Configurazione di CUCM per LDAP sicuro (LDAPS)

Sommario

Introduzione

In questo documento viene descritta la procedura per aggiornare le connessioni CUCM ad AD da una connessione LDAP non protetta a una connessione LDAPS protetta.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

· Server LDAP AD
· Configurazione LDAP CUCM

· CUCM IM & Presence Service (IM/P)

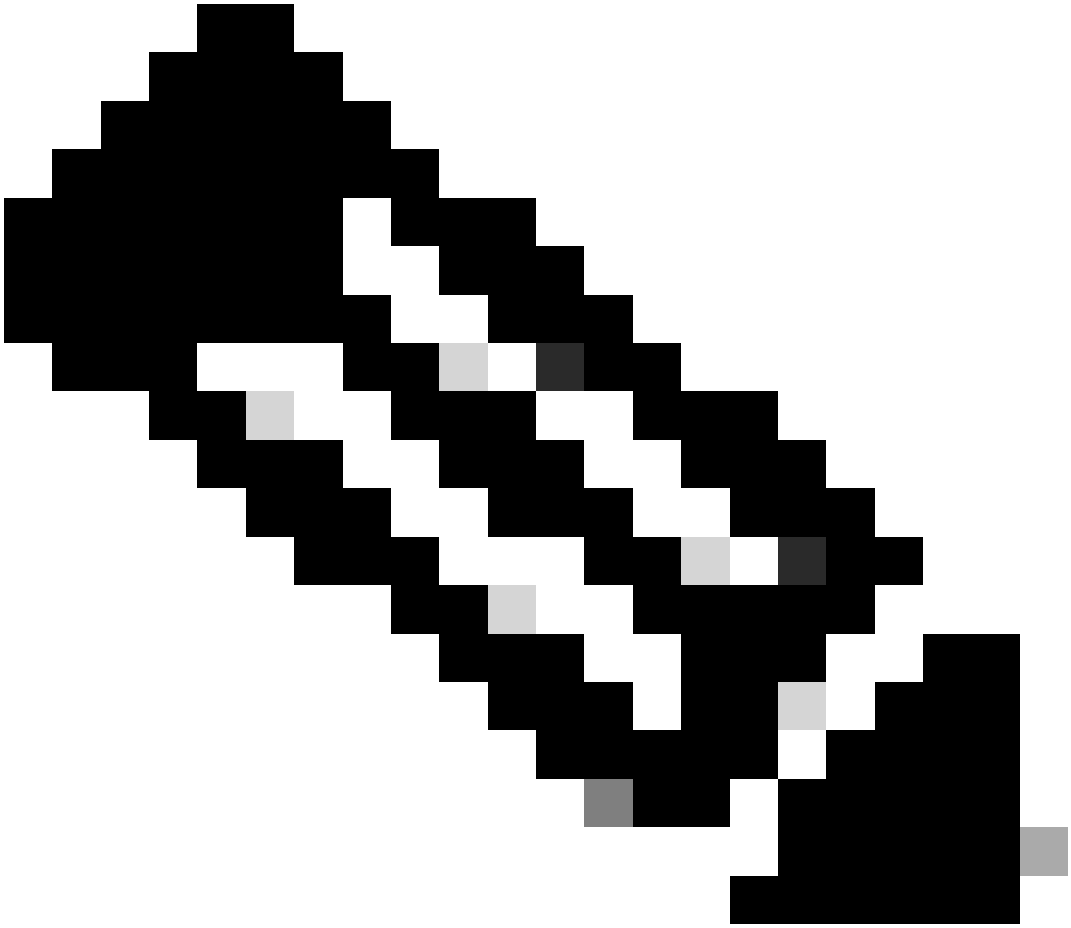
Componenti usati

Il riferimento delle informazioni contenute in questo documento è CUCM release 9.x e successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

È responsabilità dell'amministratore di Active Directory (AD) configurare AD Lightweight Directory Access Protocol (LDAP) per Lightweight Directory Access Protocol (LDAPS). È inclusa l'installazione di certificati firmati dalla CA che soddisfano i requisiti di un certificato LDAPS.



> Nota: per informazioni sull'aggiornamento da LDAP non sicuro a connessioni LDAPS sicure ad AD per altre applicazioni di collaborazione Cisco, vedere questo collegamento: Software Advisory: Secure LDAP Obbligatorio per connessioni Active Directory

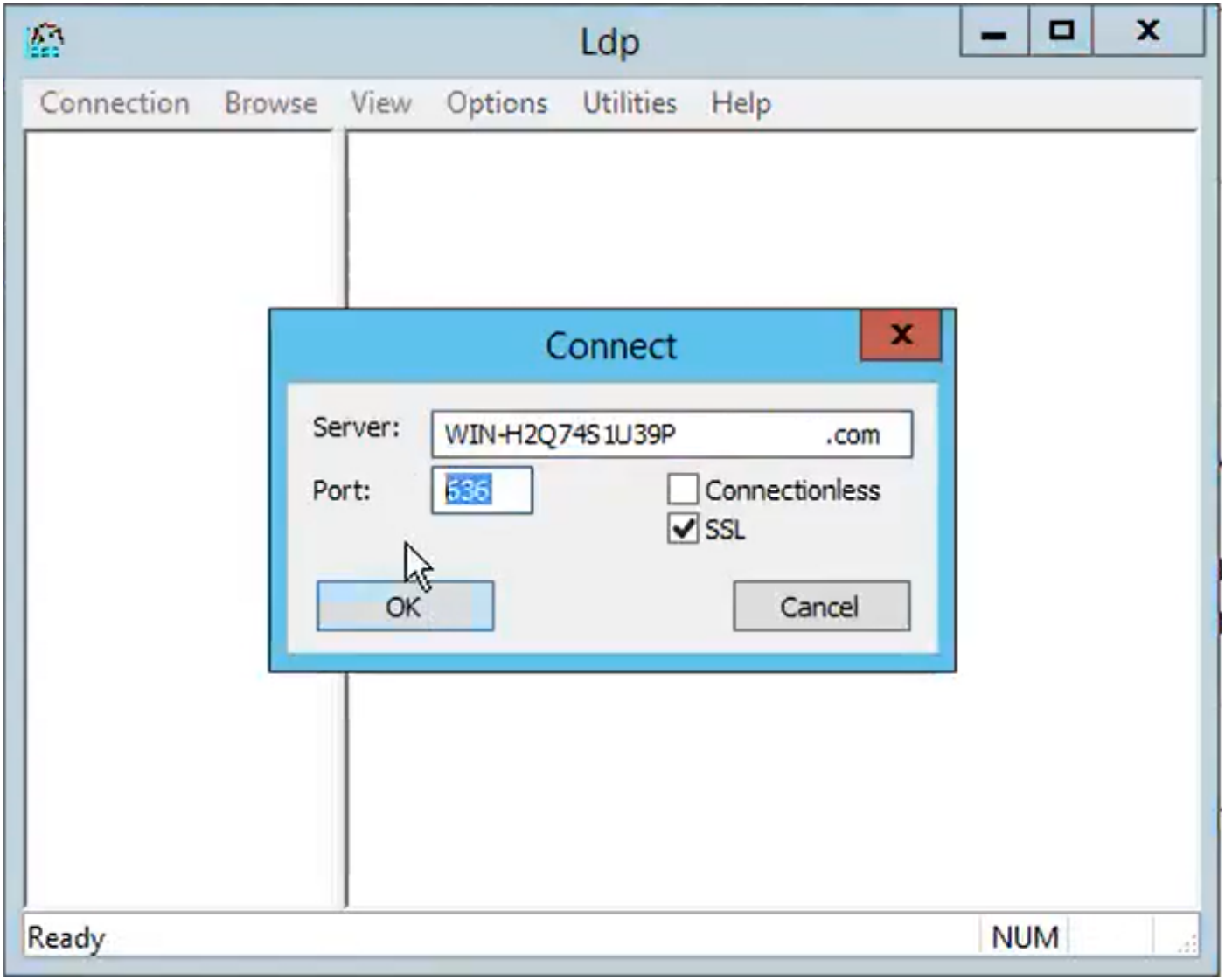
---

Verifica e installazione dei certificati LDAPS

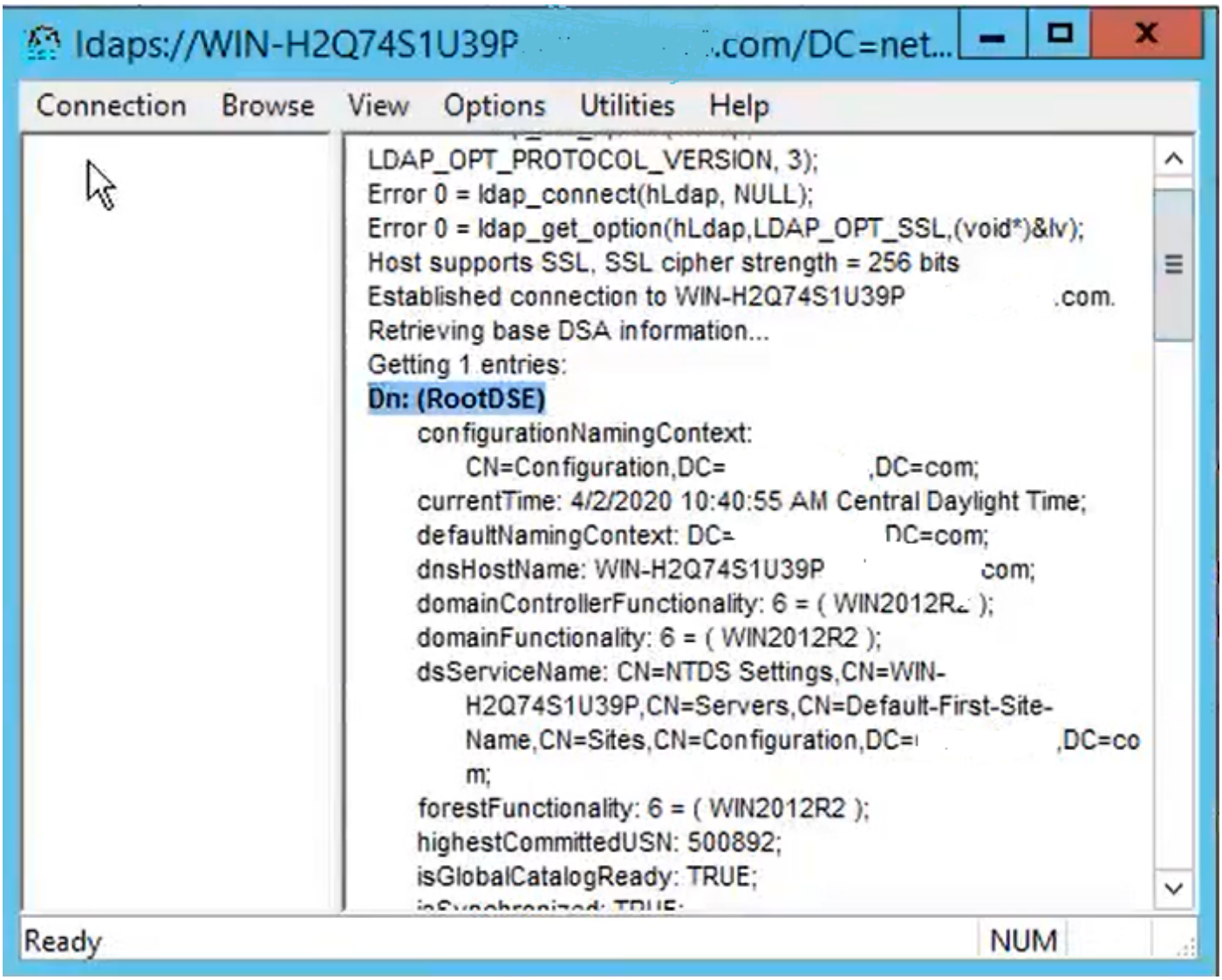
Passaggio 1. Dopo aver caricato il certificato LDAPS nel server AD, verificare che LDAPS sia abilitato nel server AD con lo strumento ldp.exe.

1. Avviare lo Strumento di amministrazione di Active Directory (Ldp.exe) nel server AD.

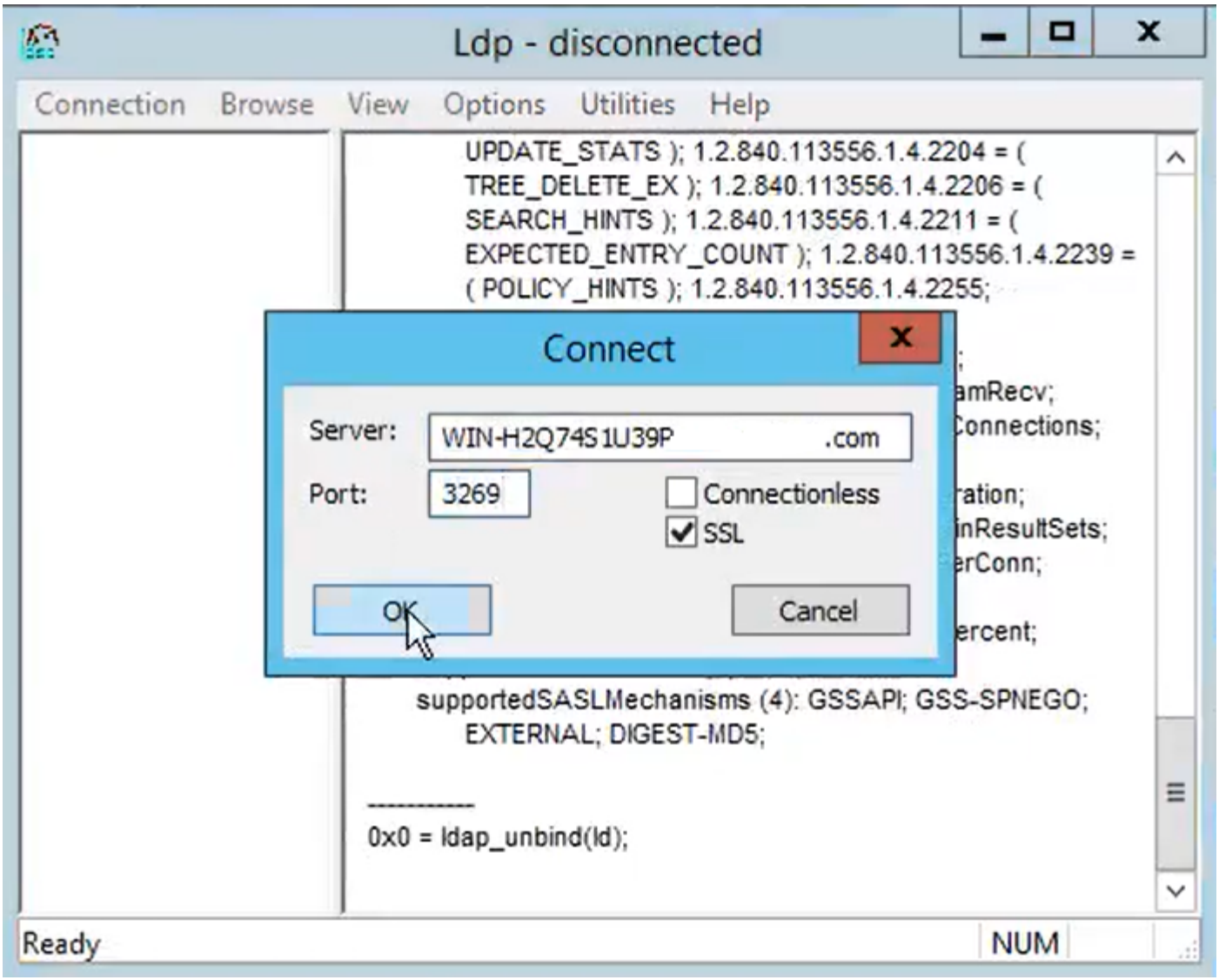
2. Scegliere Connetti dal menu Connessione.
3. Immettere il nome di dominio completo (FQDN) del server LDAPS come server.
4. Immettere 636 come numero di porta.
5. Fare clic su OK, come mostrato nell'immagine



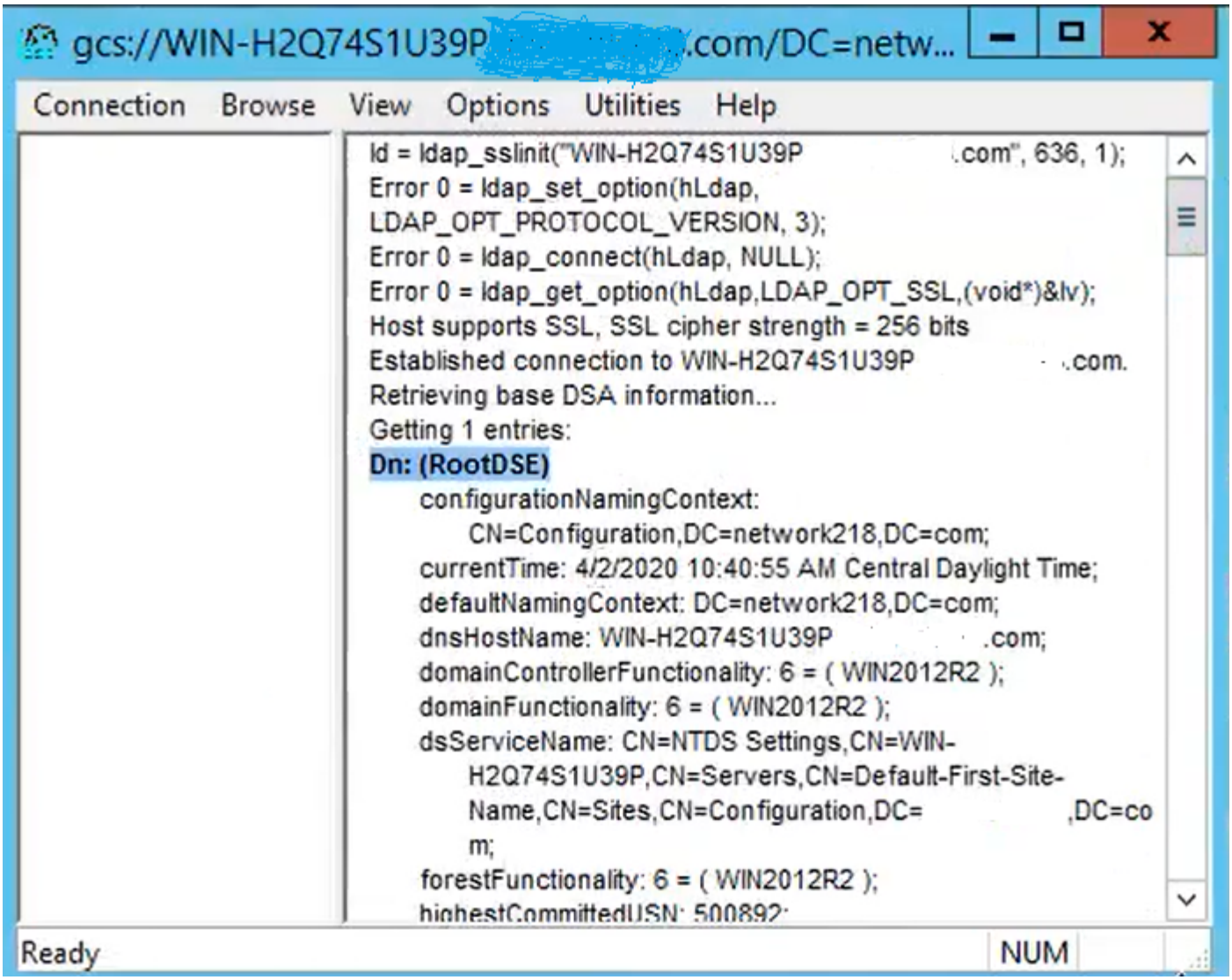
Per una connessione riuscita sulla porta 636, le informazioni di RootDSE vengono stampate nel riquadro destro, come mostrato nell'immagine:



Ripetere la procedura per la porta 3269, come mostrato nell'immagine:

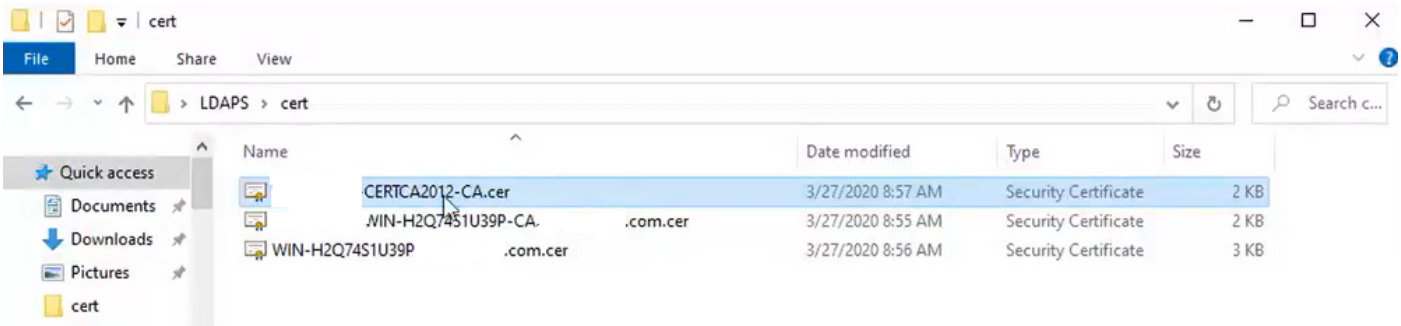


Per una connessione riuscita sulla porta 3269, le informazioni di RootDSE vengono stampate nel riquadro destro, come mostrato nell'immagine:

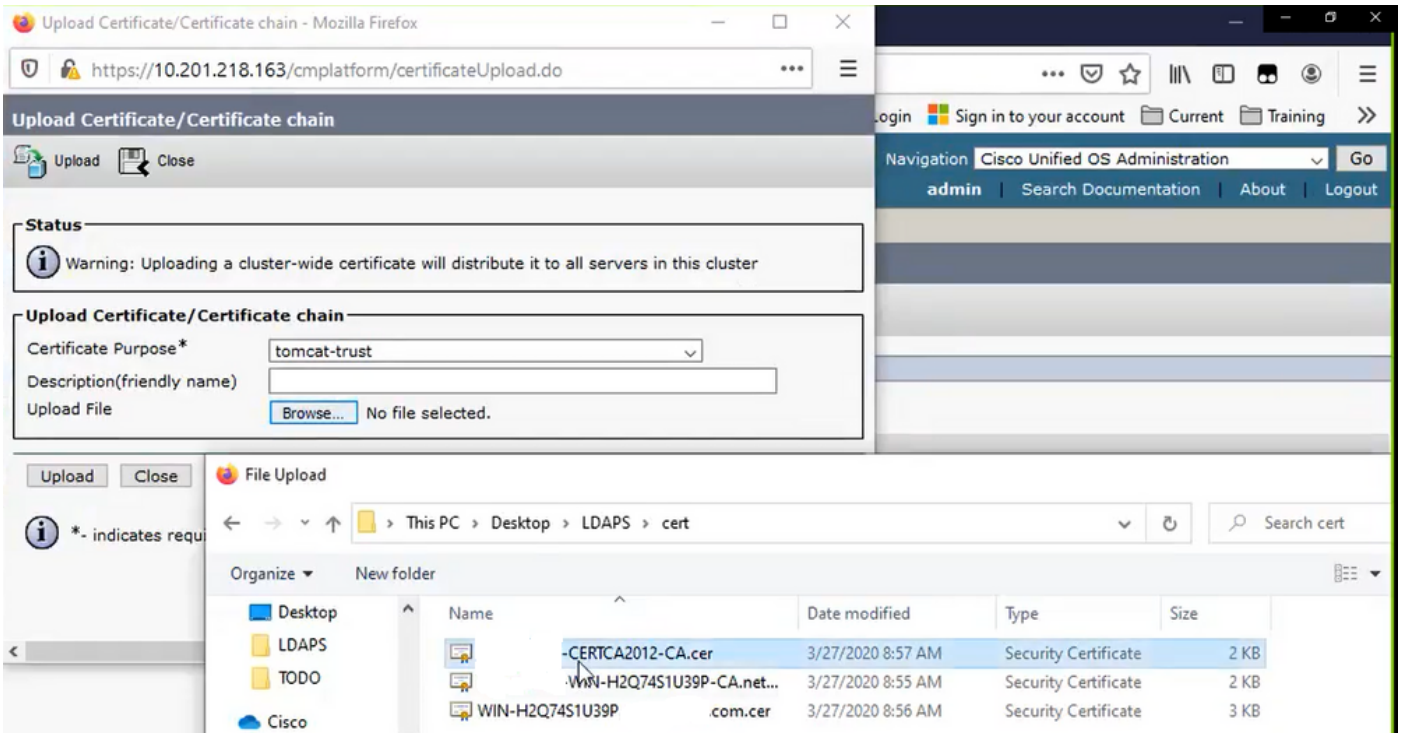


Passaggio 2. Ottenere il certificato radice e gli eventuali certificati intermedi che fanno parte del certificato del server LDAPS e installarli come certificati di attendibilità per gli utenti su ciascuno dei nodi di pubblicazione CUCM e IM/P e come CallManager-trust sull'autore CUCM.

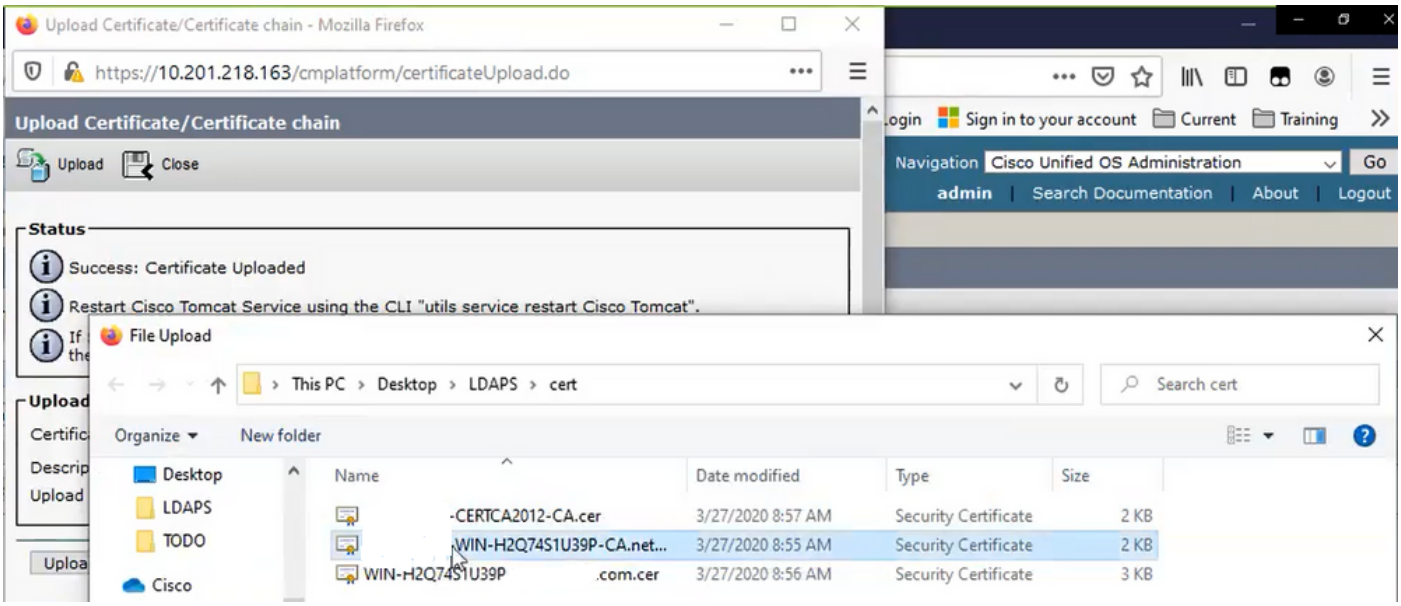
I certificati radice e intermedi che fanno parte di un certificato server LDAPS, <nomehost>.<Dominio>.cer, sono mostrati nell'immagine:



Passare a CUCM publisher Cisco Unified OS Administration > Security > Certificate Management (Amministrazione del sistema operativo unificato Cisco > Protezione > Gestione certificati). Caricare la radice come tomcat-trust (come mostrato nell'immagine) e come CallManager-trust (non mostrato):



Caricare la parte intermedia come tomcat-trust (come mostrato nell'immagine) e come CallManager-trust (non mostrato):

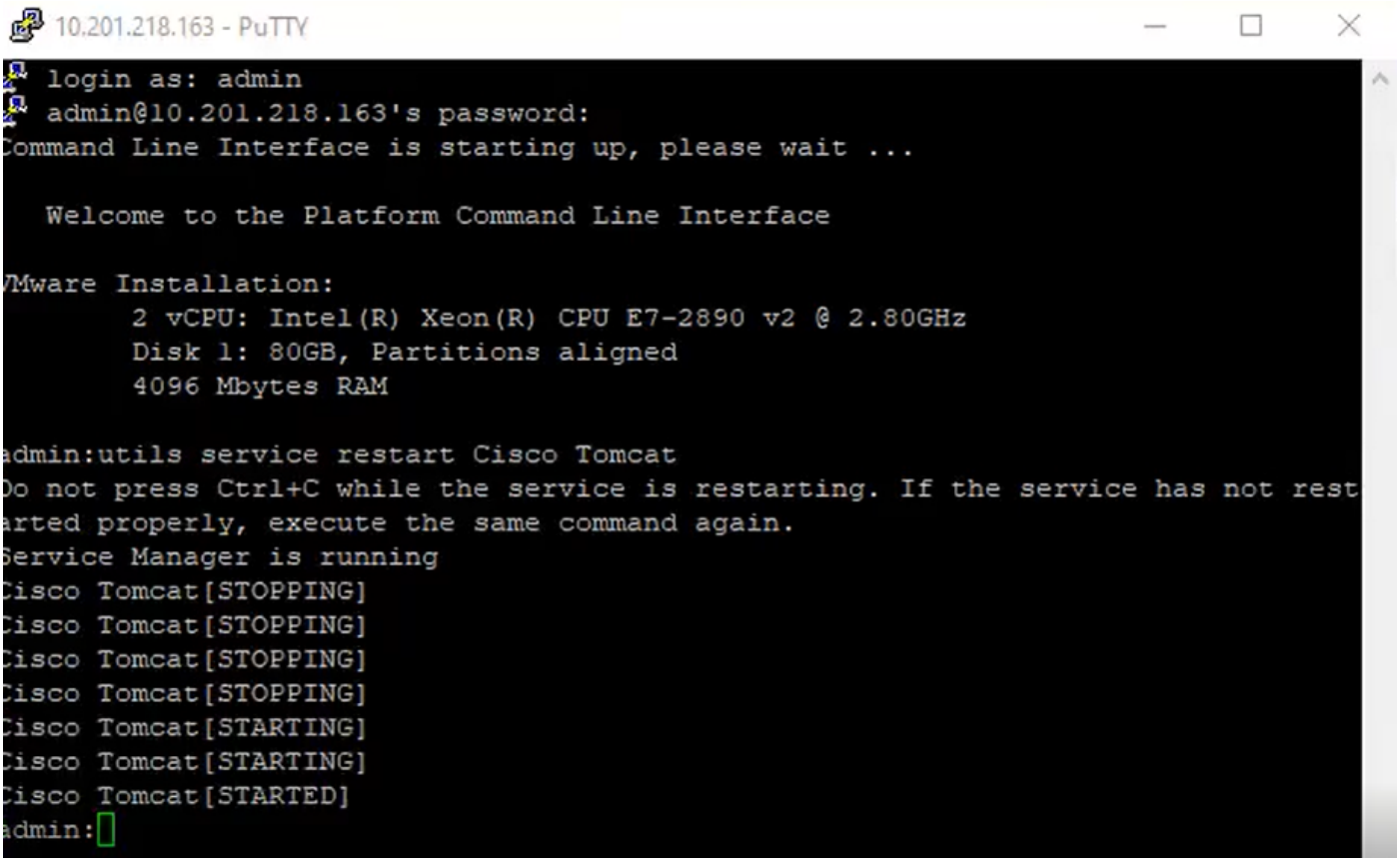


Nota: se si dispone di server IM/IP che fanno parte del cluster CUCM, è inoltre necessario caricare questi certificati in questi server IM/IP.

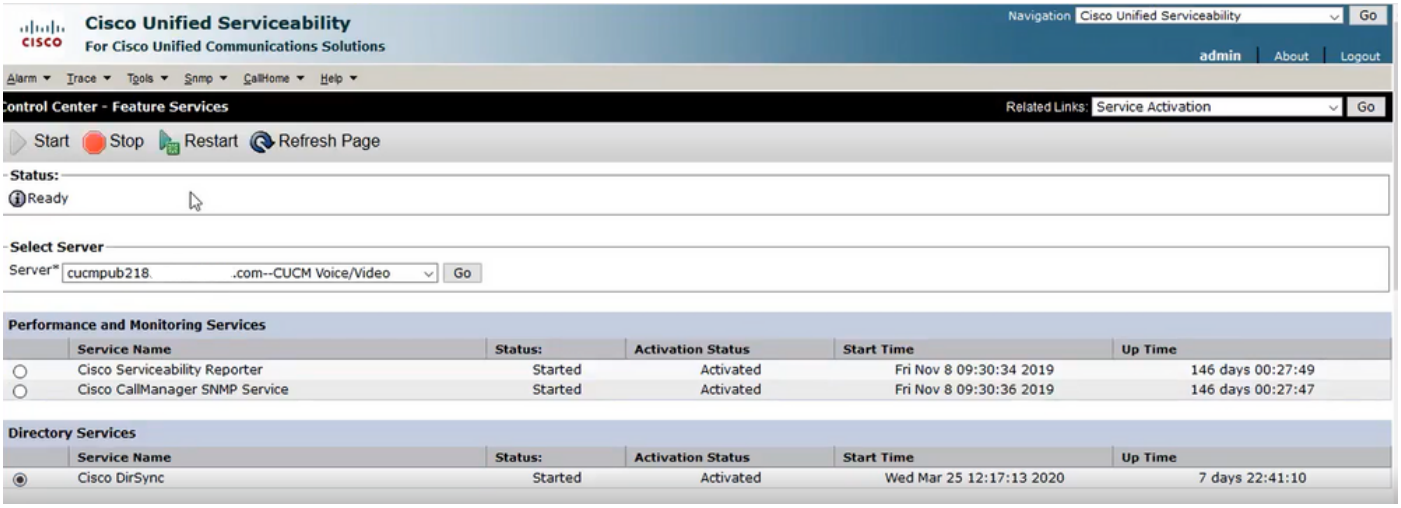
Nota: in alternativa, è possibile installare il certificato del server LDAPS come tomcat-trust.

Passaggio 3. Riavviare Cisco Tomcat dalla CLI di ciascun nodo (CUCM e IM/P) nei cluster. Inoltre, per il cluster CUCM, verificare che il servizio Cisco DirSync sul nodo del server di pubblicazione sia avviato.

Per riavviare il servizio Tomcat, è necessario aprire una sessione CLI per ciascun nodo ed eseguire il comando utils service restart Cisco Tomcat, come mostrato nell'immagine:



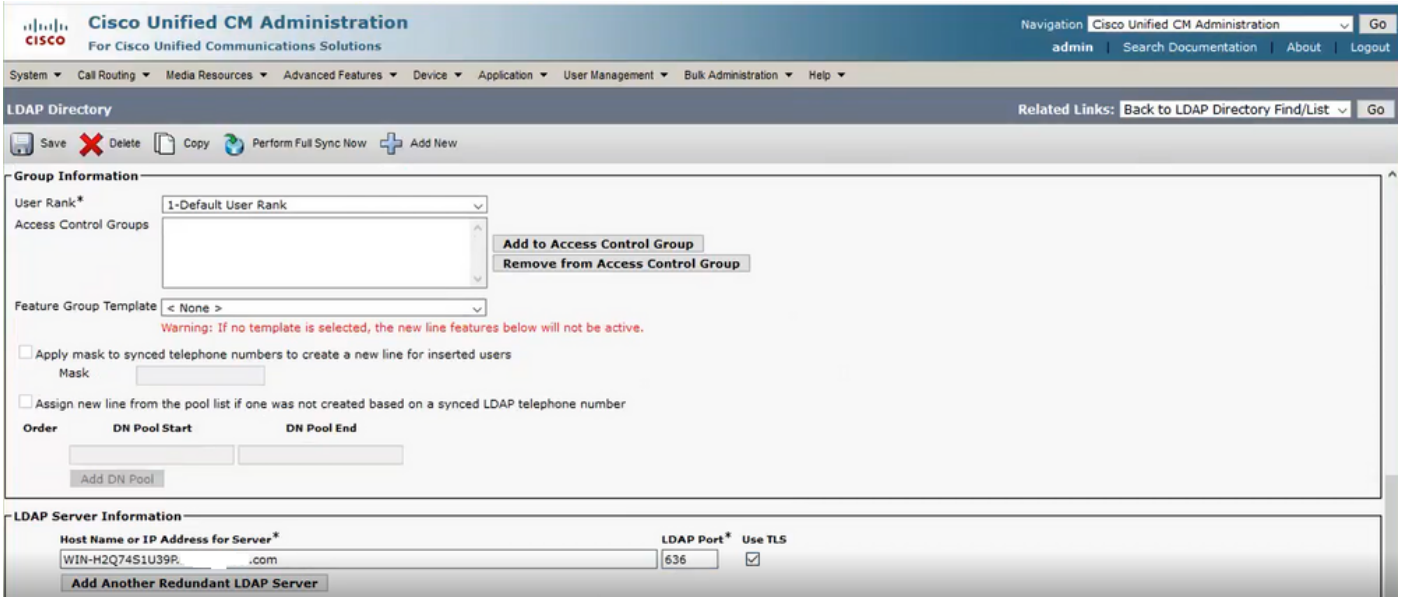
Passaggio 4. Passare a Cisco Unified Serviceability > Strumenti > Control Center - Servizi funzionalità, verificare che il servizio Cisco DirSync sia attivato e avviato (come mostrato nell'immagine), quindi riavviare il servizio Cisco CTIManager su ogni nodo, se utilizzato (non visualizzato):

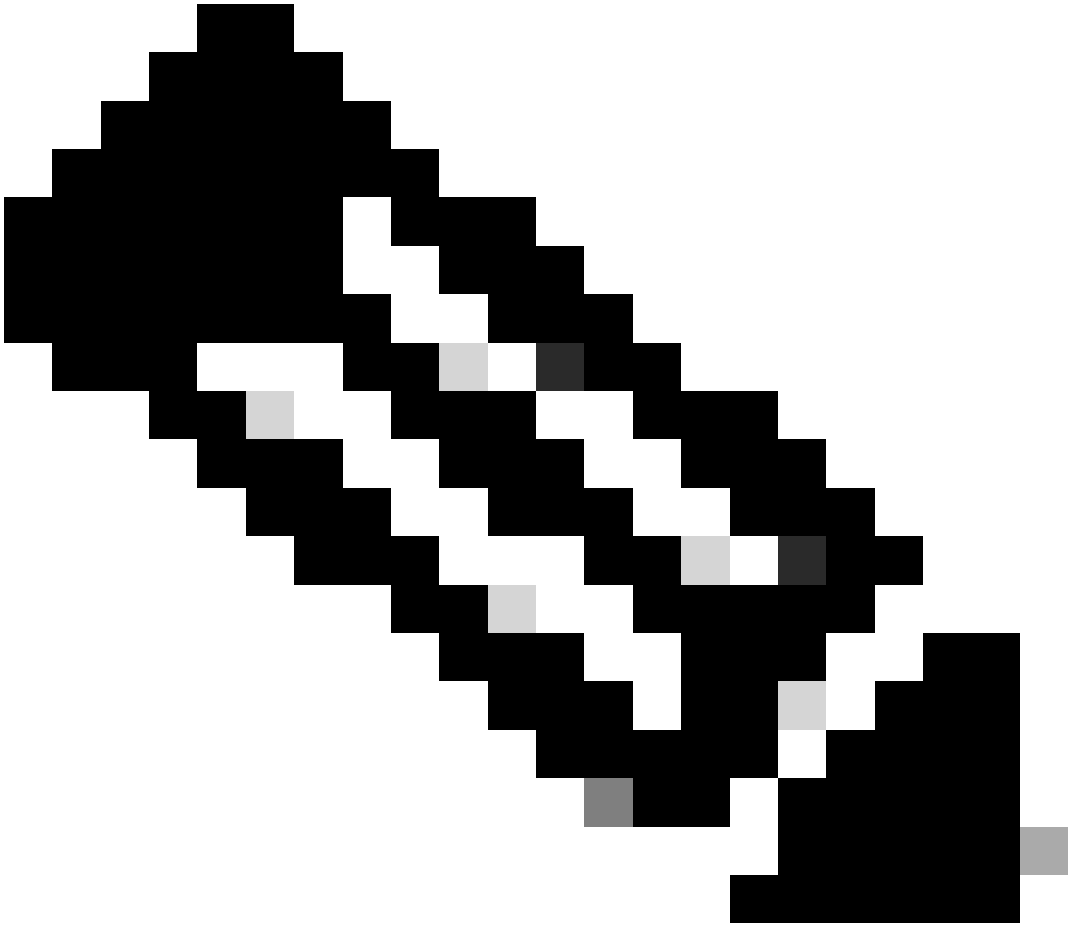


Configura directory LDAP protetta

Passaggio 1. Configurare l'elenco LDAP di CUCM per utilizzare la connessione LDAPS TLS ad AD sulla porta 636.

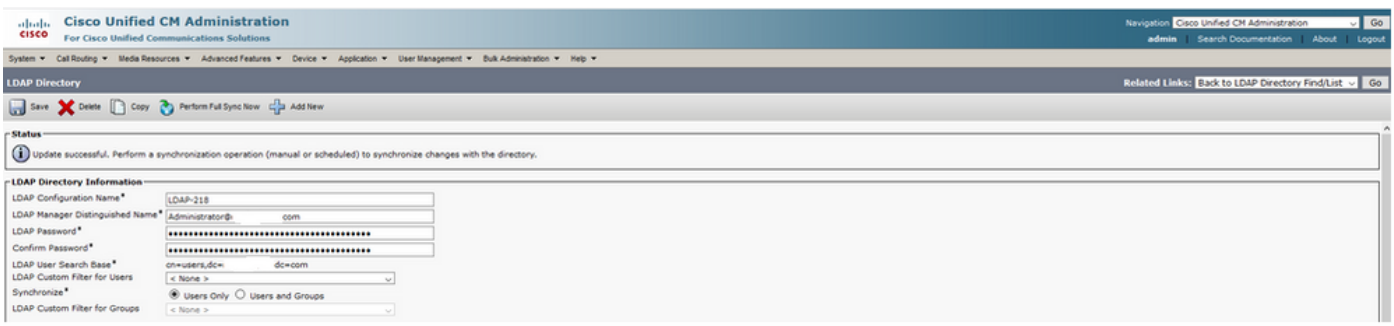
Passare a Amministrazione CUCM > Sistema > LDAP Directory. Digitare il nome di dominio completo (FQDN) o l'indirizzo IP del server LDAPS per Informazioni server LDAP. Specificare la porta LDAPS di 636 e selezionare la casella Use TLS (Usa TLS), come mostrato nell'immagine:



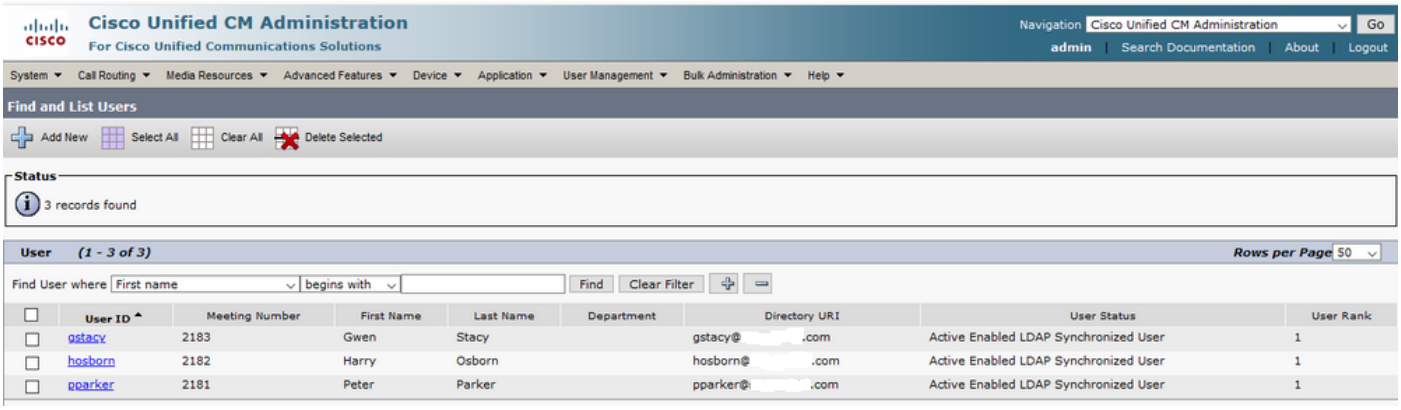


Nota: per impostazione predefinita, dopo che le versioni 10.5(2)SU2 e 9.1(2)SU3 FQDN configurate in Informazioni server LDAP sono state confrontate con il nome comune del certificato, nel caso in cui venga utilizzato l'indirizzo IP anziché il nome di dominio completo (FQDN), il comando utilizza il comando ldap config ipaddr per interrompere l'applicazione del nome di dominio completo alla verifica CN.

Passaggio 2. Per completare la modifica alla configurazione di LDAPS, fare clic su Perform Full Sync Now (Esegui sincronizzazione completa ora), come mostrato nell'immagine:

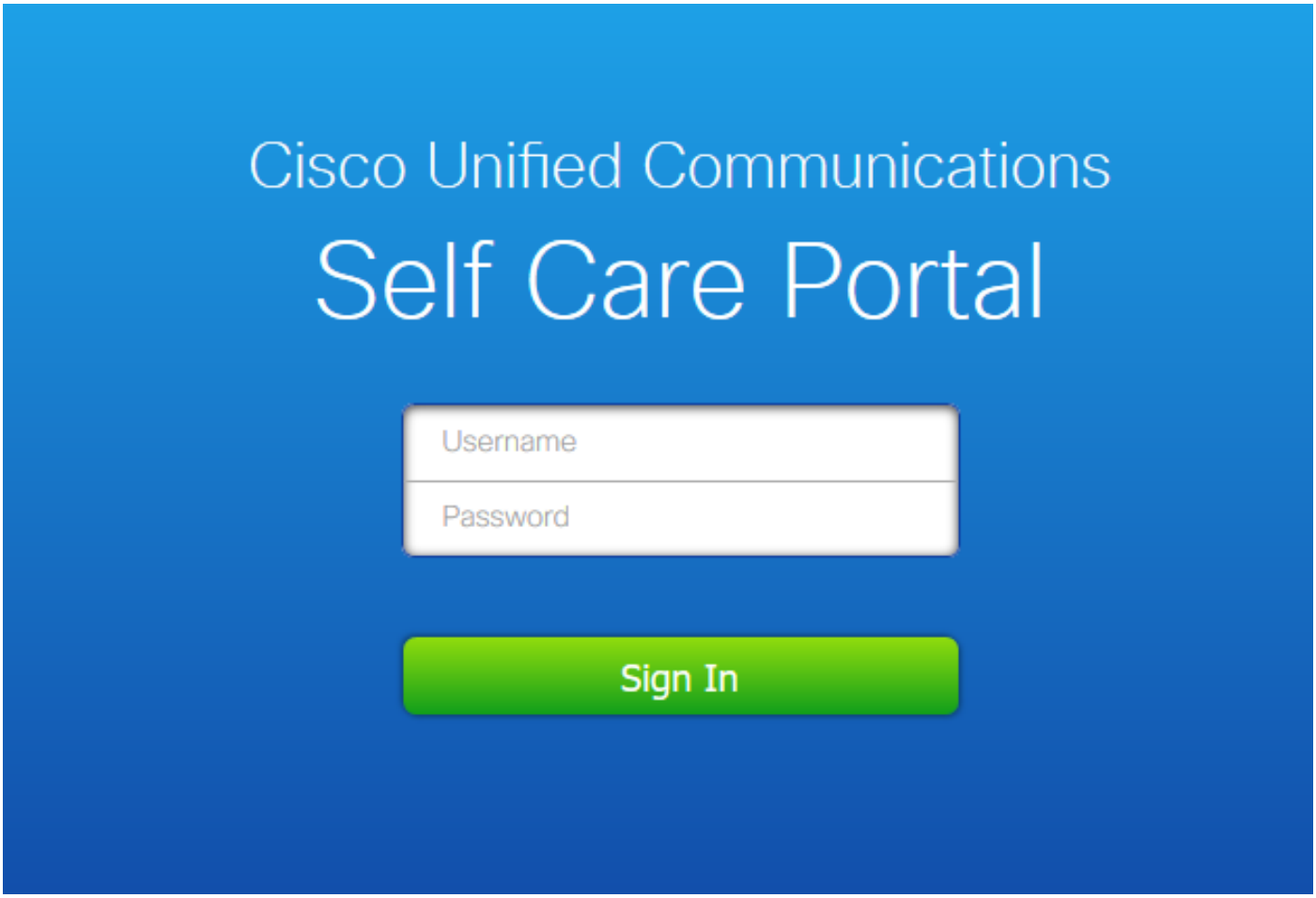


Passaggio 3. Passare a Amministrazione CUCM > Gestione utente > Utente finale e verificare che gli utenti finali siano presenti, come mostrato nell'immagine:

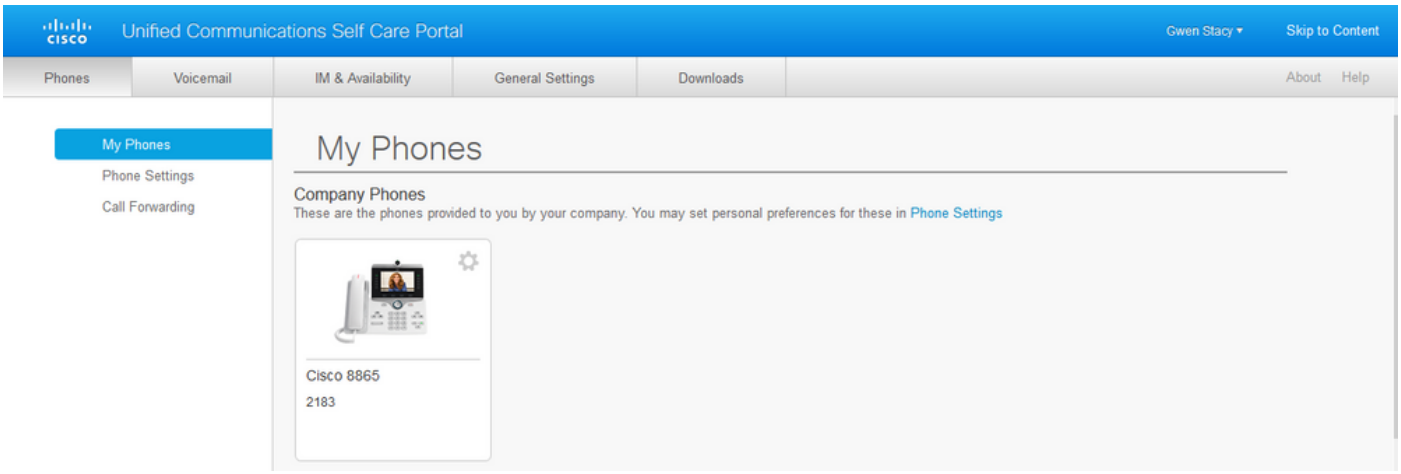


Passaggio 4. Accedere alla pagina ccmuser (https://<indirizzo ip di cucm pub>/ccmuser) per verificare che l'utente abbia eseguito correttamente il login.

La pagina ccmuser per CUCM versione 12.0.1 ha il seguente aspetto:



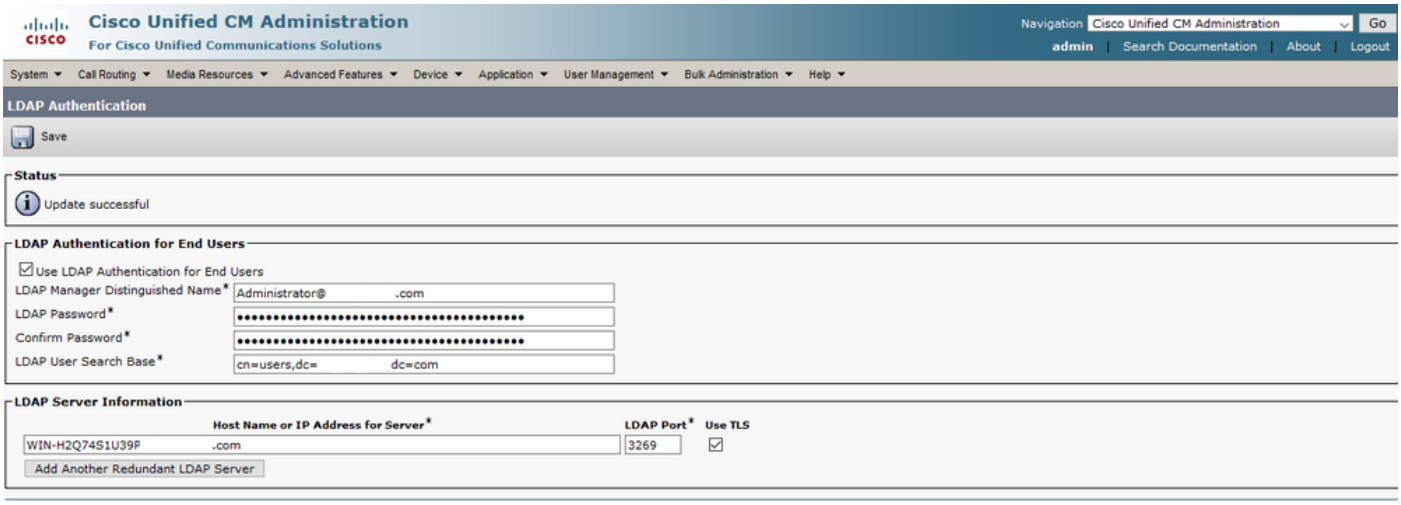
L'utente può eseguire correttamente il login dopo aver immesso le credenziali LDAP, come mostrato nell'immagine:

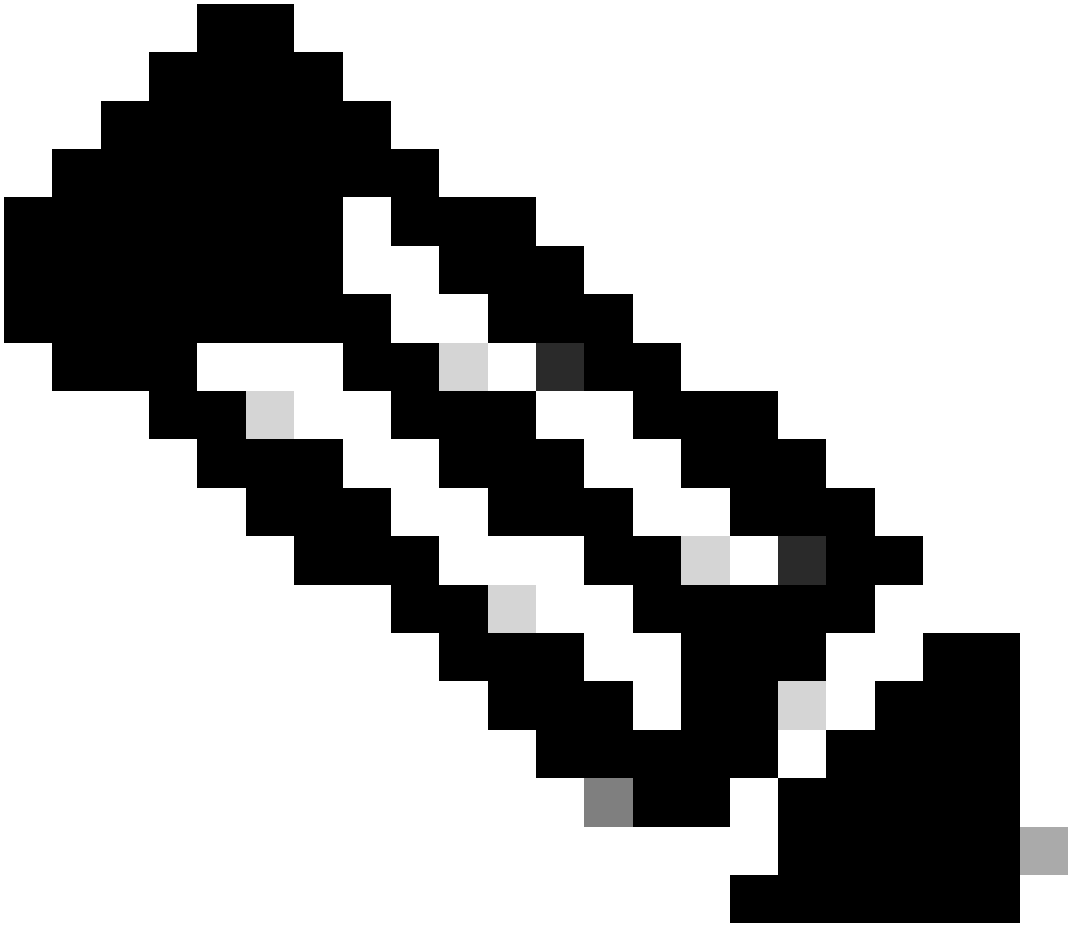


Configura autenticazione LDAP sicura

Configurare l'autenticazione LDAP CUCM per utilizzare la connessione LDAPS TLS ad AD sulla porta 3269.

Passare a Amministrazione CUCM > Sistema > Autenticazione LDAP. Digitare il nome di dominio completo (FQDN) del server LDAPS per Informazioni server LDAP. Specificare la porta LDAPS di 3269 e selezionare la casella Use TLS (Usa TLS), come mostrato nell'immagine:



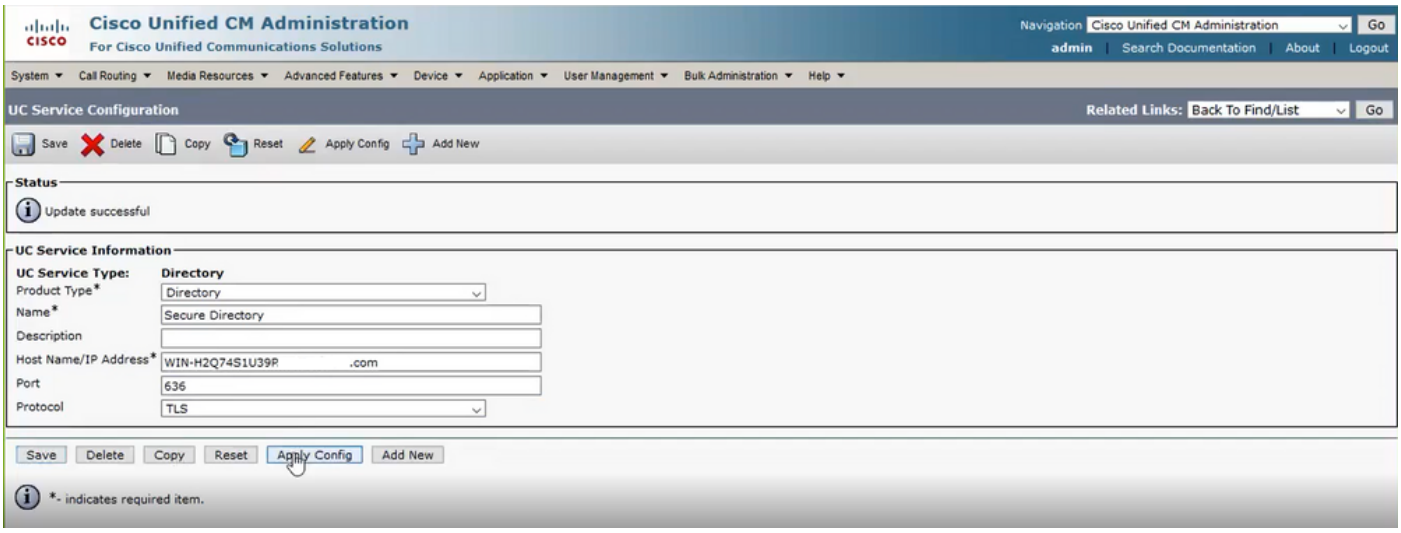


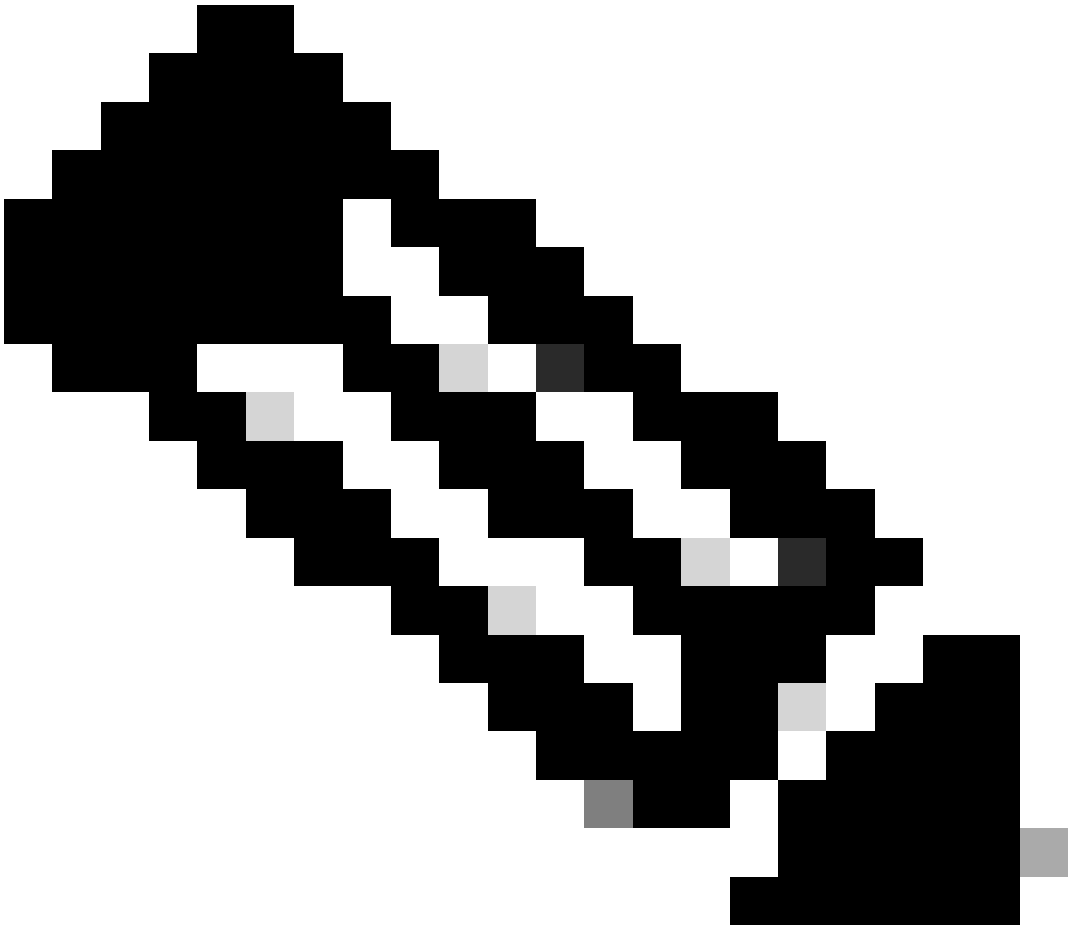
Nota: se si dispone di client Jabber, si consiglia di utilizzare la porta 3269 per l'autenticazione LDAPS, in quanto il timeout di Jabber per l'accesso può verificarsi se non viene specificata una connessione protetta al server di catalogo globale.

Configura connessioni protette ad AD per i servizi UC

Se è necessario proteggere i servizi UC che utilizzano LDAP, configurare questi servizi UC in modo che utilizzino la porta 636 o 3269 con TLS.

Passare a Amministrazione CUCM > Gestione utente > Impostazioni utente > Servizio UC. Trova il servizio directory che punta ad AD. Digitare il nome di dominio completo (FQDN) del server LDAPS come Nome host/Indirizzo IP. Specificare la porta come 636 o 3269 e il protocollo TLS, come mostrato nell'immagine:





Nota: per consentire al client Jabber di stabilire una connessione LDAPS ad AD, i computer client Jabber devono anche avere i certificati LDAPS tomcat-trust installati su CUCM installato nell'archivio di certificati attendibili di gestione del computer client Jabber.

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Per verificare l'effettiva catena di certificati/certificati LDAPS inviata dal server LDAP a CUCM per la connessione TLS, esportare il certificato TLS LDAPS dall'acquisizione di un pacchetto CUCM. Questo collegamento fornisce informazioni su come esportare un certificato TLS da un'acquisizione pacchetti CUCM: Come esportare un certificato TLS da un'acquisizione pacchetti CUCM

Risoluzione dei problemi

Non sono attualmente disponibili informazioni specifiche per risolvere i problemi relativi a questa configurazione.

Informazioni correlate

- Questo collegamento fornisce l'accesso a un video che passa attraverso le configurazioni LDAPS: Directory LDAP protetta e autenticazione Walkthrough Video
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).