Configuración de CUCM para LDAP seguro (LDAP)

Contenido

Introducción

Este documento describe el procedimiento para actualizar las conexiones de CUCM a AD desde una conexión LDAP no segura a una conexión LDAP segura.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

· Servidor LDAP de AD
· Configuración LDAP de CUCM

· CUCM IM & Presence Service (IM/P)

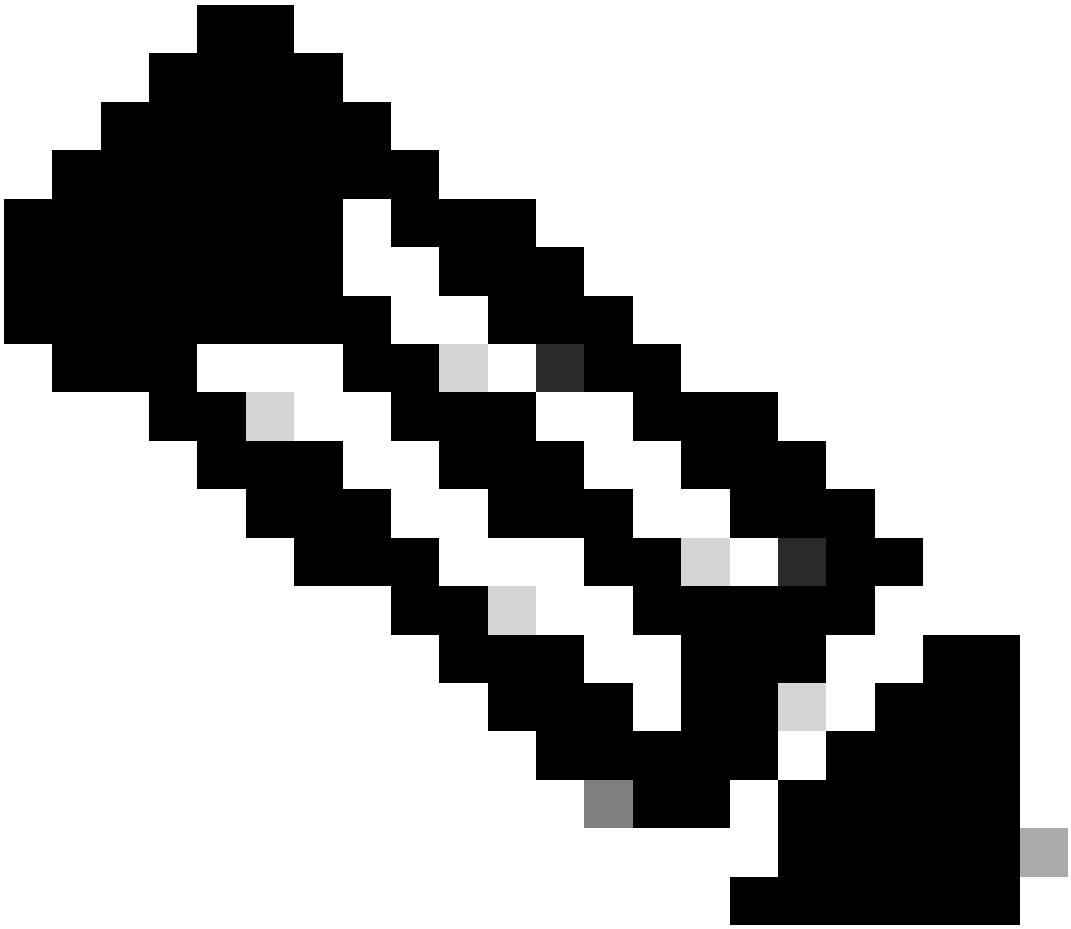
Componentes Utilizados

La información de este documento se basa en CUCM versión 9.x y superior.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Es responsabilidad del administrador de Active Directory (AD) configurar el protocolo ligero de acceso a directorios (LDAP) de AD para el protocolo ligero de acceso a directorios (LDAP) . Esto incluye la instalación de certificados firmados por CA que cumplen los requisitos de un certificado LDAPS.



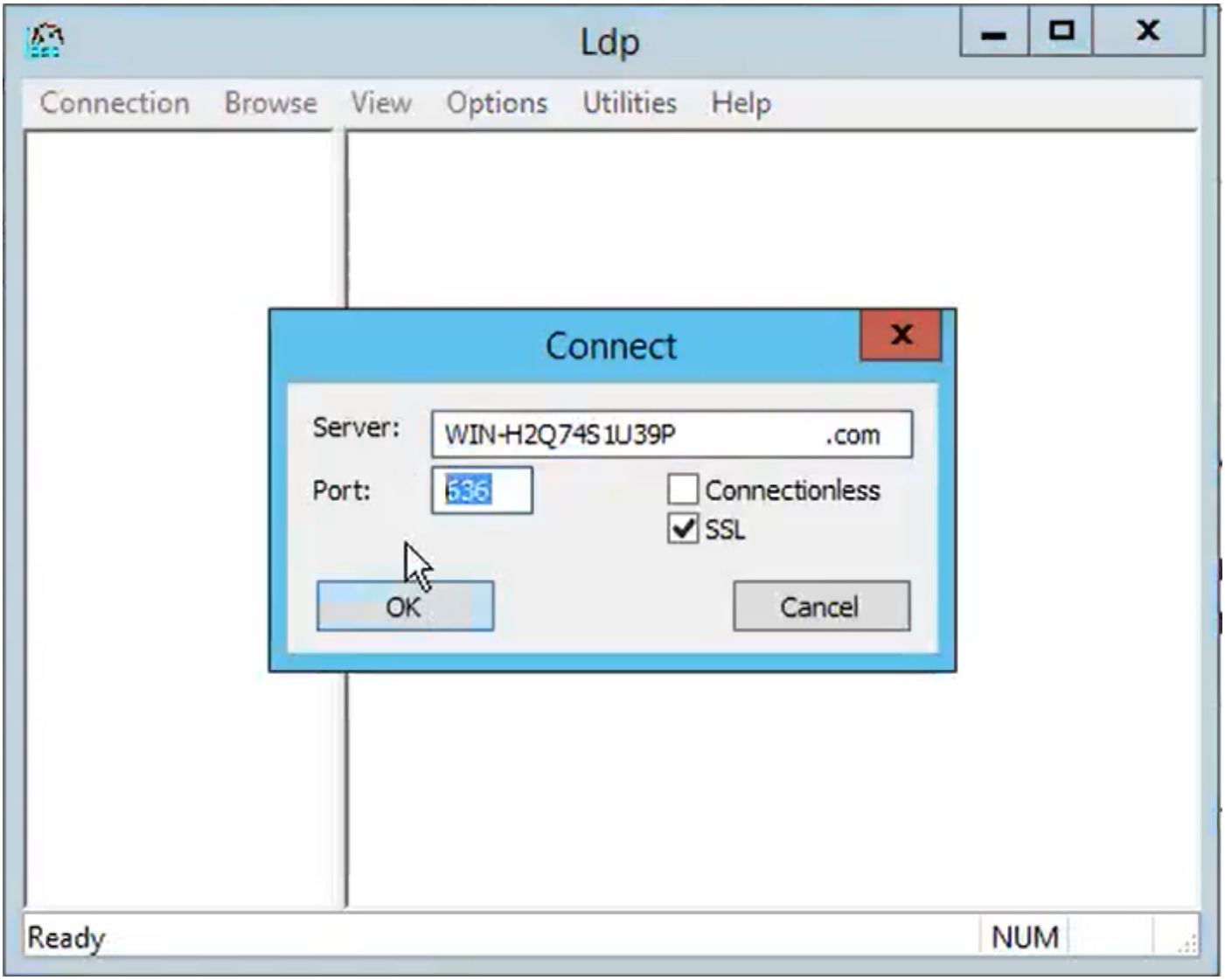
Nota: Consulte este enlace para obtener información sobre cómo actualizar de LDAP no seguro a conexiones LDAP seguras a AD para otras aplicaciones de Cisco Collaboration: Software Advisory: Secure LDAP Obligatorio para Conexiones de Active Directory

---

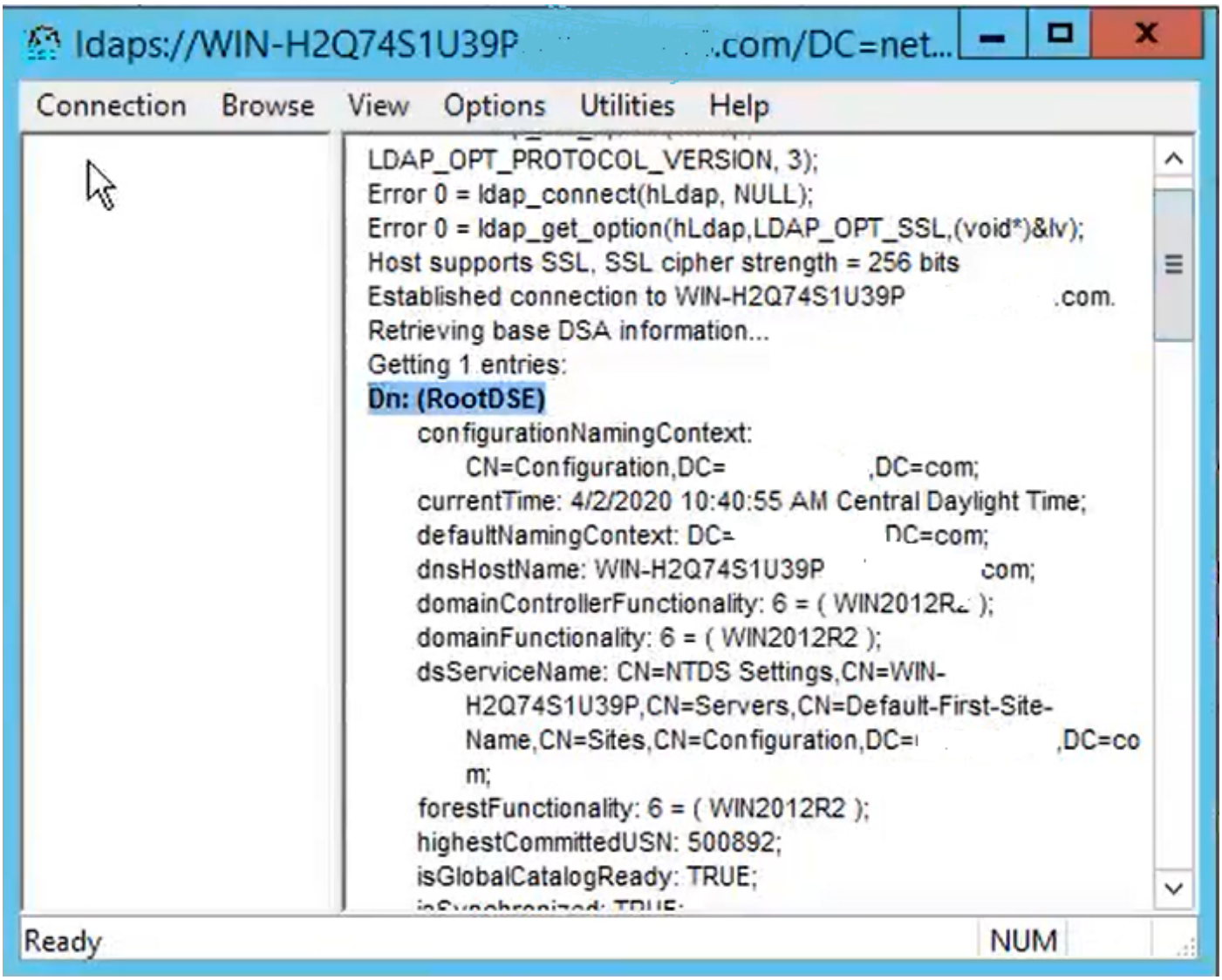
Verificación e instalación de certificados LDAPS

Paso 1. Después de cargar el certificado LDAPS en el servidor AD, compruebe que LDAPS está habilitado en el servidor AD con la herramienta ldp.exe.

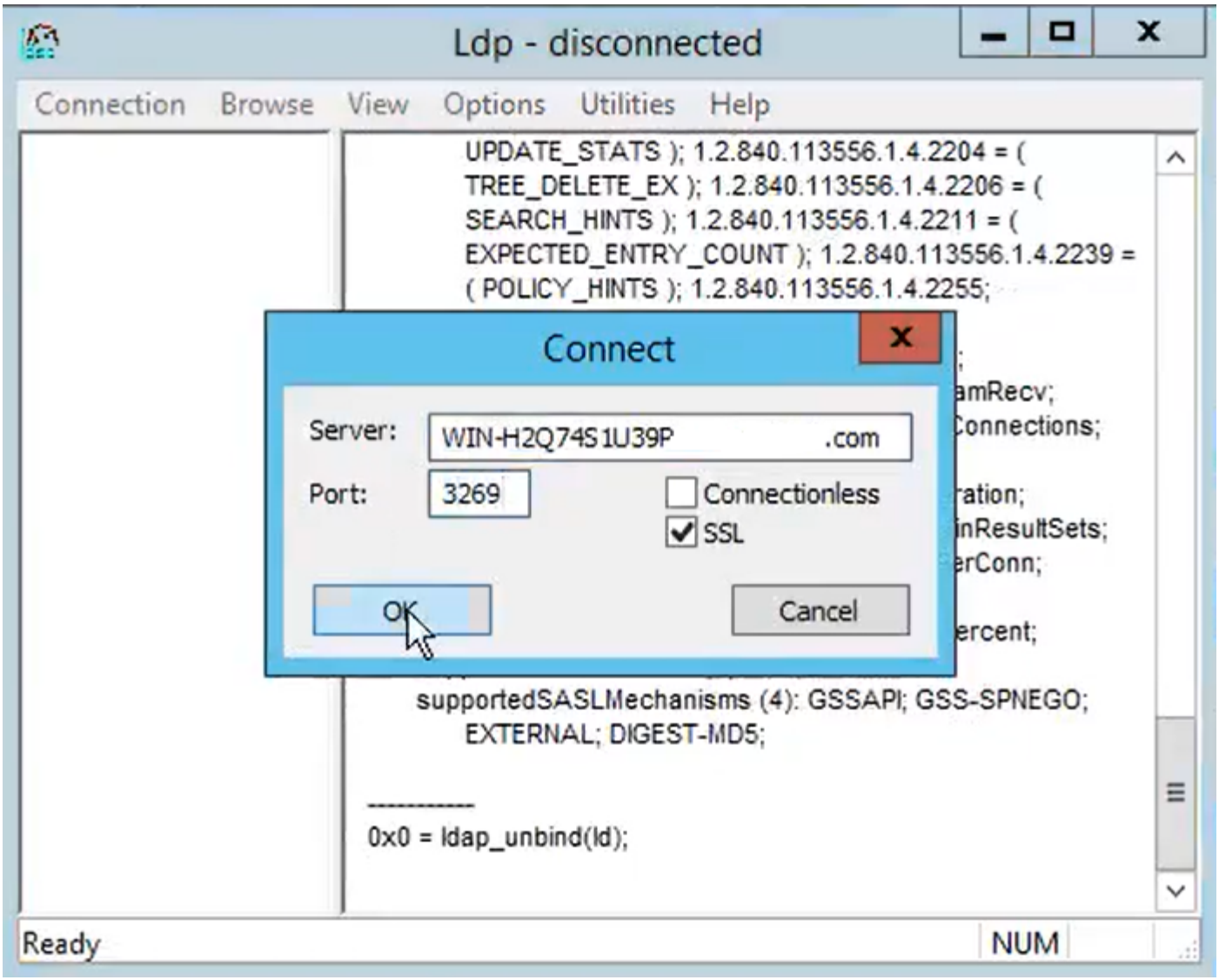
1. Inicie la Herramienta de administración de AD (Ldp.exe) en el servidor de AD.
2. En el menú Conexión, seleccione Conectar.
3. Introduzca el nombre de dominio completo (FQDN) del servidor LDAP.
4. Introduzca 636 como el número de puerto.
5. Haga clic en OK, como se muestra en la imagen



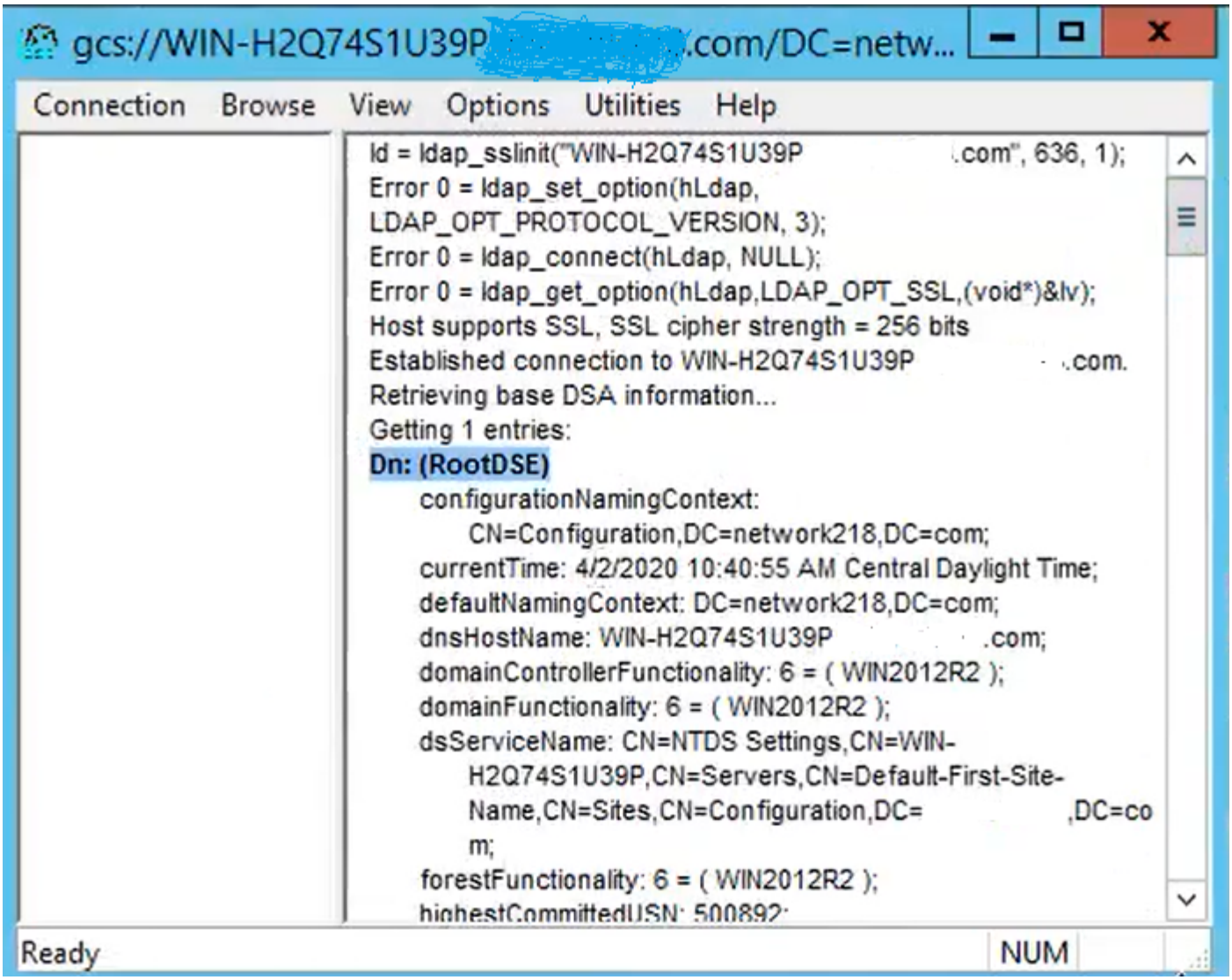
Para una conexión exitosa en el puerto 636, la información de RootDSE se imprime en el panel derecho, como se muestra en la imagen:



Repita el procedimiento para el puerto 3269, como se muestra en la imagen:

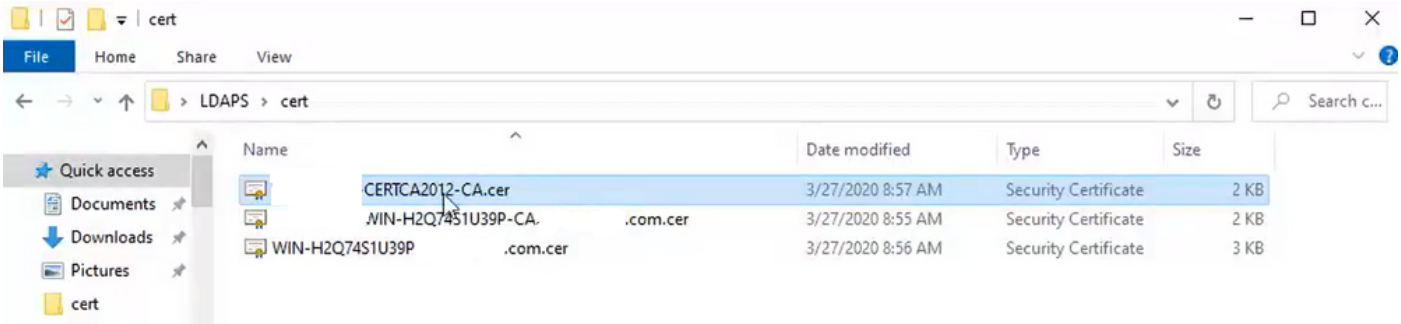


Para una conexión exitosa en el puerto 3269, la información de RootDSE se imprime en el panel derecho, como se muestra en la imagen:

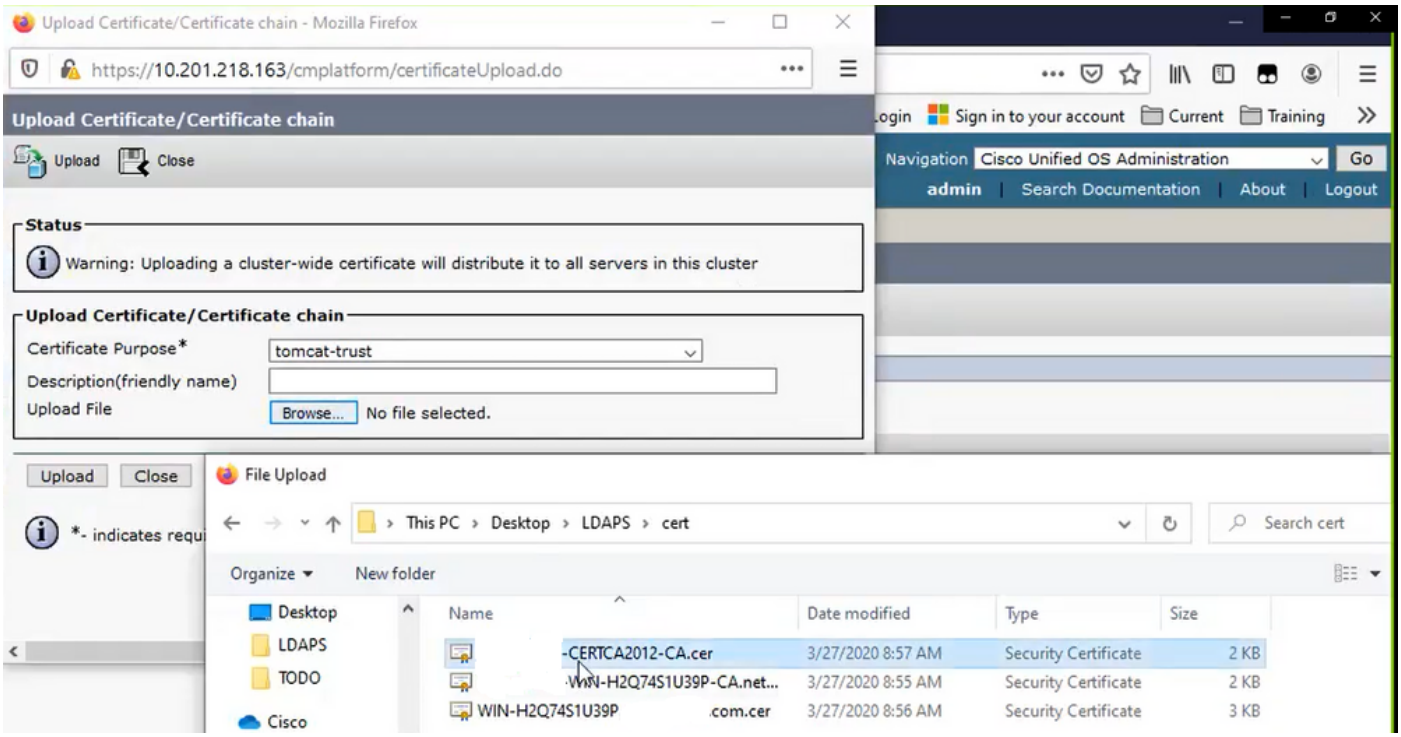


Paso 2. Obtenga la raíz y cualquier certificado intermedio que forme parte del certificado del servidor LDAPS e instálelos como certificados de confianza tomcat en cada uno de los nodos del editor de CUCM e IM/P y como certificados de confianza de CallManager en el editor de CUCM.

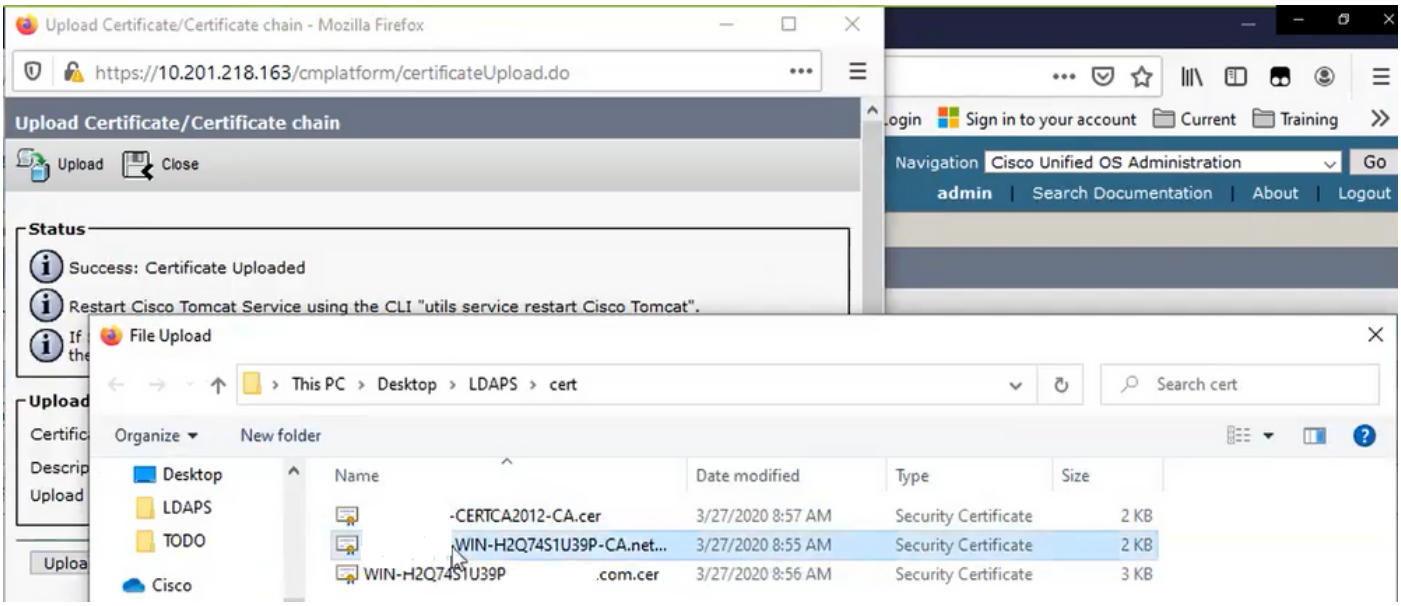
Los certificados raíz e intermedios que forman parte de un certificado de servidor LDAP, <hostname>.<Domain>.cer, se muestran en la imagen:



Vaya a Cisco Unified OS Administration > Security > Certificate Management del editor de CUCM. Cargar raíz como tomcat-trust (como se muestra en la imagen) y como CallManager-trust (no se muestra):



Cargar intermedio como tomcat-trust (como se muestra en la imagen) y como CallManager-trust (no se muestra):

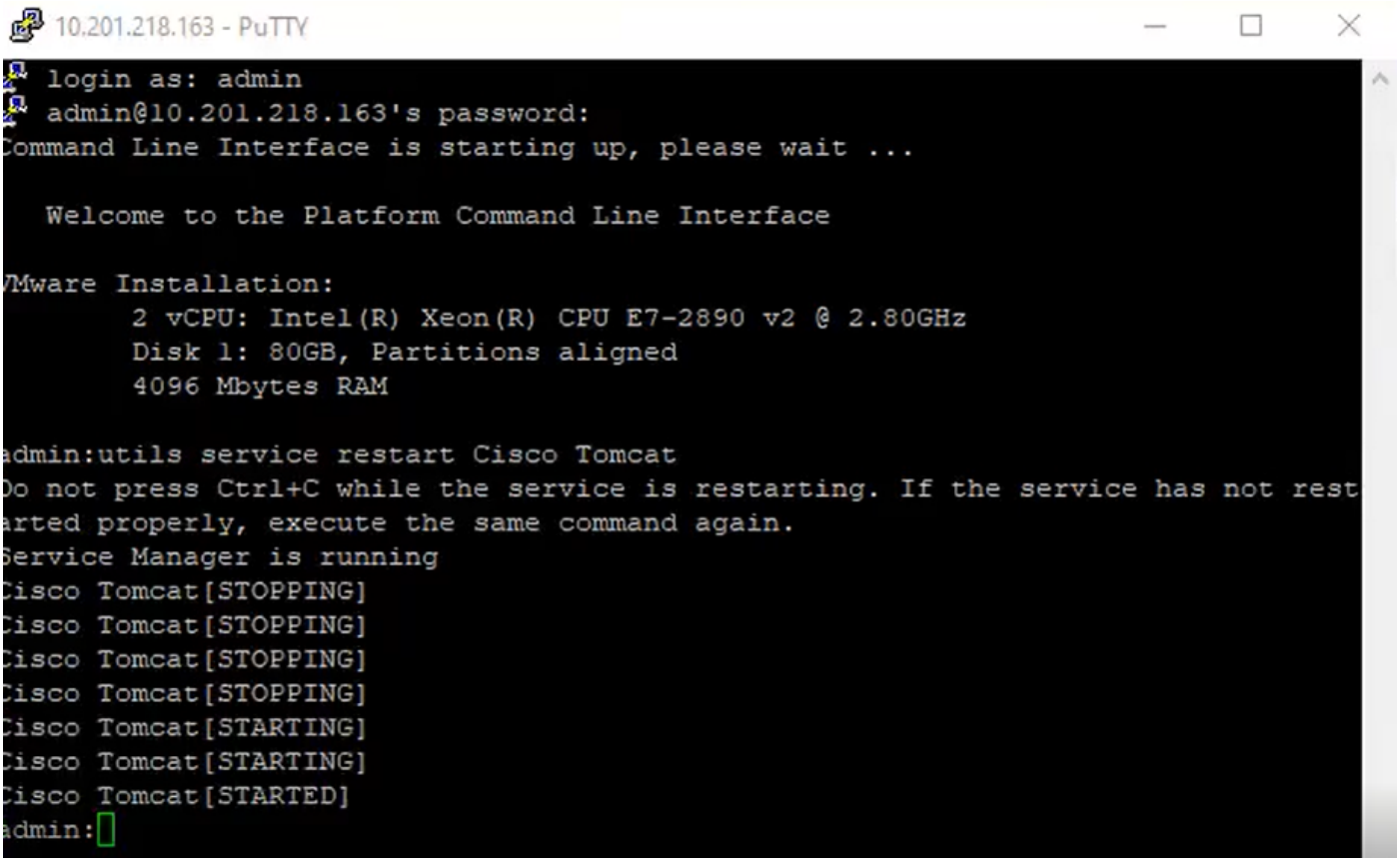


Nota: Si tiene servidores IM/P que forman parte del clúster de CUCM, también debe cargar estos certificados en estos servidores IM/P.

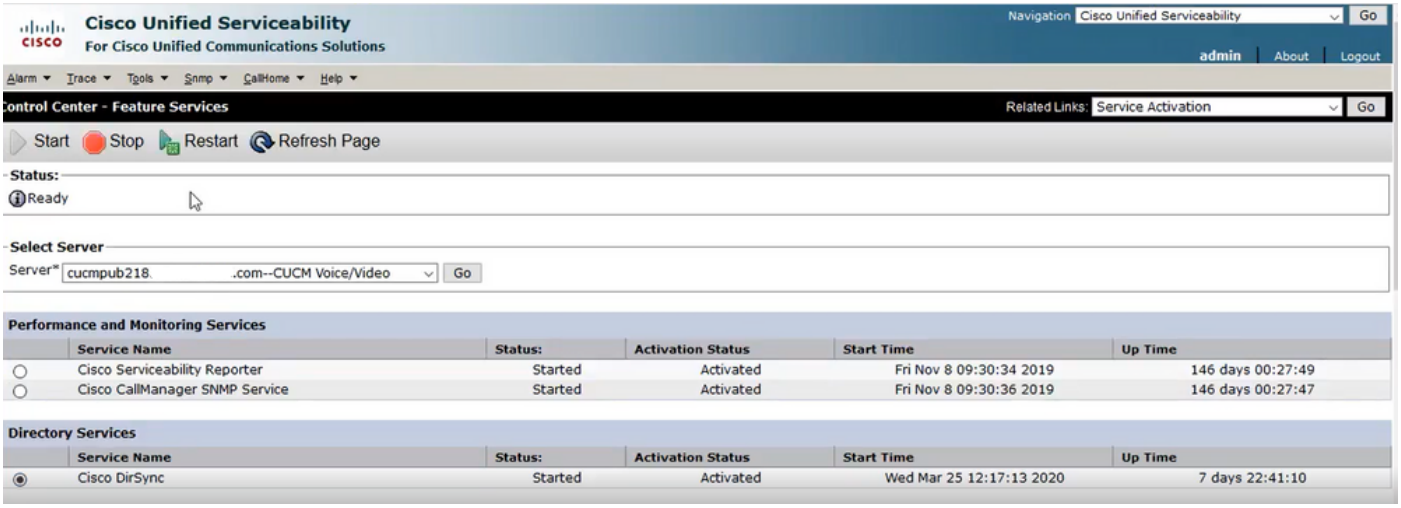
Nota: Como alternativa, puede instalar el certificado del servidor LDAPS como tomcat-trust.

Paso 3. Reinicie Cisco Tomcat desde la CLI de cada nodo (CUCM e IM/P) en clústeres. Además, para el clúster de CUCM, compruebe que se ha iniciado el servicio Cisco DirSync en el nodo del editor.

Para reiniciar el servicio Tomcat, debe abrir una sesión CLI para cada nodo y ejecutar el comando utils service restart Cisco Tomcat, como se muestra en la imagen:



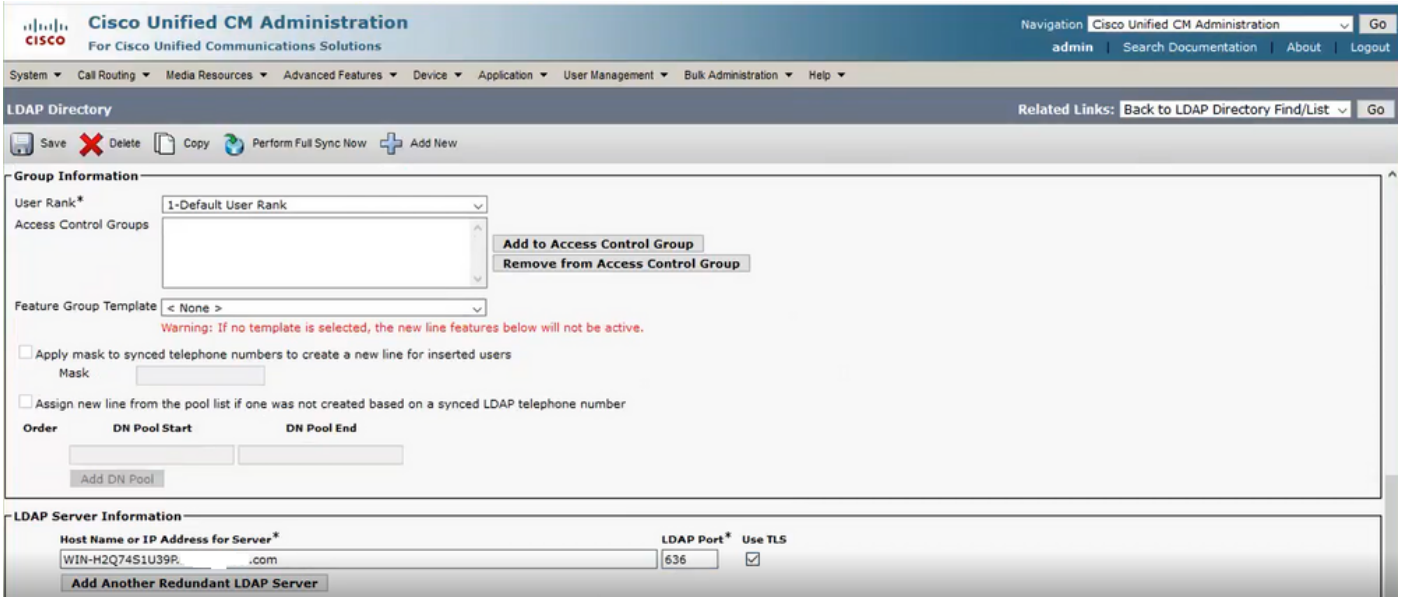
Paso 4. Navegue hasta CUCM publisher Cisco Unified Serviceability > Tools > Control Center - Feature Services, verifique que el servicio Cisco DirSync esté activado e iniciado (como se muestra en la imagen) y reinicie el servicio Cisco CTIManager en cada nodo si se utiliza (no se muestra):

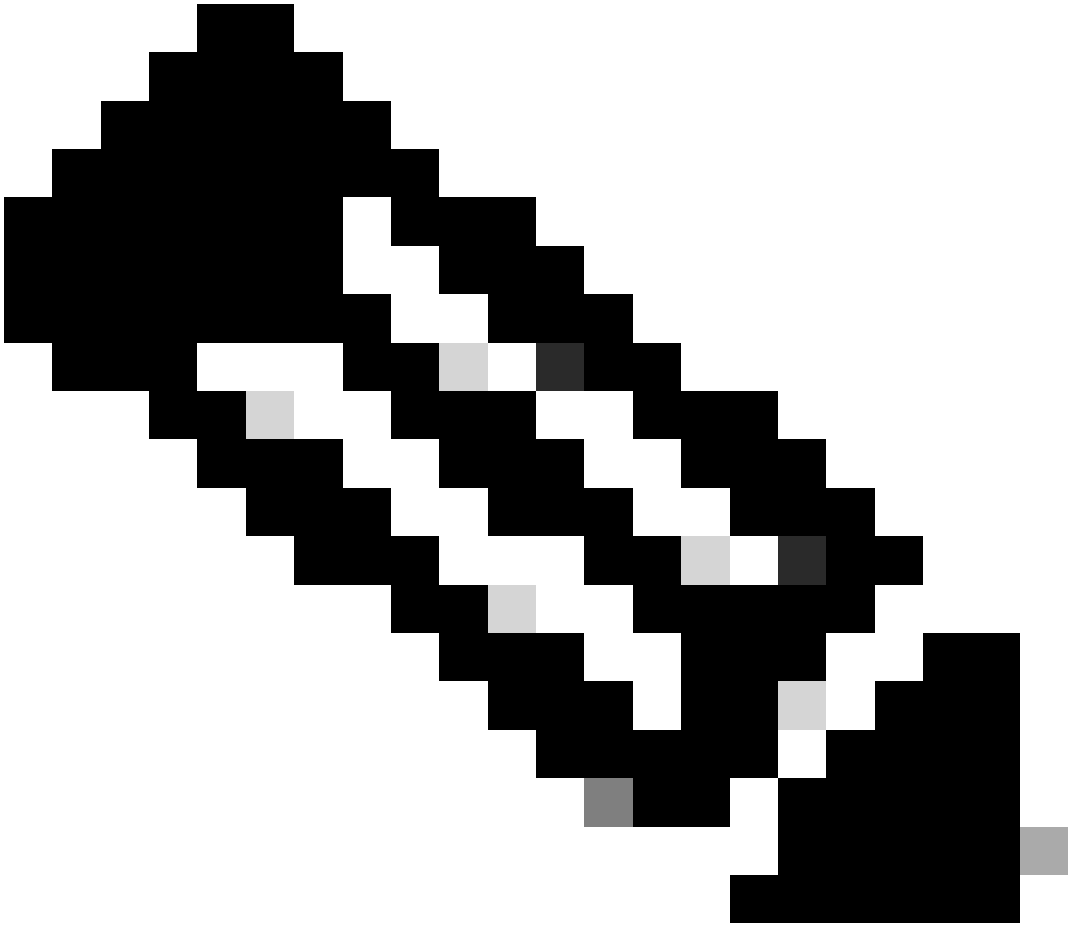


Configurar el directorio LDAP seguro

Paso 1. Configure el directorio LDAP de CUCM para utilizar la conexión TLS de LDAP con AD en el puerto 636.

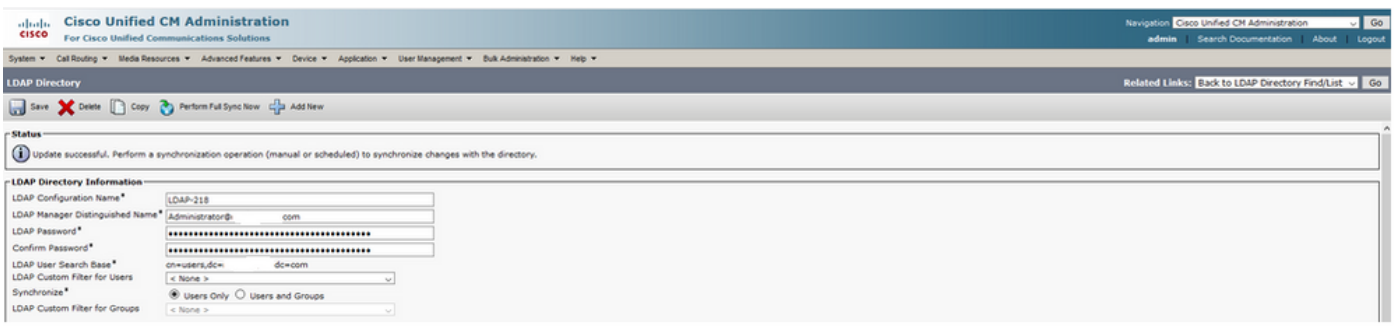
Vaya a Administración de CUCM > Sistema > Directorio LDAP. Escriba el FQDN o la dirección IP del servidor LDAP para la información del servidor LDAP. Especifique el puerto LDAPS de 636 y marque la casilla Use TLS, como se muestra en la imagen:



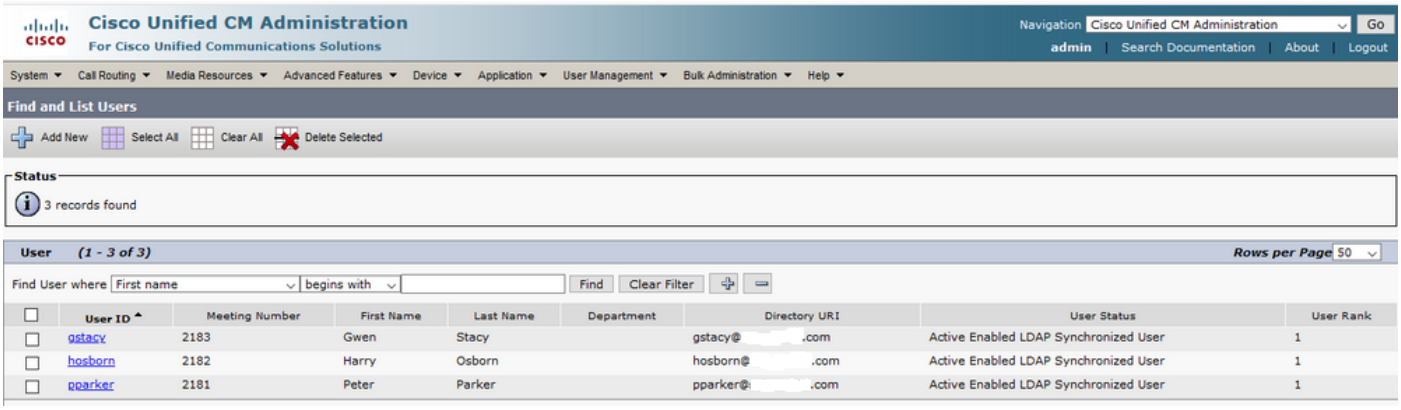


Nota: De forma predeterminada, después de comprobar el FQDN de las versiones 10.5(2)SU2 y 9.1(2)SU3 configurado en Información del servidor LDAP con el nombre común del certificado, en caso de que se utilice la dirección IP en lugar del FQDN, el comando utils ldap config ipaddr se ejecuta para detener la aplicación del FQDN en la verificación CN.

Paso 2. Para completar el cambio de configuración a LDAPS, haga clic en Perform Full Sync Now, como se muestra en la imagen:

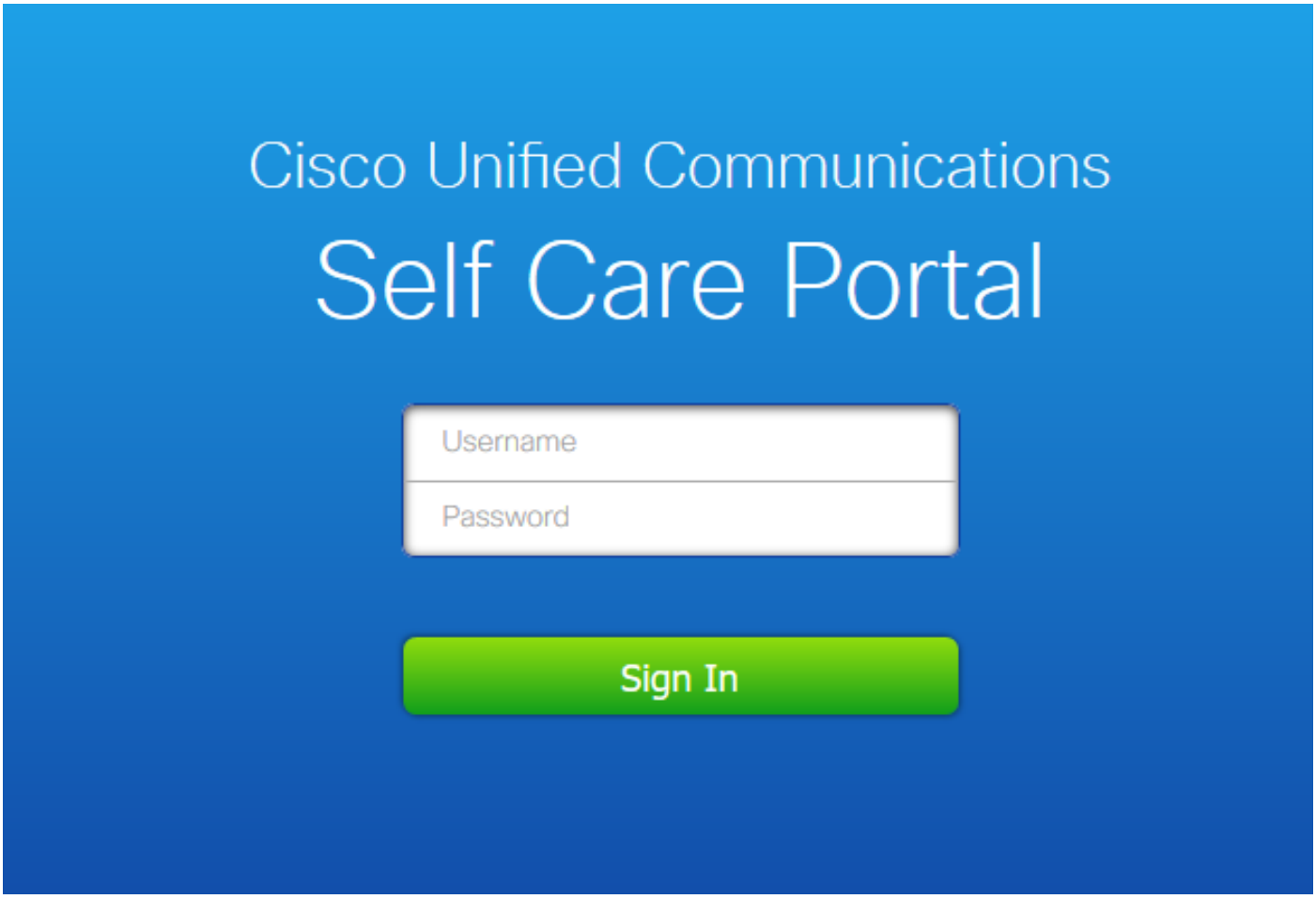


Paso 3. Vaya a CUCM Administration > User Management > End User y verifique que los usuarios finales están presentes, como se muestra en la imagen:

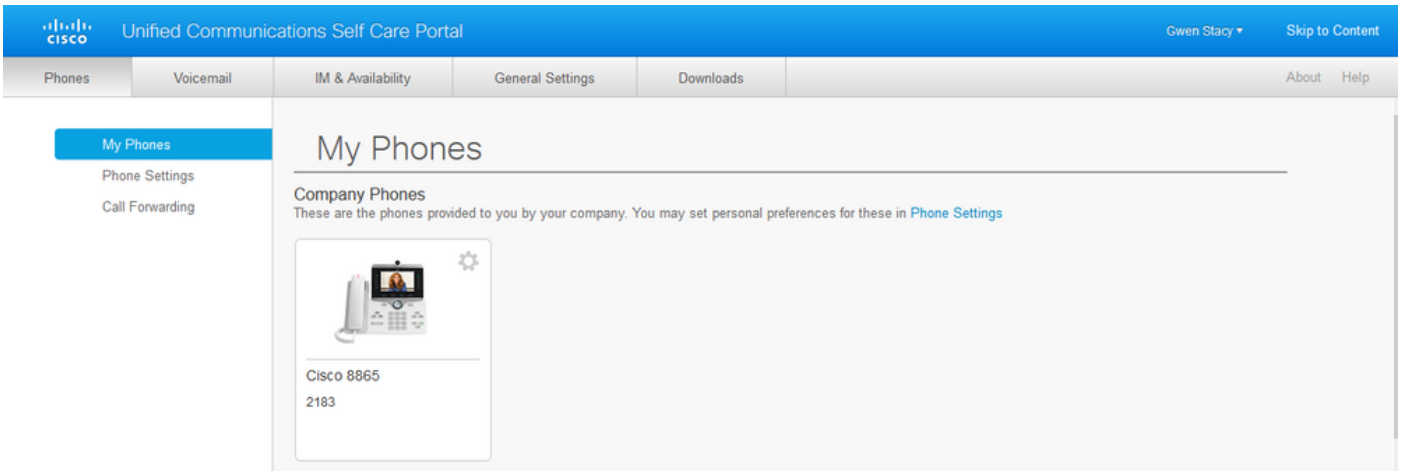


Paso 4. Navegue hasta la página ccmuser (https://<dirección ip de cucm pub>/ccmuser) para verificar que el inicio de sesión del usuario sea exitoso.

La página ccmuser para la versión 12.0.1 de CUCM es similar a lo siguiente:



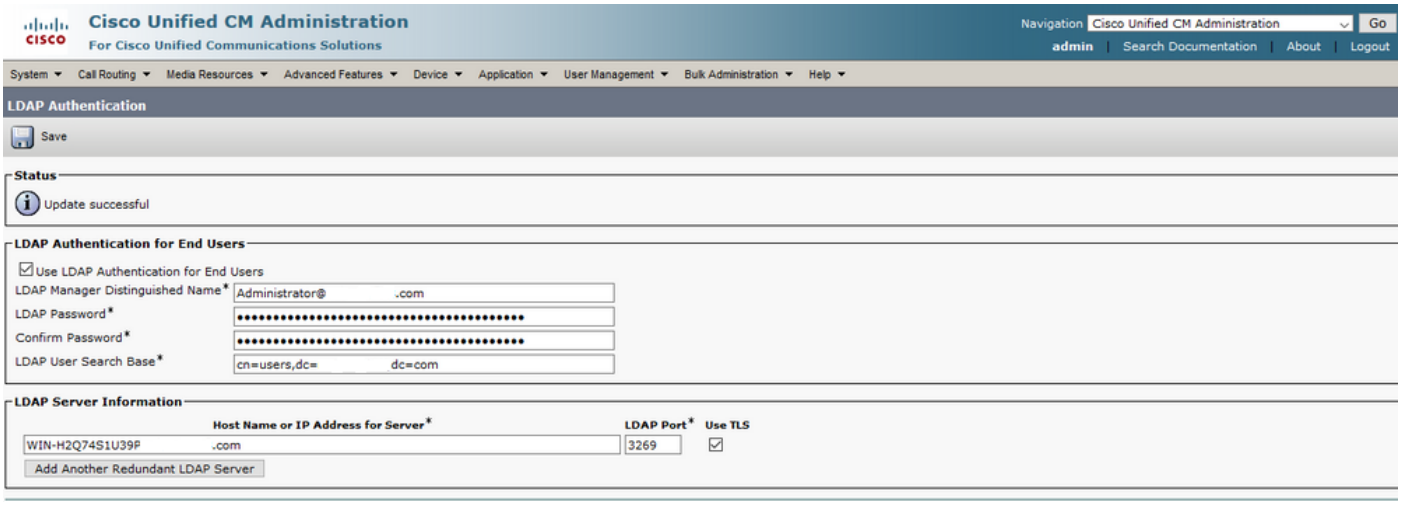
El usuario puede iniciar sesión correctamente después de introducir las credenciales LDAP, como se muestra en la imagen:

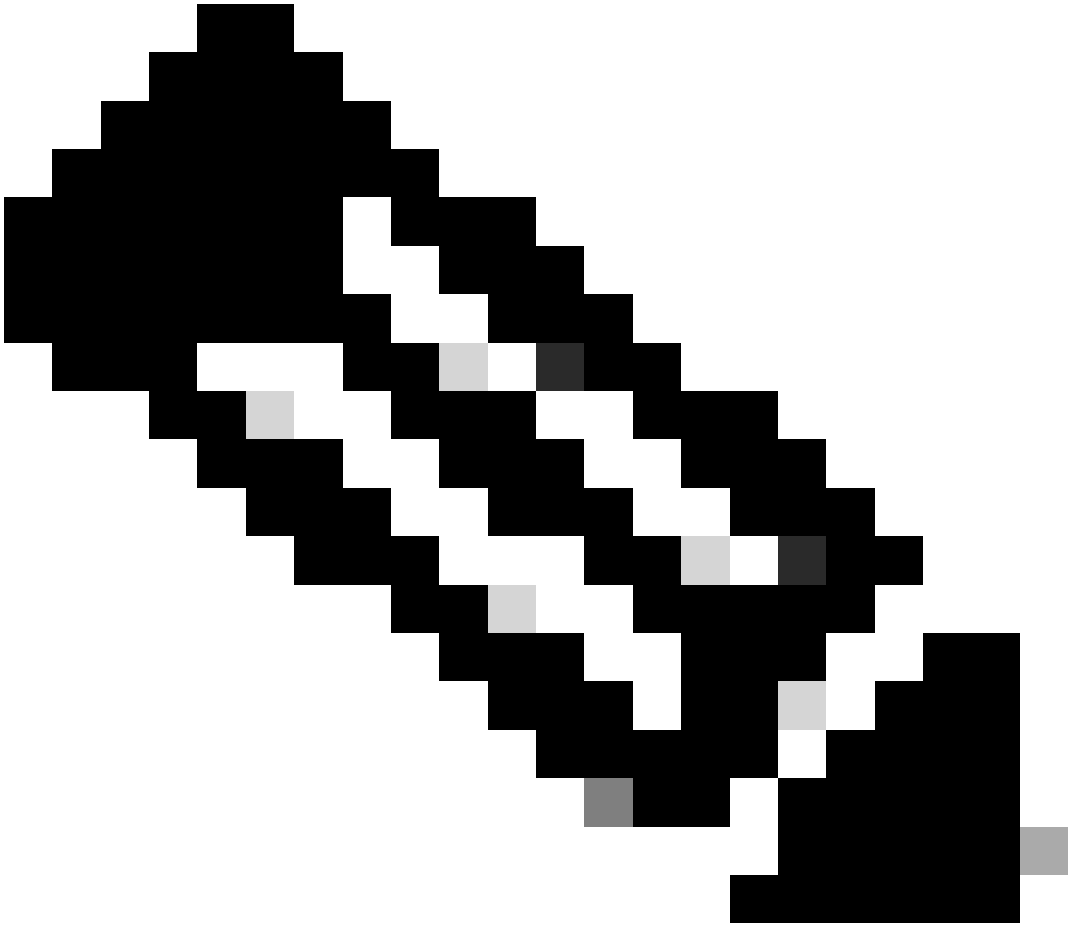


Configurar autenticación LDAP segura

Configure la autenticación LDAP de CUCM para utilizar la conexión TLS de LDAP con AD en el puerto 3269.

Vaya a Administración de CUCM > Sistema > Autenticación LDAP. Escriba el FQDN del servidor LDAP para información del servidor LDAP. Especifique el puerto LDAPS de 3269 y marque la casilla Use TLS, como se muestra en la imagen:



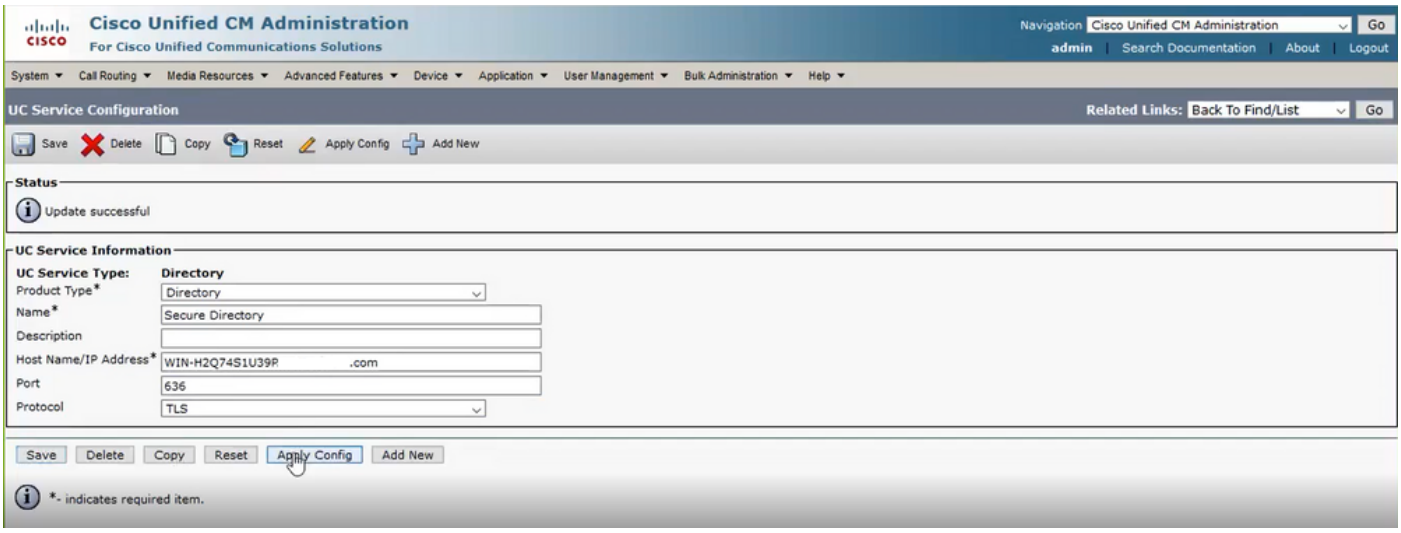


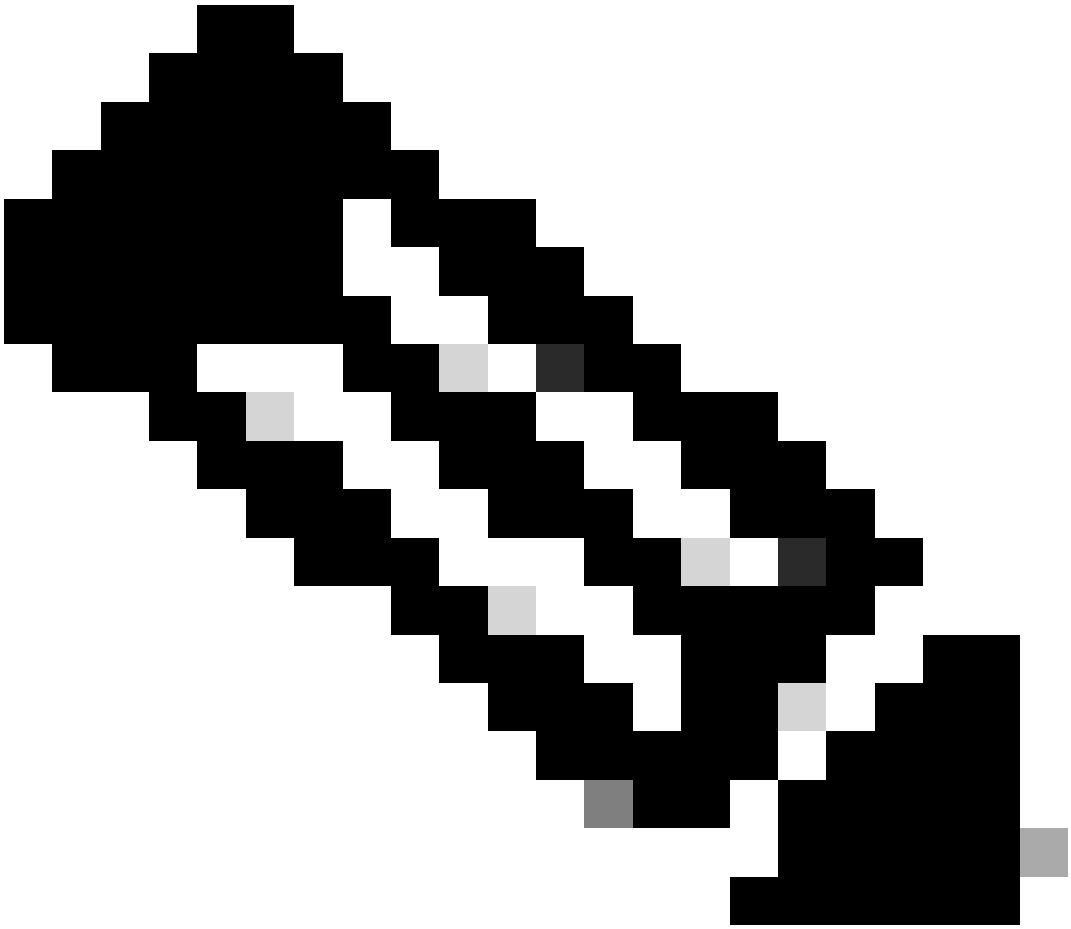
Nota: Si tiene clientes Jabber, se recomienda utilizar el puerto 3269 para la autenticación LDAPS, ya que el tiempo de espera de Jabber para el inicio de sesión puede ocurrir si no se especifica una conexión segura al servidor de catálogo global.

Configuración de conexiones seguras a AD para servicios de UC

Si necesita proteger los servicios de UC que utilizan LDAP, configure estos servicios de UC para utilizar el puerto 636 o 3269 con TLS.

Vaya a Administración de CUCM > Administración de usuarios > Configuración de usuario > Servicio de UC. Busque el servicio de directorio que apunta a AD. Escriba el FQDN del servidor LDAP como Nombre de host/Dirección IP. Especifique el puerto como 636 o 3269 y el protocolo TLS, como se muestra en la imagen:





Nota: Las máquinas cliente Jabber también necesitan tener los certificados LDAPS de confianza de tomcat instalados en CUCM instalados en el almacén de confianza de administración de certificados de la máquina cliente Jabber para permitir que el cliente Jabber establezca una conexión LDAPS con AD.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Para verificar la cadena real de certificado/certificado LDAPS enviada desde el servidor LDAP a CUCM para la conexión TLS, exporte el certificado LDAPS TLS desde una captura de paquetes CUCM. Este enlace proporciona información sobre cómo exportar un certificado TLS desde una captura de paquetes de CUCM: Cómo exportar un certificado TLS desde una captura de paquetes de CUCM

Troubleshoot

Actualmente, no hay información específica disponible sobre cómo solucionar los problemas de esta configuración.

Información Relacionada

- Este enlace proporciona acceso a un vídeo que recorre las configuraciones de LDAP: Directorio LDAP seguro y Vídeo del tutorial de autenticación
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).