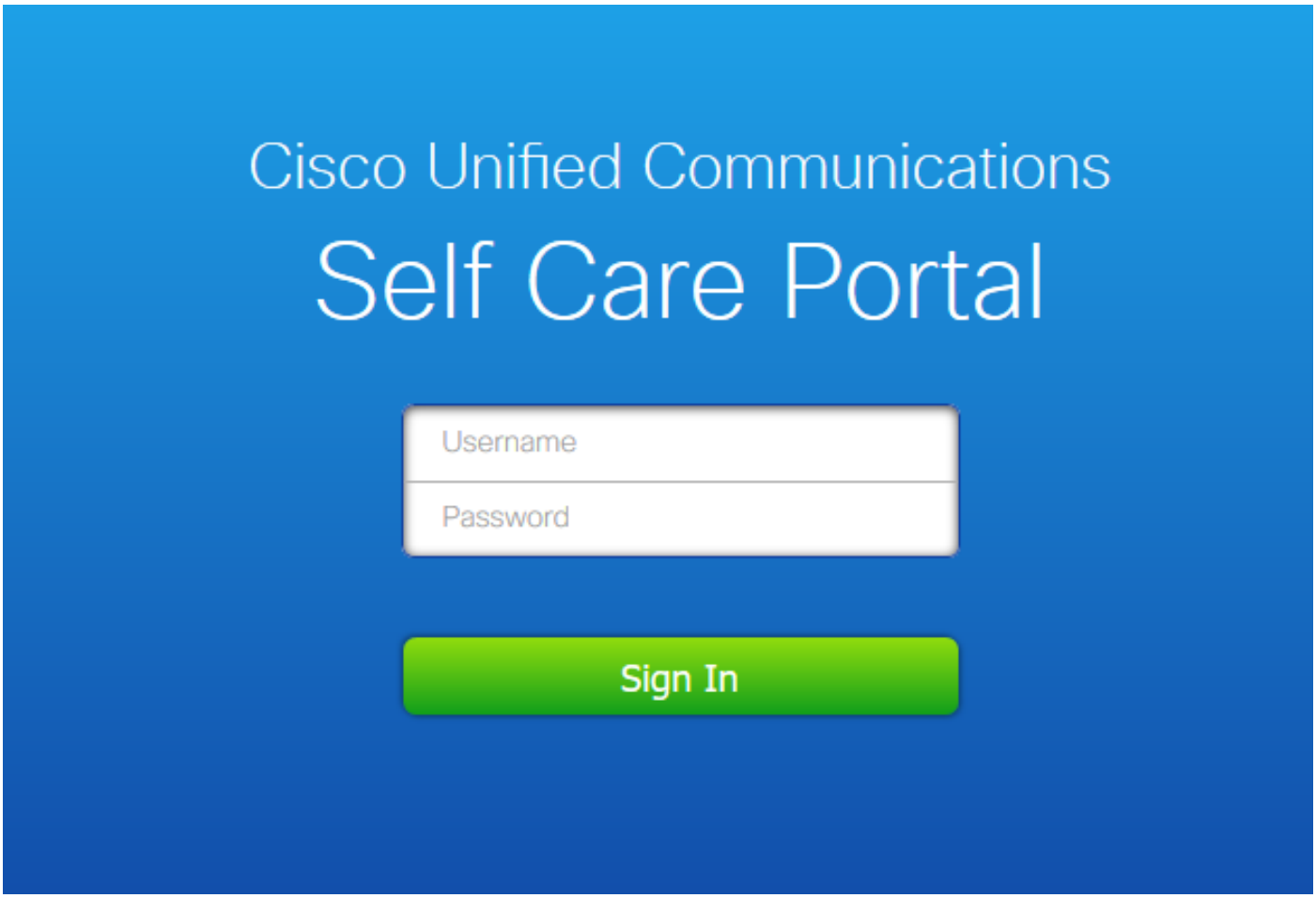


步驟 3.導航到CUCM管理>使用者管理>終端使用者，確認存在終端使用者，如下圖所示：

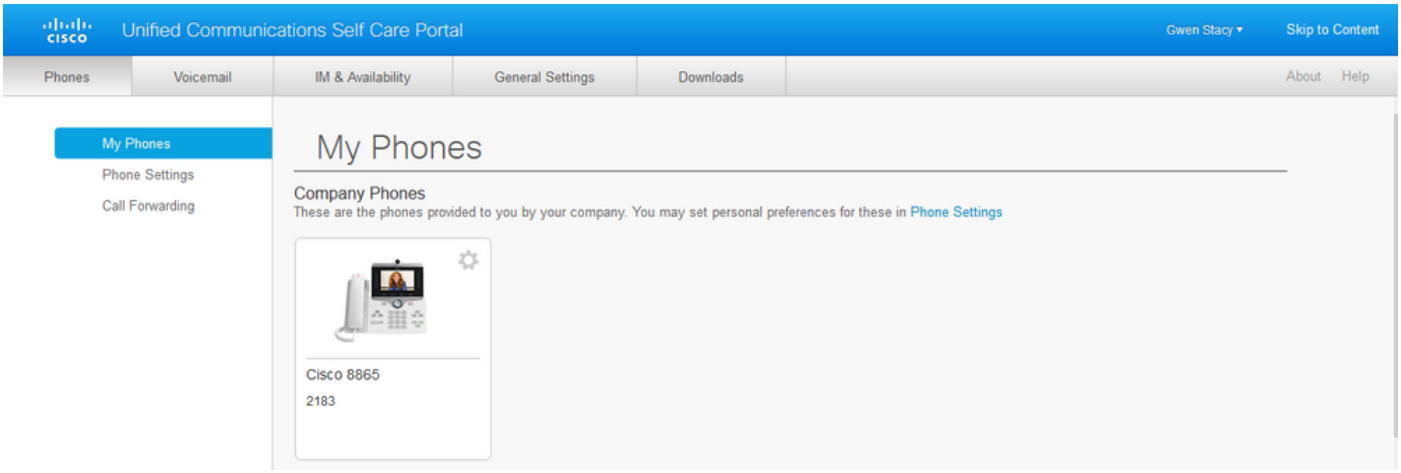


步驟 4.導航到ccmuser頁(https://<cucm pub的ip地址>/ccmuser)驗證使用者登入是否成功。

CUCM版本12.0.1的ccmuser頁面如下所示：



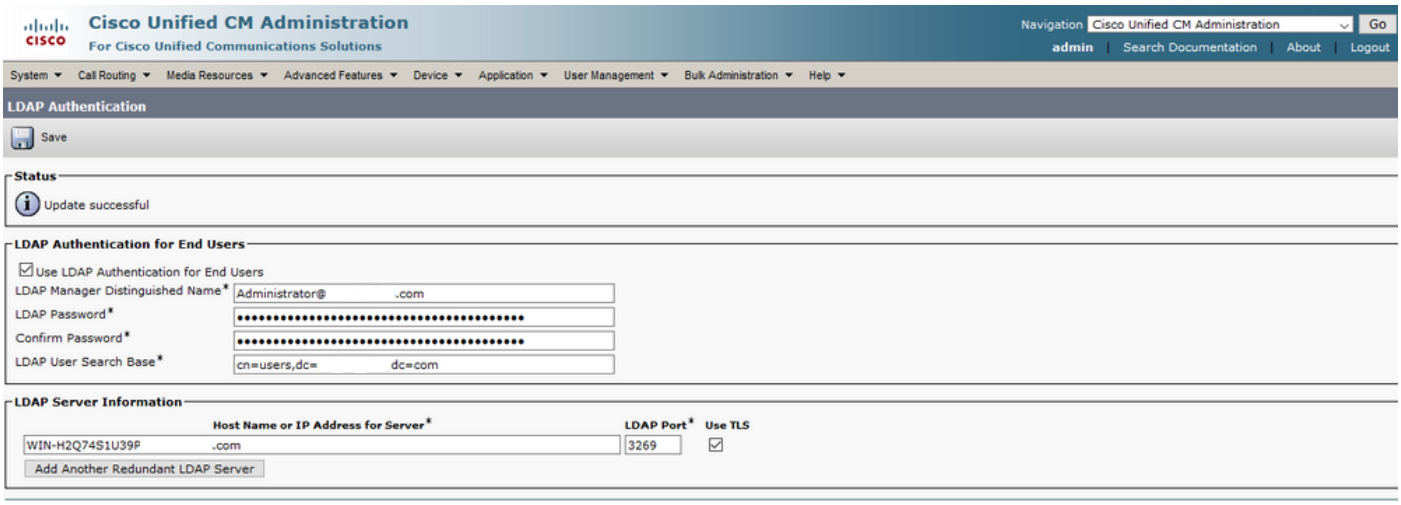
輸入LDAP憑證後，使用者即可成功登入，如下圖所示：

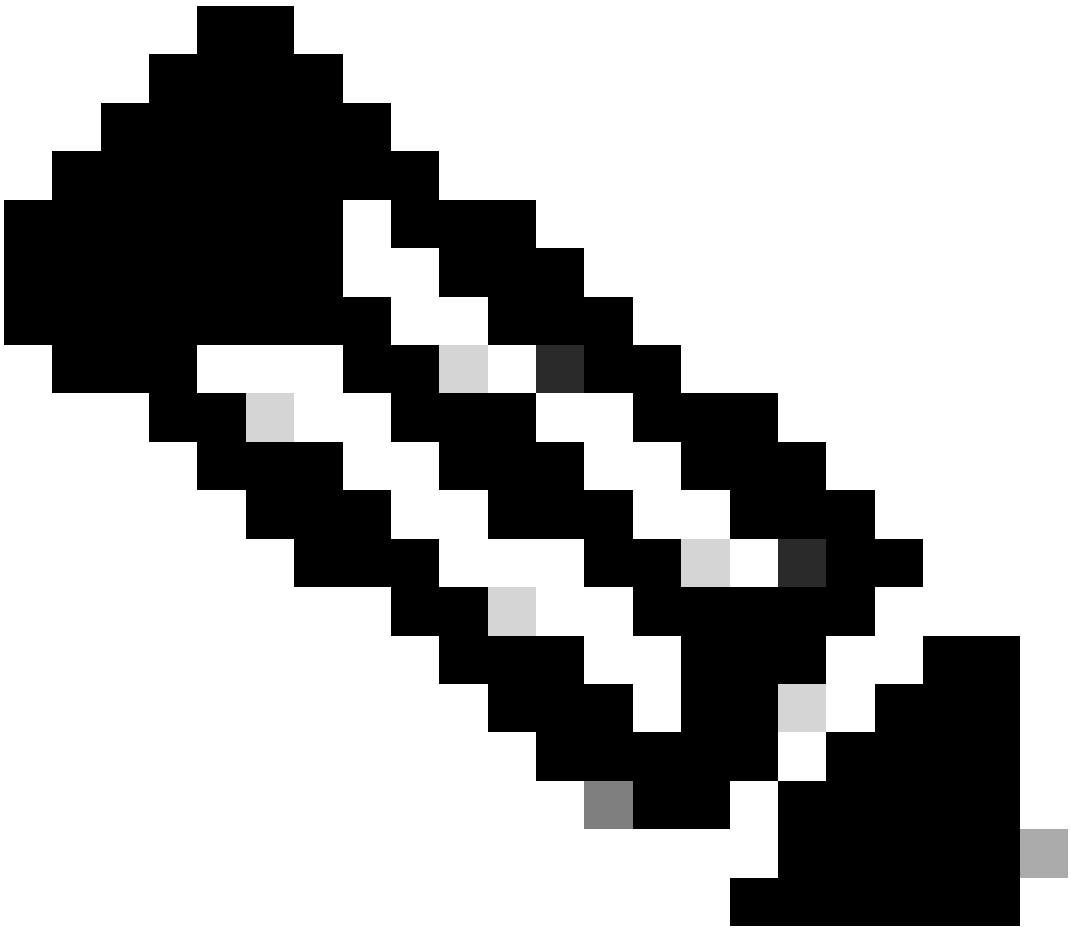


配置安全LDAP身份驗證

配置CUCM LDAP身份驗證以利用到埠3269上的AD的LDAPS TLS連線。

導航到CUCM管理>系統> LDAP身份驗證。鍵入LDAP伺服器資訊的LDAPS伺服器的FQDN。指定LDAPS埠3269，並選中Use TLS框，如下圖所示：



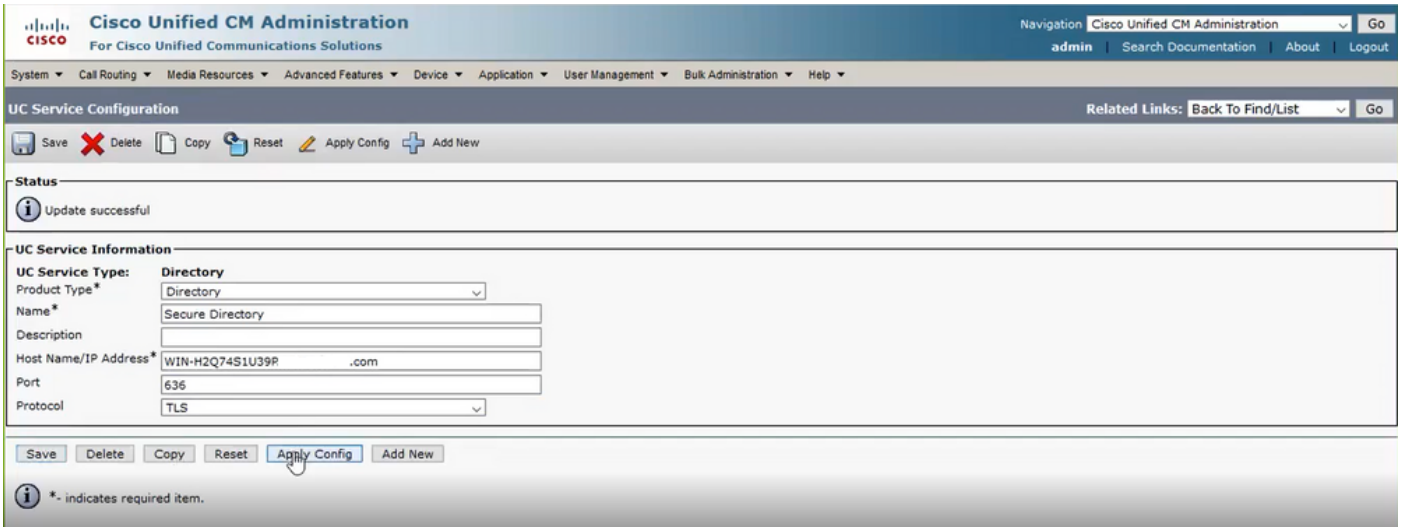


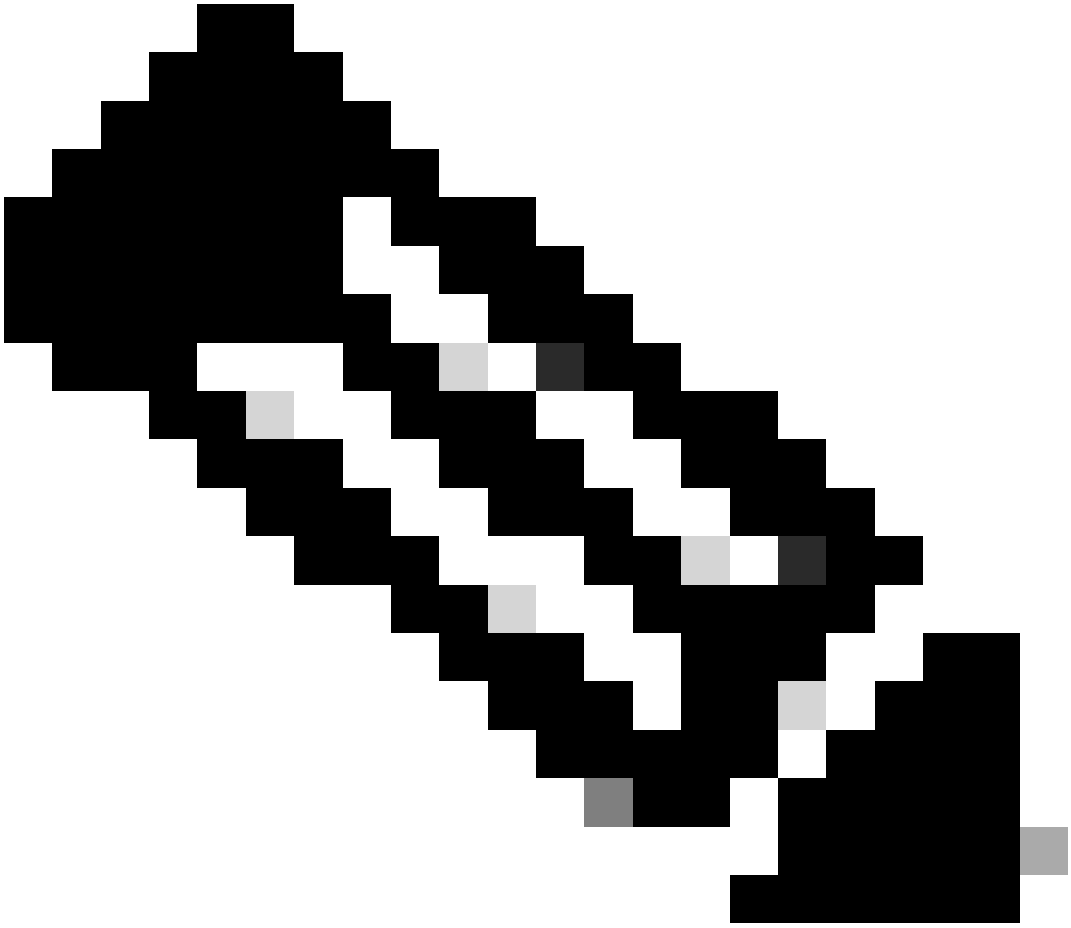
注意：如果您有Jabber客戶端，建議使用3269埠進行LDAPS身份驗證，因為如果未指定到全局目錄伺服器的安全連線，則可能會發生登入時Jabber超時。

為UC服務配置與AD的安全連線

如果需要保護利用LDAP的UC服務，請配置這些UC服務以利用TLS的埠636或3269。

導航到CUCM管理>使用者管理>使用者設定> UC服務。尋找指向AD的目錄服務。鍵入LDAPS伺服器的FQDN作為主機名/IP地址。將埠指定為636或3269以及協定TLS，如下圖所示：





注意：Jabber客戶端電腦還需要在Jabber客戶端電腦的證書管理信任儲存中安裝CUCM上安裝的tomcat-trust LDAPS證書，以便允許Jabber客戶端建立到AD的LDAPS連線。

驗證

使用本節內容，確認您的組態是否正常運作。

要驗證從LDAP伺服器傳送到CUCM的TLS連線的實際LDAPS證書/證書鏈，請從CUCM資料包捕獲導出LDAPS TLS證書。此連結提供有關如何從CUCM資料包捕獲導出TLS證書的資訊：如何從CUCM資料包捕獲導出TLS證書

疑難排解

目前沒有特定資訊可用於對此組態進行疑難排解。

相關資訊

- 此連結提供對穿越LDAPS配置的影片的訪問：安全LDAP目錄和身份驗證穿透影片
- 技術支援與文件 - Cisco Systems

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）。