Configuration de CUCM pour LDAP sécurisé (LDAPS)

Table des matières

Introduction Conditions préalables Exigences Composants utilisés Informations générales Vérification et installation des certificats LDAPS Configurer l'annuaire LDAP sécurisé Configurer l'authentification LDAP sécurisée Configurer des connexions sécurisées à Active Directory pour les services de communications unifiées Vérifier Dépannage Informations connexes

Introduction

Ce document décrit la procédure de mise à jour des connexions CUCM à AD à partir d'une connexion LDAP non sécurisée vers une connexion LDAP sécurisée.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- · Serveur AD LDAP
- Configuration LDAP CUCM
- · CUCM IM & Presence Service (IM/P)

Composants utilisés

Les informations contenues dans ce document sont basées sur CUCM version 9.x et ultérieure.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Il est de la responsabilité de l'administrateur Active Directory (AD) de configurer le protocole LDAP (Lightweight Directory Access Protocol) AD pour le protocole LDAPS (Lightweight Directory Access Protocol) . Cela inclut l'installation de certificats signés par une autorité de certification qui répondent aux exigences d'un certificat LDAPS.



Remarque : consultez ce lien pour obtenir des informations afin de mettre à jour les connexions LDAP non sécurisées vers les connexions LDAP sécurisées vers AD pour d'autres applications de collaboration Cisco : <u>Software Advisory : Secure LDAP</u> <u>Mandatory for Active Directory Connections</u>

Vérification et installation des certificats LDAPS

Étape 1. Une fois que le certificat LDAPS a été téléchargé sur le serveur AD, vérifiez que LDAPS est activé sur le serveur AD avec l'outil ldp.exe.

- 1. Démarrez l'outil d'administration AD (Ldp.exe) sur le serveur AD.
- 2. Dans le menu Connection, sélectionnez Connect.
- 3. Saisissez le nom de domaine complet (FQDN) du serveur LDAP en tant que serveur.
- 4. Entrez 636 comme numéro de port.
- 5. Cliquez sur OK, comme illustré dans l'image

Connection Browse View Options Utilities Help	<u>*</u>	Ldp	_ _ ×
Port: SSL OK Cancel	Connection Browse	View Options Utilities Help Connect ver: WIN-H2Q74S1U39P .com	
Paadu	Po	rt: Gonectionless SSL OK Cancel	NUM

Pour une connexion réussie sur le port 636, les informations RootDSE s'impriment dans le volet droit, comme illustré dans l'image :

M Idaps://WIN-H2	2Q74S1U39P .com/DC=net ×	¢
Connection Browse	View Options Utilities Help	
	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_L); 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; isSupplycenterized: TDUE-	< 111
Ready	NUM	

Répétez la procédure pour le port 3269, comme indiqué dans l'image :



Pour une connexion réussie sur le port 3269, les informations RootDSE s'impriment dans le volet droit, comme illustré dans l'image :

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_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=network218,DC=com; currentTime: 4/2/2020 10:40:55 AM Central Daylight Time; defaultNamingContext: DC=network218,DC=com; domainControllerFunctionality: 6 = (WIN2012R2); domainFunctionality: 6 = (WIN2012R2); domainFunctionality: 6 = (WIN2012R2); Mame,CN=Sites,CN=Configuration,DC= mame,CN=Sites,CN=Configuration,DC= min forestFunctionality: 6 = (WIN2012R2); highestCommittedUSN: 500892'
Ready	NUM

Étape 2. Procurez-vous le certificat racine et tout certificat intermédiaire faisant partie du certificat du serveur LDAPS et installez-les en tant que certificats de confiance de chat sur chacun des noeuds CUCM et de l'éditeur IM/P et en tant que CallManager-trust sur l'éditeur CUCM.

Les certificats racine et intermédiaires qui font partie d'un certificat de serveur LDAP, <hostname>.<Domain>.cer, sont indiqués dans l'image :

🔜 🛃 📘 🖛 cert						-	
File Home Share	View						~ 📀
← → * ↑ □ > LD	APS > cert					v Ö 🗸	Search c
A Quick access	Name	^		Date modified	Туре	Size	
Decumente d		CERTCA2012-CA.cer		3/27/2020 8:57 AM	Security Certificate	2 KB	
Documents x	E.	WIN-H2Q7451U39P-CA	.com.cer	3/27/2020 8:55 AM	Security Certificate	2 KB	
Uownloads 🖈	WIN-H2Q	74S1U39P .com.cer		3/27/2020 8:56 AM	Security Certificate	3 KB	
E Pictures 🖈							

Accédez à CUCM publisher Cisco Unified OS Administration > Security > Certificate Management. Téléchargez la racine comme tomcat-trust (comme illustré dans l'image) et comme CallManagertrust (non illustré) :

(a) Upload Certificate/Certifi	ficate chain - Mozilla Firefox	_					- 0 X
🔽 🔬 https://10.201.	.218.163/cmplatform/certi	ficateUpload.do	=		⊠ ☆	III\ 🗊 💀	
Upload Certificate/Cer	rtificate chain			.ogin 📒 Sign	in to your account	Current 🗎 Tr	aining ≫
Upload 🖳 Close				Navigation G	isco Unified OS Adm Search Documer	inistration ntation About	✓ Go t Logout
Status Warning: Uploading Upload Certificate/Ce Certificate Purpose* Description(friendly nam Upload File	a cluster-wide certificate w ertificate chain tomcat-trust Browse No file so File Upload	ill distribute it to all servers in this cluster	r				
(i) *- indicates requi	\leftarrow \rightarrow \checkmark \uparrow \square \Rightarrow This	PC > Desktop > LDAPS > cert			~	ی ک Se	arch cert
	Organize 👻 New folder	t					8== •
	Desktop ^	Name	Date mo	dified	Туре	Size	
<	LDAPS	-CERTCA2012-CA.cer	3/27/202	0 8:57 AM	Security Certificate	2 KB	
	TODO	WnN-H2Q74S1U39P-CA.n	et 3/27/202	0 8:55 AM	Security Certificate	2 KB	
	Cisco	WIN-H2Q74S1U39P .com.c	er 3/27/202	0 8:56 AM	Security Certificate	3 KB	

Téléchargez l'intermédiaire comme tomcat-trust (comme illustré dans l'image) et comme CallManager-trust (non illustré) :

🙆 Upload	Certificate/Certific	ate chain -	Mozilla Firefox		_					-	-	ø ×
🔂 h	https://10.201.2	18.163/cr	nplatform/certif	icateUpload.do		=		(פרב I	I\ 🗊		
Upload Ce	ertificate/Certi	ificate ch	ain				^ .ogin 🚦 Sign in to	your ac	count 🗎 C	Current 🗎] Trainin	g »
Upload	Close						Navigation Cisco admin S	Unified Search I	OS Adminis Documentat	tration	bout	Go Logout
i Succ Rest i Rest	cess: Certificate	Uploaded t Service u	sing the CLI "uti s PC → Desktop	Is service restart Cisco To	mcat".			Ū.	D Sear	ch cert		×
- Upload Certific	Organize 🔻	New folde	r					Ţ				0
Descrip Upload	Desktop	^	Name	-CERTCA2012-CA.cer	Date modi 3/27/2020	fied 8:57 AM	Type Security Certificate	Size	2 KB			
Linka	TODO			WIN-H2Q74S1U39P-CA.ne	t 3/27/2020	8:55 AM	Security Certificate		2 KB			
opida	📥 Cisco		🔄 WIN-H2Q7	4\$1U39P .com.co	er 3/27/2020	8:56 AM	Security Certificate		3 KB			

Remarque : si des serveurs IM/P font partie du cluster CUCM, vous devez également télécharger ces certificats vers ces serveurs IM/P.

Remarque : vous pouvez également installer le certificat du serveur LDAPS en tant que tomcat-trust.

Étape 3. Redémarrez Cisco Tomcat à partir de l'interface de ligne de commande de chaque noeud (CUCM et IM/P) dans les clusters. En outre, pour le cluster CUCM, vérifiez que le service Cisco DirSync sur le noeud éditeur est démarré.

Pour redémarrer le service Tomcat, vous devez ouvrir une session CLI pour chaque noeud et exécuter la commande utils service restart Cisco Tomcat, comme indiqué dans l'image :

```
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:
```

Étape 4. Accédez à CUCM publisher Cisco Unified Serviceability > Tools > Control Center -Feature Services, vérifiez que le service Cisco DirSync est activé et démarré (comme illustré dans l'image), et redémarrez le service Cisco CTIManager sur chaque noeud si ce dernier est utilisé (non illustré) :

abab	Cisco Unified Serviceability			Navigation C	isco Unified Serviceability	√ Go
cisco	For Cisco Unified Communications Solutions				admin About	Logout
Alarm 👻	Trace - Tools - Snmp - CallHome - Help -					
Control Ce	enter - Feature Services			Related Links:	Service Activation	√ Go
Star	t 🛑 Stop har Restart 🔇 Refresh Page					
Status:						
(Read)						
	-9					
-Select S	erver					
Server*	cucmpub218comCUCM Voice/Video V Go	1				
Perform	ance 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	
Director	y 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	

Configurer l'annuaire LDAP sécurisé

Étape 1. Configurez l'annuaire LDAP CUCM afin d'utiliser la connexion TLS LDAP à AD sur le port 636.

Accédez à CUCM Administration > System > LDAP Directory. Tapez le nom de domaine complet ou l'adresse IP du serveur LDAP pour obtenir des informations sur le serveur LDAP. Spécifiez le port LDAPS 636 et cochez la case Use TLS, comme indiqué dans l'image :

Cisco Unified CM Administration For Cisco Unified Communications Solutions	Navigation Cisco Unified CM Administration V G admin Search Documentation About Logo
System 🔻 Call Routing 👻 Media Resources 👻 Advanced Features 👻 Device 👻 Application 👻 User Management 👻 Bulk Administration 👻 Help 👻	
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* I-Default User Rank Access Control Group Feature Group Template < None > Warning: If no template is selected, the new line features below will not be active. 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 Start DN Pool End	
LDAP Server Information Kost Name or IP Address for Server* LDAP Port* Use TLS	
Add Another Redundant LDAP Server	



Remarque : par défaut, après vérification du nom de domaine complet (FQDN) des versions 10.5(2)SU2 et 9.1(2)SU3 configurées dans les informations du serveur LDAP par rapport au nom commun du certificat, dans le cas où l'adresse IP est utilisée à la place du nom de domaine complet (FQDN), la commande utils ldap config ipaddr est émise pour arrêter l'application du nom de domaine complet (FQDN) à la vérification CN.

Étape 2. Afin de terminer la modification de configuration en LDAPS, cliquez sur Perform Full Sync Now, comme indiqué dans l'image :

cisco Unified CM Administration For Cisco Unified Communications Solutions	Nevigation Cisco Unified CH Administration v Go admin Search Documentation About Logout						
System * Call Routing * Media Resources * Advanced Features * Device * Application * User Man	apenent + Buik Administration + Kelp +						
LDAP Directory	Related Links: Back to LDAP Directory FindList 🗸 Go						
😡 Save 🗶 Delete 🗈 Copy 👌 Perform Full Sync Now 👍 Add New							
Ratus							
LDAP Conformation Name* LDAP Anager Distinguished Name* LDAP Search Sard* LDAP User Search Sard* LDAP User Search Sard* LDAP User Search Sard* LDAP Custom Filter for User							

Étape 3. Accédez à CUCM Administration > User Management > End User et vérifiez que les utilisateurs finaux sont présents, comme illustré dans l'image :

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	User (1 - 3 of 3) Rows per Page 50 🗸									
Find Use	Find User where First name 🗸 begins with 🤟 Find Clear Filter 🖶 🛥									
	User ID *	Meeting Number	First Name	Last Name	Department	Directory	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

Étape 4. Accédez à la page ccmuser (https://<ip address of cucm pub>/ccmuser) afin de vérifier que la connexion de l'utilisateur a réussi.

La page ccmuser pour CUCM version 12.0.1 ressemble à ceci :

Cisco Se	Unified Communicated Communicated Communicated Contract C	ations t <mark>al</mark>
	Username	
	Password	
	Sign In	

L'utilisateur peut se connecter une fois les informations d'identification LDAP saisies, comme indiqué dans l'image :



Configurer l'authentification LDAP sécurisée

Configurez l'authentification LDAP CUCM afin d'utiliser la connexion TLS LDAP à AD sur le port 3269.

Accédez à CUCM Administration > System > LDAP Authentication. Tapez le nom de domaine complet du serveur LDAP pour obtenir des informations sur le serveur LDAP. Spécifiez le port LDAPS 3269 et cochez la case Use TLS, comme indiqué dans l'image :

							_
diada Cisco Unified C	M Administration			Naviga	tion Cisco Unified CM Administr	ation	✓ G0
For Cisco Unified Com	munications Solutions			ć	dmin Search Documentatio	n About	Logout
System - Call Routing - Media Resour	rces 👻 Advanced Features 👻 Device 👻 Application 👻 User Mar	agement 👻 Bulk Administration 👻	Help 👻				
LDAP Authentication							
Save							
_ Status							
(i) Update successful							
LDAP Authentication for End Use	75						
Vilce I DAR Authentication for End I	lears						
LDAP Manager Distinguished Name*	Administrator®	1					
LDAP Password*		1					
Confirm Password*]					
LDAP User Search Base*	cn=users,dc= dc=com]					
L DAP Server Information							
Hor	t Name or IP Address for Server*	LDAP Port* Use TLS					
WIN-H2Q74S1U39P .com	WIN-H2074S1U39P .com						
Add Another Redundant LDAP Ser	ver						



Remarque : si vous avez des clients Jabber, il est recommandé d'utiliser le port 3269 pour l'authentification LDAPS, car le délai d'attente Jabber pour la connexion peut se produire si aucune connexion sécurisée au serveur de catalogue global n'est spécifiée.

Configurer des connexions sécurisées à Active Directory pour les services de communications unifiées

Si vous avez besoin de sécuriser des services de communications unifiées qui utilisent LDAP, configurez ces services de communications unifiées pour utiliser le port 636 ou 3269 avec TLS.

Accédez à CUCM administration > User Management > User Settings > UC Service. Recherchez le service d'annuaire qui pointe vers AD. Saisissez le nom de domaine complet (FQDN) du serveur LDAP comme nom d'hôte/adresse IP. Spécifiez le port 636 ou 3269 et le protocole TLS, comme indiqué dans l'image :

alulu Cisco Unified CM Administration	Navigation Cisco Unified CM Administration 🗸 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	
(i) Update successful	
UC Service Information	
UC Service Type: Directory	
Product Type* Directory ~	
Name* Secure Directory	
Description	
Host Name/IP Address* wtw.w202491128P	
Bad and a set and a set	
636	
Protocol TLS	
Save Delete Copy Reset Apply Config Add New	
(i) *. indicates required item	



Remarque : les ordinateurs clients Jabber doivent également disposer des certificats LDAPS de confiance tomcat qui ont été installés sur CUCM dans le magasin de confiance de gestion des certificats de l'ordinateur client Jabber afin de permettre au client Jabber d'établir une connexion LDAPS à AD.

Vérifier

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Afin de vérifier la chaîne de certificats LDAPS réelle envoyée du serveur LDAP à CUCM pour la connexion TLS, exportez le certificat LDAPS TLS à partir d'une capture de paquets CUCM. Ce lien fournit des informations sur la façon d'exporter un certificat TLS à partir d'une capture de paquets CUCM : <u>Comment exporter un certificat TLS à partir de la capture de paquets CUCM</u>

Dépannage

Il n'y a actuellement aucune information spécifique disponible pour dépanner cette configuration.

Informations connexes

- Ce lien permet d'accéder à une vidéo présentant les configurations LDAP : <u>Vidéo de</u> <u>présentation de l'annuaire LDAP sécurisé et de l'authentification</u>
- <u>Assistance et documentation techniques Cisco Systems</u>

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.