# Configuración de CUCM para LDAP seguro (LDAP)

## Contenido

Introducción Prerequisites Requirements Componentes Utilizados Antecedentes Verificación e instalación de certificados LDAPS 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 Iroubleshoot 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: <u>Software Advisory: Secure LDAP Obligatorio para Conexiones de Active Directory</u>

#### 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

<u>8</u>	Ldp	_ <b>D</b> X
Connection Browse	View Options Utilities Help Connect  View View Options Utilities Help Connect	
Baadu	rt: Connectioniess ✓ SSL OK Cancel	
Ready		NUM

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

Maps://WIN-H	12Q74S1U39P .com/DC=net	
Connection Brows	e View Options Utilities Help	
4	LDAP_OPT_PROTOCOL_VERSION, 3); Error 0 = Idap_connect(hLdap, NULL); Error 0 = Idap_get_option(hLdap,LDAP_OPT_SSL,(void*)&Iv); Host supports SSL, SSL cipher strength = 256 bits Established connection to WIN-H2Q74S1U39P .com. Retrieving base DSA information Getting 1 entries: Dn: (RootDSE) configurationNamingContext: CN=Configuration,DC= ,DC=com; currentTime: 4/2/2020 10:40:55 AM Central Daylight Time; defaultNamingContext: DC= DC=com; dnsHostName: WIN-H2Q74S1U39P com; domainControllerFunctionality: 6 = (WIN2012R_2); domainFunctionality: 6 = (WIN2012R2); dsServiceName: CN=NTDS Settings,CN=WIN- H2Q74S1U39P,CN=Servers,CN=Default-First-Site- Name,CN=Sites,CN=Configuration,DC= ,DC=co m; forestFunctionality: 6 = (WIN2012R2); highestCommittedUSN: 500892; isGlobalCatalogReady: TRUE; inStructorenamed: TDUE:	< III >
Ready	NUM	at

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:

gcs://WIN-H2Q	74S1U39P .com/DC=netw ×
Connection Browse	View Options Utilities Help
	Id = Idap_sslinit("WIN-H2Q74S1U39P .com", 636, 1); Error 0 = Idap_set_option(hLdap, LDAP_OPT_PROTOCOL_VERSION, 3); Error 0 = Idap_get_option(hLdap,LDAP_OPT_SSL,(void*)&Iv); Host supports SSL, SSL cipher strength = 256 bits Established connection to WIN-H2Q74S1U39P .com. Retrieving base DSA information Getting 1 entries: Dn: (RootDSE) configurationNamingContext: CN=Configuration,DC=network218,DC=com; currentTime: 4/2/2020 10:40:55 AM Central Daylight Time; defaultNamingContext: DC=network218,DC=com; dnsHostName: WIN-H2Q74S1U39P .com; domainControllerFunctionality: 6 = (WIN2012R2 ); domainFunctionality: 6 = (WIN2012R2 ); domainFunctionality: 6 = (WIN2012R2 ); dsServiceName: CN=NTDS Settings,CN=WIN- H2Q74S1U39P,CN=Servers,CN=Default-First-Site- Name,CN=Sites,CN=Configuration,DC= ,DC=co m; forestFunctionality: 6 = (WIN2012R2 ); highestCommittedUSN: 500892
Ready	NUM

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:

🔜   🔄 📘 🖛   cert							-	
File       Home       Share       View         ←       →       ↑       ►       LDAPS > cert       ✓       ♥       Sec		~ 🔞						
← → ~ ↑ 📑 > LC	DAPS > cert					5 v	P	Search c
A Quick access	Name	^		Date modified	Туре	Size		
P Deservents	<b></b>	CERTCA2012-CA.cer		3/27/2020 8:57 AM	Security Certificate		2 KB	
Documents 🛒 —	<b>E</b>	NIN-H2Q7451U39P-CA.	.com.cer	3/27/2020 8:55 AM	Security Certificate		2 KB	
Downloads 🖈	🔄 WIN-H2Q	74S1U39P .com.cer		3/27/2020 8:56 AM	Security Certificate		3 KB	
Pictures *	🖏 WIN-H2Q	74S1U39P .com.cer		3/27/2020 8:56 AM	Security Certificate		3 KB	

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):

🙆 Upload Certificate/Certif	ricate chain - Mozilla Firefox			×			- 0 X
🔽 🔬 https://10.201.	218.163/cmplatform/certi	ficateUpload.do	•••	=	⊠ ☆	III\ 🗉 🖬	. ≡
Upload Certificate/Cer	tificate chain			.ogin 🚦 Sig	n in to your account	Current 🛅 Tra	aining ≫
Upload Close				Navigation admir	Cisco Unified OS Adm Search Documer	inistration ntation About	✓ Go Logout
Status Warning: Uploading Upload Certificate/Ce Certificate Purpose* Description(friendly nam Upload File	a cluster-wide certificate w <b>:rtificate chain</b> tomcat-trust ne) Browse No file s	ill distribute it to all servers in this clu v	uster				
Upload Close	<ul> <li>ie Upload</li> <li>→ &lt; ↑ </li> <li>→ This</li> <li>Organize </li> <li>New folder</li> </ul>	PC > Desktop > LDAPS > cert			~	ۍ رم	arch cert
	Desktop ^	Name	Dat	e modified	Туре	Size	
<	LDAPS	-CERTCA2012-CA.cer	3/21	7/2020 8:57 AM 7/2020 8:55 AM	Security Certificate Security Certificate	2 KB 2 KB	
	Cisco	WIN-H2Q74S1U39P	om.cer 3/2	7/2020 8:56 AM	Security Certificate	3 KB	

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

🙆 Upload (	Certificate/Certific	ate chain -	Mozilla Firefox							- a ×		
🛈 🔒 h	nttps://10.201.2	18.163/cm	nplatform/certifi	icateUpload.do		=			☆ III (			
Upload Ce	ertificate/Certi	ficate ch	ain				^ .ogin 🚦 Sign in to	your accoun	t 🗎 Curren	t 🗎 Tra	aining >>	
Upload	Close					Navigation Cisco admin S	Unified OS / Search Docu	Administratio	n About	✓ Go t Logout		
i Succ Rest	cess: Certificate	Uploaded	sPC > Desition	Is service restart Cisco Tomo	at".			7.	) Search ce	+	×	
Certific	Organize 🔻	New folde	r									
Descrip Upload	Desktop	^	Name	-CERTCA2012-CA.cer	Date modif	ied 3:57 AM	Type Security Certificate	Size 2	KB			
Unlos	TODO		<b></b>	WIN-H2Q74S1U39P-CA.net	3/27/2020	3:55 AM	Security Certificate	2	КВ			
Upida	📥 Cisco		🔄 WIN-H2Q7	4\$1U39P .com.cer	3/27/2020	3:56 AM	Security Certificate	3	KB			

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:

```
PuTTY 10.201.218.163 - PuTTY
                                                                           X
  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
Mware 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
o not press Ctrl+C while the service is restarting. If the service has not rest
rted properly, execute the same command again.
Service Manager is running
isco Tomcat[STOPPING]
isco Tomcat[STOPPING]
isco Tomcat[STOPPING]
isco Tomcat[STOPPING]
isco Tomcat[STARTING]
isco Tomcat[STARTING]
isco Tomcat[STARTED]
dmin:
```

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):

abab	Cisco Unified Serviceability	Navigation Cisco Unified Serviceability					
cisco	For Cisco Unified Communications Solutions				admin About	Logout	
Alarm -	Irace 🕶 Tools 👻 Snmp 👻 CallHome 👻 Help 👻						
Control Ce	nter - Feature Services			Related Links:	Service Activation 🗸	Go	
Start	🛑 Stop  har Restart 🔇 Refresh Page						
Status:							
() Ready							
	**						
Select S	erver						
Server*	cucmpub218comCUCM Voice/Video v	0					
Performa	nce and Monitoring Services						
	Service Name	Status:	Activation Status	Start Time	Up Time		
0	Cisco Serviceability Reporter	Started	Activated	Fri Nov 8 09:30:34 2019	146 days 00:27:49		
0	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		
۲	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:

Cisco Unified CM Administration For Cisco Unified Communications Solutions	Navigation Cisco Unified CM Administration V Go admin Search Documentation About Logou
System V Call Routing V Media Resources V Advanced Features V Device V Application V User Management V Bulk Administration V Help V	
LDAP Directory	Related Links: Back to LDAP Directory Find/List 🧹 Go
🔚 Save 💥 Delete 🗈 Copy 贅 Perform Full Sync Now 🖓 Add New	
Group Information         User Rank*         1-Default User Rank         Access Control Groups         Add to Access Control Group         Remove from Access Control Group         Remove from Access Control Group         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         Assign new line from the pool list if one was not created based on a synced LDAP telephone number         Order       DN Pool End         Add DN Pool	
- LDAP Server Information	
WIN-H2Q74S1U39P	
Add Another Redundant LDAP Server	



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 Idap 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:

			_
Cisco Unified	CM Administration	Nevigeton Osco Unifed CM Administration V	0
For Cisco Unified Cor	nmunications Solutions	admin Search Documentation About Log	
System + Call Routing + Media Reso	arces * Advanced Features * Device * Application * User Mana	gement ▼ Duk Administration ▼ Heb ▼	
LDAP Directory		Related Links: Eack to LDAP Directory Find/List 🗤 📭	0
😡 Save 🗶 Delete 🗋 Copy i	Perform Full Sync Now 👍 Add New		
Status			1
Dudate successful, Perform a s	unchronization operation (manual or scheduled) to synchronize chr	anoes with the directory.	11
•	,		11
- LDAP Directory Information			4
1040 Conference Same	(		11
LOW Computation Name	LDAP-218		11
LDAP Manager Distinguished Name*	Administrator@ com		18
LDAP Password*			11
Confirm Password*			U.
LDAP User Search Base*	cn+users,dc+i dc+com		11
LDAP Custom Filter for Users	< None > v		11
Synchronize*	Users Only     Users and Groups		Ш
LDAP Custom Filter for Groups	< None > v		11
			10

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

cisco	For Cisco Un	ified CM Admini	stration olutions					Navigation <mark>Cisco L</mark> admin S	Unified CM Administration learch Documentation	→ G0 About Logout		
System •	Call Routing 🔻	lledia Resources 👻 Advance	d Features 👻 Device		User Management 🔻	Bulk Administration 👻	Help 🔻					
Find and	l List Users											
🕂 Add	Add New 🌐 Select All 🔛 Clear All 💥 Delete Selected											
Status 3 r	Status											
User	(1 - 3 of 3)								Rows p	per Page 50 🔍		
Find Use	r where First nam	e v begi	ns with 🧹		Find Clear Fil	ter 🕂 🛥						
	User ID *	Meeting Number	First Name	Last Name	Department	Director	y URI	User Statu:	5	User Rank		
	<u>ostacy</u>	2183	Gwen	Stacy		gstacy@ .c	com	Active Enabled LDAP Synchronized	d User	1		
	hosborn	2182	Harry	Osborn		hosborn@	.com	Active Enabled LDAP Synchronized	d User	1		
	pparker	2181	Peter	Parker		pparker@:	.com	Active Enabled LDAP Synchronized	d 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 comuser para la versión 12.0.1 de CUCM es similar a lo siguiente:

Cisco Se	Unified Communicates Of Care Porta	tions al
	Username	
	Password	
	Sign In	

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:

ababa	Cisco Un	ified Cl	M Ad	ministra	tion										Navigation	Cis	co Unifie	d CM Adr	ministrati	on	✓ Go
cisco	For Cisco Un	ified Comm	nunicat	ions Solutio	ns										adm	in	Search	Docume	entation	About	Logout
System -	Call Routing 👻 🛛	ledia Resourc	ces 🕶 🔺	dvanced Featu	res 🔻	Device 👻	Application -	User	Management 👻	Bulk Administ	ation 🔻	Help 🔻									
LDAP Aut	hentication																				
Save																					
Status -																					
0																					
Upda	te successful																				
			-																		
LDAP AU	inentication for	r End Users	s																		
Use LC	DAP Authenticatio	in for End U	sers																		
LDAP Man	ager Distinguishe	ed Name* 🖌	Administ	rator@		m															
LDAP Pase	sword*	•	•••••		•••••		•••••														
Confirm P	assword*	•																			
LDAP Use	r Search Base*	•	cn=users	,dc=	dc=	com															
LDAP Set	rver Informatio	on																			
		Host	Name o	TD Address	for Serv	*				ort* Ure TIS											
WIN-H2	0746111205	HOST	manne o	TIP Audress	or serv	er			2260												
WIN-H2	Q7451039P	.com							3269												
Add Ar	nother Redundan	t LDAP Serv	/er																		
<u> </u>													_	 		_					



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:

Inductor Cisco Unified CM Administration	Navigation Cisco Unified CM Administration V Go
CISCO For Cisco Unified Communications Solutions	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	
r Status	
Update successful	
r UC Service Information	
UC Service Type: Directory	
Product Type* Directory	
Name* Secure Directory	
Description	
Host Name/IP Address* wtw.whotaetuizee com	
Port See	
Save Delete Copy Reset Apply Config Add New	
(i) *- 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: <u>Cómo exportar un certificado TLS desde una captura de paquetes de CUCM</u>

#### 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: <u>Directorio LDAP seguro y Vídeo del tutorial de autenticación</u>
- 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).