セキュアLDAP(LDAPS)用のCUCMの設定

内容
 はじめに
 前提条件
 要件
 使用するコンポーネント
 背景説明
 LDAPS証明書の確認とインストール
 セキュアLDAPディレクトリの設定
 セキュアLDAP認証の設定
 UCサービスのADへのセキュアな接続の設定
 確認
 トラブルシュート
 関連情報

はじめに

このドキュメントでは、非セキュアLDAP接続からセキュアLDAPS接続へのADへのCUCM接続を 更新する手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

・ AD LDAPサーバ •CUCM LDAP の設定

・ CUCM IM & Presenceサービス(IM/P)

使用するコンポーネント

このドキュメントの情報は、CUCMリリース9.x以降に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

背景説明

Lightweight Directory Access Protocol(LDAPS)用のAD Lightweight Directory Access Protocol(LDAP)の設定は、Active Directory(AD)管理者が行います。これには、LDAPS証明書の要 件を満たすCA署名付き証明書のインストールが含まれます。



注:他のCisco Collaboration Applications: <u>Software Advisory: Secure LDAP Mandatory</u> <u>for Active Directory Connections</u>に対して、非セキュアLDAPからADへのセキュア LDAPS接続を更新するための情報については、このリンクを参照してください。

LDAPS証明書の確認とインストール

ステップ1:LDAPS証明書がADサーバにアップロードされたら、ldp.exeツールを使用して、 ADサーバでLDAPSが有効になっていることを確認します。

- 1. ADサーバでAD管理ツール(Ldp.exe)を起動します。
- 2. ConnectionメニューからConnectを選択します。
- 3. LDAPSサーバの完全修飾ドメイン名(FQDN)をサーバとして入力します。
- 4. ポート番号として636を入力します。

5. 図に示すように、OKをクリックします

	Ldp	- 0 X
Connection Browse	View Options Utilities Help	
	Connect	
Po	ver: WIN-H2Q74S1U39P .com t: €35 Connectionless ✓ SSL	
	OK	
Ready		NUM

ポート636での接続が正常に行われると、図に示すように、右側のペインにRootDSE情報が出力 されます。

Maps://WIN-	H2Q74S1U39P .com/DC=net ×	
Connection Brow	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_); 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; isSupphresized: TRUE;	
Ready	NUM	ai

図に示すように、ポート3269に対してこの手順を繰り返します。



ポート3269での接続が正常に行われると、図に示すように、RootDSE情報が右側のペインに表示 されます。

gcs://WIN-H2Q	74S1U39P .com/DC=netw	ĸ
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/igurationNamingContext: CN=Configuration,DC=network218,DC=com; currentTime: 4/2/2020 10:40:55 AM Central Daylight Time; defaultNamingContext: 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); domainfunctionality: 6 = (WIN2012R2); highestCommittedUSN: 500892'	< 111 >
Ready	NUM	, at

ステップ2:LDAPSサーバ証明書の一部であるルート証明書と中間証明書を取得し、これらを tomcat-trust証明書として各CUCMおよびIM/Pパブリッシャノードにインストールし、 CallManager-trustとしてCUCMパブリッシャにインストールします。

LDAPSサーバ証明書<hostname>.<Domain>.cerの一部であるルート証明書と中間証明書を図に示します。

Home Shi	are View						~
· -> • 1	LDAPS > cert					~ Ö ~	Search c.
1 Ouistanses	 Name 	^		Date modified	Туре	Size	
		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-H2	Q74S1U39P .com.cer		3/27/2020 8:56 AM	Security Certificate	3 KB	

CUCMパブリッシャのCisco Unified OS Administration > Security > Certificate Managementに移 動します。ルート(root)をtomcat-trust(図を参照)およびCallManager-trust(図を参照)として アップロードします。

🔞 Upload Certificate/Certif	ficate chain - Mozilla Firefox		- 0	X			—	- a ×
🔽 🔬 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 data	Cisco Unified OS Adm Search Documer	inistration ntation About	GO GO
Status Warning: Uploading Upload Certificate/Cee Certificate Purpose* Description(friendly nam Upload File	ertificate chain tomcat-trust Browse No file si	ill distribute it to all serv	vers in this cluster					
(i) *- indicates requi	\leftarrow \rightarrow \checkmark \uparrow \square \rightarrow This	PC > Desktop > LDAP	S⇒ cert			~	ۍ کې Se	arch cert
	Organize 👻 New folde							
	Desktop ^	Name	`	Date mo	dified	Туре	Size	
<	LDAPS	-CERTCA	2012-CA.cer	3/27/202	0 8:57 AM	Security Certificate	2 KB	
	TODO	White H	2Q74S1U39P-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	

intermediateをtomcat-trust(図を参照)およびCallManager-trust(図を参照)としてアップロー ドします。

ۏ Upload (Certificate/Certifica	ate chain -	Mozilla Firefox			- [X				-		Ø	
🖸 🔒 h	ttps://10.201.21	8.163/cr	nplatform/certif	ficateUpload.	do		≡		•••	⊠ ☆	III\ 🗊	•	۲	Ξ
Upload Ce	ertificate/Certif	icate ch	ain				~	.ogin 🚦 Sign in to	your a	account 🗎	Current	🛅 Trai	ining	>>
Dipload	Close							Navigation Cisco admin	Unifie Search	d OS Admin Document	istration ation	About	~ L	Go .ogou
i Succ Resta i If the	ess: Certificate U art Cisco Tomcat	Iploaded <u>Service u</u> 	sing the CLI "uti s PC → Desktop	ils service rest	tart <u>Cisco Tomca</u> cert	ıt".		~	5	, P Sei	arch cert			×
Certific	Organize 🔻	New folde	r									-		0
Descrip Upload	Desktop	^	Name	-CERTCA2012-	CA.cer	Date modifie 3/27/2020 8:5	ed 57 AM	Type Security Certificate	Siz	e 2 KB				
Uplan	TODO			WIN-H2Q74S	1U39P-CA.net	3/27/2020 8:5	55 AM	Security Certificate		2 KB				
Uploa	📥 Cisco		WIN-H2Q7	4\$1U39P	.com.cer	3/27/2020 8:	56 AM	Security Certificate		3 KB				

◇ 注:CUCMクラスタの一部であるIM/Pサーバがある場合、これらの証明書をこれらの IM/Pサーバにアップロードする必要もあります。

◇ 注:別の方法として、LDAPSサーバ証明書をtomcat-trustとしてインストールすることもで きます。

ステップ 3:クラスタ内の各ノード(CUCMおよびIM/P)のCLIからCisco Tomcatを再起動します 。また、CUCMクラスタでは、パブリッシャノードでCisco DirSyncサービスが起動していること を確認します。 tomcatサービスを再起動するには、各ノードのCLIセッションを開き、図に示すようにコマンド utils service restart Cisco Tomcatを実行する必要があります。

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:

ステップ 4:CUCMパブリッシャのCisco Unified Serviceability > Tools > Control Center - Feature Servicesの順に移動し、Cisco DirSyncサービスがアクティブで開始されていることを確認し(図 を参照)、これが使用されている場合は各ノードでCisco CTIManagerサービスを再起動します (図を参照)。

abab	Cisco Unified Serviceability			Navigation (Cisco Unified Serviceability 🗸 🗸	Go
cisco	For Cisco Unified Communications Solutions				admin About	Logout
Alarm 🔻	Trace + Tools + Snmp + CallHome + Help +					
Control C	enter - Feature Services			Related Links	Service Activation 🗸 🗸	Go
Sta	rt 🛑 Stop har Restart 🔇 Refresh Page					
Status:						
Read	ly D					
Select	Server					
Server*	cucmpub218comCUCM Voice/Video V	o				
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	

セキュアLDAPディレクトリの設定

ステップ 1:ポート636でのADへのLDAPS TLS接続を利用するために、CUCM LDAPディレクト リを設定します。 CUCM Administration > System > LDAP Directoryの順に移動します。LDAPサーバ情報の LDAPSサーバのFQDNまたはIPアドレスを入力します。図に示すように、LDAPSポートとして 636を指定して、Use TLSのボックスにチェックマークを付けます。

Cisco Unified CM Administration For Cisco Unified Communications Solutions	Navigation Cis admin	sco Unified CM Administrat Search Documentation	tion About	Go Logout
System 🔻 Call Routing 👻 Media Resources 👻 Advanced Features 👻 Device 👻 Application 👻 User Management 👻 Bulk Administration 👻 Help 👻				
LDAP Directory	Related Links	Back to LDAP Director	ry Find/List	~ G0
🔜 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. 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				
WIN-H2Q74S1U39Pcom 636 🗹				
Add Another Redundant LDAP Server				



注:デフォルトでは、LDAPサーバ情報で設定されているバージョン10.5(2)SU2および 9.1(2)SU3のFQDNが証明書のCommon Nameに照らしてチェックされた後、FQDNの代 わりにIPアドレスが使用されている場合は、コマンドutils Idap config ipaddrを発行して FQDNからCNへの検証の適用を停止します。

ステップ 2:LDAPSの設定変更を完了するには、図に示すように、Perform Full Sync Nowをクリックします。

Cisco Unified Con	CM Administration mmunications Solutions	Nevipsion Coso United OH Administration v 66 admin Search Documentation About Logout					
System • Call Routing • Media Reso	urces Advanced Features Device Application User Mana	jenert + Buk Administration + Heb +					
LDAP Directory		Related Links: Back to LDAP Directory Find(List ~ 60					
🕞 Save 🗶 Delete 🗋 Copy 🕯	Perform Full Sync Now Car Add New						
Update successful. Perform a s	atlas						
LDAP Directory Information							
LDAP Configuration Name*	LOAP-218						
LDAP Manager Distinguished Name*	Administrator@ com						
LOAP 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 >						

ステップ3: CUCM Administration > User Management > End Userの順に移動し、図に示すよう にエンドユーザが存在することを確認します。

cisco	Cisco U For Cisco U	nified CM Admini	stration olutions					Navigation Cisco Unified CM Administr admin Search Documentatio	ation n About	✓ G0 Logout
System -	Call Routing 🔻	Media Resources 👻 Advance	d Features - Devic	e • Application •	User Management 🔻	Bulk Administration 👻	Help 👻			
Find and	List Users									
👍 Add	New Elect	All 🔛 Clear All 💥 Dele	te Selected							
Status										
() 3 r	ecords found									
User	(1 - 3 of 3)							Ro	ws per Page	e 50 🗸
Find Use	r where First nar	ne v beg	ins with ↓		Find Clear File	ter 🕂 🛥				
	User ID *	Meeting Number	First Name	Last Name	Department	Directo	ory URI	User Status	Us	er 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	

ステップ4:ユーザログインが成功したことを確認するために、ccmuserページ(https://<ip address of cucm pub>/ccmuser)に移動します。

CUCMバージョン12.0.1のccmuserページは次のようになります。

Cisco Se	o Unified Communica elf Care Port	ations t <mark>al</mark>
	Username	
	Password	
	Sign In	

図に示すように、ユーザはLDAPクレデンシャルの入力後に正常にログインできます。



セキュアLDAP認証の設定

ポート3269でのADへのLDAPS TLS接続を利用するために、CUCM LDAP認証を設定します。

CUCM Administration > System > LDAP Authenticationの順に移動します。LDAPサーバ情報の LDAPSサーバのFQDNを入力します。図に示すように、LDAPSポートとして3269を指定して、 Use TLSのボックスにチェックマークを付けます。

ululu Cisco Unified CM Administration	Navigation Cisco Unified CM Administration 🗸 G
CISCO For Cisco Unified Communications Solutions	admin Search Documentation About Logo
System 👻 Call Routing 👻 Media Resources 👻 Advanced Features 👻 Device 👻 Application 👻 User Management 👻 Bulk Administration 🍷 Help 👻	
LDAP Authentication	
Save	
_ Status	
Indate successful	
O optice succession	
- I DAP Authentication for End Users	
Use LDAP Authentication for End Users	
LDAP Manager Distinguished Name* Administrator® .com	
LDAP Password*	
Confirm Password*	
LDAP User Search Base* comusers dc= dc=com	
r LDAP Server Information	
Host Name or IP Address for Server* LOAP Port* Use TIS	
WIN-H2074S1U39P .com 3269	
Add andhar Dadundark 1940 Carray	
Add Another Redundant LDAP Server	



注:Jabberクライアントを使用している場合は、LDAPS認証にポート3269を使用することをお勧めします。これは、グローバルカタログサーバへのセキュアな接続が指定されていないと、ログイン時にJabberがタイムアウトする可能性があるためです。

UCサービスのADへのセキュアな接続の設定

LDAPを使用するUCサービスを保護する必要がある場合は、TLSでポート636または3269を使用 するようにこれらのUCサービスを設定します。

CUCM administration > User Management > User Settings > UC Serviceの順に移動します。ADを 指すディレクトリサービスを検索します。LDAPSサーバのFQDNをホスト名/IPアドレスとして入 力します。図に示すように、ポートを636または3269、およびプロトコルTLSとして指定します 。

alulu Cisco Unified CM Administration	Navigation Cisco Unified CM Administration 🗸 Go
CISCO For Cisco Unified Communications Solutions	admin Search Documentation About Logout
Surtem + Cali Division + Madia Dassurgas + Advascad Eastwas + Davisa + Application + Hansanamant + Bulk Administration + Halb +	
System * Cali Rodaling * Inicial Resources * Auvanced Features * Device * Application * Oser Heinagement * Dok Administration * hep *	
UC Service Configuration	Related Links: Back To Find/List 🗸 Go
🔚 Save 🗶 Delete 🗈 Copy 🎦 Reset 🖉 Apply Config 🖶 Add New	
r Status	
Update successful	
- If Candica Telemation	
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:JabberクライアントがADへのLDAPS接続を確立できるようにするには、Jabberクラ イアントマシンの証明書管理信頼ストアにインストールされているCUCMにインストー ルされているtomcat-trust LDAPS証明書も、Jabberクライアントマシンに必要です。

確認

このセクションでは、設定が正常に動作していることを確認します。

TLS接続のためにLDAPサーバからCUCMに送信された実際のLDAPS証明書/証明書チェーンを確認するには、CUCMパケットキャプチャからLDAPS TLS証明書をエクスポートします。CUCMパケットキャプチャからTLS証明書をエクスポートする方法については、<u>CUCMパケットキャプチ</u> <u>ャからTLS証明書をエクスポートする方法</u>を参照してください。

トラブルシュート

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- LDAPS設定を確認できるビデオ(セキュアLDAPディレクトリおよび認証ウォークスルービ デオ)へのアクセスを提供します。
- <u>テクニカル サポートとドキュメント Cisco Systems</u>

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。