为安全LDAP (LDAPS)配置CUCM

目录

简介 <u>先决条件</u> <u>要求</u> <u>使用的组件</u> <u>背景信息</u> 验证和安装LDAPS证书 配置Secure LDAP目录 配置安全LDAP身份验证 为UC服务配置与AD的安全连接 验证

<u>相关信息</u>

简介

本文档介绍从非安全LDAP连接更新到安全LDAPS连接的CUCM连接AD的过程。

先决条件

要求

Cisco 建议您了解以下主题:

·AD LDAP服务器

· CUCM LDAP配置

· CUCM IM & Presence服务(IM/P)

使用的组件

本文档中的信息基于CUCM版本9.x及更高版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

背景信息

Active Directory (AD)管理员负责为轻型目录访问协议(LDAPS)配置AD轻型目录访问协议(LDAP)。 这包括安装符合LDAPS证书要求的CA签名证书。



注意:有关从非安全LDAP更新以保护LDAP到AD的连接以用于其他思科协作应用的信息 ,请参阅以下链接:<u>软件建议:对于Active Directory连接,安全LDAP是必需的</u>

验证和安装LDAPS证书

步骤1:将LDAPS证书上传到AD服务器之后,请使用ldp.exe工具验证是否已在AD服务器上启用 LDAPS。

- 1. 在AD服务器上启动AD管理工具(Ldp.exe)。
- 2. 在"Connection"菜单上,选择Connect。
- 3. 输入LDAPS服务器的完全限定域名(FQDN)作为服务器。
- 4. 输入636作为端口号。
- 5. 单击OK,如图所示

A	Ldp	- 0 X
Connection Browse	View Options Utilities Help	
Se Po	Connect X rver: WIN-H2Q74S1U39P .com rt: Image: Connectionless Image: SSL Image: OK Cancel	
Ready		NUM:

对于端口636上的成功连接,RootDSE信息会打印在右窗格中,如图所示:

Maps://WIN-Ha	2Q74S1U39P .com/DC=net ×	
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_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; inSupplemented: TDUE-	< III >
Ready	NUM	

对端口3269重复上述步骤,如图所示:



要在端口3269上成功连接,RootDSE信息会打印在右窗格中,如图所示:

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	at.

第二步:获取作为LDAPS服务器证书一部分的根证书和任何中间证书,并将这些证书作为tomcattrust证书安装在每个CUCM和IM/P发布方节点上,作为CallManager-trust安装在CUCM发布方节点 上。

LDAPS服务器证书<hostname>.<Domain>.cer中的根证书和中间证书如下图所示:

I I I cert File Home Share View					-	□ × ~ ()
$\leftarrow \rightarrow \checkmark \uparrow$ \bigcirc LDAPS \rightarrow cert					< 5 v	Search c
Name Name	^		Date modified	Туре	Size	
	CERTCA2012-CA.cer		3/27/2020 8:57 AM	Security Certificate	2 KB	
	NIN-H2Q7451U39P-CA.	.com.cer	3/27/2020 8:55 AM	Security Certificate	2 KB	
Downloads WIN-H2Q Pictures	74S1U39P .com.cer		3/27/2020 8:56 AM	Security Certificate	3 KB	

导航到CUCM Publisher Cisco Unified OS Administration > Security > Certificate Management。将 根桥上传为tomcat-trust(如图所示)和CallManager-trust(未显示):

(a) Upload Certificate/Certifi	ficate chain - Mozilla Firefox	- 0	×				- a ×
🔽 🔬 https://10.201.	.218.163/cmplatform/certi	ficateUpload.do •	•• =		⊠ ☆	III\ 🗉 💀	. ≡
Upload Certificate/Cer	rtificate chain			.ogin 🚦 Sigr	n in to your account	Current 🛅 Tr	aining ≫
Upload 🖳 Close				Navigation data	Cisco Unified OS Adm Search Documer	inistration ntation Abou	<mark>√ Go</mark> 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 s	ill distribute it to all servers in this cluster					
(i) *- indicates requi	\leftarrow \rightarrow \checkmark \uparrow \square \rightarrow This	; PC > Desktop > LDAPS > cert			~	ق ب Se	arch cert
	Organize 🔻 New folder	r					
	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.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	

将中间上传为tomcat-trust(如图所示)和CallManager-trust(未显示):

🙆 Upload	Certificate/Certifi	cate chain - I	Mozilla Firefox		- 0	×		-	- a >
0 🔒	https:// 10.201.2	18.163/cm	platform/certifi	icateUpload.do	•••	=	⊠ ☆		B (8) =
Upload Co	ertificate/Cert	ificate cha	in			^ .ogin 🚦 Sign in to	your account	Current 🗎	Training >>>
Upload	d 🖳 Close					Navigation Cisco admin	Unified OS Admir Search Document	istration ation Abo	✓ Go out Logout
Status -	cess: Certificate	Uploaded	ing the CLT "will	le ana ina mata di Cinca Tama			-	-	
I Res	File Upload	t Service us	sing the CLI util	s service restart Cisco Tomca	1.				×
Upload	$\leftarrow \ \ \rightarrow \ \ \uparrow \uparrow$	🔒 > This	PC > Desktop	> LDAPS > cert		~	ر ک ا	arch cert	
Certific	Organize 🔻	New folder							
Descrip Upload	LDAPS	^	Name	-CERTCA2012-CA.cer	Date modified 3/27/2020 8:57 AM	Type Security Certificate	Size 2 KB		
	TODO			WIN-H2Q74S1U39P-CA.net	3/27/2020 8:55 AM	Security Certificate	2 KB		
Uploa	📥 Cisco		win-H2Q74	dS1U39P .com.cer	3/27/2020 8:56 AM	Security Certificate	3 KB		

✤ 注意:如果您的IM/P服务器是CUCM集群的一部分,则还需要将这些证书上传到这些IM/P服 务器。

^እ注意:作为替代方法,您可以将LDAPS服务器证书安装为tomcat-trust。

第三步:从集群中每个节点(CUCM和IM/P)的CLI重新启动Cisco Tomcat。此外,对于CUCM集 群,请验证发布方节点上的思科DirSync服务是否已启动。

要重新启动Tomcat服务,您需要为每个节点打开一个CLI会话并运行命令utils service restart Cisco Tomcat,如图所示:

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			
<pre>/Mware Installation: 2 vCPU: Intel(R) Xeon(R) CPU E7-2890 v2 @ 2.80GHz Disk 1: 80GB, Partitions aligned 4096 Mbytes RAM</pre>			
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[STARTING] Cisco Tomcat[STARTING] Cisco Tomcat[STARTING] Cisco Tomcat[STARTED] admin:	≥ has	not	rest

第四步:导航到CUCM发布服务器Cisco Unified Serviceability > Tools > Control Center - Feature Services,验证是否已激活并启动Cisco DirSync服务(如图所示),如果使用此服务(未显示),请在每个节点上重新启动Cisco CTIManager服务:

ahaha	Cisco Unified Serviceability			Navigation C	isco Unified Serviceability V Go
cisco	For Cisco Unified Communications Solutions				admin About Logout
Alarm -]	[race + Tools + Snmp + CallHome + Help +				
Control Ce	nter - Feature Services			Related Links:	Service Activation v Go
Start	🛑 Stop 🛛 📗 Restart 🔇 Refresh Page				
Status:					
Ready					
-	P0				
-Select Se	erver				
Server*	.comCUCM Voice/Video	Go			
Performa	nce 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
Directory	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目录

步骤1:配置CUCM LDAP目录,以便在端口636上利用与AD的LDAPS TLS连接。

导航到CUCM管理>系统> LDAP目录。键入LDAP服务器信息的FQDN或LDAP服务器的IP地址。指 定LDAPS端口636,然后选中Use TLS框,如图所示:

aluda Cisco Unified CM Administration	Navigation Cisco Unified CM Administration 🗸 Go
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 Directory	Related Links: Back to LDAP Directory Find/List 🗸 Go
🔚 Save 💥 Delete 🗈 Copy 🏷 Perform Full Sync Now 🖧 Add New	
- Group Information	
User Rank* I_Dofault 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 goal list if one was not created based on a sweed LDAR telephone symbol	
Assign new me rom the poor list if one was not created based on a synced LOAP 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-H2Q/451039Rcom 636	
Add Another Redundant LDAP Server	



注意:默认情况下,在LDAP服务器信息中配置的10.5(2)SU2和9.1(2)SU3 FQDN版本根据 证书的公用名进行检查后,如果使用的是IP地址而不是FQDN,则会发出utils Idap config ipaddr命令以停止将FQDN实施到CN验证。

第二步:要完成LDAPS的配置更改,请单击Perform Full Sync Now,如图所示:

abala Cisco Unified	CM Administration	Nevipation Cisco Unified CH Administration 🗸 Go
CISCO For Cisco Unified Cor	nmunications Solutions	admin Search Documentation About Logout
System • Call Routing • Media Reso	rces • Advanced Features • Device • Application • User Man	agement • Bulk Administration • Help •
LDAP Directory		Related Links: Back to LDAP Directory Find(List - Go
📊 Save 🗶 Delete 🛅 Copy	🕐 Perform Full Sync Now 🖓 Add New	
- Etalor		
A		
Update successful. Perform a s	vnchronization operation (manual or scheduled) to synchronize cl	anges with the directory.
CLOAP Directory Information		
LDAP Configuration Name*	1010-318	
1040 Manager Distinguished Name	1000-210	
Loro Hanager Clauriguaries Harre	Administratoria 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 O Users and Groups	
LDAP Custom Filter for Groups	< None > v	

第三步:导航到CUCM管理>用户管理>最终用户,验证是否存在最终用户,如图所示:

cisco	Cisco U For Cisco U	nified CM Admini	istration iolutions					Navigation Cisco Unified admin Search D	CM Administration Documentation Al	✓ G0 bout Logout
System -	Call Routing 🔻	Media Resources 👻 Advance	ed Features - Device	e 🕶 Application 👻	User Management 👻	Bulk Administration 💌	Help 🔻			
Find and	List Users									
🕂 Add	New Select	All 🔛 Clear All 💥 Dele	te Selected							
Status										
(i) 3 r	ecords found									
User	(1 - 3 of 3)								Rows per	Page 50 🗸
Find Use	r where First nar	ne v beg	ins with $\ arphi$		Find Clear Fil	ter 🕂 🛥				
	User ID *	Meeting Number	First Name	Last Name	Department	Director	ry URI	User Status		User Rank
	gstacy	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

第四步:导航到ccmuser页(https://<cucm pub>的ip地址/ccmuser)验证用户登录是否成功。

CUCM版本12.0.1的ccmuser页面如下所示:

Cisco Unified Communications Self Care Portal

Username
Password
Sign In

输入LDAP凭证后,用户可以成功登录,如图所示:

cisco (Jnified Communica	ations Self Care Porta	al		Gwen	Skip to (Content
Phones	Voicemail	IM & Availability	General Settings	Downloads		About	Help
My I Pho Call	Phones ne Settings Forwarding	My Phone Company Phones These are the phones provide Cisco 8865 2183	ees	You may set personal pre	ferences for these in Phone Settings	-	

配置安全LDAP身份验证

配置CUCM LDAP身份验证以利用到端口3269上的AD的LDAPS TLS连接。

导航到CUCM管理>系统> LDAP身份验证。键入LDAP服务器信息的LDAPS服务器的FQDN。指定 LDAPS端口3269,然后选中Use TLS复选框,如图所示:

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							
LDAP Authentication for End Us	iers						
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 [*]	LDAP Port* Use TLS					
WIN-H2Q74S1U39P .c	om	3269					
Add Another Redundant LDAP S	erver						



注意:如果您有Jabber客户端,建议使用端口3269进行LDAPS身份验证,因为如果未指定 到全局目录服务器的安全连接,则可能会发生登录的Jabber超时。

为UC服务配置与AD的安全连接

如果需要保护利用LDAP的统一通信服务,请配置这些统一通信服务以使用TLS的端口636或3269。

导航到CUCM管理>用户管理>用户设置>统一通信服务。查找指向AD的目录服务。键入LDAPS服务器的FQDN作为主机名/IP地址。将端口指定为636或3269以及协议TLS,如图所示:

cisco For Cisco	Jnified CM Administration Unified Communications Solutions	Navigation Cisco Unified CM Administration V Go admin Search Documentation About Logout				
System - Call Routing -	Media Resources 👻 Advanced Features 👻 Device 👻 Application 👻 User Management 👻 Bulk Administration 👻 Help 👻					
UC Service Configura	tion	Related Links: Back To Find/List 🗸 Go				
Save 🗙 Delete	🗋 Copy 省 Reset 🥒 Apply Config 🖶 Add New					
Status						
(i) Update successful						
L Cervice 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 Agaly Config Add New						
(i) *- indicates required item.						



注意:Jabber客户端计算机还需要在Jabber客户端计算机的证书管理信任库中安装 CUCM上安装的tomcat-trust LDAPS证书,以允许Jabber客户端建立到AD的LDAPS连接。

验证

使用本部分可确认配置能否正常运行。

要验证从LDAP服务器发送到CUCM的TLS连接的实际LDAPS证书/证书链,请从CUCM数据包捕获 中导出LDAPS TLS证书。此链接提供有关如何从CUCM数据包捕获导出TLS证书的信息:<u>如何从</u> <u>CUCM数据包捕获导出TLS证书</u>

故障排除

当前没有故障排除此配置的特定可用资料。

相关信息

- 此链接提供对穿过LDAPS配置的视频的访问:<u>安全LDAP目录和身份验证穿透视频</u>
- <u>技术支持和文档 Cisco Systems</u>

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。