

Configuración de CUCM para LDAP seguro (LDAP)

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Verificación e instalación de certificados LDAPS](#)

[Configurar el directorio LDAP seguro](#)

[Configurar autenticación LDAP segura](#)

[Configuración de conexiones seguras a AD para servicios de UC](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

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)

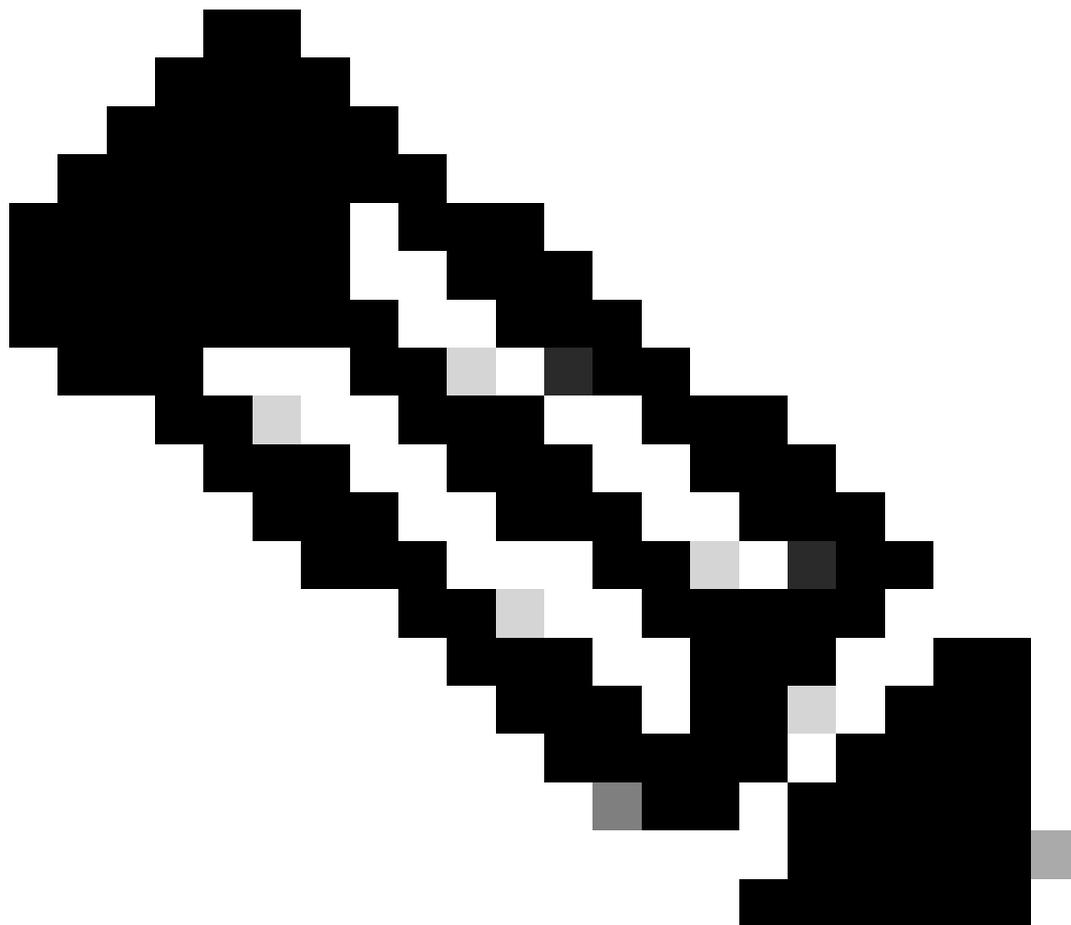
Componentes Utilizados

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.

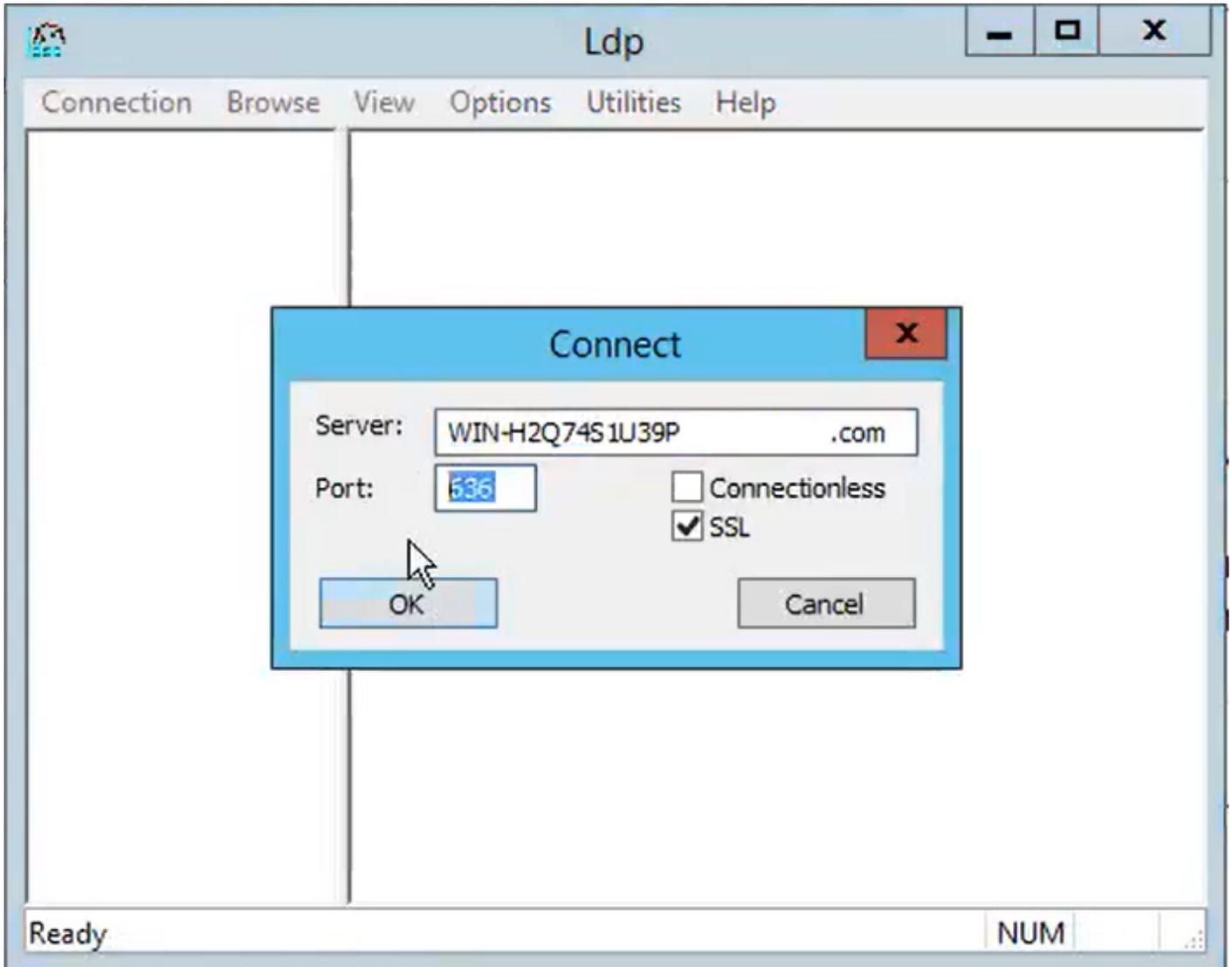


Nota: Consulte este enlace para obtener información sobre cómo actualizar de LDAP no seguro a conexiones LDAP seguras a AD para otras aplicaciones de Cisco Collaboration: [Software Advisory: Secure LDAP Obligatorio para Conexiones de Active Directory](#)

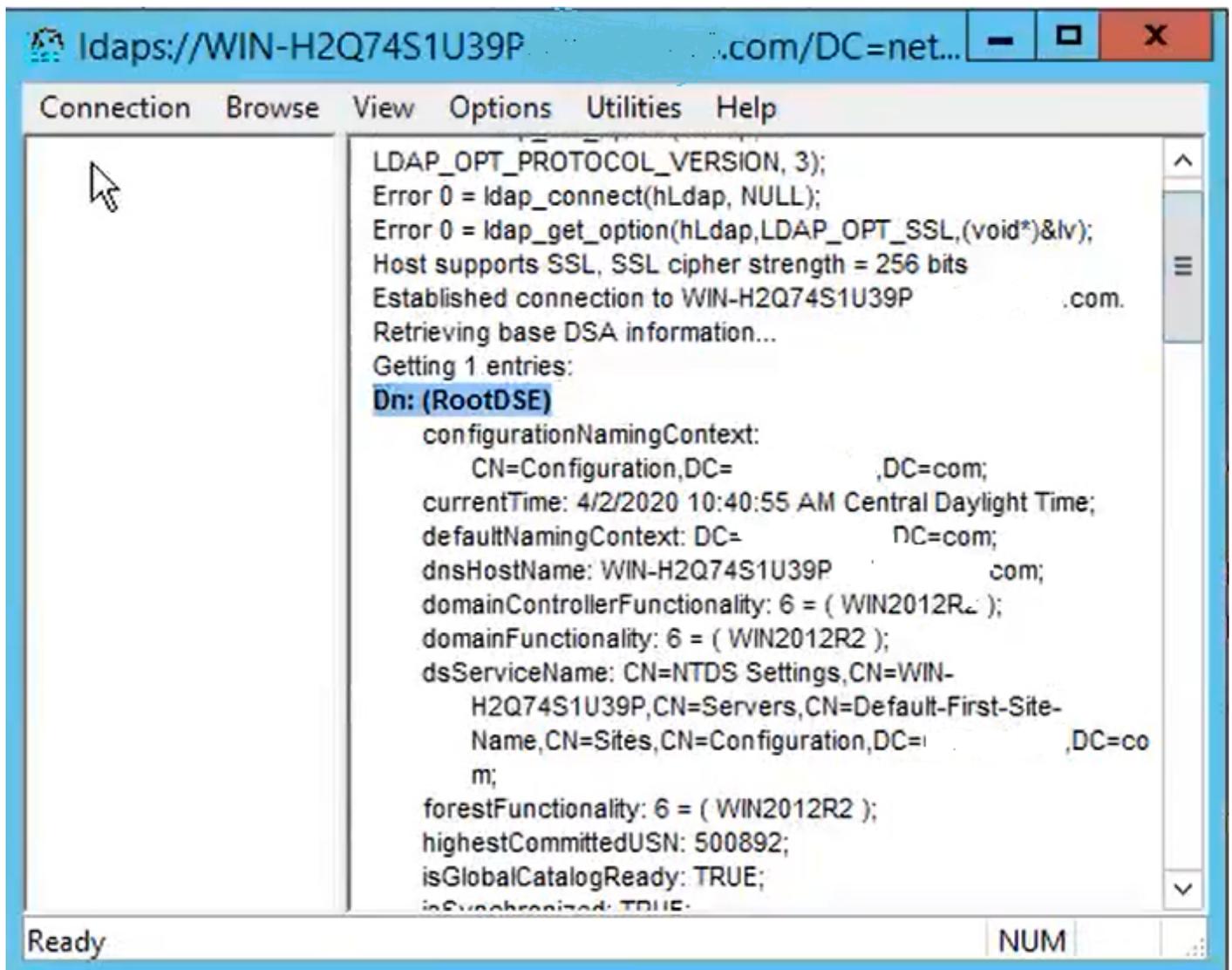
Verificación e instalación de certificados LDAPS

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.

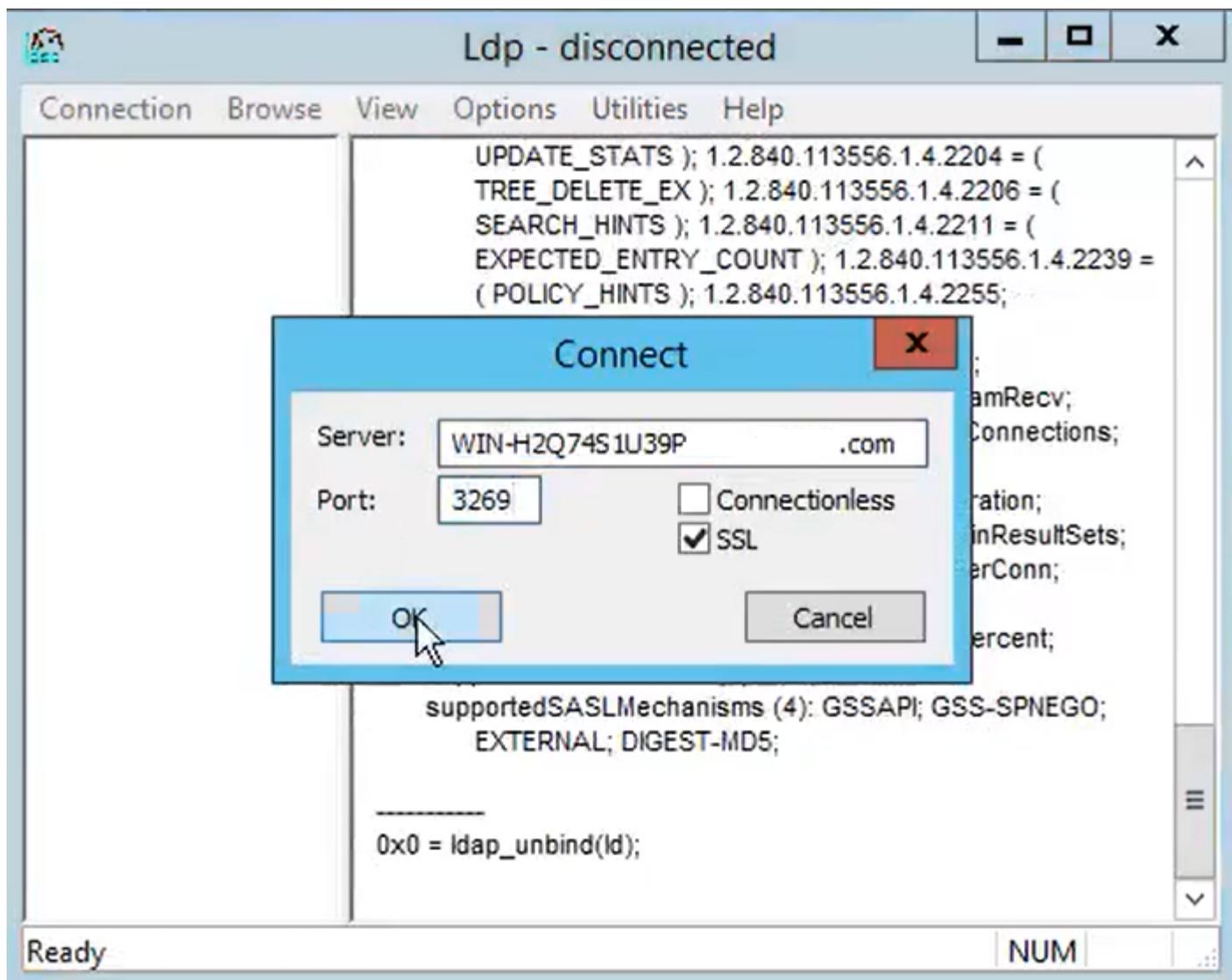
1. Inicie la Herramienta de administración de AD (Ldp.exe) en el servidor de AD.
2. En el menú Conexión, seleccione Conectar.
3. Introduzca el nombre de dominio completo (FQDN) del servidor LDAP.
4. Introduzca 636 como el número de puerto.
5. Haga clic en OK, como se muestra en la imagen



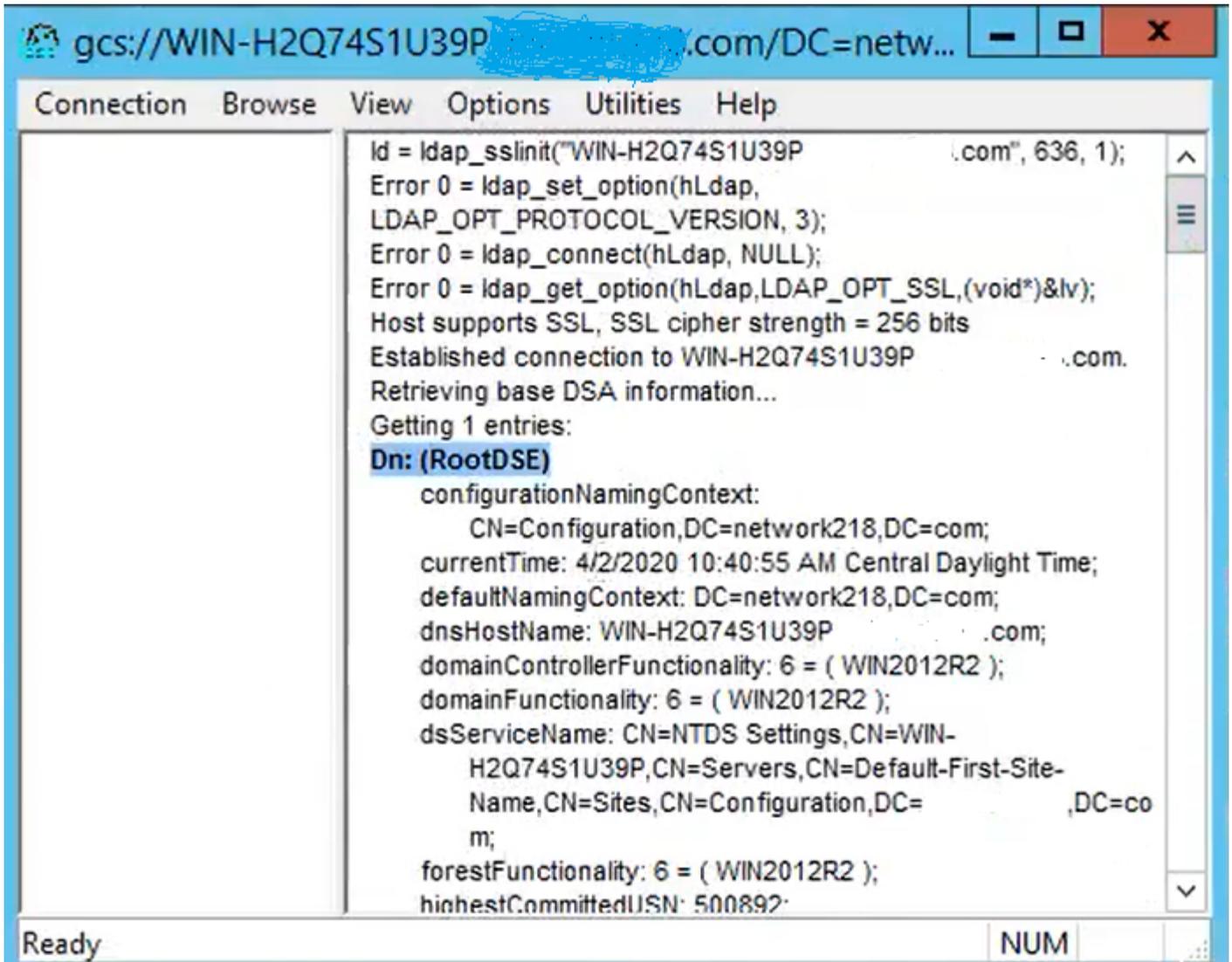
Para una conexión exitosa en el puerto 636, la información de RootDSE se imprime en el panel derecho, como se muestra en la imagen:



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

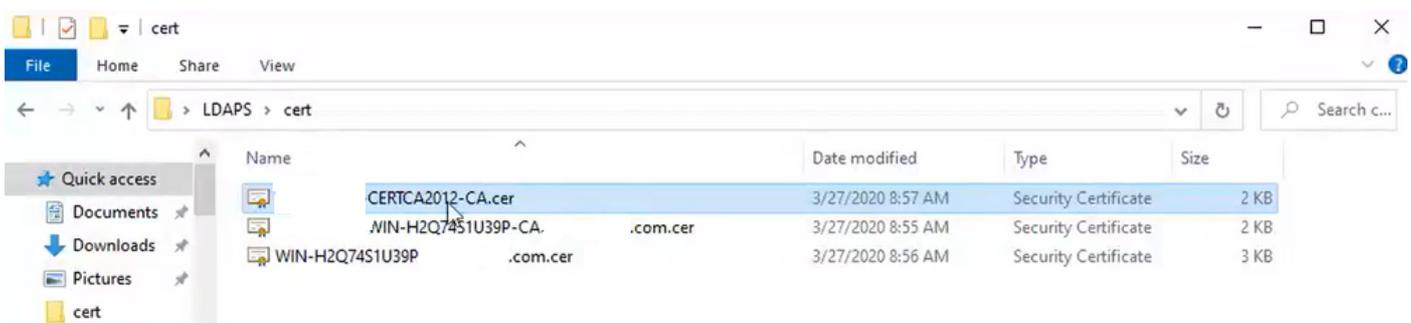


Para una conexión exitosa en el puerto 3269, la información de RootDSE se imprime en el panel derecho, como se muestra en la imagen:

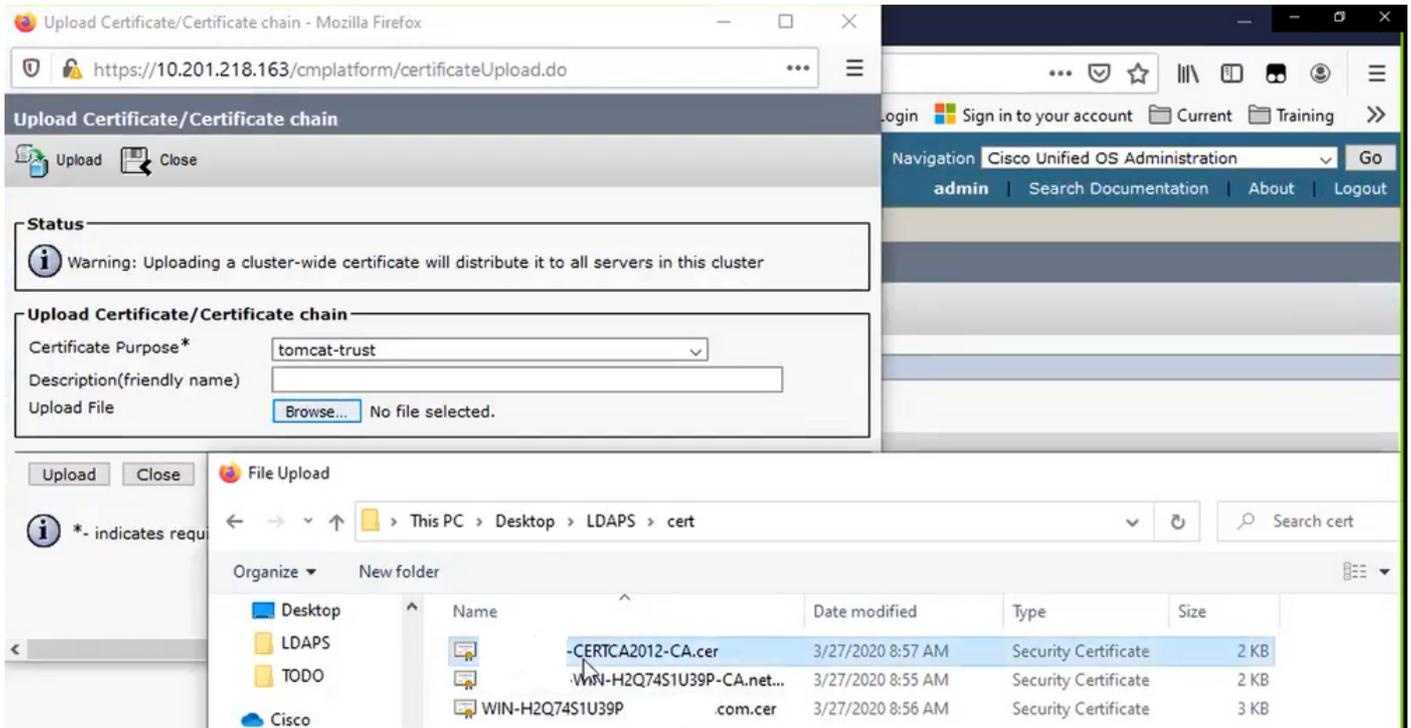


Paso 2. Obtenga la raíz y cualquier certificado intermedio que forme parte del certificado del servidor LDAPS e instálelos como certificados de confianza tomcat en cada uno de los nodos del editor de CUCM e IM/P y como certificados de confianza de CallManager en el editor de CUCM.

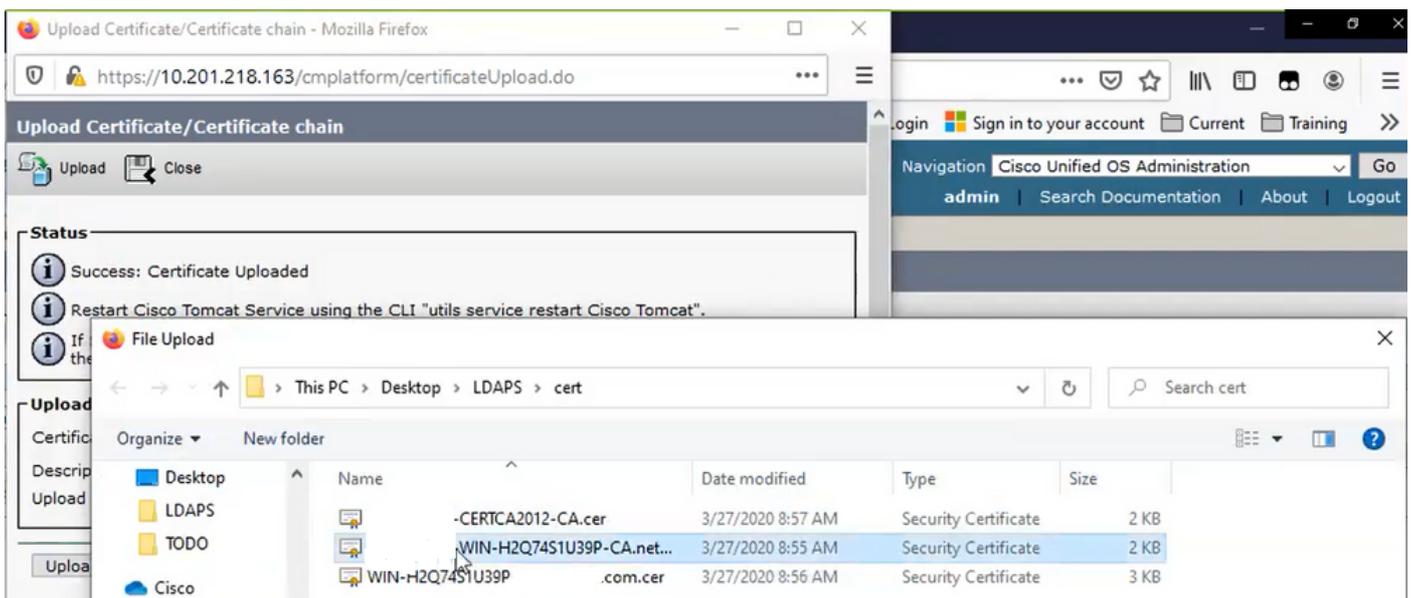
Los certificados raíz e intermedios que forman parte de un certificado de servidor LDAP, <hostname>.<Domain>.cer, se muestran en la imagen:



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):

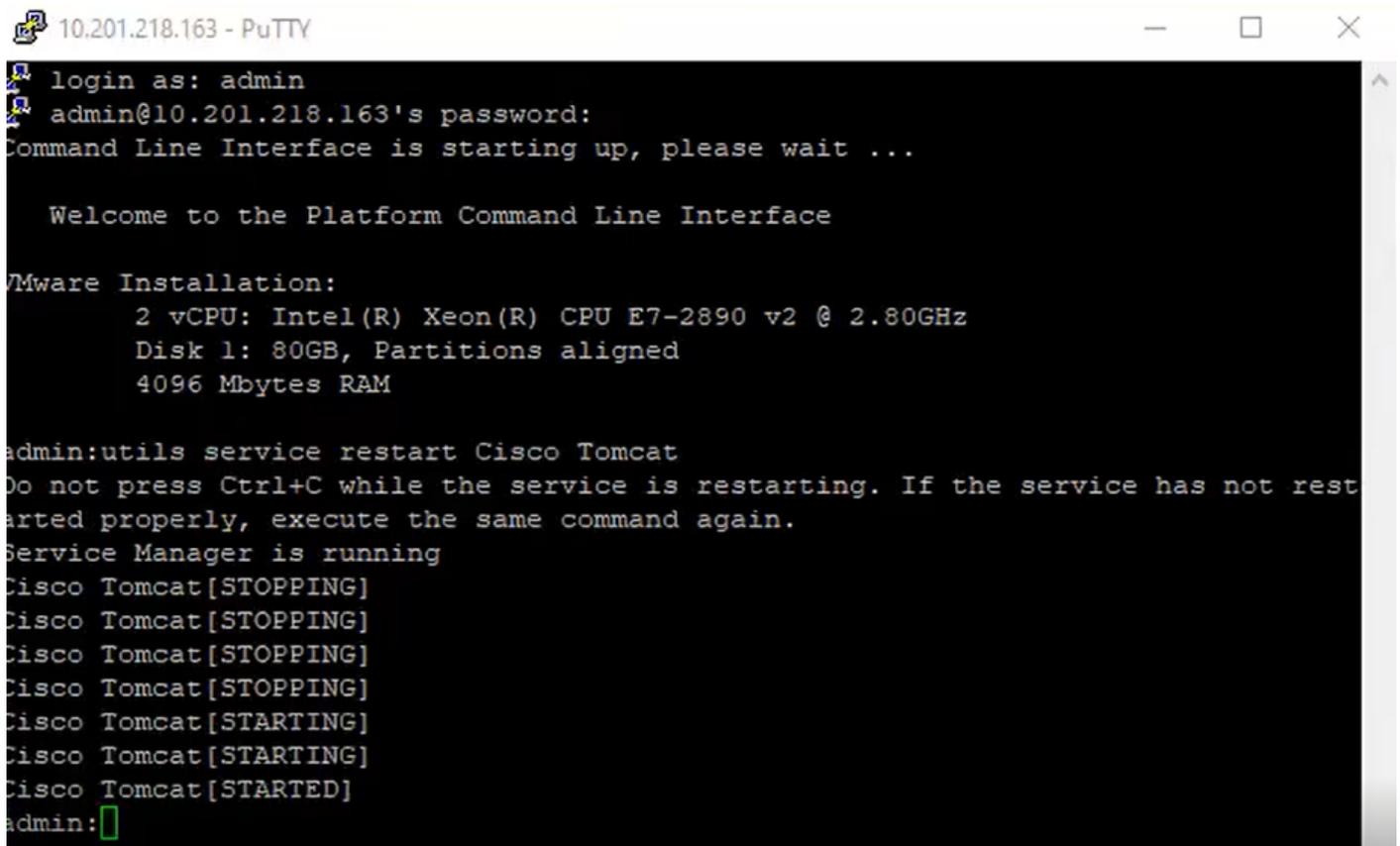


 Nota: Si tiene servidores IM/P que forman parte del clúster de CUCM, también debe cargar estos certificados en estos servidores IM/P.

 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:



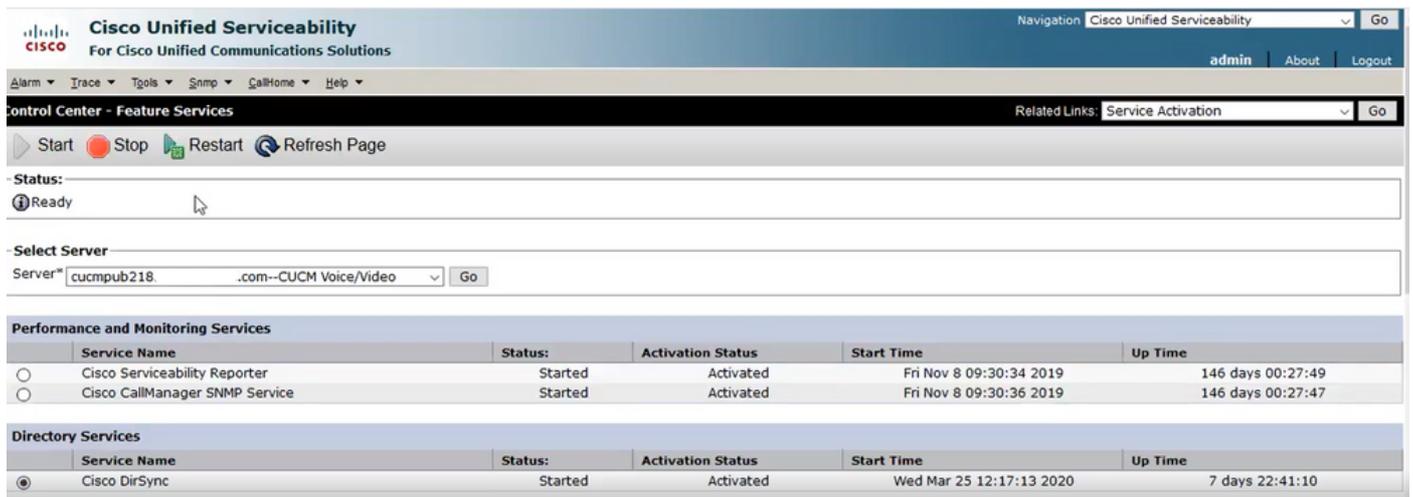
```
10.201.218.163 - PuTTY
login as: admin
admin@10.201.218.163's password:
Command Line Interface is starting up, please wait ...

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:
```

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):



Cisco Unified Serviceability
For Cisco Unified Communications Solutions

Navigation: Cisco Unified Serviceability Go

admin About Logout

Alarm Trace Tools Snmp CallHome Help

Control Center - Feature Services Related Links: Service Activation Go

Start Stop Restart Refresh Page

Status: Ready

Select Server
Server: cucmpub218 .com--CUCM Voice/Video Go

Performance and Monitoring Services					
	Service Name	Status	Activation Status	Start Time	Up Time
<input type="radio"/>	Cisco Serviceability Reporter	Started	Activated	Fri Nov 8 09:30:34 2019	146 days 00:27:49
<input type="radio"/>	Cisco CallManager SNMP Service	Started	Activated	Fri Nov 8 09:30:36 2019	146 days 00:27:47

Directory Services					
	Service Name	Status	Activation Status	Start Time	Up Time
<input checked="" type="radio"/>	Cisco DirSync	Started	Activated	Wed Mar 25 12:17:13 2020	7 days 22:41:10

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:

The screenshot shows the Cisco Unified CM Administration interface for the LDAP Directory configuration. The page is titled "LDAP Directory" and includes a navigation menu at the top with options like System, Call Routing, Media Resources, etc. The main content area is divided into two sections: "Group Information" and "LDAP Server Information".

Group Information:

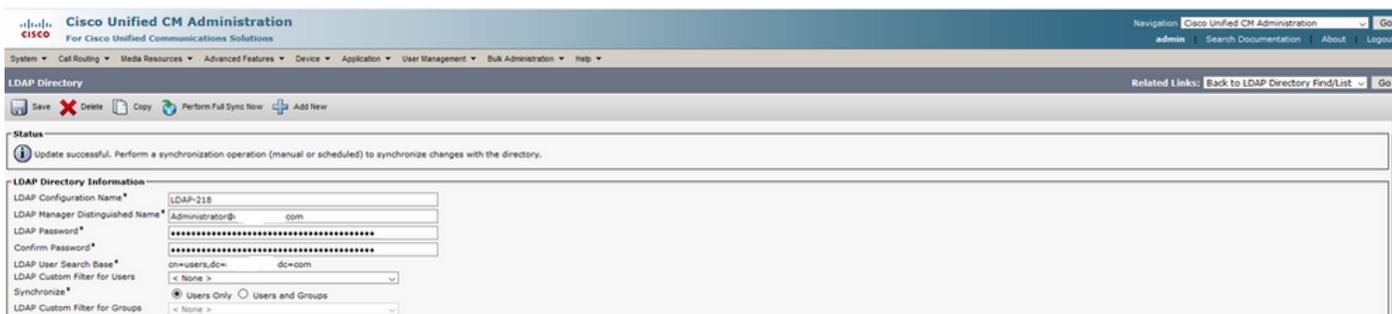
- User Rank*: 1-Default User Rank
- Access Control Groups: A list box with "Add to Access Control Group" and "Remove from Access Control Group" buttons.
- Feature Group Template: < None >
- Warning: If no template is selected, the new line features below will not be active.
- Apply mask to synced telephone numbers to create a new line for inserted users
- Mask: [Text Input]
- Assign new line from the pool list if one was not created based on a synced LDAP telephone number
- Order: [Text Input]
- DN Pool Start: [Text Input]
- DN Pool End: [Text Input]
- Add DN Pool: [Button]

LDAP Server Information:

- Host Name or IP Address for Server*: WIN-H2Q74S1U39P...com
- LDAP Port*: 636
- Use TLS:
- Add Another Redundant LDAP Server: [Button]

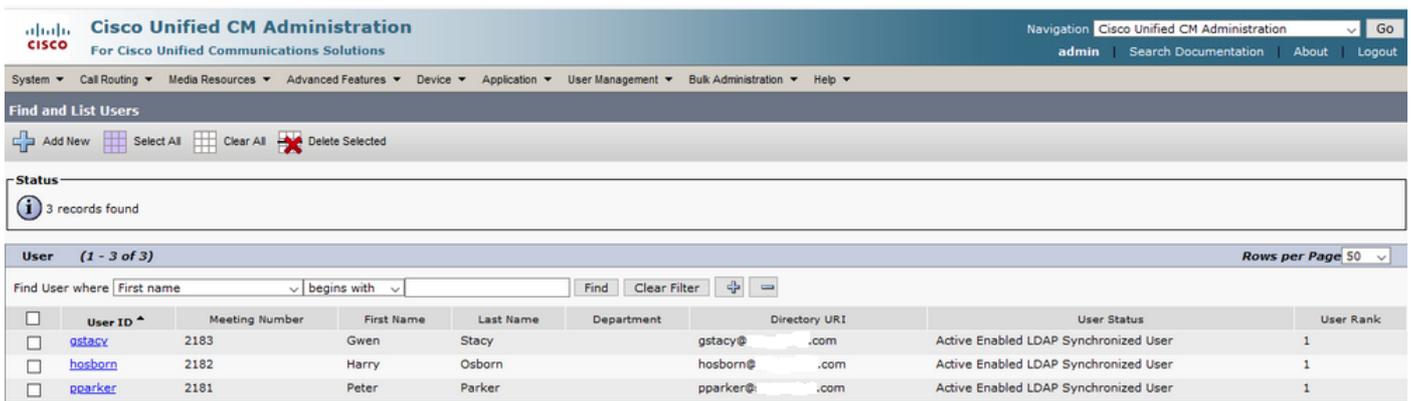
Nota: De forma predeterminada, después de comprobar el FQDN de las versiones 10.5(2)SU2 y 9.1(2)SU3 configurado en Información del servidor LDAP con el nombre común del certificado, en caso de que se utilice la dirección IP en lugar del FQDN, el comando `utils ldap config ipaddr` se ejecuta para detener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



The screenshot displays the Cisco Unified CM Administration web interface. At the top, the navigation bar includes 'Cisco Unified CM Administration' and 'admin'. Below the navigation bar, the breadcrumb trail shows 'System > Call Routing > Media Resources > Advanced Features > Device > Application > User Management > Bulk Administration > Help'. The main content area is titled 'LDAP Directory' and contains a status message: 'Update successful. Perform a synchronization operation (manual or scheduled) to synchronize changes with the directory.' Below this, the 'LDAP Directory Information' section is visible, showing various configuration fields such as 'LDAP Configuration Name' (LDAP-218), 'LDAP Manager Distinguished Name' (Administrator@.com), and 'LDAP User Search Base' (cn=users,dc=,dc=com). The 'Synchronize' section has radio buttons for 'Users Only' (selected) and 'Users and Groups'. The 'Perform Full Sync Now' button is highlighted with a green border and a plus icon.

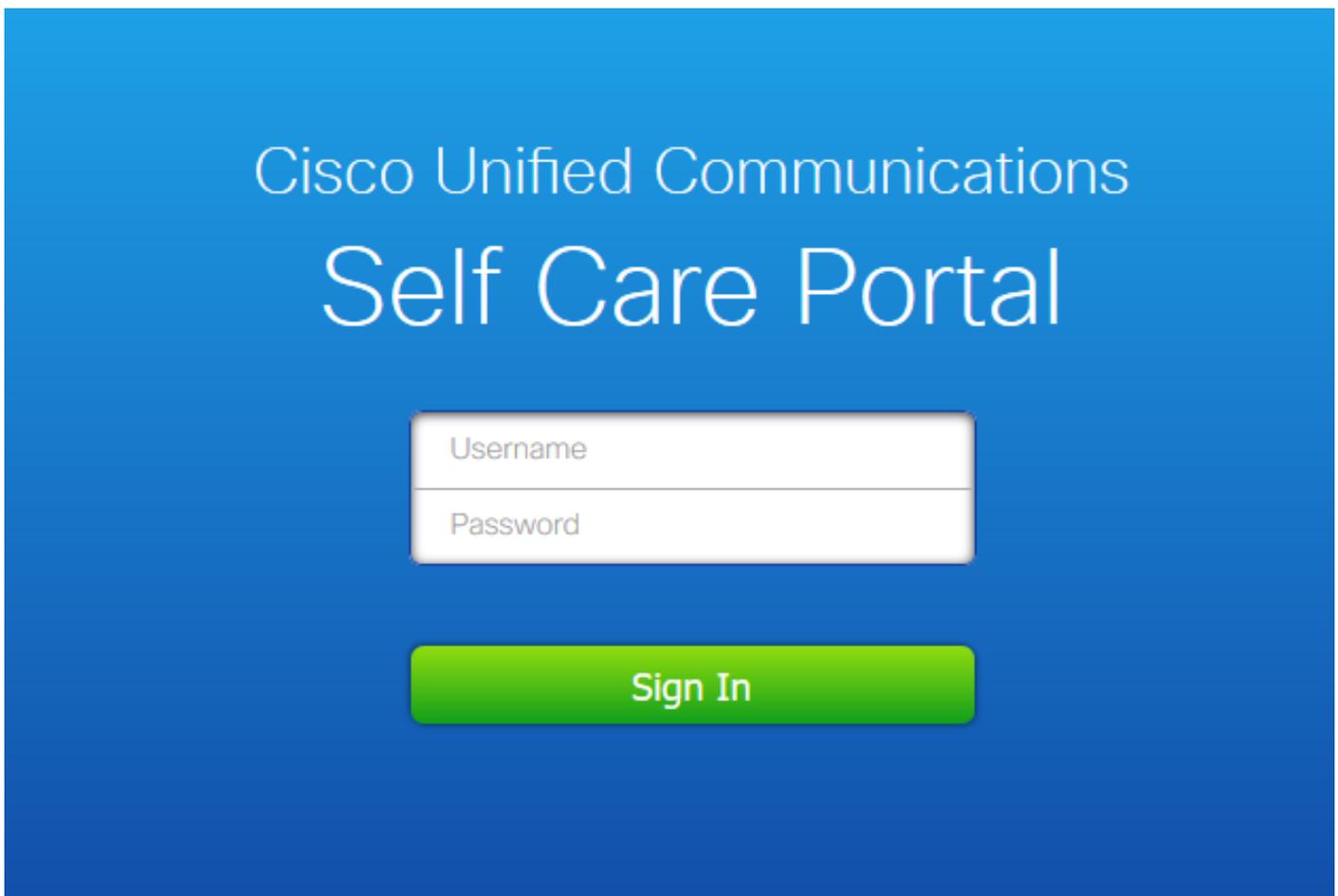
Paso 3. Vaya a CUCM Administration > User Management > End User y verifique que los usuarios finales están presentes, como se muestra en la imagen:



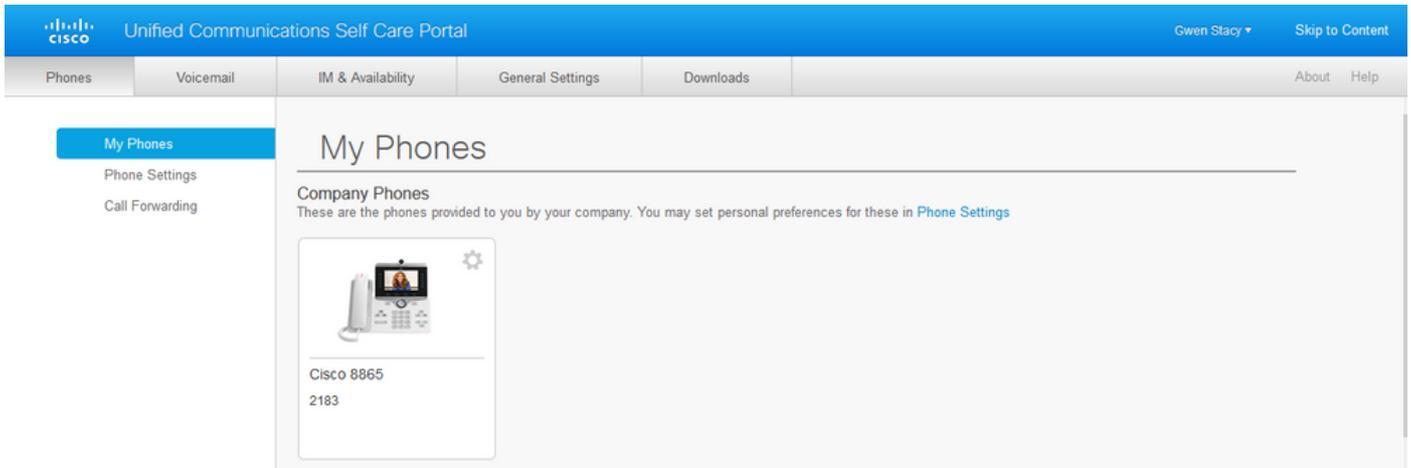
<input type="checkbox"/>	User ID	Meeting Number	First Name	Last Name	Department	Directory URI	User Status	User Rank
<input type="checkbox"/>	gstacy	2183	Gwen	Stacy		gstacy@...com	Active Enabled LDAP Synchronized User	1
<input type="checkbox"/>	hosborn	2182	Harry	Osborn		hosborn@...com	Active Enabled LDAP Synchronized User	1
<input type="checkbox"/>	pparker	2181	Peter	Parker		pparker@...com	Active Enabled LDAP Synchronized User	1

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:



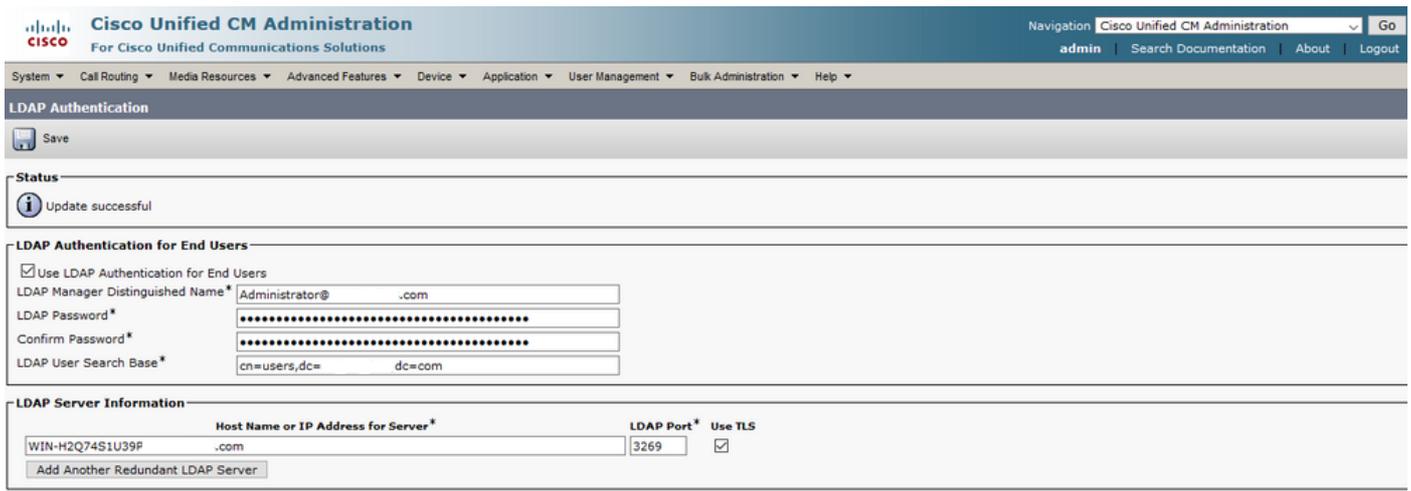
El usuario puede iniciar sesión correctamente después de introducir las credenciales LDAP, como se muestra en la imagen:



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:

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

UC Service Configuration | Related Links: Back To Find/List | Go

Save | Delete | Copy | Reset | Apply Config | Add New

Status
Update successful

UC Service Information

UC Service Type: **Directory**

Product Type*: Directory

Name*: Secure Directory

Description:

Host Name/IP Address*: WIN-H2Q74S1U39P .com

Port: 636

Protocol: TLS

Save | Delete | Copy | Reset | Apply Config | Add New

*. indicates required item.

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).