Gerenciar certificado de componentes PCCE para SPOG

Contents

Introduction **Prerequisites** Requirements Componentes Utilizados Informações de Apoio Nova interface de usuário - SPOG Exportação de certificado SSL Estação de trabalho de administração (AW) Finesse **Cisco ECE** CUIC IDs da Cisco LiveData **VVB** Importação de certificado SSL para armazenamento de chaves Servidor de Chamadas CVP e Servidor de Relatórios Estação de Trabalho Administrativa Finesse, CUIC, Cisco idS e VVB Troca de certificado entre Finesse e CUIC/LiveData

Introduction

Este documento descreve como trocar os certificados SSL autoassinados pela Estação de Trabalho Administrativa (AW) para o Portal de Voz do Cliente (CVP), Finesse, Cisco Enterprise Chat and Email (ECE), Cisco Unified Intelligence Center (CUIC), Cisco Identity Service (idS) e Virtualized Voice Browser (VVB) para Painel de Vidro Único do Package Contact Center Enterprise (PCCE) (SPOG).

Contribuído por Nagarajan Paramasivam e Robert Rogier, engenheiros do Cisco TAC.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Pacotes/Unified Contact Center Enterprises (PCCE/UCCE)
- Plataforma VOS
- Gerenciamento de Certificados

Armazenamento de chaves de certificado

Componentes Utilizados

As informações neste documento são baseadas nestes componentes:

- Estação de trabalho administrativa (CCEADMIN/SPOG)
- CVP
- Finesse
- CUIC, IDS
- VVB
- Cisco ECE

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Recomenda-se que você tenha lido e compreendido o Guia de Administração e Configuração do PCCE, especificamente o apêndice de Referência no final, que abrange a configuração e a configuração do certificado. <u>Guia de administração e configuração do PCCE</u>

Nova interface de usuário - SPOG

O Packaged CCE 12.0 tem uma nova interface de usuário que está de acordo com outras aplicações da central de contatos. A interface de usuário permite que você configure a solução por meio de um aplicativo. Entre no novo Unified CCE Administration em https://<IP Address>/cceadmin. <Endereço IP> é o endereço do AW do Side A ou B do Unified CCE ou do HDS externo opcional.

Nesta versão, a interface do Unified CCE Administration permite configurar:

- Campanhas
- Cortesia de retorno
- Grupos de servidores SIP
- Transferências de arquivo: A transferência de arquivos é possível somente através do AW principal (AW do lado A em 2000 implantação de agente e AW configurado em 4000 implantações de agente e 12000 implantações de agente).
- Padrões de roteamento: O padrão do número discado no Unified CVP Operations Console agora é chamado de Padrão de roteamento no Unified CCE Administration.
- Locais: No Unified CCE Administration, o código de roteamento agora é o prefixo do local em vez da ID do site.
- Configuração do dispositivo: O Unified CCE Administration permite configurar os seguintes dispositivos: CVP Server, CVP Reporting Server, VVB, Finesse, Identity Service (Configuração de login único).
- Recursos da equipe: O Unified CCE Administration permite definir e associar os seguintes recursos para equipes de agentes: Layout das variáveis de chamada, layout da área de trabalho, agendas telefônicas, fluxos de trabalho, motivos (Não pronto, encerrar sessão, finalizar).

• E-mail e bate-papo

Antes de tentar gerenciar o sistema por meio do SPOG, é necessário trocar os certificados SSL entre o Customer Voice Portal (CVP), Finesse, Cisco Enterprice Chat and Email (ECE), Cisco Unified Intelligence Center (CUIC), Cisco Identity Service (idS) e Virtual Voice Browser (VVB) e Admin Workstation (AW) para estabelecer uma comunicação de confiança.

Exportação de certificado SSL

Estação de trabalho de administração (AW)

Etapa 1. Acesse o<u>URL https://localhost</u> no servidor AW e faça o download dos certificados SSL do servidor.



Etapa 2. Na janela de certificado, navegue até a guia Detalhes e clique no botão Copiar para arquivo.



Etapa 3.Selecione X.509 (CER) codificado na base 64 e armazene o certificado no armazenamento local.



Finesse

Etapa 1. Acesse o https://Finesseserver:8443/cmplatform e baixe o certificado tomcat.



Etapa 2. Na janela de certificado, navegue até a guia Detalhes e clique no botão Copiar para arquivo.

Etapa 3. Selecione X.509 (CER) codificado em Base 64 e armazene o certificado no armazenamento local.

	THEFT & LOURSER CO & Call			r 6	100-1-17
	New T	two endired	fight .	140	
-	Carlos	12-09-2016 15-09 12-09-2016 15-09	Source Centrary Source Centrary		240 240
	California and	0.00.000.000	Include Cattlense		246

Cisco ECE

Etapa 1. Acesse o https://ECEWebServer e baixe o certificado SSL do servidor.



Etapa 2. Na janela de certificado, navegue até a guia Detalhes e clique no botão Copiar para arquivo.

Etapa 3. Selecione X.509 (CER) codificado em Base 64 e armazene o certificado no armazenamento local.

Takin.	Can multiple	1.00	104
12 and on	10.00 (200 (1.00)	Investment	198
12 Additor	1-14-224 1228	heirty Catholie	110
10 ACM/VP	10.00.0000.0000	Innally Carrings	1198.
12408-0	11-00-0110 75/4	Salaria California	1.64

CUIC

Etapa 1. Acesse o https://CUICServer:8443/cmplatform e baixe o certificado tomcat.



Etapa 2. Na janela de certificado, navegue até a guia Detalhes e clique no botão Copiar para arquivo.

Etapa 3. Selecione X.509 (CER) codificado em Base 64 e armazene o certificado no armazenamento local.

	NUTL & LOUGHNEED & CAL-			· · · · · · · · · · · · · · · · · · ·
	None -	interesting.	(for	24
	C ANALM	10-09-009-03/9	Includy Cartilly also	119
*	CQ AND on	10-49-2014 TB/W	Secondy Cardinale	118
hini i	CHOK.mm	10 pt (21 10 pt 11	Density Destitution	118
	C# CHURCH OF	15-26-2019-06-201	Jacoby Cattlength	1.00
	Top HOLLAN	10-04-0018 Talle	Security Cathlopie	
	C2 Web.in	10-09-2019 (3-9)	Samaly Carbleon.	- 248

IDs da Cisco

Etapa 1. Acesse o https://IDSServer:8553/idsadmin/ e baixe o certificado tomcat.



Etapa 2. Na janela de certificado, navegue até a guia Detalhes e clique no botão Copiar para arquivo.

Etapa 3. Selecione X.509 (CER) codificado em Base 64 e armazene o certificado no armazenamento local.

	tere .	The southed	141	
	12 Adda.com	12-08-0419-10-08	through Landson	3.68
etc :	LL ANNUA	11-00-021112-02	Security Calificate	3.488
nin 1	To Oblance	11-00-2010-00107	Security Carolinate	1.48
	THE CONCELSES	14-08-029-030-07	Second Laboration	0.00
	SQ FPH-OF	12-46-2010 12:00	Second General	248
	To Pathon	10 cm land holds	Include Cathlands	0.000
	Cig (Children)	15-00-0291-00/07	South California	248
	California (California)	15-06-0014-06/07	Investo Carolinani	10.00

LiveData

Etapa 1. Acesse o https://LiveDataServer:8444/cuic/gadget/LiveData/ e baixe o certificado tomcat.



Etapa 2. Na janela de certificado, navegue até a guia Detalhes e clique no botão Copiar para arquivo.

Etapa 3. Selecione X.509 (CER) codificado em Base 64 e armazene o certificado no armazenamento local.

	No.PC & Goodballoo x Get		1.00	(A) Derivite
	here *	Des worthat	1.04	Sec
	C Antoniour	104-011-028	Security Entries	140
÷.	Contract of the second	101-061-0018-01-02	betung Detrives	3.448
to:	CE CECKINF	0.44.000.002	Balany Carthole	1.46
	G Other	15.06.0014.0014	Annually (unifying)	110
	Cil Photo.com	10-09-0713-0124	Security Celificate	198
	(2768.cm)	10.05.275.019	Security Centilians	199
	C2 Whitem	10-08-00144-00-07	Innerty Lintcharp	1.04
	(1) 000um	114.244-017	Industry Continues	140
	[] liveletator	12-08-0218-08187	Security Certificate	1.00
	122 Graduation	0.26-2214-00.07	laute Calificate	140

VVB

Etapa 1. Acesse o https://VVBServer/appadmin/main e baixe o certificado tomcat.



Etapa 2. Na janela de certificado, navegue até a guia Detalhes e clique no botão Copiar para arquivo.

Etapa 3. Selecione X.509 (CER) codificado em Base 64 e armazene o certificado no armazenamento local.

	and a residence of the			
	time .	The weather	7.00	Sec. 1
	Tel Artelant	10-09-0474 (AVM	Texasty Cardooni	2.48
÷	TH AND OF	0.04.049.038	Investigation and a second science	2.98
	Tel Chica.com	16 de 2019 de 11	Security Carolinate	0.68
	12 OKOLON	100.06-2010.06.07	Investige Carthouse	118
	12 Healing	10.05.000076.00	Innets Cardoom	148
	California.com	10-04-07911538	Density Carolinase	1.01
	12-05e.ce	10.00.00000000	Talanta Cardinian	148
	12-018.im	20-08-001000-01	Design Tarritore	148
	Tatosheak.cer	100.00-2019-00127	Initial Cardinate	148.7
	T2 lond and co	10108-0018-0047	Investige Carefronte	1.48
	12 Weiger	10.05-051917-018	Incode Cartholine	1481
	C2 WHILE	10.00.0000000000	Canada, Carolinata	1.08

Importação de certificado SSL para armazenamento de chaves

Servidor de Chamadas CVP e Servidor de Relatórios

Etapa 1. Faça login no servidor CVP e copie os certificados AW CCE Admin para o **diretório** C:\cisco\cvp\conf\security.

	tenti e terestine (11 e cher e chi	a used a secondar		+ 41	ine in
	fore 1	Descention	for	24	
	13 Hepters	19-08-2019-20-01	vertilena.		110
18	100 0000	12-28-209-509	Swanty Celificate		2.492
id on	1000	1.06.019.029	Second General		1.40

Etapa 2. Navegue até **%CVP_HOME%\conf** e abra security.properties para copiar a senha do Keystore.

	termine and the second se	Sale restlies	Sec.	14	
	(and)	a state of the	Manager al Ala		148
-	Market and a second second				
	the Lat Annual Time Help			-	

Etapa 3. Abra o prompt de comando como administrador e execute o comando **cd %CVP_HOME%\jre\bin**.



Etapa 4. Use este comando para importar os certificados AW para o servidor CVP.

keytool -import -trustcacerts -keystore %CVP_HOME%\conf\security\.keystore -storetype JCEKS - alias awa.nag.com -file C:\Cisco\CVP\conf\security\AWA.cer

Chinese Constanting and the start of the second start of the secon

Etapa 5. No prompt de senha, cole a senha copiada de security.properties.

Etapa 6. Digite **yes** para confiar no certificado e garantir que o resultado **Certificado foi adicionado ao keystore.**



Passo 7. Há um aviso avisado junto com a importação bem-sucedida. Isso é devido ao formato proprietário Keystore, você pode ignorá-lo.

aviso:

O armazenamento de chaves JCEKS usa um formato proprietário. É recomendável migrar para PKCS12, que é um formato padrão do setor usando "keytool -import-srckeystore C:\Cisco\CVP\conf\security\.keystore -destkeystore C:\Cisco\CVP\conf\security\.keystore - deststoretype pkcs12".

dare bend	100100100000000000000000000000000000000
the ACRES beneficing atoms is prosperinting disposed, by in party	empieded (a schrede to PK
there. Conditional and the second resident at the therein the	Case of the second second second
itr'sbrychers -destatorstype plants".	

Estação de Trabalho Administrativa

Etapa 1. Faça login no servidor AW e abra o prompt de comando como administrador.

Etapa 2. Navegue até C:\Program Files(x86)\Java\jre1.8.0_181\lib\security and ensure the cacerts file exist.

	Auto A.	Tan motion	7,94	int.
	a entry	10-04-0110-0110	Roa Automo-	
÷ .	Max Adve	to be directure.		110
***	Mainteniumb	This Jin 1919	COPPLEM .	110
	intern b	0.04.009.014	The .	114/9
	produce	10104-0010-0010	AUGUSTIN .	140
	(produced by	10.04.079.10.10	manni Fa	0.01
	(anterial delive)	2014/01/01/01	Rischie	
	In case of the second	Trans. Street Spring	Laboration in the second	1.00

Etapa 3. Digite o comando cd %JAVA_HOME% e digite.

C:\>ed	×JAU	A_HOME	De l	
CINPros	Iran	Files	(x86)\Java\jre1.8.0	181)

Etapa 4. Use este comando para importar os certificados Finesse para o servidor AW.

keytool -import -file C:\Users\Administrator.NAG\Downloads\Cert\FINA.cer -alias fina.nag.com-

Collemptin Films (2003) Oncolleged E.R. (8) Reported -tagent -Film Colleged Medican and a Million lands (2003) Million - allow Filmstery and Reporters - (2005) and of point

Etapa 5. Na primeira vez que utilizar esta ferramenta de chave, utilize a **alteração de** senha para alterar a senha de um arquivo de certificados.

Etapa 6. Insira uma nova senha para o Keystore e insira novamente para confirmar a senha.



Passo 7. Digite **yes** para confiar no certificado e garantir que você obtenha o resultado **Certificado** adicionado ao keystore.



Note: As etapas 1 a 7 devem ser repetidas com todos os outros nós Finesse e todos os nós CUIC também

Etapa 8. Se a senha do keystore tiver sido inserida incorretamente ou executado sem redefinir, é esperado que ela obtenha essa exceção.

Confiar neste certificado? [não]: sim

O certificado foi adicionado ao keystore

erro de ferramenta de chave: java.io.FileNotFoundException: .\lib\security\cacerts (O sistema não consegue encontrar o caminho especificado)

Digite a senha do armazenamento de chaves: erro de ferramenta de chave: java.io.IOExceção: Keystore foi violado ou a senha estava incorreta

Etapa 9. Para alterar a senha do armazenamento de chaves, use esse comando e reinicie o procedimento novamente da Etapa 4 com a nova senha.

keytool -storepasswd -keystore .\lib\security\cacerts

Erdingene Viles (oblisions)erd.8.6,0000eptex) -mempared dispersor .ddfree participationers participationers participationers for features pareners for features pareners for features and hyperex pareners

Etapa 10. Após a importação bem-sucedida, use este comando para exibir o certificado do keystore.

keytool -list -keystore .\lib\security\cacerts -alias fina.nag.com

keytool -list -keystore .\lib\security\cacerts -alias cuic.nag.com



Finesse, CUIC, Cisco idS e VVB

Etapa 1. Faça login na página de administração do SO do servidor Finesse e carregue os certificados SSL AW na confiança tomcat.

Etapa 2. Navegue até OS Administration > Security > Certificate Management.

The second s	THE R. LANSING MICH.			
COLUMN TWO IS NOT				
- management of the second sec	the second second			
Contra bit of				
the second second				
THE PARTY NAMES AND ADDRESS OF				
and the second second	the second second second second	and the second se	and the second se	the second se
the second secon	a bolow he complianted	second on the support of the second	section or other privation	the state of the s
All and a second	100 I			-
the second	station into the state	10000-0	diada includes	
	And and a second second	and the second s		
	- TAN 10 - 10 - 10		10.00	
	and a second			
and the second s			and a second sec	
the second se			a construction of the second s	

Etapa 3. Clique em Carregar certificado\cadeia de certificados e selecione o tomcat-trust no menu suspenso.

Etapa 4. Navegue pelo armazenamento de certificados no armazenamento local e clique no botão Carregar.

Same R ton			
Partus () Ramma Carinating a C	uder-ede antificate et distribute (a artamana in Ora planter	
And Contractor, Co	ale chain		
Enterplant/handy care) Uploal file	Dura fitte 1000 cm		
(spear) (diss.)			
· seture report her.		A	

Etapa 5. Repita as etapas para carregar todo o certificado do servidor AW para o cluster Finesse.

Note: Não é necessário carregar o certificado tomcat-trust para o nó secundário, isso é replicado automaticamente.

Etapa 6. Reinicie o serviço tomcat para que as alterações de certificado entrem em vigor.

Passo 7. No CUIC, IDS e VVB, siga as etapas de 2 a 4 e carregue o certificado AW.

Troca de certificado entre Finesse e CUIC/LiveData

Etapa 1. Mantenha os certificados Finesse, CUIC e LiveData em uma pasta separada.

	Tagend .	Data-readilitat	140	104	
	CO RADAR	11-01-07-01-01	Second Contrasts		i sali.
60	DOM: +	11-18-1219-12121	Investo Cettinate		3,480
**	Call Philocol	12-04-2012/044	Samply Light and		1.66
	100 1100 yes	10.000.0000.004	Investig-Contraste		1.00
	The Excellence	11-09-22-9-0031	Security Calificate		1.00
	(i) instead or	11.04.014.001	Inches Contrast		100

Etapa 2. Faça login na página Finesse, CUIC e LiveData OS Administration.

Etapa 3. Navegue até OS Administration > Security > Certificate Management.

Etapa 4. Clique em Carregar certificado\cadeia de certificados e selecione o tomcat-trust no menu

suspenso.

Etapa 5. Navegue pelo armazenamento de certificados no armazenamento local e selecione Certificado de servidor como abaixo e clique no botão Carregar.

No servidor Finesse - CUIC e LiveData como confiabilidade Tomcat

No servidor CUIC - Finesse e LiveData como confiança tomcat

No LiveData Server - CUIC e Finesse como confiabilidade Tomcat

Note: Não é necessário carregar o certificado tomcat-trust para o nó secundário, isso é replicado automaticamente.

Etapa 6. Reinicie o serviço tomcat em cada nó para que as alterações de certificado entrem em vigor.