Configurar CUCM para LDAP seguro (LDAPS)

Contents

Introdução Pré-requisitos Requisitos Componentes Utilizados Informações de Apoio Verificar e instalar certificados LDAPS Configurar diretório LDAP seguro Configurar Autenticação LDAP Segura Configurar conexões seguras com o AD para serviços de UC Verificar Troubleshooting Informações Relacionadas

Introdução

Este documento descreve o procedimento para atualizar conexões CUCM para o AD de uma conexão LDAP não segura para uma conexão LDAPS segura.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

· Servidor AD LDAP

· Configuração LDAP do CUCM

· Serviço de mensagens instantâneas e presença (IM/P) do CUCM

Componentes Utilizados

As informações neste documento são baseadas no CUCM versão 9.x e superior.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

É responsabilidade do Administrador do Ative Diretory (AD) configurar o AD LDAPS (Lightweight Diretory Access Protocol) para LDAPS (Lightweight Diretory Access Protocol). Isso inclui a instalação de certificados assinados por CA que atendem ao requisito de um certificado LDAPS.



Observação: consulte este link para obter informações para atualizar de LDAP não seguro para conexões LDAPS seguras para AD para outros Aplicativos de Colaboração da Cisco: <u>Consultoria de Software: LDAP Seguro Obrigatório para Conexões do Ative</u> <u>Diretory</u>

Verificar e instalar certificados LDAPS

Etapa 1. Depois que o certificado LDAPS tiver sido carregado no servidor AD, verifique se o LDAPS está habilitado no servidor AD com a ferramenta ldp.exe.

- 1. Inicie a Ferramenta de Administração do AD (Ldp.exe) no servidor do AD.
- 2. No menu Conexão, selecione Conectar.
- 3. Insira o FQDN (Fully Qualified Domain Name, Nome de domínio totalmente qualificado) do

servidor LDAPS como servidor.

- 4. Insira 636 como o número da porta.
- 5. Clique em OK, como mostrado na imagem

<u>A</u>	Ldp	_ D X
Connection Browse	View Options Utilities Help	
Ser	Connect ver: WIN-H2Q74S1U39P .com t: Connectionless ✓ SSL OK Cancel	
Ready		NUM

Para uma conexão bem-sucedida na porta 636, as informações do RootDSE são impressas no painel direito, como mostrado na imagem:

Maps://WIN-H	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_2); 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; inStructoreneited: TDUE:	< III >
Ready	NUM	at

Repita o procedimento para a porta 3269, como mostrado na imagem:



Para uma conexão bem-sucedida na porta 3269, as informações do RootDSE são impressas no painel direito, como mostrado na imagem:

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) 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

Etapa 2. Obtenha a raiz e todos os certificados intermediários que fazem parte do certificado de servidor LDAPS e instale-os como certificados tomcat-trust em cada um dos nós de editor de CUCM e IM/P e como CallManager-trust no editor de CUCM.

Os certificados raiz e intermediários que fazem parte de um certificado de servidor LDAPS, <hostname>.<Domain>.cer, são mostrados na imagem:

I I I I cert File Home Sh	hare View					-	□ × ~ ()
$\leftarrow \rightarrow \neg \uparrow \square$	LDAPS > cert					م ت v	Search c
1 Orish second	^ Name	^		Date modified	Туре	Size	
Quick access		CERTCA2012-CA.cer		3/27/2020 8:57 AM	Security Certificate	2 KB	
Documents *	nts 🖈 🔤	.NIN-H2Q7451U39P-CA.	.com.cer	3/27/2020 8:55 AM	Security Certificate	2 KB	
🕂 Downloads 🖈	WIN-H2Q7	4S1U39P .com.cer		3/27/2020 8:56 AM	Security Certificate	3 KB	
Notures 📌							
cert							

Navegue até o editor do CUCM Cisco Unified OS Administration > Security > Certificate Management. Carregue o root como tomcat-trust (como mostrado na imagem) e como CallManager-trust (não mostrado):

🥹 Upload Certificate/Certi	ficate chain - Mozilla Firefox	_				-	- 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	ining >>
Upload 🖳 Close				Navigation C admin	isco Unified OS Adm	inistration htation About	✓ Go Logout
Status Warning: Uploading Upload Certificate/Ce Certificate Purpose* Description(friendly nam Upload File Upload Close	a cluster-wide certificate w ertificate chain tomcat-trust Browse No file so	ill distribute it to all servers in this cluste	er				
(i) *- indicates requi	$\leftarrow \rightarrow \land \uparrow \square \rightarrow$ This	PC > Desktop > LDAPS > cert			~	ر ک Sea	arch cert
	Organize New folder						
	Desktop ^	Name	Date mo	odified	Туре	Size	
<	LDAPS	-CERTCA2012-CA.cer	3/27/202	20 8:57 AM	Security Certificate	2 KB	
	TODO	Whit-H2Q74S1U39P-CA.	net 3/27/202	20 8:55 AM	Security Certificate	2 KB	
	Cisco	WIN-H2Q74S1U39P .com	.cer 3/27/202	20 8:56 AM	Security Certificate	3 KB	

Carregue o intermediário como tomcat-trust (como mostrado na imagem) e como CallManagertrust (não mostrado):

🔞 Upload Certificate/Certificate chain - Mozilla Firefox — 🗌 🔿					X C				-	- 0	×	
🔽 🔒 h	nttps://10.201.2	18.163/cm	nplatform/certi	ficateUpload.do		≡		⊌	☆≣∖		۲	Ξ
Upload Ce	ertificate/Cert	ificate ch	ain			^	.ogin 🚦 Sign in to	your accou	unt 🗎 Curr	rent 🗎 T	raining	»
Upload	Close						Navigation Cisco admin S	Unified OS Search Do	S Administra cumentation	ition Abou	√ G ut Loga	30 put
i Succ Rest	cess: Certificate art Cisco Tomca 🕹 File Upload	Uploaded t Service u	using the CLI "ut	ils service restart Cisco Tomca	ət".				-		,	×
Upload	$\leftarrow \rightarrow -$	📙 > Thi	s PC > Desktop	> LDAPS > cert			~	ē	, Search	cert		
Certific	Organize 🔻	New folde	r							-		
Descrip Deskt	LDAPS	LDAPS	Name	-CERTCA2012-CA.cer	Date modifie 3/27/2020 8:5	d 7 AM	Type Security Certificate	Size	2 KB			
	TODO			WIN-H2Q74S1U39P-CA.net	3/27/2020 8:5	5 AM	Security Certificate		2 KB			
Uploa	Uploa Cisco		WIN-H2Q	7459U39P .com.cer	3/27/2020 8:5	6 AM	Security Certificate		3 KB			

Observação: se você tiver servidores IM/P que fazem parte do cluster CUCM, também precisará carregar esses certificados para esses servidores IM/P.

Nota: como alternativa, você pode instalar o certificado do servidor LDAPS como tomcattrust.

Etapa 3. Reinicie o Cisco Tomcat a partir da CLI de cada nó (CUCM e IM/P) em clusters. Além disso, para o cluster CUCM, verifique se o serviço Cisco DirSync no nó do editor foi iniciado.

Para reiniciar o serviço Tomcat, você precisa abrir uma sessão CLI para cada nó e executar o comando utils service restart Cisco Tomcat, como mostrado na imagem:

```
PuTTY 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:
```

Etapa 4. Navegue para o editor do CUCM Cisco Unified Serviceability > Tools > Control Center - Feature Services, verifique se o serviço Cisco DirSync está ativado e iniciado (como mostrado na imagem) e reinicie o serviço Cisco CTIManager em cada nó se ele for usado (não mostrado):

abab	Cisco Unified Serviceability			Navigation C	isco 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 V Go
Star	t 🥚 Stop har Restart 🔇 Refresh Page				
Status:					
Read					
-Select S	erver				
Server*	cucmpub218	0			
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 00:27:49
0	Cisco CallManager SNMP Service	Started	Activated	Fri Nov 8 09:30:36 2019	146 days 00:27:47
Director	v 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

Configurar diretório LDAP seguro

Etapa 1. Configure o Diretório LDAP do CUCM para utilizar a conexão TLS LDAPS com o AD na porta 636.

Navegue até CUCM Administration > System > LDAP Diretory. Digite o FQDN ou o endereço IP

do servidor LDAP para Informações do servidor LDAP. Especifique a porta LDAPS de 636 e marque a caixa para Usar TLS, como mostrado na imagem:

Cisco Unified CM Administration For Cisco 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 👻	
LDAP Directory	Related Links: Back to LDAP Directory Find/List 🤟 Go
🔚 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 Host Name or IP Address for Server* UDAP Port* Use TLS WIN-H2Q74S1U39Pcom 636	
Add Another Redundant LDAP Server	



Nota: Por padrão, depois que as versões 10.5(2)SU2 e 9.1(2)SU3 FQDN configuradas nas Informações do Servidor LDAP são verificadas em relação ao Nome Comum do certificado, no caso de o endereço IP ser usado em vez do FQDN, o comando utils Idap config ipaddr é emitido para interromper a imposição do FQDN à verificação do CN.

Etapa 2. Para concluir a alteração de configuração para LDAPS, clique em Perform Full Sync Now, como mostrado na imagem:



Etapa 3. Navegue até CUCM Administration > User Management > End User e verifique se os usuários finais estão presentes, como mostrado na imagem:

cisco	For Cisco U	nified CM Admin	istration Solutions					Navigation <mark>Cis</mark> admin	co Unified CM Administration Search Documentation	<mark>√ G0</mark> About Logout
System -	Call Routing 🔻	Media Resources 👻 Advance	ed Features 👻 Devic	e 👻 Application 👻	User Management 🔻	Bulk Administration 👻	Help 👻			
Find and	l List Users									
Add	New Select	All 🔛 Clear All 💥 Dele	te Selected							
Status -	r Status									
User	(1 - 3 of 3)								Rows pe	er Page S0 🗸
Find Use	r where First na	me v beg	ins with 🗸		Find Clear Fi	ter 🕂 🛥				
	User ID *	Meeting Number	First Name	Last Name	Department	Directo	ry URI	User St	tatus	User Rank
	gstacy	2183	Gwen	Stacy		gstacy@	.com	Active Enabled LDAP Synchron	ized User	1
	hosborn	2182	Harry	Osborn		hosborn@	.com	Active Enabled LDAP Synchron	ized User	1
	pparker	2181	Peter	Parker		pparker@:	.com	Active Enabled LDAP Synchron	ized User	1

Etapa 4. Navegue até a página ccmuser (https://<endereço ip do cucm pub>/ccmuser) para verificar se o logon do usuário foi bem-sucedido.

A página ccmuser do CUCM versão 12.0.1 é semelhante a esta:

Cisco Se	Unified Communicated Communicat	ations al
	Username	
	Password	
	Sign In	

O usuário pode fazer login com êxito depois que as credenciais LDAP são inseridas, como mostrado na imagem:



Configurar Autenticação LDAP Segura

Configure a autenticação LDAP do CUCM para utilizar a conexão TLS LDAPS com o AD na porta 3269.

Navegue até CUCM Administration > System > LDAP Authentication. Digite o FQDN do servidor LDAPS para Informações do servidor LDAP. Especifique a porta LDAPS de 3269 e marque a caixa para Usar TLS, como mostrado na imagem:

deale Cisco Unified	CM Administration		Navigation Cisco Unified CM Administration	60
CISCO For Cisco Unified Co	mmunications Solutions		admin Search Documentation About	Logout
System - Call Routing - Media Reso	ources • Advanced Features • Device • Application • User Ma	nagement 🔻 Bulk Administration 👻 Help 💌		
LDAP Authentication				
Save				
Status				
Update successful				
LDAP Authentication for End Us	ers			
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]		
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			
•				



Observação: se você tiver clientes Jabber, é recomendável usar a porta 3269 para autenticação LDAPS, pois o tempo limite do Jabber para logon poderá ocorrer se uma conexão segura com o servidor de catálogo global não for especificada.

Configurar conexões seguras com o AD para serviços de UC

Se precisar proteger serviços UC que utilizam LDAP, configure esses serviços UC para utilizar a porta 636 ou 3269 com TLS.

Navegue até Administração do CUCM > Gerenciamento de usuário > Configurações do usuário > Serviço UC. Localize o Serviço de Diretório que aponte para AD. Digite o FQDN do servidor LDAPS como o nome do host/endereço IP. Especifique a porta como 636 ou 3269 e protocolo TLS, como mostrado na imagem:

Cisco U For Cisco U	nified CM Administration	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 Configurati	on	Related Links: Back To Find/List 🗸 Go
🔜 Save 🗙 Delete [🗋 Copy 🎦 Reset 🥒 Apply Config 🛟 Add New	
Status		
(i) Update successful		
UC Service Informatio	0	
UC Service Type:	Directory	
Product Type*	Directory v	
Name*	Secure Directory	
Description		
Host Name/IP Address*	WIN-H2074S1U39R .com	
Port	636	
Protocol	TLS	
Save Delete C	opy Reset Apply Config Add New	
(i) *- indicates require	d item.	



Observação: as máquinas cliente Jabber também precisam ter os certificados LDAPS tomcat-trust que foram instalados no CUCM instalado no armazenamento confiável de gerenciamento de certificados da máquina cliente Jabber para permitir que o cliente Jabber estabeleça uma conexão LDAPS com o AD.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Para verificar a cadeia real de certificado/certificado LDAPS enviada do servidor LDAP para o CUCM para a conexão TLS, exporte o Certificado TLS LDAPS de uma captura de pacote CUCM. Este link fornece informações sobre como exportar um certificado TLS de uma captura de pacote CUCM: <u>Como exportar o certificado TLS da captura de pacote CUCM</u>

Troubleshooting

No momento, não há informações específicas disponíveis para solucionar esse problema de configuração.

Informações Relacionadas

- Esse link fornece acesso a um vídeo que percorre as configurações de LDAPS: <u>Secure</u> <u>LDAP Diretory and Authentication Walkthrough Video</u>
- <u>Suporte Técnico e Documentação Cisco Systems</u>

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.