

Configurar CUCM para LDAP seguro (LDAPS)

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Verificar e instalar certificados LDAPS](#)

[Configurar diretório LDAP seguro](#)

[Configurar Autenticação LDAP Segura](#)

[Configurar conexões seguras com o AD para serviços de UC](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve o procedimento para atualizar conexões CUCM para o AD de uma conexão LDAP não segura para uma conexão LDAPS segura.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Servidor AD LDAP
- Configuração LDAP do CUCM
- Serviço de mensagens instantâneas e presença (IM/P) do CUCM

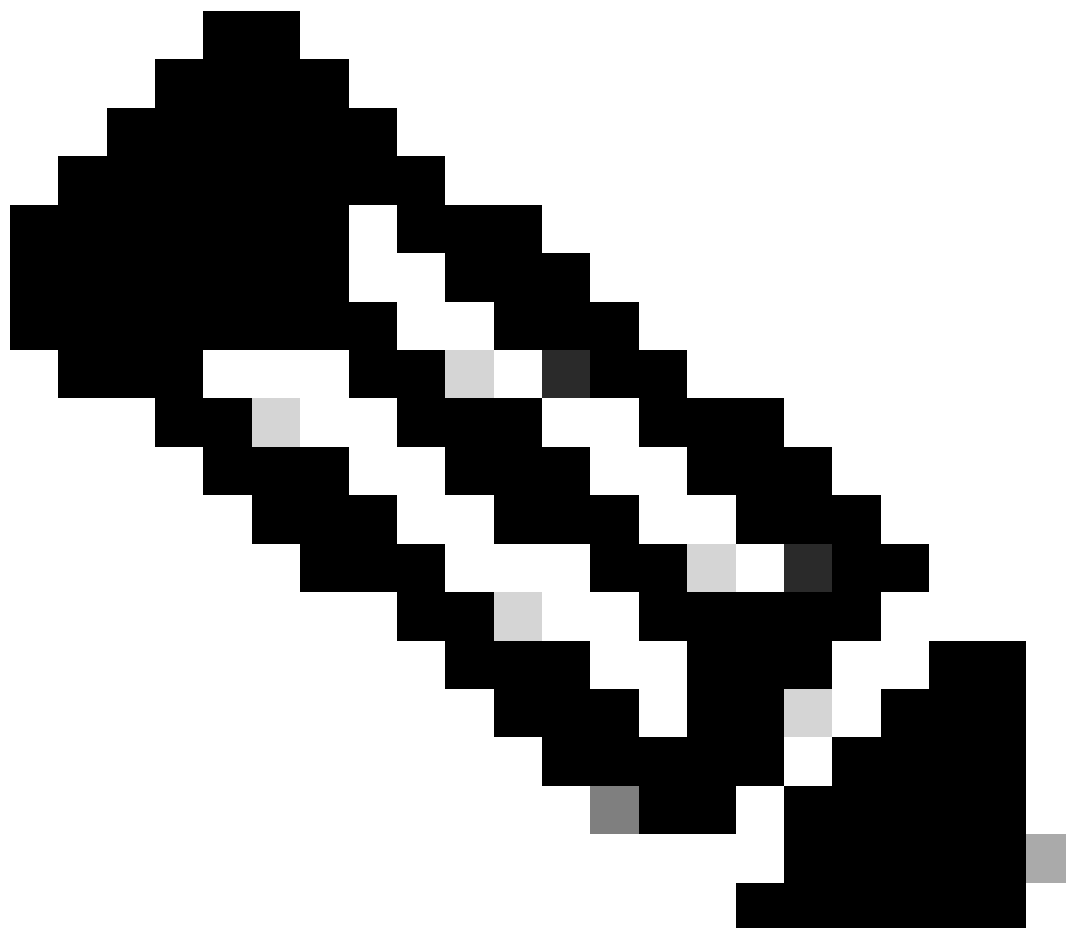
Componentes Utilizados

As informações neste documento são baseadas no CUCM versão 9.x e superior.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

É responsabilidade do Administrador do Ative Diretory (AD) configurar o AD LDAPS (Lightweight Diretory Access Protocol) para LDAPS (Lightweight Diretory Access Protocol). Isso inclui a instalação de certificados assinados por CA que atendem ao requisito de um certificado LDAPS.



Observação: consulte este link para obter informações para atualizar de LDAP não seguro para conexões LDAPS seguras para AD para outros Aplicativos de Colaboração da Cisco: [Consultoria de Software: LDAP Seguro Obrigatório para Conexões do Ative Diretory](#)

Verificar e instalar certificados LDAPS

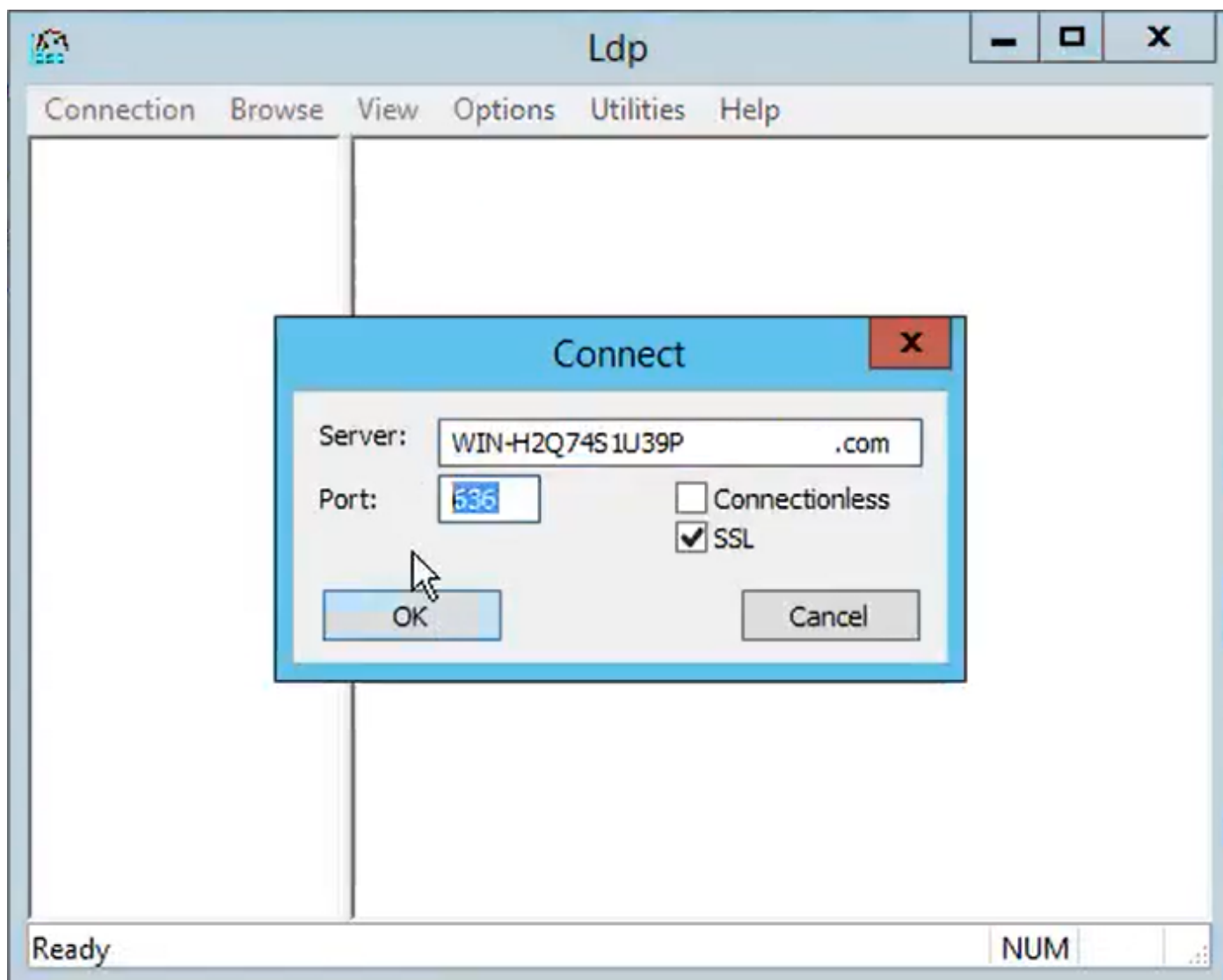
Etapa 1. Depois que o certificado LDAPS tiver sido carregado no servidor AD, verifique se o LDAPS está habilitado no servidor AD com a ferramenta Ldp.exe.

1. Inicie a Ferramenta de Administração do AD (Ldp.exe) no servidor do AD.
2. No menu Conexão, selecione Conectar.
3. Insira o FQDN (Fully Qualified Domain Name, Nome de domínio totalmente qualificado) do

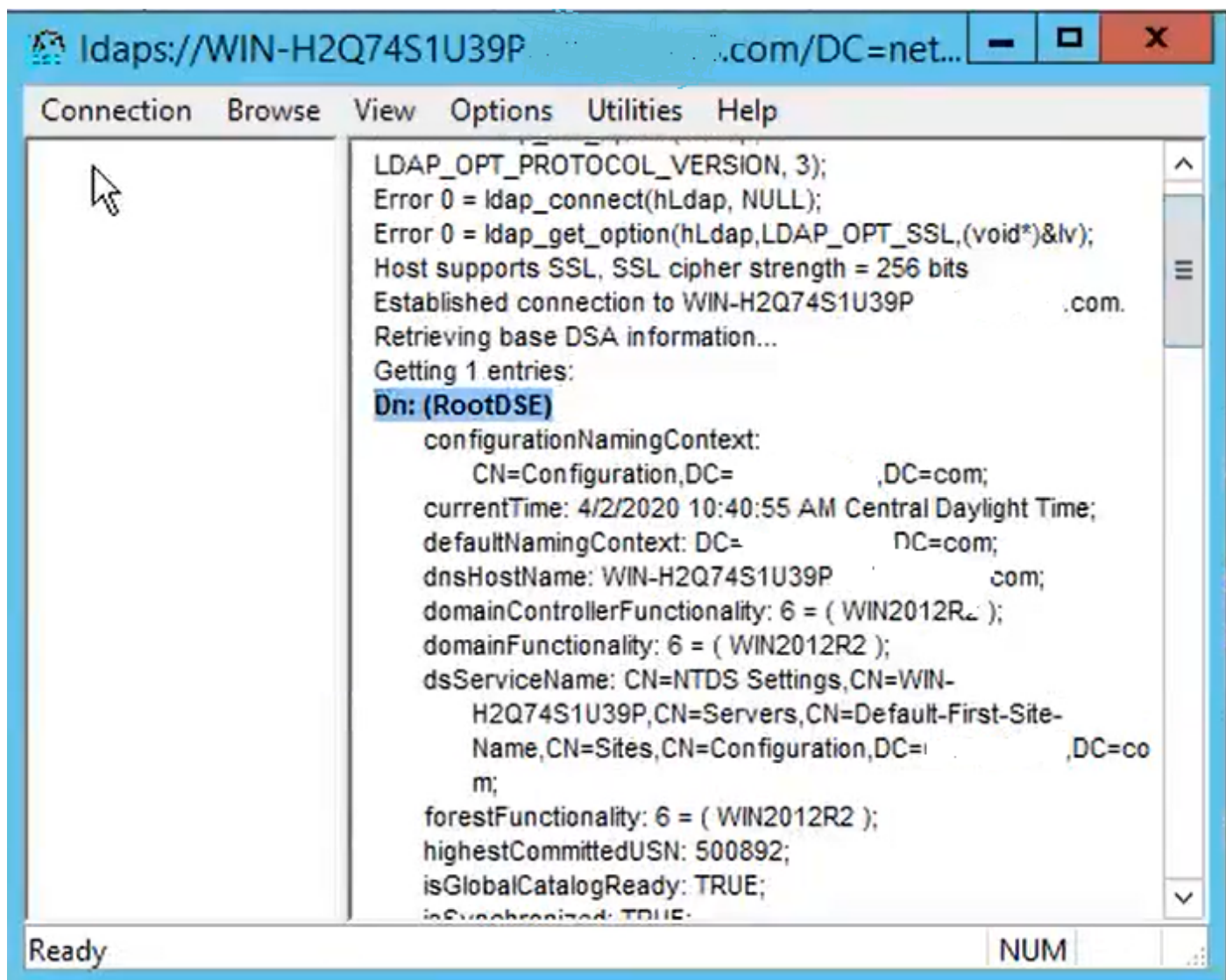
servidor LDAPS como servidor.

4. Insira 636 como o número da porta.

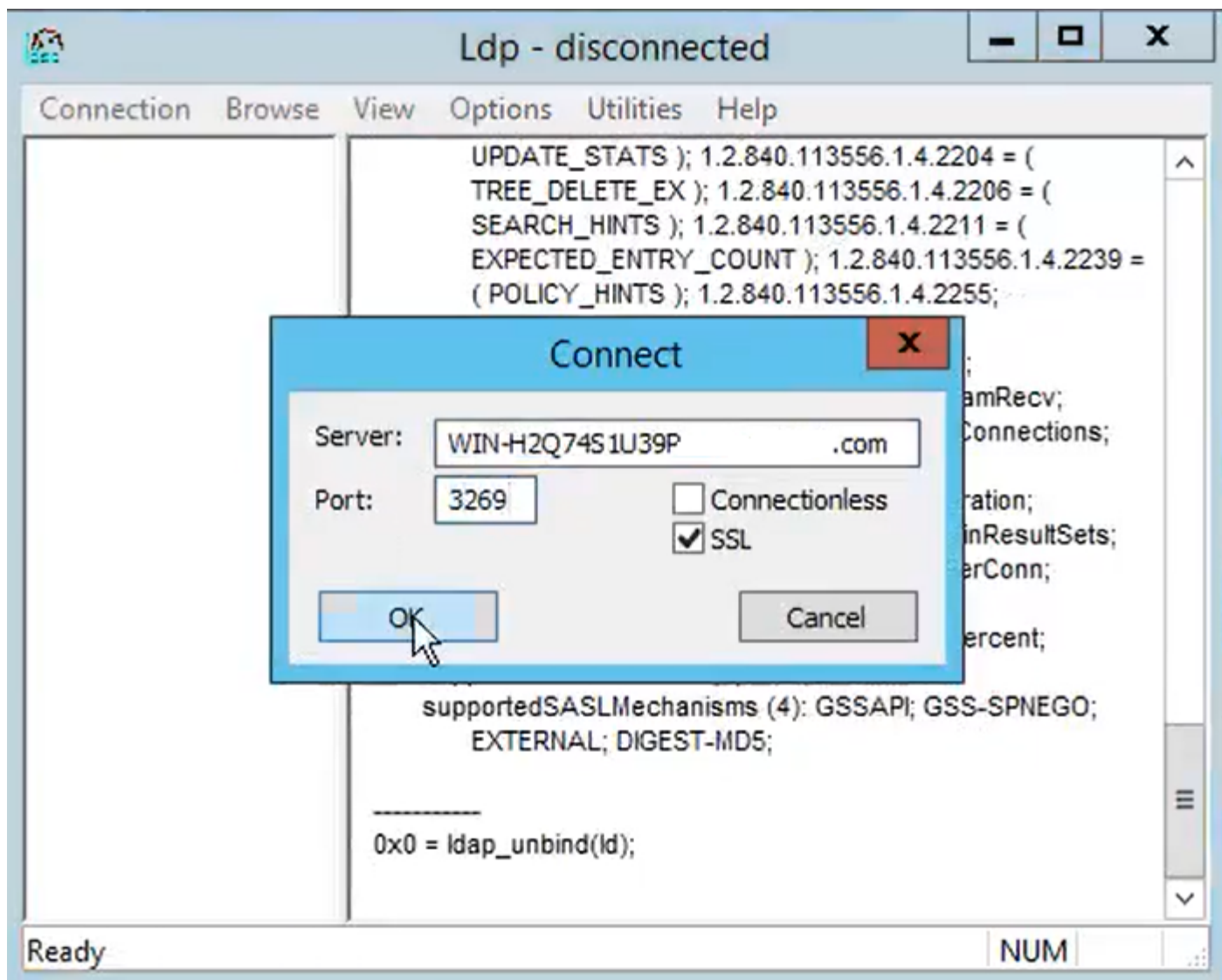
5. Clique em OK, como mostrado na imagem



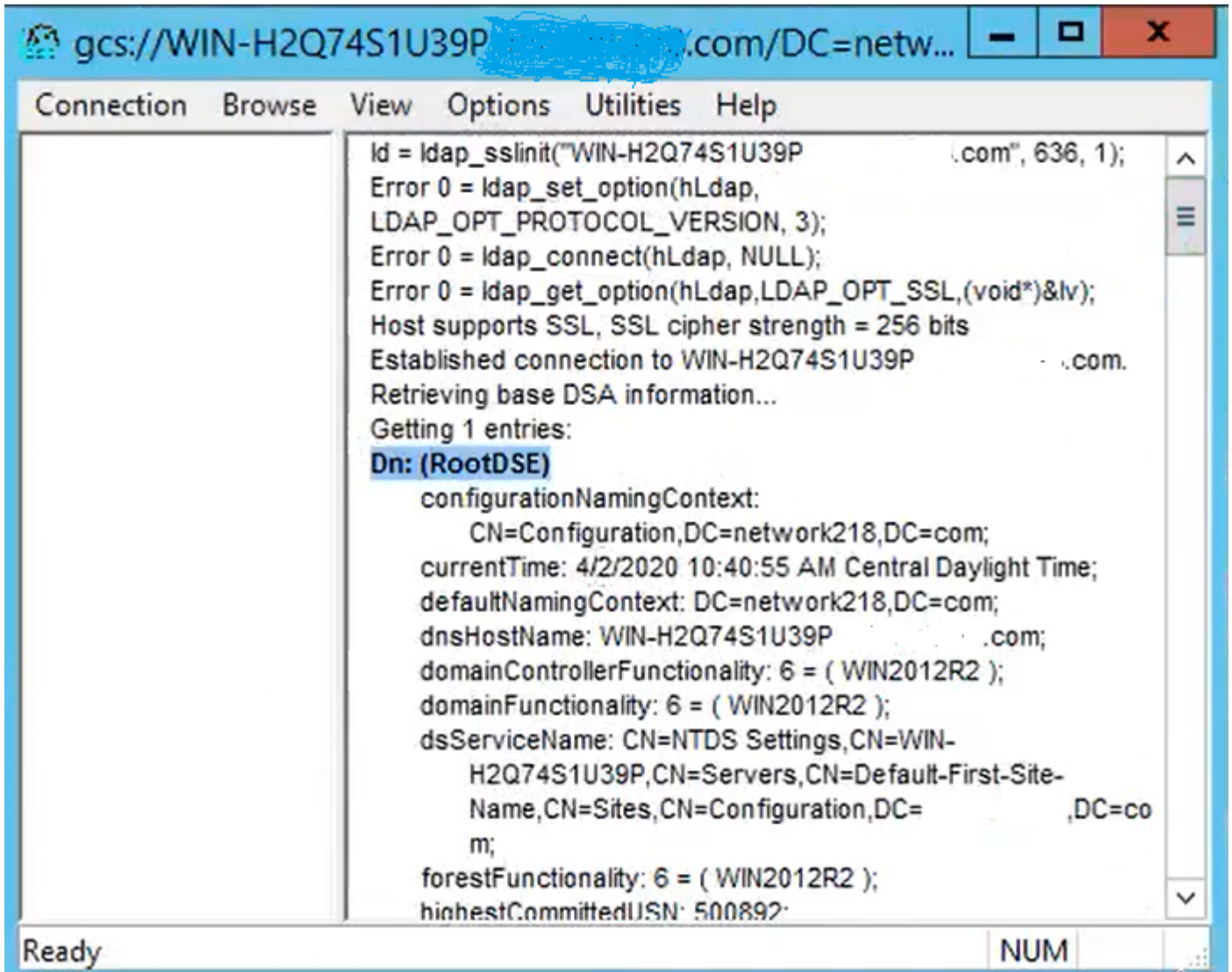
Para uma conexão bem-sucedida na porta 636, as informações do RootDSE são impressas no painel direito, como mostrado na imagem:



Repita o procedimento para a porta 3269, como mostrado na imagem:

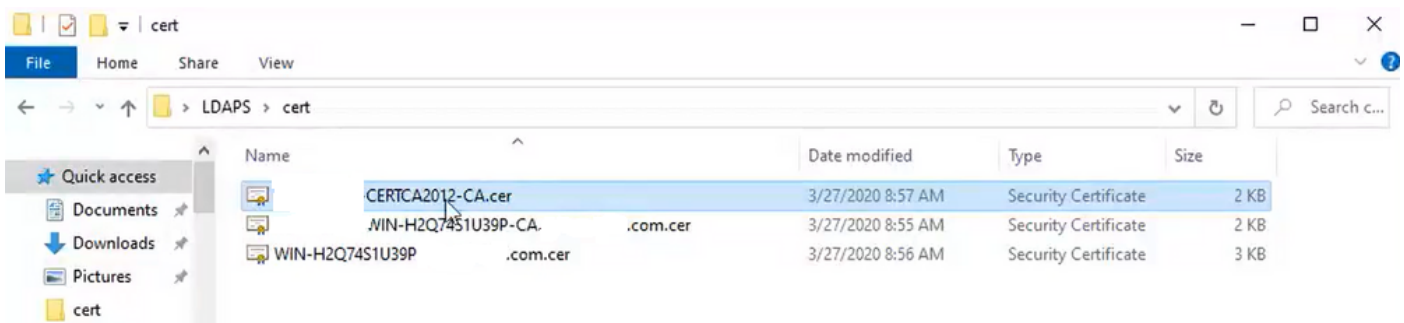


Para uma conexão bem-sucedida na porta 3269, as informações do RootDSE são impressas no painel direito, como mostrado na imagem:

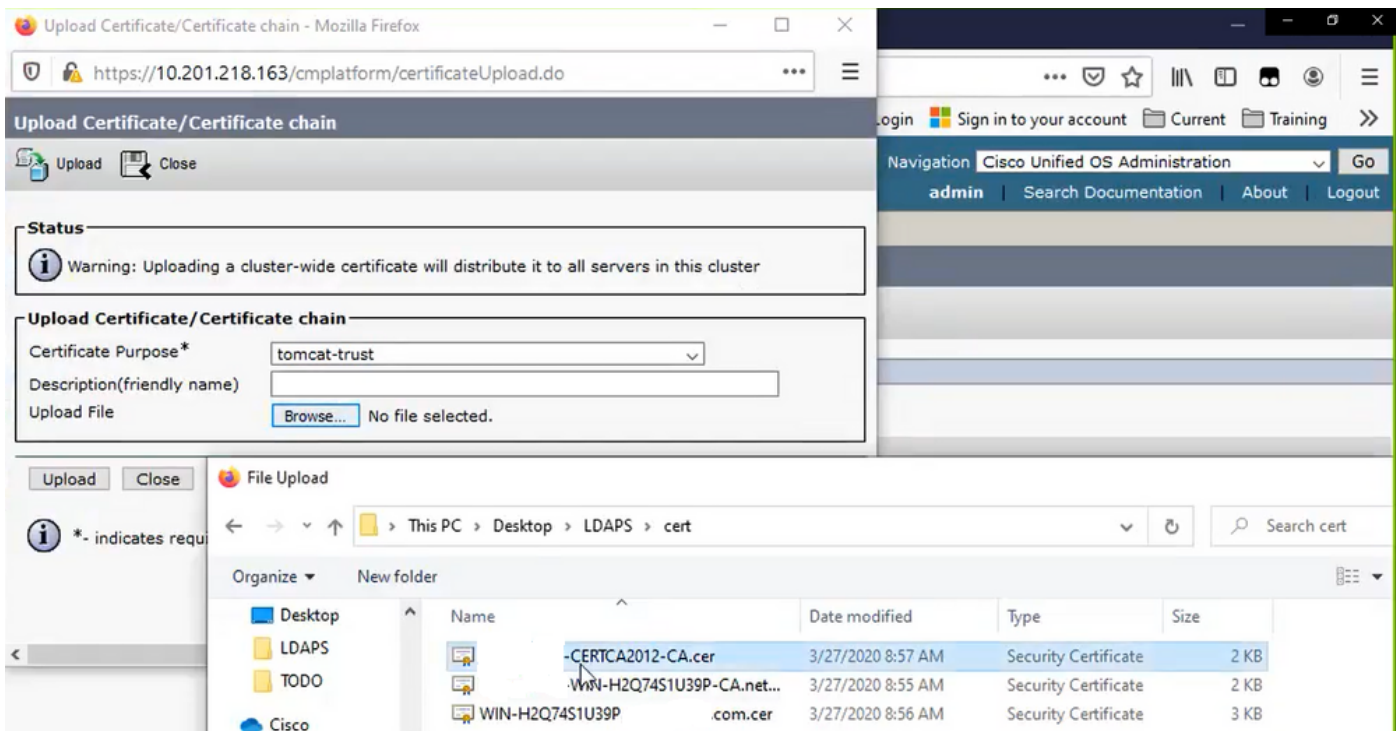


Etapa 2. Obtenha a raiz e todos os certificados intermediários que fazem parte do certificado de servidor LDAPS e instale-os como certificados tomcat-trust em cada um dos nós de editor de CUCM e IM/P e como CallManager-trust no editor de CUCM.

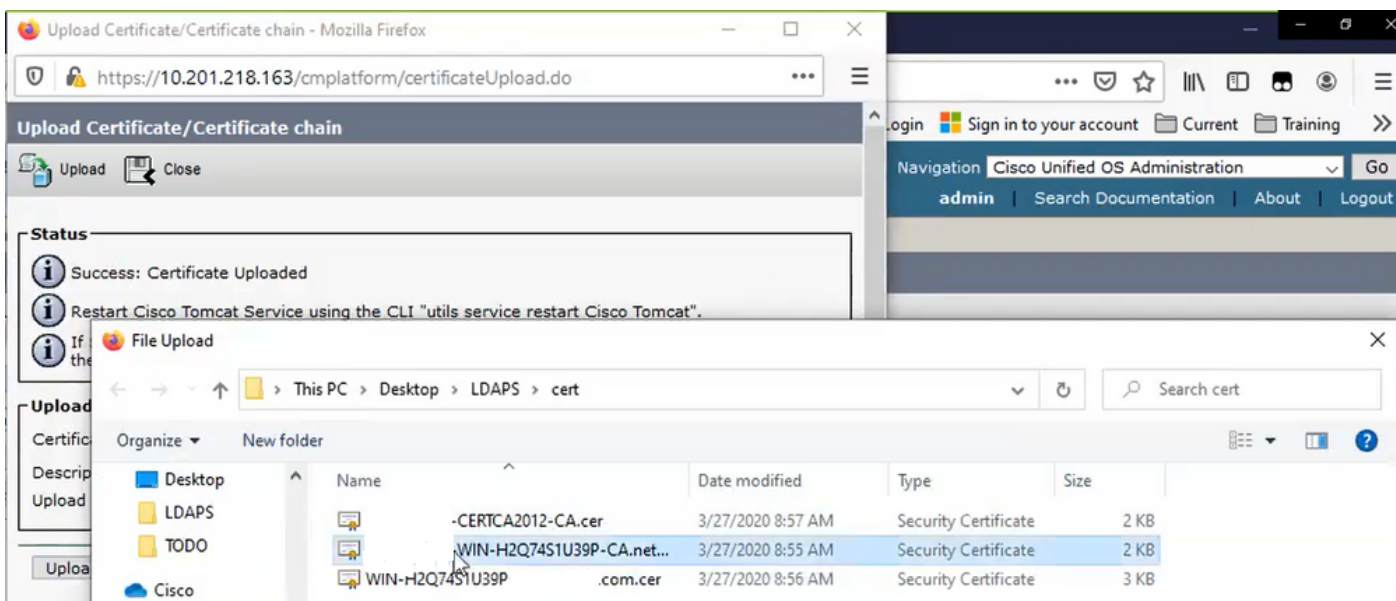
Os certificados raiz e intermediários que fazem parte de um certificado de servidor LDAPS, <hostname>.<Domain>.cer, são mostrados na imagem:



Navegue até o editor do CUCM Cisco Unified OS Administration > Security > Certificate Management. Carregue o root como tomcat-trust (como mostrado na imagem) e como CallManager-trust (não mostrado):



Carregue o intermediário como tomcat-trust (como mostrado na imagem) e como CallManager-trust (não mostrado):

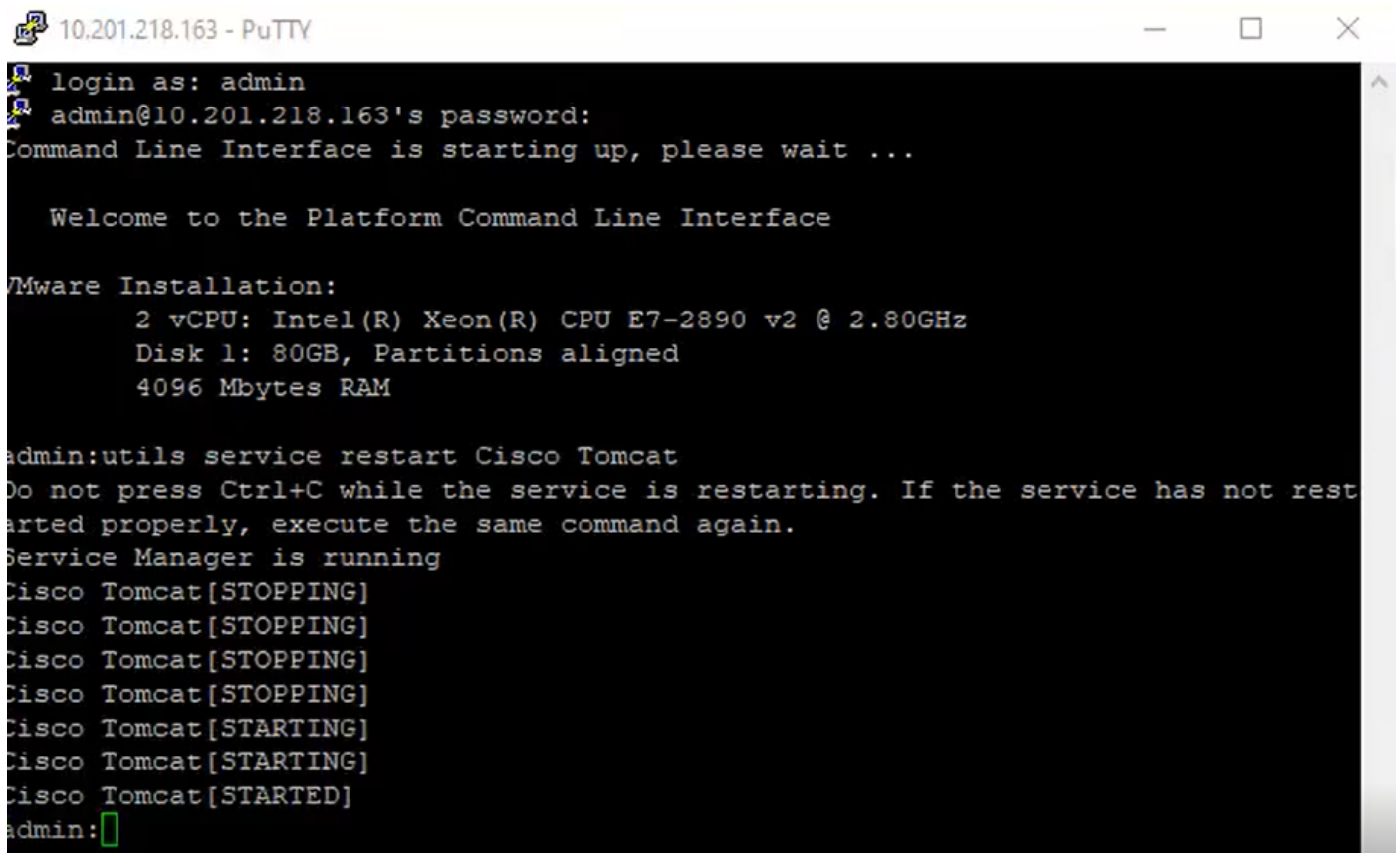


Observação: se você tiver servidores IM/P que fazem parte do cluster CUCM, também precisará carregar esses certificados para esses servidores IM/P.

Nota: como alternativa, você pode instalar o certificado do servidor LDAPS como tomcat-trust.

Etapa 3. Reinicie o Cisco Tomcat a partir da CLI de cada nó (CUCM e IM/P) em clusters. Além disso, para o cluster CUCM, verifique se o serviço Cisco DirSync no nó do editor foi iniciado.

Para reiniciar o serviço Tomcat, você precisa abrir uma sessão CLI para cada nó e executar o comando `utils service restart Cisco Tomcat`, como mostrado na imagem:



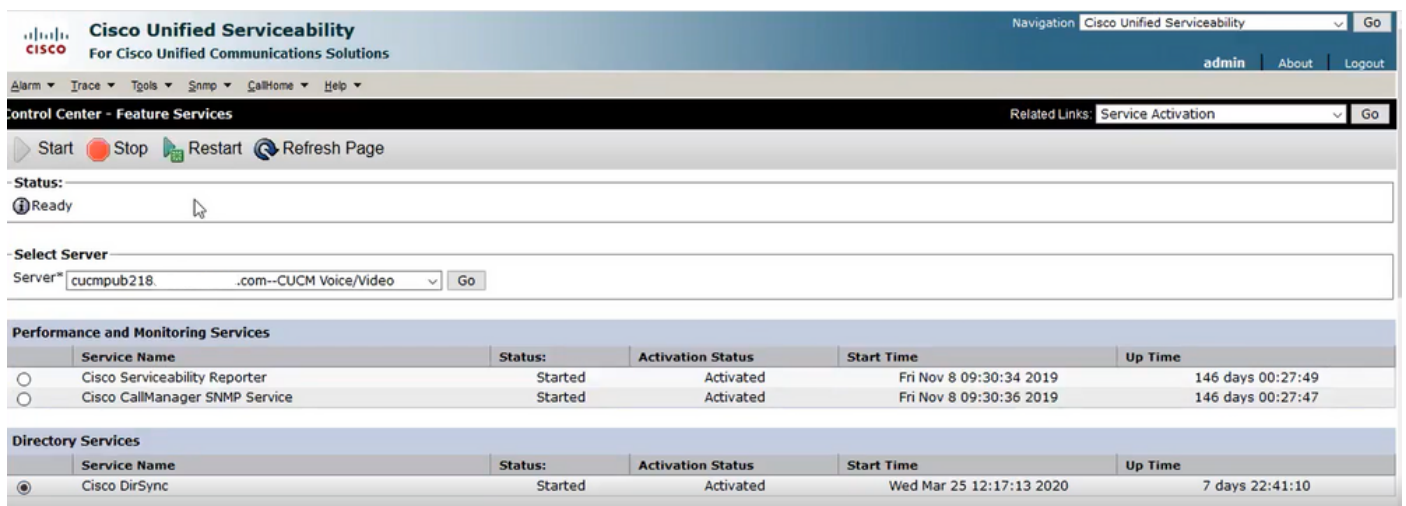
```
10.201.218.163 - PuTTY
login as: admin
admin@10.201.218.163's password:
Command Line Interface is starting up, please wait ...

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:
```

Etapa 4. Navegue para o editor do CUCM Cisco Unified Serviceability > Tools > Control Center - Feature Services, verifique se o serviço Cisco DirSync está ativado e iniciado (como mostrado na imagem) e reinicie o serviço Cisco CTIManager em cada nó se ele for usado (não mostrado):



Configurar diretório LDAP seguro

Etapa 1. Configure o Diretório LDAP do CUCM para utilizar a conexão TLS LDAPS com o AD na porta 636.

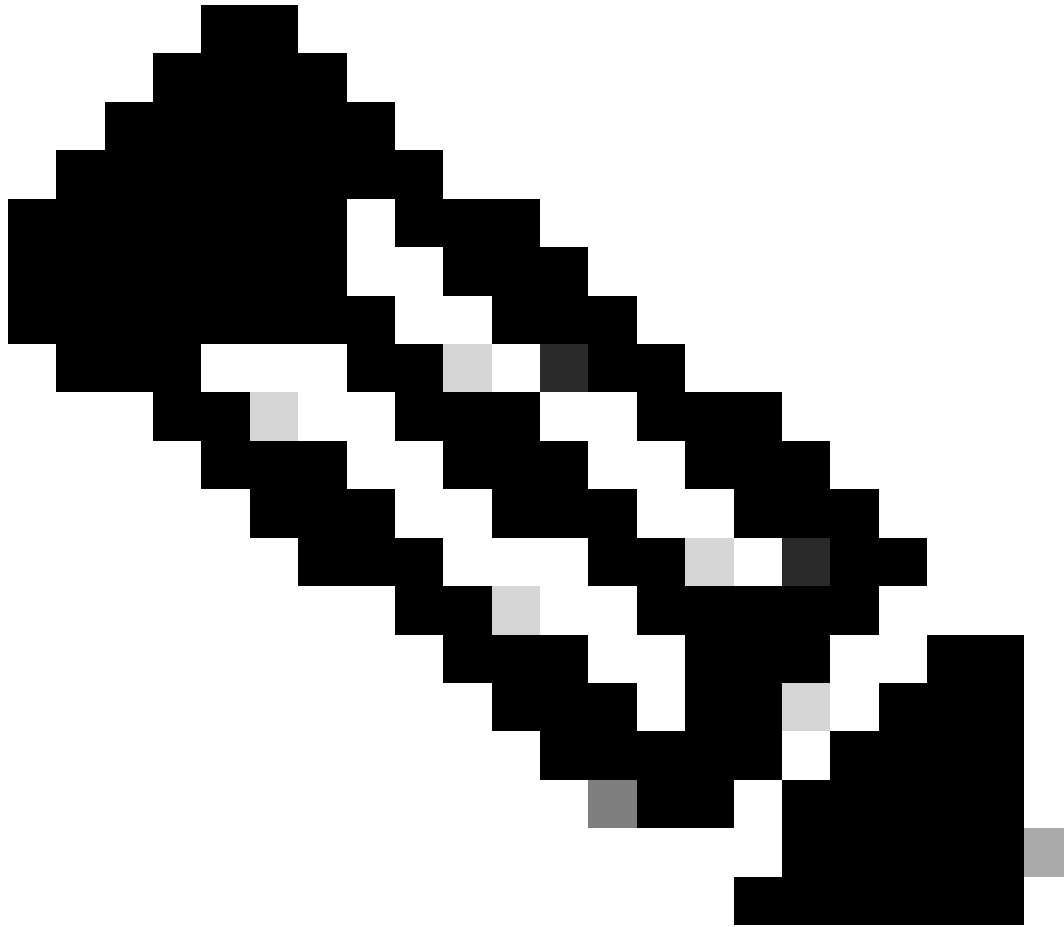
Navegue até CUCM Administration > System > LDAP Directory. Digite o FQDN ou o endereço IP

do servidor LDAP para Informações do servidor LDAP. Especifique a porta LDAPS de 636 e marque a caixa para Usar TLS, como mostrado na imagem:

The screenshot shows the 'LDAP Server Information' section of the Cisco Unified CM Administration interface. The form includes the following fields and options:

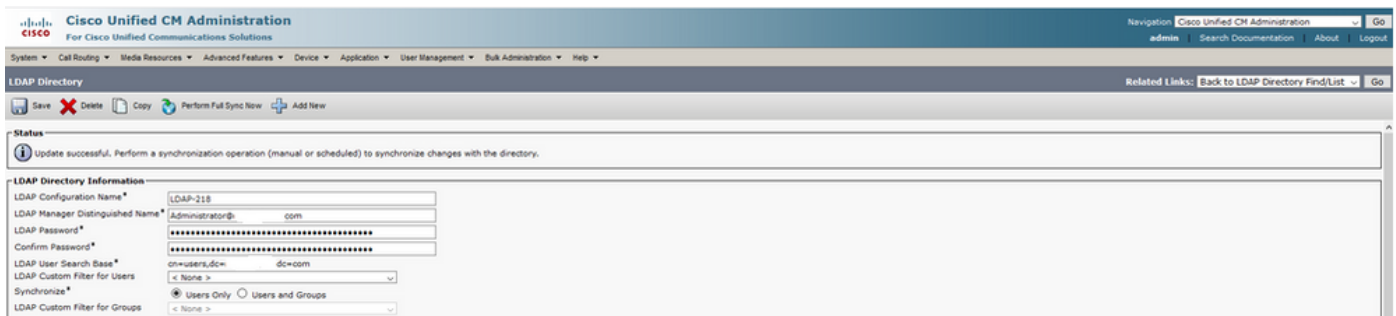
- Host Name or IP Address for Server*:** WIN-H2Q7451U39R.com
- LDAP Port*:** 636
- Use TLS:**
- Buttons:** Add Another Redundant LDAP Server

The 'Group Information' section above contains fields for User Rank (1-Default User Rank), Access Control Groups, Feature Group Template (< None >), and checkboxes for applying masks and assigning new lines from a pool list. A warning message states: 'Warning: If no template is selected, the new line features below will not be active.'

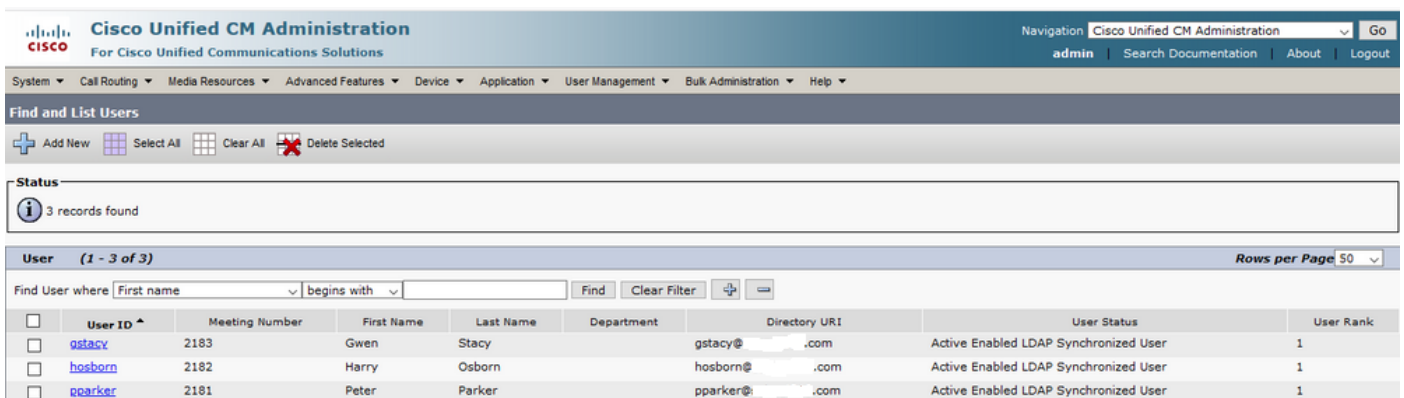


Nota: Por padrão, depois que as versões 10.5(2)SU2 e 9.1(2)SU3 FQDN configuradas nas Informações do Servidor LDAP são verificadas em relação ao Nome Comum do certificado, no caso de o endereço IP ser usado em vez do FQDN, o comando `utils ldap config ipaddr` é emitido para interromper a imposição do FQDN à verificação do CN.

Etapa 2. Para concluir a alteração de configuração para LDAPS, clique em **Perform Full Sync Now**, como mostrado na imagem:



Etapa 3. Navegue até **CUCM Administration > User Management > End User** e verifique se os usuários finais estão presentes, como mostrado na imagem:



Etapa 4. Navegue até a página `ccmuser` (<https://<endereço ip do cucm pub>/ccmuser>) para verificar se o logon do usuário foi bem-sucedido.

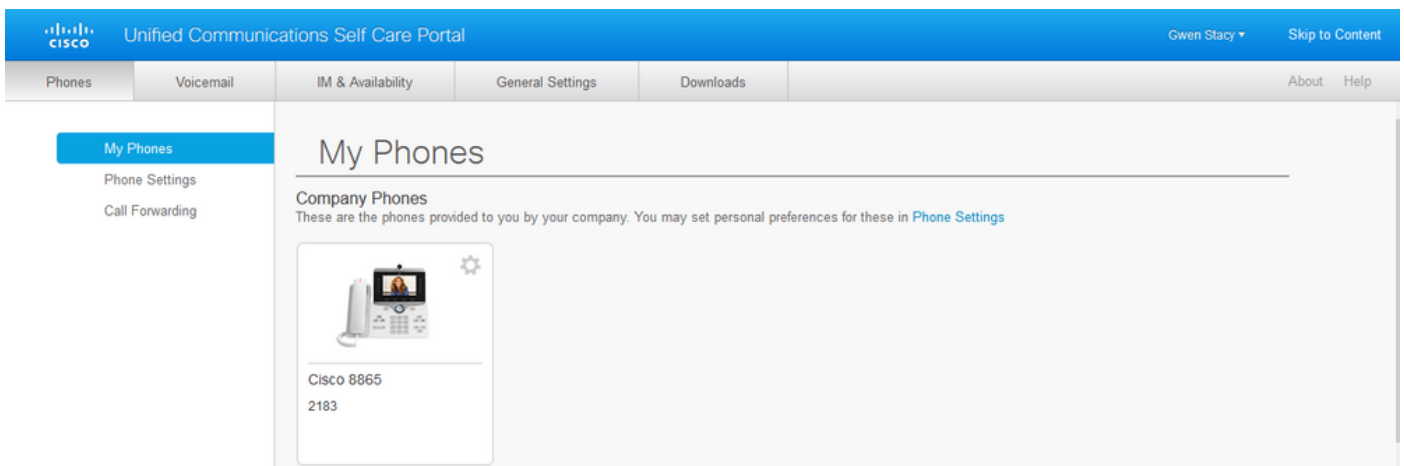
A página `ccmuser` do CUCM versão 12.0.1 é semelhante a esta:

Cisco Unified Communications Self Care Portal

Username
Password

Sign In

O usuário pode fazer login com êxito depois que as credenciais LDAP são inseridas, como mostrado na imagem:



Configurar Autenticação LDAP Segura

Configure a autenticação LDAP do CUCM para utilizar a conexão TLS LDAPS com o AD na porta 3269.

Navegue até CUCM Administration > System > LDAP Authentication. Digite o FQDN do servidor LDAPS para Informações do servidor LDAP. Especifique a porta LDAPS de 3269 e marque a caixa para Usar TLS, como mostrado na imagem:

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

LDAP Authentication

Save

Status
Update successful

LDAP Authentication for End Users

Use LDAP Authentication for End Users

LDAP Manager Distinguished Name* Administrator@ .com

LDAP Password*

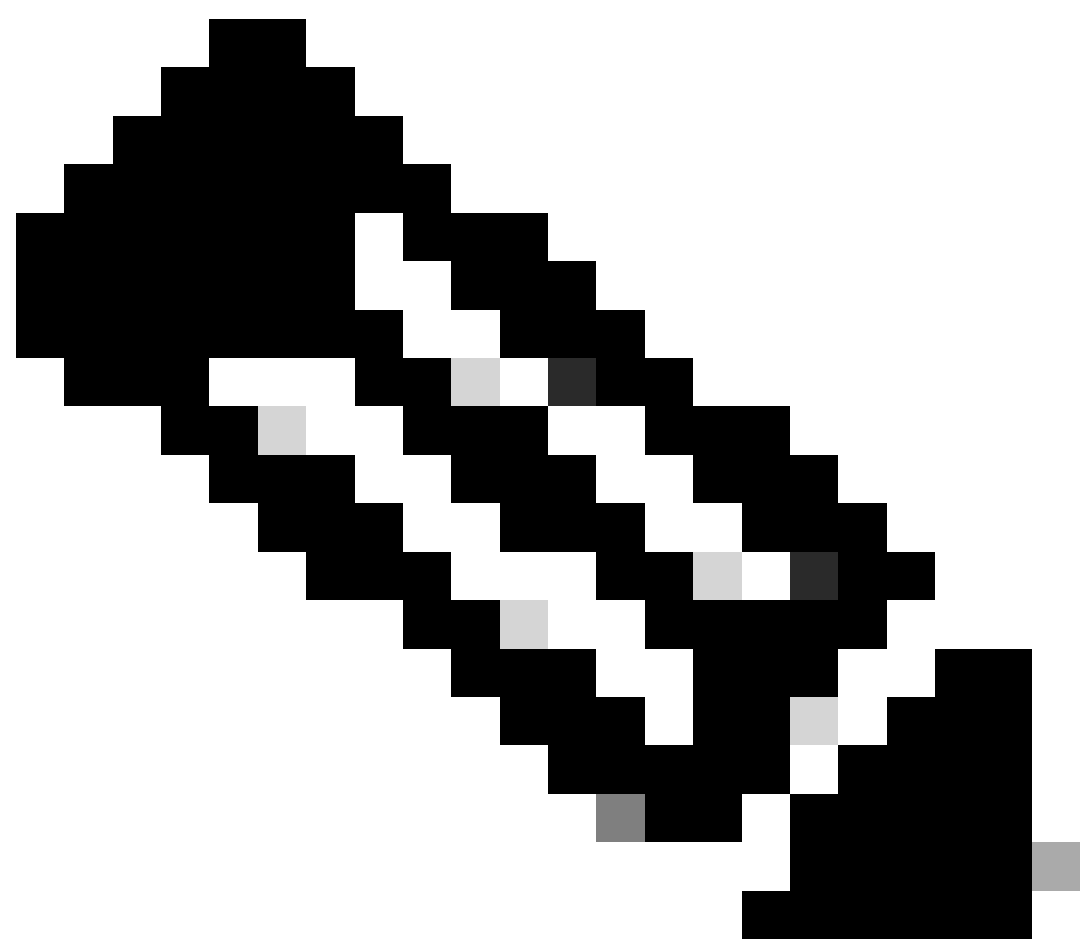
Confirm Password*

LDAP User Search Base* cn=users,dc= dc=com

LDAP Server Information

Host Name or IP Address for Server*	LDAP Port*	Use TLS
WIN-H2Q74S1U39P .com	3269	<input checked="" type="checkbox"/>

Add Another Redundant LDAP Server

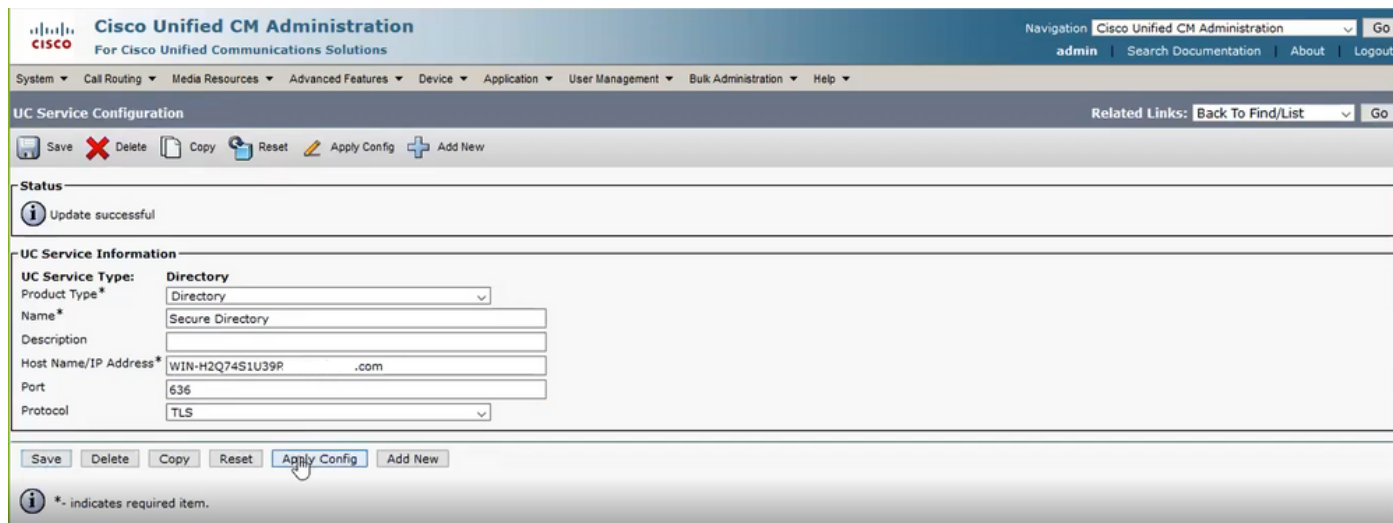


Observação: se você tiver clientes Jabber, é recomendável usar a porta 3269 para autenticação LDAPS, pois o tempo limite do Jabber para logon poderá ocorrer se uma conexão segura com o servidor de catálogo global não for especificada.

Configurar conexões seguras com o AD para serviços de UC

Se precisar proteger serviços UC que utilizam LDAP, configure esses serviços UC para utilizar a porta 636 ou 3269 com TLS.

Navegue até Administração do CUCM > Gerenciamento de usuário > Configurações do usuário > Serviço UC. Localize o Serviço de Diretório que aponte para AD. Digite o FQDN do servidor LDAPS como o nome do host/endereço IP. Especifique a porta como 636 ou 3269 e protocolo TLS, como mostrado na imagem:



The screenshot displays the Cisco Unified CM Administration web interface. The page title is "Cisco Unified CM Administration" with the subtitle "For Cisco Unified Communications Solutions". The navigation menu includes "System", "Call Routing", "Media Resources", "Advanced Features", "Device", "Application", "User Management", "Bulk Administration", and "Help". The current page is "UC Service Configuration".

The "UC Service Information" section is visible, showing the following configuration details:

- UC Service Type:** Directory
- Product Type*:** Directory
- Name*:** Secure Directory
- Description:** (empty field)
- Host Name/IP Address*:** WIN-H2Q74S1U39P .com
- Port:** 636
- Protocol:** TLS

At the bottom of the configuration section, there are buttons for "Save", "Delete", "Copy", "Reset", "Apply Config", and "Add New". A status message at the top left of the configuration area indicates "Update successful". A legend at the bottom left states: "i * indicates required item."



Observação: as máquinas cliente Jabber também precisam ter os certificados LDAPS tomcat-trust que foram instalados no CUCM instalado no armazenamento confiável de gerenciamento de certificados da máquina cliente Jabber para permitir que o cliente Jabber estabeleça uma conexão LDAPS com o AD.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Para verificar a cadeia real de certificado/certificado LDAPS enviada do servidor LDAP para o CUCM para a conexão TLS, exporte o Certificado TLS LDAPS de uma captura de pacote CUCM. Este link fornece informações sobre como exportar um certificado TLS de uma captura de pacote CUCM: [Como exportar o certificado TLS da captura de pacote CUCM](#)

Troubleshooting

No momento, não há informações específicas disponíveis para solucionar esse problema de configuração.

Informações Relacionadas

- Esse link fornece acesso a um vídeo que percorre as configurações de LDAPS: [Secure LDAP Directory and Authentication Walkthrough Video](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.