## 為安全LDAP (LDAPS)配置CUCM

目錄

 簡介

 必要條件

 蓋求

 採用元件

 背景資訊

 驗證和安裝LDAPS證書

 配置Secure LDAP目錄

 配置安全LDAP身份驗證

 為UC服務配置與AD的安全連線

 驗證

 短難排解

 相關資訊

簡介

本文檔介紹從非安全LDAP連線更新到安全LDAPS連線的CUCM與AD連線的過程。

必要條件

需求

思科建議您瞭解以下主題:

·AD LDAP伺服器

· CUCM LDAP配置

·CUCM IM和線上狀態服務(IM/P)

採用元件

本文檔中的資訊基於CUCM版本9.x及更高版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

#### 背景資訊

Active Directory (AD)管理員負責為輕型目錄訪問協定(LDAPS)配置AD輕型目錄訪問協定(LDAP)。 這包括安裝符合LDAPS證書要求的CA簽名證書。



注意:如需從非安全LDAP更新以保護LDAPS連線至AD的其他思科協同合作應用程式的資 訊,請參閱此連結:<u>軟體建議:Active Directory連線必須使用Secure LDAP</u>

#### 驗證和安裝LDAPS證書

步驟 1.將LDAPS證書上傳到AD伺服器後,請使用ldp.exe工具驗證是否已在AD伺服器上啟用 LDAPS。

- 1. 在AD伺服器上啟動AD管理工具(Ldp.exe)。
- 2. 在「連線」選單上,選擇連線。
- 3. 輸入LDAPS伺服器作為伺服器的完整網域名稱(FQDN)。
- 4. 輸入636作為埠號。
- 5. 按一下OK(如圖所示)

<u>*</u>	Ldp		- 0 X
Connection Browse	View Options Utili	ties Help	
	Conn	ect 🔼	
s	erver: WIN-H2Q74S1U	39P .com	
P	ort: 635	Connectionless	
	R.	▼ 55L	
	OK	Cancel	
_			
Ready			NUM

要在埠636上成功連線,RootDSE資訊會列印在右窗格中,如圖所示:

M Idaps://WIN-I	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_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; isSuppresented: TDUE:	
Ready	NUM	

對埠3269重複該過程,如圖所示:



要在埠3269上成功連線,RootDSE資訊會列印在右窗格中,如圖所示:

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	111

步驟 2.獲取根證書和屬於LDAPS伺服器證書一部分的任何中間證書,並將這些證書作為tomcattrust證書安裝在CUCM和IM/P發佈伺服器節點上,作為CallManager-trust安裝在CUCM發佈伺服器 上。

LDAPS伺服器證書<hostname>.<Domain>.cer中的根證書和中間證書如下圖所示:

File     Home	t Share	View					-	□ × ~ (3
← → • ↑ 📙	> LDA	APS > cert					× 0 ×	Search c
10:1	^	Name	^		Date modified	Туре	Size	
Quick access		<b></b>	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	*	WIN-H2Q74	IS1U39P .com.cer		3/27/2020 8:56 AM	Security Certificate	3 KB	
cert	×							

導航到CUCM發佈伺服器思科統一作業系統管理>安全>證書管理。將根上傳為tomcat-trust (如圖 所示)和CallManager-trust (未顯示):

🙆 Upload Certificate/Certif	ficate chain - Mozilla Firefox	- 0	×				- a ×
🔽 🔬 https://10.201.	.218.163/cmplatform/cert	ificateUpload.do •	•• =		⊘ ☆	III\ 🗊 🖶	
Upload Certificate/Cer	rtificate chain			.ogin 📒 Sigr	n in to your account 📋	🗍 Current  🗎 Tra	aining >>
Upload 🖳 Close				Navigation admin	Cisco Unified OS Adm Search Documer	inistration ntation About	✓ Go Logout
Status Warning: Uploading Upload Certificate/Ce Certificate Purpose* Description(friendly nam Upload File	ertificate chain tomcat-trust Browse No file s	vill distribute it to all servers in this cluster					
indicates requi		s PC > Desktop > LDAPS > cert			~	<mark>ک</mark> کې Sea	arch cert
		Name	Data ma	diffed	Time	Cine	8== •
<		-CERTCA2012-CA.cer	3/27/202 3/27/202	0 8:57 AM	Security Certificate	2 KB	
	Cisco	WIN-H2Q74S1U39P .com.cer	3/27/202	0 8:56 AM	Security Certificate	3 KB	

將intermediate上傳為tomcat-trust (如圖所示)和CallManager-trust (未顯示):

🔕 Upload C	Certificate/Certificate	e chain -	Mozilla Firefox			_	×				-	-	0
🔂 ht	ttps://10.201.218	.163/cm	nplatform/certif	ficateUpload.do		••	• =		5	0 ☆	II\ 🗊	•	۵ =
Upload Ce	rtificate/Certific	cate cha	ain				^	ogin 🚦 Sign in to	your acc	ount 🗎	Current	🗎 Traii	ning 🔀
Upload	Close							Navigation Cisco admin S	Unified ( Search D	OS Admini ocumenta	stration tion	About	✓ Go Logou
i Succe	ess: Certificate Up art Cisco Tomcat S	loaded ervice u	sing the CLI "uti	ils service restart	Cisco Tomca	t".							
Upload		> This	PC > Desktop	> LDAPS > cert				~	õ	,⊂ Sea	rch cert		
Certific	Organize - N	ew folder	r									• [	
Descrip Upload	Desktop	^	Name	-CERTCA2012-CA.	er	Date modified 3/27/2020 8:57	AM	Type Security Certificate	Size	2 KB			
Uploa	Cisco		WIN-H2Q7	WIN-H2Q74S1U39 4S1U39P	P-CA.net	3/27/2020 8:55 3/27/2020 8:56	AM AM	Security Certificate Security Certificate		2 KB 3 KB			
		_											

✤ 注意:如果您的IM/P伺服器是CUCM集群的一部分,則還需要將這些證書上傳到這些IM/P伺服器。

✤ 注意:您也可以將LDAPS伺服器憑證安裝為tomcat-trust。

步驟 3.從集群中每個節點(CUCM和IM/P)的CLI重新啟動Cisco Tomcat。此外,對於CUCM集群 ,驗證發佈伺服器節點上的Cisco DirSync服務是否已啟動。

要重新啟動Tomcat服務,需要為每個節點打開一個CLI會話並運行utils service restart Cisco Tomcat命令,如下圖所示:

P 10.201.218.163 - PuTTY	-		$\times$
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 Do not press Ctrl+C while the service is restarting. If the service 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[STARTING] Cisco Tomcat[STARTING]	e has	not	rest
admin:			

步驟 4.導航到CUCM發佈伺服器Cisco Unified Serviceability > Tools > Control Center - Feature Services,驗證Cisco DirSync服務是否已啟用和啟動(如圖所示),如果使用了Cisco CTIManager服務(未顯示),請在每個節點上重新啟動該服務:

cisco	Cisco Unified Serviceability For Cisco Unified Communications Solutions			Navigation C	isco Unified Serviceability V Go
Alarm 🔻	Irace + Tools + Snmp + CallHome + Help +				admin About Logout
control (	Center - Feature Services			Related Links:	Service Activation V Go
Sta	rt 🛑 Stop  la Restart 🔇 Refresh Page				
Status					
Read	tv N				
	· 48				
Select	Server				
Server	cucmpub218comCUCM Voice/Video v	Go			
Perform	nance 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
Directo	ry 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

#### 配置Secure LDAP目錄

步驟 1.配置CUCM LDAP目錄,以便在埠636上利用LDAPS TLS與AD的連線。

導航到CUCM管理>系統> LDAP目錄。鍵入LDAP伺服器資訊的FQDN或LDAP伺服器的IP地址。指 定LDAPS埠636,並選中Use TLS框,如下圖所示:

aluda Cisco Unified CM Administration	Navigation Cisco Unified CM Administration 🗸 Go
CISCO For Cisco Unified Communications Solutions	admin Search Documentation About Logou
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 🏷 Perform Full Sync Now 🖧 Add New	
Group Information	
User Rank* Is-Default liser Pank	
Access Control Groups	
Add to Access Control Group	
Remove from Access Control Group	
2	
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 next list if one was not created based on a surged LDAD telephone surgery	
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	
Add Another Redundant LDAP Server	



注意:預設情況下,在LDAP伺服器資訊中配置的10.5(2)SU2和9.1(2)SU3 FQDN版本根據 證書的公用名進行檢查後,如果使用的是IP地址而不是FQDN,則會發出utils Idap config ipaddr命令停止將FQDN強制實施到CN驗證。

步驟 2.要完成對LDAPS的配置更改,請按一下Perform Full Sync,如圖所示:

aluda Cisco Unified (	CM Administration	Navipation Cisco Unified CM Administration 🗸 🐻
CISCO For Cisco Unified Con	nmunications Solutions	admin Search Documentation About Logout
System + Call Routing + Media Resou	rces • Advanced Features • Device • Application • User Man	gement ≠ Bulk Administration ≠ Help +
LDAP Directory		Related Links: Back to LDAP Directory Find/Lint
🕞 Save 🗶 Delete 🗋 Copy 🕻	Perform Full Sync Now 👍 Add New	
- Status		
A		
Update successful. Perform a sy	inchronization operation (manual or scheduled) to synchronize ch	anges with the directory.
1010 Directory Information		
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+i dc+com	
LDAP Custom Filter for Users	< None > v	
Synchronize*	Users Only     Users and Groups	
LDAP Custom Filter for Groups	< None >	

步驟 3.導航到CUCM管理>使用者管理>終端使用者,確認存在終端使用者,如下圖所示:

cisco	<b>Cisco U</b> For Cisco U	nified CM Admi	nistration s Solutions					Navigation Cisco Unified CM Administr admin Search Documentation	ation 🔍	G0 Logout
System -	Call Routing 👻	Media Resources 👻 Adva	nced Features · Device	- Application -	User Management 👻	Bulk Administration 👻	Help 👻			
Find and	List Users									
👍 Add	New Select	All 🔛 Clear All 💥 D	Delete Selected							
Status -	cords found									
User	(1 - 3 of 3)							Ro	ws per Page S	50 🗸
Find Use	where First nam	ne v b	begins with $\neg$		Find Clear Fi	lter 🕂 🛥				
	User ID *	Meeting Number	First Name	Last Name	Department	Direct	ory URI	User Status	User I	Rank
	<u>ostacy</u>	2183	Gwen	Stacy		gstacy@	.com	Active Enabled LDAP Synchronized User	1	
	hosborn	2182	Harry	Osborn		hosborn@	.com	Active Enabled LDAP Synchronized User	1	
	pparker	2181	Peter	Parker		pparker@:	.com	Active Enabled LDAP Synchronized User	1	

步驟 4.導航到ccmuser頁(https://<cucm pub的ip地址>/ccmuser)驗證使用者登入是否成功。

CUCM版本12.0.1的ccmuser頁面如下所示:

# Cisco Unified Communications Self Care Portal

Username
Password
Sign In

輸入LDAP憑證後,使用者即可成功登入,如下圖所示:

cisco (	Unified Communications Self Care Portal Gwen St			Gwen Stacy <del>*</del>	Skip to Content		
Phones	Voicemail	IM & Availability	General Settings	Downloads			About Help
My Pho Call	Phones ne Settings Forwarding	My Phone Company Phones These are the phones prov Disco 8865 2183	es ided to you by your company.	You may set personal pre	ferences for these in Phone Settings		

#### 配置安全LDAP身份驗證

配置CUCM LDAP身份驗證以利用到埠3269上的AD的LDAPS TLS連線。

導航到CUCM管理>系統> LDAP身份驗證。鍵入LDAP伺服器資訊的LDAPS伺服器的FQDN。指定 LDAPS埠3269,並選中Use TLS框,如下圖所示:

Cisco Unified	CM Administration						
cisco Eor Circo Unified Co	mmunications Solutions		Navigation Ci	sco Unified CM Administratio	About	~ G0	
			aumin	Search Documentation	About	Logout	
System      Call Routing      Media Reso	ources  Advanced Features  Device  Application  User Man	agement 👻 Bulk Administration 👻 Help 👻					
LDAP Authentication							
Save							
Status							
Update successful							
CLDAP Authentication for End Users							
Use LDAP Authentication for En	d Users						
LDAP Manager Distinguished Name	* Administrator® .com	]					
LDAP Password*	•••••	]					
Confirm Password*	•••••	]					
LDAP User Search Base*	cn=users,dc=dc=com	]					
c LDAP Server Information							
н	ost Name or IP Address for Server <sup>*</sup>	LDAP Port* Use TLS					
WIN-H2Q74S1U39P .c	om	3269					
Add Another Redundant LDAP Server							



注意:如果您有Jabber客戶端,建議使用3269埠進行LDAPS身份驗證,因為如果未指定到 全局目錄伺服器的安全連線,則可能會發生登入時Jabber超時。

#### 為UC服務配置與AD的安全連線

如果需要保護利用LDAP的UC服務,請配置這些UC服務以利用TLS的埠636或3269。

導航到CUCM管理>使用者管理>使用者設定> UC服務。尋找指向AD的目錄服務。鍵入LDAPS伺服器的FQDN作為主機名/IP地址。將埠指定為636或3269以及協定TLS,如下圖所示:

cisco For Cisco	Inified CM Administration Unified Communications Solutions	Navigation Cisco Unified CM Administration Cisco Unified CM Administration GO admin Search Documentation About Logout				
System - Call Routing -	Media Resources 👻 Advanced Features 👻 Device 👻 Application 👻 User Management 👻 Bulk Administration 👻 Help 👻					
UC Service Configurat	UC Service Configuration Related Links: Back To Find/List 🗸 Go					
🔜 Save 🗙 Delete	🗋 Copy 🎦 Reset 🥒 Apply Config 🖶 Add New					
Status						
Update successful						
r UC Service Information						
UC Service Type: Directory						
Product Type*	Directory					
Name*	Secure Directory					
Description						
Host Name/IP Address*	WIN-H2Q74S1U39R .com					
Port	636					
Protocol	TLS v					
Save Delete Copy Reset Apply Config Add New						
*- indicates required item.						



注意:Jabber客戶端電腦還需要在Jabber客戶端電腦的證書管理信任儲存中安裝CUCM上 安裝的tomcat-trust LDAPS證書,以便允許Jabber客戶端建立到AD的LDAPS連線。

#### 驗證

使用本節內容,確認您的組態是否正常運作。

要驗證從LDAP伺服器傳送到CUCM的TLS連線的實際LDAPS證書/證書鏈,請從CUCM資料包捕獲 導出LDAPS TLS證書。此連結提供有關如何從CUCM資料包捕獲導出TLS證書的資訊:<u>如何從</u> <u>CUCM資料包捕獲導出TLS證書</u>

#### 疑難排解

目前沒有特定資訊可用於對此組態進行疑難排解。

### 相關資訊

- 此連結提供對穿越LDAPS配置的影片的訪問:<u>安全LDAP目錄和身份驗證穿透影片</u>
- <u>技術支援與文件 Cisco Systems</u>

#### 關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。