Configurazione di CUCM per LDAP sicuro (LDAPS)

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Premesse Verifica e installazione dei certificati LDAPS Configura directory LDAP protetta Configura autenticazione LDAP sicura Configura connessioni protette ad AD per i servizi UC Verifica Risoluzione dei problemi Informazioni correlate

Introduzione

In questo documento viene descritta la procedura per aggiornare le connessioni CUCM ad AD da una connessione LDAP non protetta a una connessione LDAPS protetta.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- · Server LDAP AD
- · Configurazione LDAP CUCM
- · CUCM IM & Presence Service (IM/P)

Componenti usati

Il riferimento delle informazioni contenute in questo documento è CUCM release 9.x e successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

È responsabilità dell'amministratore di Active Directory (AD) configurare AD Lightweight Directory Access Protocol (LDAP) per Lightweight Directory Access Protocol (LDAPS). È inclusa l'installazione di certificati firmati dalla CA che soddisfano i requisiti di un certificato LDAPS.



Nota: per informazioni sull'aggiornamento da LDAP non sicuro a connessioni LDAPS sicure ad AD per altre applicazioni di collaborazione Cisco, vedere questo collegamento: <u>Software Advisory: Secure LDAP Obbligatorio per connessioni Active Directory</u>

Verifica e installazione dei certificati LDAPS

Passaggio 1. Dopo aver caricato il certificato LDAPS nel server AD, verificare che LDAPS sia abilitato nel server AD con lo strumento Idp.exe.

1. Avviare lo Strumento di amministrazione di Active Directory (Ldp.exe) nel server AD.

- 2. Scegliere Connetti dal menu Connessione.
- 3. Immettere il nome di dominio completo (FQDN) del server LDAPS come server.
- 4. Immettere 636 come numero di porta.
- 5. Fare clic su OK, come mostrato nell'immagine

A	Ldp	_ 🗆 X
Connection Browse	View Options Utilities Help	
	Connect rver: WIN-H2Q74S1U39P .com rt: Image: Connectionless Image: SSL OK Cancel	
Ready		NUM

Per una connessione riuscita sulla porta 636, le informazioni di RootDSE vengono stampate nel riquadro destro, come mostrato nell'immagine:

🕼 Idaps://WIN-H2Q74S1U39P								
Connection Browse	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,); domainFunctionality: 6 = (WIN2012R2,); dsServiceName: CN=NTDS Settings,CN=WIN- H2Q74S1U39P,CN=Servers,CN=Default-First-Site- Name,CN=Sites,CN=Configuration,DC=: ,DC=com m; forestFunctionality: 6 = (WIN2012R2,); highestCommittedUSN: 500892; isGlobalCatalogReady: TRUE; isSupptremined: TDUE:	< 111						
Ready	NUM	at						

Ripetere la procedura per la porta 3269, come mostrato nell'immagine:



Per una connessione riuscita sulla porta 3269, le informazioni di RootDSE vengono stampate nel riquadro destro, come mostrato nell'immagine:

🕼 gcs://WIN-H2Q74S1U39P .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) configuration,DC=network218,DC=com; currentTime: 4/2/2020 10:40:55 AM Central Daylight Time; defaultNamingContext: CN=Configuration,DC=network218,DC=com; com; domainControllerFunctionality: 6 = (WIN2012R2); domainFunctionality: 6 = (WIN2012R2); domainFunctionality: 6 = (WIN2012R2); Mame,CN=Sites,CN=Configuration,DC= Mame,CN=Sites,CN=Configuration,DC= ,DC=co m; forestFunctionality: 6 = (WIN2012R2); highestCommittedUSN: 500892 v							
Ready	NUM							

Passaggio 2. Ottenere il certificato radice e gli eventuali certificati intermedi che fanno parte del certificato del server LDAPS e installarli come certificati di attendibilità per gli utenti su ciascuno dei nodi di pubblicazione CUCM e IM/P e come CallManager-trust sull'autore CUCM.

I certificati radice e intermedi che fanno parte di un certificato server LDAPS, <nomehost>.<Dominio>.cer, sono mostrati nell'immagine:

🔜 🛃 📕 🖛 cert							-	
File Home Share	View							~ 📀
← → ~ ↑ 📑 > LC	APS → cert					5 v	2	Search c
A Quick access	Name	^		Date modified	Туре	Size		
P Deservents		CERTCA2012-CA.cer		3/27/2020 8:57 AM	Security Certificate		2 KB	
	E.	NIN-H2Q7451U39P-CA.	.com.cer	3/27/2020 8:55 AM	Security Certificate		2 KB	
Downloads * Pictures *	🗐 WIN-H2Q7	4S1U39P .com.cer		3/27/2020 8:56 AM	Security Certificate		3 KB	
cert								

Passare a CUCM publisher Cisco Unified OS Administration > Security > Certificate Management (Amministrazione del sistema operativo unificato Cisco > Protezione > Gestione certificati). Caricare la radice come tomcat-trust (come mostrato nell'immagine) e come CallManager-trust (non mostrato):

🙆 Upload Certificate/Certi	ficate chain - Mozilla Firefox	- (X C				- ø x
🔽 🔬 https://10.201.	.218.163/cmplatform/cert	ficateUpload.do	=		⊠ ☆	III\ 🗉 🖬	
Upload Certificate/Cer	rtificate chain			.ogin 🚦 Sign	in to your account	Current 🗎 Tra	aining ≫
Upload 🖳 Close				Navigation d admin	isco Unified OS Adm Search Documer	inistration ntation About	✓ Go Logout
Status Warning: Uploading Upload Certificate/Cer Certificate Purpose* Description(friendly nam Upload File	a cluster-wide certificate w ertificate chain tomcat-trust ne) Browse No file s	ill distribute it to all servers in this cluster					
Upload Close	File Upload $\leftarrow \rightarrow \checkmark \uparrow \square \rightarrow This$	PC > Desktop > LDAPS > cert			~	Ö 🔎 Se	arch cert
	Desktop	Name	Date mo	dified	Туре	Size	8== •
٢	LDAPS	-CERTCA2012-CA.cer	3/27/202	0 8:57 AM 0 8:55 AM	Security Certificate Security Certificate	2 KB 2 KB	
	Cisco	Com.cer	5/21/202	NA 00:5 U	security Certificate	3 KB	

Caricare la parte intermedia come tomcat-trust (come mostrato nell'immagine) e come CallManager-trust (non mostrato):

🙆 Upload	Certificate/Certific	ate chain -	Mozilla Firefox		_					-	-	ø ×
🔂 h	https://10.201.2	18.163/cr	nplatform/certif	icateUpload.do		=		(פרב ו	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			

Nota: se si dispone di server IM/IP che fanno parte del cluster CUCM, è inoltre necessario caricare questi certificati in questi server IM/IP.

Nota: in alternativa, è possibile installare il certificato del server LDAPS come tomcat-trust.

Passaggio 3. Riavviare Cisco Tomcat dalla CLI di ciascun nodo (CUCM e IM/P) nei cluster. Inoltre, per il cluster CUCM, verificare che il servizio Cisco DirSync sul nodo del server di pubblicazione sia avviato.

Per riavviare il servizio Tomcat, è necessario aprire una sessione CLI per ciascun nodo ed eseguire il comando utils service restart Cisco Tomcat, come mostrato nell'immagine:

```
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:
```

Passaggio 4. Passare a Cisco Unified Serviceability > Strumenti > Control Center - Servizi funzionalità, verificare che il servizio Cisco DirSync sia attivato e avviato (come mostrato nell'immagine), quindi riavviare il servizio Cisco CTIManager su ogni nodo, se utilizzato (non visualizzato):

abab	Cisco Unified Serviceability			Navigation C	isco Unified Serviceability	√ Go
cisco	For Cisco Unified Communications Solutions				admin About	Logout
Alarm 👻	Irace ▼ Tgols ▼ _Snmp ▼ _GallHome ▼ _Help ▼					
ontrol Ce	enter - Feature Services			Related Links:	Service Activation	√ Go
Start	t 🛑 Stop har Restart 🔇 Refresh Page					
Status:						
() Ready						
	τų.					
Select S	erver					
Server*	cucmpub218comCUCM Voice/Video v	io				
Performa	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	

Configura directory LDAP protetta

Passaggio 1. Configurare l'elenco LDAP di CUCM per utilizzare la connessione LDAPS TLS ad AD sulla porta 636.

Passare a Amministrazione CUCM > Sistema > LDAP Directory. Digitare il nome di dominio completo (FQDN) o l'indirizzo IP del server LDAPS per Informazioni server LDAP. Specificare la porta LDAPS di 636 e selezionare la casella Use TLS (Usa TLS), come mostrato nell'immagine:

System + Cal Routing + Meda Resources + Advanced Features + Device + Application + User Management + Buk Administration + Heb + LDAP Directory Related Links: Back to LDAP Directory Find/List Save Corp Perform Full Sync Now Add New Group Information User Rank* Access Control Group Feature Group Template Nank Add to Access Control Group Feature Group Template Nank 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 DI Pool Start DI Pool End LDAP Port* Use TLS USAP Total Start Server* LDAP Port* Use TLS USAP Total Server Information LDAP Podres for Server* LDAP Port* Use TLS USA Add Not Total Com Com Com Com Com Com Com Co	Cisco Unified	CM Administration		Navigation Cisco Unified CM Administration V Go admin Search Documentation About Logo
LDAP Directory Related Links: Back to LDAP Directory Find/List Save Coroup Information User Rank* Access Control Groups	System - Call Routing - Media Re	sources · Advanced Features · Device	✓ Application ▼ User Management ▼ Bulk Administration ▼ Help ▼	
Save Save Copy Save Perform Full Sync Now Add New	LDAP Directory			Related Links: Back to LDAP Directory Find/List 🗸 Go
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 >	🕞 Save 🗶 Delete 🗋 Copy	Perform Full Sync Now 👍 Add No	w	
LDAP Server Information Host Name or IP Address for Server* USe TLS WIN-H2Q74S1U39Pcom 636	Group Information User Rank* I-Defa Access Control Groups Feature Group Template < None Warning: Apply mask to synced telepho Mask Assign new line from the pool Order DN Pool Start	> It User Rank > If no template is selected, the new line for ins list if one was not created based on a s DN Pool End	Add to Access Control Group Remove from Access Control Group features below will not be active. erted users ynced LDAP telephone number	
WIN-H2Q74S1U39P	-LDAP Server Information Host Name or IP Address	for Server*	LDAP Port* Use TLS	
Add Another Redundant LDAP Server	Add Another Redund	ant LDAP Server	636 M	



Nota: per impostazione predefinita, dopo che le versioni 10.5(2)SU2 e 9.1(2)SU3 FQDN configurate in Informazioni server LDAP sono state confrontate con il nome comune del certificato, nel caso in cui venga utilizzato l'indirizzo IP anziché il nome di dominio completo (FQDN), il comando utilizza il comando Idap config ipaddr per interrompere l'applicazione del nome di dominio completo alla verifica CN.

Passaggio 2. Per completare la modifica alla configurazione di LDAPS, fare clic su Perform Full Sync Now (Esegui sincronizzazione completa ora), come mostrato nell'immagine:

Cisco Unified Con Cisco For Cisco Unified Con	CM Administration munications Solutions	Navigation Cisco Unified CH Administration admin Search Documentation Abou	↓ G0 ut Logou					
System • Call Routing • Media Resou	rces * Advanced Features * Device * Application * User Man	agement * Buik Administration * Help *						
LDAP Directory		Related Links: SJck to LDUP Directory Find/L	ist ∨ Go					
🕞 Save 🗶 Delete 🗋 Copy 🕻	Perform Full Sync Now Car Add New							
Update successful. Perform a sy	Alabas - D Update successful. Perform a synchronization operation (manual or scheduled) to synchronize changes with the directory.							
LDAP Directory Information	LCAP-218							
LDAP Manager Distinguished Name* LDAP Password*	Administrator@ com							
Confirm Password*								
LDAP User Search Base* LDAP Custom Filter for Users	<pre>cn=users,dc=: dc=com </pre>							
Synchronize* LDAP Custom Filter for Groups	Users Only O Users and Groups < None >							

Passaggio 3. Passare a Amministrazione CUCM > Gestione utente > Utente finale e verificare che gli utenti finali siano presenti, come mostrato nell'immagine:

cisco	For Cisco U	nified CM Admini	stration olutions				Navigation d admin	Cisco Unified CM Administration Search Documentation	✓ Go About Logout
System -	Call Routing 🔻	Media Resources 👻 Advance	d Features - Device	e 👻 Application 👻	User Management 🔻	Bulk Administration 👻 Help	-		
Find and	l List Users								
🕂 Add	New Select	All 🔛 Clear All 💥 Delet	te Selected						
Status 3 r	Status i) 3 records found								
User	(1 - 3 of 3)							Rows p	er Page 50 🗸
Find Use	r where First nan	ne v begi	ins with $\ arphi$		Find Clear Filt	er 🕂 🛥			
	User ID *	Meeting Number	First Name	Last Name	Department	Directory UR	I User	Status	User Rank
	gstacy	2183	Gwen	Stacy		gstacy@.com	Active Enabled LDAP Synchr	onized User	1
	hosborn	2182	Harry	Osborn		hosborn@ .con	Active Enabled LDAP Synchr	onized User	1
	pparker	2181	Peter	Parker		pparker@: .com	Active Enabled LDAP Synchr	onized User	1

Passaggio 4. Accedere alla pagina ccmuser (https://<indirizzo ip di cucm pub>/ccmuser) per verificare che l'utente abbia eseguito correttamente il login.

La pagina ccmuser per CUCM versione 12.0.1 ha il seguente aspetto:

Cisco Se	OUnified Communication Of Care Porta	ons
	Username	
	Password	
	Sign In	

L'utente può eseguire correttamente il login dopo aver immesso le credenziali LDAP, come mostrato nell'immagine:



Configura autenticazione LDAP sicura

Configurare l'autenticazione LDAP CUCM per utilizzare la connessione LDAPS TLS ad AD sulla porta 3269.

Passare a Amministrazione CUCM > Sistema > Autenticazione LDAP. Digitare il nome di dominio completo (FQDN) del server LDAPS per Informazioni server LDAP. Specificare la porta LDAPS di 3269 e selezionare la casella Use TLS (Usa TLS), come mostrato nell'immagine:

abab. Cisco Unified	CM Administration		Navigation Cisco Unified CM Administration
CISCO For Cisco Unified Co	mmunications Solutions		admin Search Documentation About Logout
System - Call Routing - Media Res	ources 👻 Advanced Features 👻 Device 👻 Application 👻 User Ma	nagement 👻 Bulk Administration 👻 Help 👻	
LDAP Authentication			
Save			
Status			
Update successful			
LDAP Authentication for End U	sers		
Use LDAP Authentication for En	d Users		
LDAP Manager Distinguished Name	* Administrator® .com		
LDAP Password*	••••••	1	
Confirm Password*			
LDAP User Search Base*	cn=users,dc= dc=com		
LDAP Server Information			
,	ost Name or IP Address for Server*	LDAP Port* Use TLS	
WIN-H2Q74S1U39P	om	3269	
Add Another Redundant LDAP 5	ierver		



Nota: se si dispone di client Jabber, si consiglia di utilizzare la porta 3269 per l'autenticazione LDAPS, in quanto il timeout di Jabber per l'accesso può verificarsi se non viene specificata una connessione protetta al server di catalogo globale.

Configura connessioni protette ad AD per i servizi UC

Se è necessario proteggere i servizi UC che utilizzano LDAP, configurare questi servizi UC in modo che utilizzino la porta 636 o 3269 con TLS.

Passare a Amministrazione CUCM > Gestione utente > Impostazioni utente > Servizio UC. Trova il servizio directory che punta ad AD. Digitare il nome di dominio completo (FQDN) del server LDAPS come Nome host/Indirizzo IP. Specificare la porta come 636 o 3269 e il protocollo TLS, come mostrato nell'immagine:

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: per consentire al client Jabber di stabilire una connessione LDAPS ad AD, i computer client Jabber devono anche avere i certificati LDAPS tomcat-trust installati su CUCM installato nell'archivio di certificati attendibili di gestione del computer client Jabber.

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Per verificare l'effettiva catena di certificati/certificati LDAPS inviata dal server LDAP a CUCM per la connessione TLS, esportare il certificato TLS LDAPS dall'acquisizione di un pacchetto CUCM. Questo collegamento fornisce informazioni su come esportare un certificato TLS da un'acquisizione pacchetti CUCM: <u>Come esportare un certificato TLS da un'acquisizione pacchetti CUCM</u>

Risoluzione dei problemi

Non sono attualmente disponibili informazioni specifiche per risolvere i problemi relativi a questa configurazione.

Informazioni correlate

- Questo collegamento fornisce l'accesso a un video che passa attraverso le configurazioni LDAPS: <u>Directory LDAP protetta e autenticazione Walkthrough Video</u>
- Documentazione e supporto tecnico Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).