CUCM configureren voor beveiligde LDAP (LDAPS)

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Achtergrondinformatie LDAPS-certificaten controleren en installeren Secure LDAP-map configureren Secure LDAP-verificatie configureren Beveiligde verbindingen met AD configureren voor UCS-services Verifiëren Problemen oplossen Gerelateerde informatie

Inleiding

In dit document wordt de procedure beschreven om CUCM-verbindingen naar AD van een nietbeveiligde LDAP-verbinding naar een beveiligde LDAPS-verbinding bij te werken.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- · AD LDAP-server
- · CUCM LDAP-configuratie
- · CUCM IM & Presence Service (IM/P)

Gebruikte componenten

De informatie in dit document is gebaseerd op CUCM release 9.x en hoger.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Het is de verantwoordelijkheid van de beheerder van Active Directory (AD) om AD Lichtgewicht Directory Access Protocol (LDAP) te configureren voor Lichtgewicht Directory Access Protocol (LDAPS). Dit omvat de installatie van CA-ondertekende certificaten die voldoen aan de eis van een LDAPS-certificaat.



Opmerking: Raadpleeg deze link voor informatie over het bijwerken van niet-beveiligde LDAP om LDAPS-verbindingen naar AD te beveiligen voor andere Cisco Collaboration Application: <u>Software Advisory: Secure LDAP verplicht voor Active Directory Connections</u>

LDAPS-certificaten controleren en installeren

Stap 1. Nadat het LDAPS-certificaat naar de AD-server is geüpload, controleert u of LDAPS op de AD-server is ingeschakeld met de tool ldp.exe.

- 1. Start het AD-beheerprogramma (Ldp.exe) op de AD-server.
- 2. Selecteer in het menu Verbinding de optie Verbinden.
- 3. Voer de volledig gekwalificeerde domeinnaam (FQDN) van de LDAPS-server in als server.
- 4. Voer 636 in als poortnummer.
- 5. Klik op OK zoals in de afbeelding.

*	Ldp	_ 🗆 X
Connection Brows	Ldp e View Options Utilities Help Connect Server: WIN-H2Q74S1U39P .com Port: €55 Connectionless € SSL OK Cancel	
Ready		NUM

Voor een succesvolle verbinding op poort 636 wordt RootDSE-informatie in het rechter deelvenster afgedrukt, zoals in de afbeelding:

Maps://WIN-H2	.com/DC=net · ·	5
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; isSupplycented to the state of the state	< III >
Ready	NUM	ai

Herhaal de procedure voor poort 3269, zoals in de afbeelding:



Voor een succesvolle verbinding op poort 3269, wordt de RootDSE-informatie in het rechterdeelvenster afgedrukt, zoals in de afbeelding:

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= m; forestFunctionality: 6 = (WIN2012R2); highestCommittedUSN: 500892'
Ready	NUM

Stap 2. Verkrijg de wortel en om het even welke middencertificaten die deel van het LDAPS servercertificaat uitmaken en installeer deze als tomcat-trust certificaten op elk van de de uitgeversknooppunten van CUCM en IM/P en als CallManager-vertrouwen op de uitgever van CUCM.

De basiscertificaten en tussentijdse certificaten die deel uitmaken van een LDAPSservercertificaat, <hostname>.<Domain>.cer, worden in de afbeelding weergegeven:

File Home	Share	View					_	
← → ~ ↑ 🚺	> LD	APS → cert					5 V	
1 O ith annu	^	Name	^		Date modified	Туре	Size	
Quick access			CERTCA2012-CA.cer		3/27/2020 8:57 AM	Security Certificate	2 KB	
Documents	*		NIN-H2Q7451U39P-CA	.com.cer	3/27/2020 8:55 AM	Security Certificate	2 KB	
Downloads	1	WIN-H2Q	74S1U39P .com.cer		3/27/2020 8:56 AM	Security Certificate	3 KB	
E Pictures	1							
cert								

Navigeer naar CUCM-uitgever Cisco Unified OS-beheer > Beveiliging > Certificaatbeheer. Upload root als tomcat-trust (zoals in de afbeelding) en als CallManager-trust (niet getoond):

🙆 Upload Certificate/Certif	ricate chain - Mozilla Firefox	- 0) ×				- 0 X
🔽 🔬 https://10.201.	218.163/cmplatform/certi	ficateUpload.do	≡		⊠ ☆	III\ 🗊 🖬	. ≡
Upload Certificate/Cer	tificate chain			.ogin 🚦 Sign	in to your account	Current 📄 Tra	aining ≫
Upload Close				Navigation G	Cisco Unified OS Adm	inistration ntation About	✓ Go Logout
Status Warning: Uploading Upload Certificate/Cee Certificate Purpose* Description(friendly nam Upload File	a cluster-wide certificate w rtificate chain tomcat-trust Browse No file se	ill distribute it to all servers in this cluster					
(i) *- indicates requi	\leftarrow \rightarrow \checkmark \uparrow \square \rightarrow This	PC > Desktop > LDAPS > cert			~	ر ک Sea	arch cert
	Organize 👻 New folder						-
	Desktop ^	Name	Date mo	dified	Туре	Size	
<	LDAPS	-CERTCA2012-CA.cer	3/27/202	0 8:57 AM	Security Certificate	2 KB	
	TODO	-WhN-H2Q74S1U39P-CA.net	3/27/202	0 8:55 AM	Security Certificate	2 KB	
	Cisco	WIN-H2Q74S1U39P .com.cer	3/27/202	0 8:56 AM	Security Certificate	3 KB	

Tussenpersoon uploaden als tomcat-trust (zoals in de afbeelding) en als CallManager-trust (niet weergegeven):

🔞 Upload Cert	ificate/Certifica	te chain -	Mozilla Firefox		-					-	- 0	a x
🛛 🔒 http:	s://10.201.21	8.163/cn	nplatform/certifi	cateUpload.do		=		©	Ø ☆ III			Ξ
Upload Certif	ficate/Certif	icate ch	ain				^ .ogin 🚦 Sign in to	your acc	ount 🗎 Cu	urrent 🗎	Training	>>
Upload [Close						Navigation Cisco admin S	Unified (Search D	OS Administ ocumentatio	ration on Ab	v out l	G0 Logout
i Success Restart (i If the	: Certificate U Cisco Tomcat : File Upload	ploaded Service u	sing the CLI "util sPC → Desktop	s service restart Cisco Tomo	cat".			Č)	Q Searc	h cert	_	×
Certific Or	ganize 👻 I	New folde	r					Ū	,	8:: •		0
Descrip Upload	Desktop	^	Name	-CERTCA2012-CA.cer	Date modi 3/27/2020	fied 8:57 AM	Type Security Certificate	Size	2 KB			
Uploa Cisco	TODO			WIN-H2Q74S1U39P-CA.net	3/27/2020	8:55 AM	Security Certificate		2 KB			
	Cisco		🔄 WIN-H2Q7	4S1U39P .com.cer	3/27/2020	8:56 AM	Security Certificate		3 KB			

Opmerking: als u IM/P-servers hebt die deel uitmaken van het CUCM-cluster, moet u deze certificaten ook uploaden naar deze IM/P-servers.

Opmerking: Als alternatief kunt u het LDAPS-servercertificaat installeren als tomcat-trust.

٩,

Stap 3. Start Cisco Tomcat opnieuw vanaf de CLI van elk knooppunt (CUCM en IM/P) in clusters. Controleer voor het CUCM-cluster bovendien dat de Cisco DirSync-service op het uitgeversknooppunt is gestart. Om de Tomcat-service te kunnen herstarten, moet u voor elke knooppunt een CLI-sessie openen en de Opnieuw opstarten van de service commando's uitvoeren op Cisco Tomcat, zoals in de afbeelding:



Stap 4. Navigeer naar de CUCM-uitgever Cisco Unified Servicability > Tools > Control Center - Feature Services, controleer of de Cisco DirSync-service is geactiveerd en gestart (zoals in de afbeelding) en start de Cisco CTIM Manager-service op elk knooppunt opnieuw als deze wordt gebruikt (niet weergegeven):

abab	Cisco Unified Serviceability			Navigation Cisco Unified Serviceability				
cisco	For Cisco Unified Communications Solutions				admin A	About Logout		
Alarm 👻	Irace ▼ Tools ▼ Snmp ▼ CallHome ▼ Help ▼							
Control Ce	enter - Feature Services			Related Links:	Service Activation	√ Go		
Star	t 🛑 Stop har Restart 🔇 Refresh Page							
Status:								
(Read)								
-Select S	erver							
Server*[cucmpub218comCUCM Voice/Video v	30						
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 00:2	27:49		
0	Cisco CallManager SNMP Service	Started	Activated	Fri Nov 8 09:30:36 2019	146 days 00:2	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	1:10		

Secure LDAP-map configureren

Stap 1. Configureer de CUCM LDAP Directory om de LDAPS TLS-verbinding met AD op poort

636 te gebruiken.

Ga naar CUCM Administration > System > LDAP Directory. Typ de FQDN of het IP-adres van de LDAPS-server voor LDAP Server-informatie. Specificeer de LDAPS-poort van 636 en controleer het vakje voor TLS gebruiken, zoals in de afbeelding:

Cisco Unified CM Administration For Cisco Unified Communications Solutions	Navigation Cisco Unified CM Administration V Go admin Search Documentation About Logou
System 👻 Call Routing 👻 Media Resources 👻 Advanced Features 👻 Device 👻 Application 👻 User Management 👻 Bulk Administration 👻 Help 💌	
DAP Directory	Related Links: Back to LDAP Directory Find/List 🤜 Go
🔚 Save 🗙 Delete 🜔 Copy 🌏 Perform Full Sync Now 👍 Add New	
Group Information User Rank* Access Control Groups Access Control Groups Add to Access Control Group Remove from Access Control Group Remove from Access Control Group 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	
Add DN Pool	
LDAP Server Information Host Name or IP Address for Server [#] LDAP Port [*] Use TLS	
WIN-H2Q74S1U39Pcom 636	
Add Another Redundant LDAP Server	



Opmerking: standaard worden de versies 10.5(2)SU2 en 9.1(2)SU3 FQDN geconfigureerd in LDAP Server Information gecontroleerd aan de algemene naam van het certificaat, als het IP-adres wordt gebruikt in plaats van de FQDN, de opdracht utils Idap config ipaddr wordt uitgegeven om de handhaving van FQDN naar CN verificatie te stoppen.

Stap 2. Klik op Full Sync Now uitvoeren om de configuratiewijziging in LDAPS te voltooien, zoals in het afbeelding wordt getoond:

Cisco Unified	CM Administration	Navigation <mark>Cisco Unifed CH Administration v admin Search Documentation About 1</mark>									
System * Cal Routing * Media Reso	arces - Advanced Features - Device - Application - User Man	agement + Bulk Administration + Help +									
LDAP Directory		Related Links: Back to LDMP Directory Find/List 🗸									
🔜 Save 🗶 Delete 🛅 Copy	Perform Full Sync Now 🖓 Add New										
Update successful. Perform a s	Status Dupdate successful. Perform a synchronization operation (manual or scheduled) to synchronize changes with the directory.										
LOAP Directory Information											
LDAP Configuration Name*	LDAP-218										
LDAP Manager Distinguished Name	Administrator@ com										
LDAP Password*											
Confirm Password*											
LDAP User Search Base*	cn+users,dc+ dc+com										
LDAP Custom Filter for Users	< None > v										
Synchronize*	Users Only O Users and Groups										
LDAP Custom Filter for Groups	< None >										

Stap 3. Ga naar CUCM-beheer > Gebruikersbeheer > Eindgebruiker en controleer of de eindgebruikers aanwezig zijn, zoals in de afbeelding wordt getoond:

cisco	Cisco Unified CM Administration Second S										
System •	Call Routing 👻 I	lledia Resources 👻 Advance	d Features 👻 Device	• • Application •	User Management 🔻	Bulk Administration 👻 Help 💌					
Find and	Find and List Users										
🕂 Add	Add New III Select All III Clear All 💥 Delete Selected										
Status 3 r	- Status i) 3 records found										
User	(1 - 3 of 3)							Rows	per Page S0 🗸		
Find Use	r where First nam	e v begi	ns with $\ arphi$		Find Clear Filt	er 🖧 🛥					
	User ID *	Meeting Number	First Name	Last Name	Department	Directory URI	User	Status	User Rank		
	<u>ostacy</u>	2183	Gwen	Stacy		gstacy@.com	Active Enabled LDAP Synchro	onized User	1		
	hosborn	2182	Harry	Osborn		hosborn@ .com	Active Enabled LDAP Synchro	onized User	1		
	pparker	2181	Peter	Parker		pparker@:	Active Enabled LDAP Synchro	onized User	1		

Stap 4. Navigeer naar de ccmuser pagina (https://<ip adres of cucm pub>/ccmuser) om te verifiëren dat de gebruiker inloggen succesvol is.

De commuser pagina voor CUCM versie 12.0.1 ziet er als volgt uit:

Cisco Se	Unified Communicated Communicated Communicated Contract C	ations tal
	Username	
	Password	
	Sign In	

De gebruiker kan met succes inloggen nadat LDAP-referenties zijn ingevoerd, zoals in de afbeelding:



Secure LDAP-verificatie configureren

Configureer CUCM LDAP-verificatie om de LDAPS TLS-verbinding met AD op poort 3269 te gebruiken.

Ga naar CUCM Administration > System > LDAP-verificatie. Typ de FQDN van de LDAPS-server voor LDAP-serverinformatie. Specificeer de LDAPS-poort van 3269 en controleer het vakje voor TLS gebruiken, zoals in de afbeelding:

abab	Cisco Unifi	ed CM A	dministra	tion							Navigation	Cisco L	Unified CM Administr	ation	√ Go
cisco	For Cisco Unifie	d Communie	cations Solutio	ns							admir	n I S	earch Documentatio	n About	Logout
System -	Call Routing 👻 Media	Resources -	Advanced Featu	res 🔻 Device 🔻	Application •	User Manage	ement 👻	Bulk Administration 🔻	Help 🔻						
LDAP Aut	hentication														
Save															
Status-										 					
(i) Upda	ate successful														
	thentication for En	d Users —													
	DAR Authentication fo	r End Lisers													
LDAP Mar	hager Distinguished N	ame* Admir	nistrator@	com											
LDAP Pas	sword*	•••••													
Confirm F	Password*														
LDAP Use	r Search Base*	cn=us	ers,dc=	dc=com											
	nuer Information-														
LUAP SE	rver information			*				·* ···							
MIN-H2	0746111205	Host Nam	e or IP Address	or server			2260	l 🖂							
WIN-H2	Q1491039h	.com					3209								
Add A	nother Redundant LD.	AP Server													



Opmerking: Als u Jabber-clients hebt, wordt aanbevolen om poort 3269 te gebruiken voor LDAPS-verificatie, omdat Jabber-time-out voor inloggen kan optreden als er geen beveiligde verbinding met de wereldwijde catalogusserver is opgegeven.

Beveiligde verbindingen met AD configureren voor UCS-services

Als u UC-services moet beveiligen die LDAP gebruiken, configureer dan deze UC-services om poort 636 of 3269 met TLS te gebruiken.

Ga naar CUCM-beheer > Gebruikersbeheer > Gebruikersinstellingen > UCS-service. Zoek Directory Service die verwijst naar AD. Typ de FQDN van de LDAPS-server als hostnaam/IPadres. Specificeer de poort als 636 of 3269 en protocol TLS, zoals in de afbeelding:

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.	



Opmerking: de Jabber-clientmachines moeten ook de Tomcat-trust LDAPS-certificaten die op CUCM zijn geïnstalleerd, hebben geïnstalleerd in de certificaatbeheertrustwinkel van de Jabber-clientmachine om de Jabber-client in staat te stellen een LDAPS-verbinding met AD tot stand te brengen.

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

Om de eigenlijke LDAPS-certificaatketen die van de LDAP-server naar CUCM is verzonden voor de TLS-verbinding te verifiëren, exporteert u het LDAPS TLS-certificaat vanuit een CUCM-pakketopname. Deze link geeft informatie over het exporteren van een TLS-certificaat vanuit een CUCM-pakketopname: <u>Hoe TLS-certificaat exporteren vanuit CUCM Packet Capture</u>

Problemen oplossen

Er is momenteel geen specifieke informatie beschikbaar om deze configuratie problemen op te lossen.

Gerelateerde informatie

- Deze link geeft toegang tot een video die door de configuraties van LDAPS loopt: <u>Secure</u> <u>LDAP Directory en Authenticatie Walkthrough Video</u>
- <u>Technische ondersteuning en documentatie Cisco Systems</u>

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.