Zertifikat für PCCE-Komponenten für SPOG verwalten

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Neue Benutzeroberfläche - SPOG SSL-Zertifikatsexport Verwaltungs-Workstation (AW) Finesse **Cisco ECE** CUIC Cisco IDs LiveData **VVB** Importieren von SSL-Zertifikaten in Keystore **CVP-Anrufserver und Reporting-Server** Administrator-Workstation Finesse, CUIC, Cisco IDS und VVB Zertifikataustausch zwischen Finesse und CUIC/LiveData

Einführung

In diesem Dokument wird beschrieben, wie Sie die selbstsignierten SSL-Zertifikate der Admin Workstation (AW) an das Customer Voice Portal (CVP), Finesse, Cisco Enterprise Chat and Email (ECE), Cisco Unified Intelligence Center (CUIC), Cisco Identity Service (IDS) und Virtualized Voice Browser (VB) for Package Contact Center Enterprise (PCCE) Single Pane of Glass (SPOG) austauschen.

Unterstützt von Nagarajan Paramasivam und Robert Rogier, Cisco TAC Engineers.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Packaged/Unified Contact Center Enterprises (PCCE/UCCE)
- VOS-Plattform
- Zertifikatsverwaltung

Zertifikatsschlüssel

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Komponenten:

- Admin-Workstation (CCEADMIN/SPOG)
- CVP
- Finesse
- CUIC, IDS
- VVB
- Cisco ECE

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Es wird empfohlen, den PCCE-Administrations- und Konfigurationsleitfaden, insbesondere den Referenzanhang am Ende, in dem die Zertifikateinrichtung und -konfiguration behandelt werden, zu lesen und zu verstehen. <u>PCCE-Administrations- und</u> <u>Konfigurationsleitfaden</u>

Neue Benutzeroberfläche - SPOG

Packaged CCE 12.0 verfügt über eine neue Benutzeroberfläche, die mit anderen Contact Center-Anwendungen übereinstimmt. Über die Benutzeroberfläche können Sie die Projektmappe über eine Anwendung konfigurieren. Melden Sie sich bei der neuen Unified CCE Administration unter https://<IP-Adresse>/cceadmin an. <IP-Adresse> ist die Adresse der Seite A oder B Unified CCE AW oder des optionalen externen HDS.

In dieser Version können Sie mit der Unified CCE Administration-Schnittstelle Folgendes konfigurieren:

- Kampagnen
- Rückruf mit freundlicher Genehmigung
- SIP-Servergruppen
- Dateiübertragungen: Die Dateiübertragung ist nur über das Principal AW möglich (Seite A AW bei der Bereitstellung von Agenten im Jahr 2000 und konfigurierte AW in Bereitstellungen mit 4.000 Agenten und 1.200 Agenten).
- Routingmuster: Das Nummernmuster in der Unified CVP Operations Console heißt jetzt Routing Pattern in der Unified CCE Administration.
- Standorte: In der Unified CCE-Administration ist Routingcode jetzt das Standortpräfix anstelle der Standort-ID.
- Gerätekonfiguration: Die Unified CCE Administration ermöglicht die Konfiguration der folgenden Geräte: CVP-Server, CVP Reporting Server, VVB, Finesse, Identity Service (Single Sign-on Setup).
- Teamressourcen: Mithilfe der Unified CCE Administration können Sie die folgenden Ressourcen für Agenten-Teams definieren und zuordnen: Layout der Anrufvariablen,

Desktop-Layout, Telefonbücher, Workflows, Gründe (nicht bereit, Abmelden, Zusammenfassung)

E-Mail und Chat

Bevor das System über SPOG verwaltet werden kann, müssen die SSL-Zertifikate zwischen Customer Voice Portal (CVP), Finesse, Cisco Enterprice Chat and Email (ECE), Cisco Unified Intelligence Center (CUIC), Cisco Identity Service (IDS) und Virtual Voice Browser (VVB) sowie Admin Workstation (AW) ausgetauscht werden, um eine Vertrauenskommunikation aufzubauen.

SSL-Zertifikatsexport

Verwaltungs-Workstation (AW)

Schritt 1: Rufen Sie die <u>https://localhost URL</u> im AW-Server auf, und laden Sie die SSL-Serverzertifikate herunter.



Schritt 2: Navigieren Sie im Zertifikatsfenster zur Registerkarte Details, und klicken Sie auf die Schaltfläche In Datei kopieren.

100	16.4	-
THE REAL PROPERTY AND ADDRESS OF ADDRES	NO.	
Server runder	10 10 10 18 12 19 10 19 10	1.0
Senature aquirem	sharten a	
odvariate user adouter	and that can	
Calif. Burn	12 444 2010 10-01-20	
rest of the	10 844 3039 10 41 10	
Address	and class class	12

Schritt 3: Wählen Sie Base-64-codiertes X.509 (CER) aus, und speichern Sie das Zertifikat im lokalen Speicher.

 Terft + Leatin+(1) + Cel			* ¢]	Innet Carl
Nets P	Tax matter	1 per	144	
12 Melline	219.811.910	International States		344
and and an	10168-0019 (0.56	incustry Centry	-	189

Finesse

Schritt 1: Rufen Sie das <u>https://Finesseserver:8443/cmplatform</u> auf, und laden Sie das Tomcat-Zertifikat herunter.



Schritt 2: Navigieren Sie im Zertifikatsfenster zur Registerkarte Details, und klicken Sie auf die Schaltfläche In Datei kopieren.

Schritt 3: Wählen Sie Base-64-codierte X.509 (CER) aus, und speichern Sie das Zertifikat im lokalen Speicher.

	the PC + Louis Shield in + Gal-			- 6 [inst-10
	New *	the entrol	fight .	ine .
	12 https://	to-on-anny ison	Internetly Common	ry 199
÷	G AND.com	12-05 2010 (0.06	Security Carries	 2x0
ion -	C Passion	205.011168	Desirely Desiring	 110.
	12 Mail.com	0.08.200.018	Include Cattley	a 346

Cisco ECE

Schritt 1: Rufen Sie das <u>https://ECEWebServer</u> auf, und laden Sie das SSL-Serverzertifikat herunter.



Schritt 2: Navigieren Sie im Zertifikatsfenster zur Registerkarte Details, und klicken Sie auf die Schaltfläche In Datei kopieren.

Schritt 3: Wählen Sie Base-64-codierte X.509 (CER) aus, und speichern Sie das Zertifikat im lokalen Speicher.

Sam	Data-month Aut	7.00	104	
12 answer	10.00 (200 (1.00)	Investigation		198
12 AML IN	5-16-225 12:28	Incompliant forthe		110
14 ACEA	10.08.000 10.05	Innaki Carringe		1198.
12408.00	10.00.000.05.00	Sample California		1.84

CUIC

Schritt 1: Rufen Sie das <u>https://CUICServer:8443/cmplatform</u> auf, und laden Sie das Tomcat-Zertifikat herunter.



Schritt 2: Navigieren Sie im Zertifikatsfenster zur Registerkarte Details, und klicken Sie auf die Schaltfläche In Datei kopieren.

Schritt 3: Wählen Sie Base-64-codierte X.509 (CER) aus, und speichern Sie das Zertifikat im lokalen Speicher.

4.4	No.PC + Location Co. + Carl			· dy hearing
	Mana -	interesting.	Terr	10.0
	C ANALM	T-0-201013/W	Includy Cartily also	119
-	C AND or	10-49-30YETE/W	Deverty Cardinate	118
hini i	CHOKAN	10 de - primilion 1	(Incode Destination)	118
	C# CHURNER	15.06.2019-06101	Jacoby (without)	1.44
	The Poly of	10-04-2019 Talle	Security Cathlopie	218
	C2 Web.in	10-09-2019 (3-9)	Samaly Carbleon.	2.08

Cisco IDs

Schritt 1: Rufen Sie das https://IDSServer:8553/idsadmin/ auf, und laden Sie das Tomcat-Zertifikat herunter.



Schritt 2: Navigieren Sie im Zertifikatsfenster zur Registerkarte Details, und klicken Sie auf die Schaltfläche In Datei kopieren.

Schritt 3: Wählen Sie Base-64-codierte X.509 (CER) aus, und speichern Sie das Zertifikat im lokalen Speicher.

	Tania .	The sufficient	100	. 24
	12 Adda.com	12-08-0812-10-08	through Landson	3.68
etc -	La Antice	11-00-021112-0	Security Calificiate	3.488
iline 👘	To Oblance	11.40.0011.0017	last of the Part of the same	1.08
	op OpCham	10-00-0229-026/97	Security Latitudes	1.00
	G PH-OF	12-60 2010 1208	Second Generalized	218
	To Path and	11 (B) (3714 (m))(B)	Include Cardinani	0.00
	100 KEA.00	15-00-09100/07	South Gentlow	248
	14 ST8-10	15-06-0014-00/07	Investo Cardinani	1.68

LiveData

Schritt 1: Rufen Sie das <u>https://LiveDataServer:8444/cuic/gadget/LiveData/</u> auf, und laden Sie das Tomcat-Zertifikat herunter.



Schritt 2: Navigieren Sie im Zertifikatsfenster zur Registerkarte Details, und klicken Sie auf die Schaltfläche In Datei kopieren.

Schritt 3: Wählen Sie Base-64-codierte X.509 (CER) aus, und speichern Sie das Zertifikat im lokalen Speicher.

	here *	Determonthalt	1,04	ine
	C Antha Con-	10/8/2011/028	Security Earthform	140
÷.	Contract of the second	101-041-0018-01-04	betang Deblyses	3.448
kon i	CIRCA INF	10-18-2000 (RVZ)	Balance Cartholia	140
	G ONNer	15.06.000 min.ht	Annual Contract	1108
	C Photos	11-09-0715-15.54	Interly Delificate	198
	G PAB.co	1045-201-018	Security Carthone	199
	G Chier	10-08-00144-00-07	Innerty Lintchase	1.010
	(2 05burg	114.249-017	Industry Continues	140
	[] hereficial and	10-08-0218-08187	Security Destillation	1.000
	12 Graduate or	0.06.2214 (0.02)	Intellig Coldinate	140

VVB

Schritt 1: Rufen Sie das <u>https://VVBServer/appadmin/main</u> auf, und laden Sie das Tomcat-Zertifikat herunter.



Schritt 2: Navigieren Sie im Zertifikatsfenster zur Registerkarte Details, und klicken Sie auf die Schaltfläche In Datei kopieren.

Schritt 3: Wählen Sie Base-64-codierte X.509 (CER) aus, und speichern Sie das Zertifikat im lokalen Speicher.

The PC + local that ICo + Cell -		+ 0.	144-11-04
tere .	The worked	Ter be	
Tel Allahow	0.0400110.00	Terrority Construme	248
THE ADD OF	12-08-20-9-12-08	Incusty-Cambridge	248
 T2 CHCs.or	5 (B. (2010) (B. (7))	Densely Carolinate	1.00
12 CHORAS	100 ph (photo stat)	Density Carthoute	118
12 Healing	10.05-0018 (10.08	Density Cardioum	148
California.com	10-04-000 class	Density Carolicom	1.01
12-105e.or	10.00.000000000	Taluth Cathline	148
12 million	10-08-001010-01	Decorp Danishum	148
12 to abrah car	10.04-2019-04:07	Initially Carolinson	148.7
Contraction -	101 08-2019 00/07	territy Carefulate	1.00
12 Webser	10.05-021010-044	Describe Carthlene	148
C2 William	10.00.000000000	Canada, Cambrida	1.01

Importieren von SSL-Zertifikaten in Keystore

CVP-Anrufserver und Reporting-Server

Schritt 1: Melden Sie sich beim CVP-Server an, und kopieren Sie die AW CCE-Administratorzertifikate auf die C:\cisco\cvp\conf\security.

	THEP: & Amatheactic & Chair & C	phane a bar of t		- 0.1	incards into the
	fare 1	Descention	for.	200	
	13 Heynes	19-08-2019-2019	vitrilities.		110
- 8	10 P.M.	12-24-229-529	incode Calification		2.49
id on	Carlos .	1.44.474.128	Second General		1.46

Schritt 2: Navigieren Sie zu **%CVP_HOME%\conf**, und öffnen Sie die security.properties, um das Keystore-Kennwort zu kopieren.

	term .	Sale incident	Sec.	14	
	2 marts	-	International Vision		148
-	Market and a second second				and a start of the
	The Lat Average Time Help		and the second second second	1000	

Schritt 3: Öffnen Sie die Eingabeaufforderung als Administrator, und führen Sie den Befehl **cd %CVP_HOME%\jre\bin aus**.



Schritt 4: Verwenden Sie diesen Befehl, um die AW-Zertifikate in den CVP-Server zu importieren.

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

Constant and a second sec

Schritt 5: Fügen Sie an der Kennworteingabeaufforderung das aus den security.properties kopierte Kennwort ein.

Schritt 6: Geben Sie **yes ein**, um dem Zertifikat zu vertrauen, und stellen Sie sicher, dass das Ergebnis-**Zertifikat zum Keystore hinzugefügt wurde.**



Schritt 7: Bei einem erfolgreichen Import wird eine Warnung angezeigt. Das liegt an dem proprietären Format Keystore, das Sie ignorieren können.

Warnung:

Der JCEKS-Keystore verwendet ein proprietäres Format. Es wird empfohlen, zu PKCS12 zu migrieren, einem Standardformat, das "keytool -importkeystore -srckeystore C:\Cisco\CVP\conf\security\.keystore -destkeystore C:\Cisco\CVP\conf\security\.keystore - deststoretype pkcs12" verwendet.

the JCDS Aparters are a proprieture farmer, 11 is set	simpleded by adjoints to PE
All eldes is an industry stabilized formet union flogter	C. The state of the second second
	 A CONTRACTOR STREET OF STREET

Administrator-Workstation

Schritt 1: Melden Sie sich beim AW-Server an, und öffnen Sie die Eingabeaufforderung als Administrator.

Schritt 2: Navigieren Sie zu C:\Program Files(x86)\Java\jre1.8.0_181\lib\security and ensure the cacerts file exist.

	Name -	Two resided.	7,94	int.
	a entry	10-04-2010 1010	Roa Automo-	
÷	manufact	to be directure.	. 104	110
÷.	maintenture	This Jin 1919	COPPLEM .	110
	Cierci D	10.04.009.004	The .	114/9
	product .	10-04-2010 10-0	ARREST IN C.	140
	- production for	10.04.079 10.16	DOM: NO	0.01
	(an transporting)	2144-0111-011	RILCOM	
	Throughout interests	Trans. Street Spice	Contracted in the	1.00

Schritt 3: Geben Sie den Befehl cd %JAVA_HOME% ein und geben Sie ein.

C:\>ed >	JAVA_H	ONEX			
C:\Progr	an Fil	15 (x86)	Java\jre1.	8.0_181	>

Schritt 4: Verwenden Sie diesen Befehl, um die Finesse-Zertifikate in den AW-Server zu

importieren.

keytool -import -file C:\Users\Administrator.NAG\Downloads\Cert\FINA.cer -alias <u>fina.nag.com</u>-keystore.\lib\security\cacerts

Colleague (Elles Autoritation) and E.S. (10) Present - transm. - File Collearest Medicated a provide Anti-Invalidation (1997) 100 - and 1997 File Autor and Invalidation - Official and Statement (1997)

Schritt 5: Wenn Sie dieses Schlüsselprogramm zum ersten Mal verwenden, können Sie das Kennwort **ändern**, um das Kennwort eines Zertifikatsspeichers zu ändern.

Schritt 6: Geben Sie ein neues Kennwort für den Keystore ein, und bestätigen Sie das Kennwort erneut.



Schritt 7: Geben Sie **yes ein**, um das Zertifikat zu vertrauen, und stellen Sie sicher, dass das Ergebnis-**Zertifikat zum Keystore hinzugefügt wurde.**

Irust	this	cert	ificate	7	(no]:	yes
Certif	icate	WAS	added	to	keysto	1.6

Schritt 8: Wenn das Schlüsselwort falsch eingegeben wurde oder die Schritte ohne Zurücksetzen ausgeführt wurden, wird diese Ausnahme erwartet.

Vertrauen Sie diesem Zertifikat? [Nein]: Ja

Zertifikat wurde dem Keystore hinzugefügt

```
Tastaturfehler: java.io.FileNotFoundException: .\lib\security\cacerts (Das System kann den angegebenen Pfad nicht finden.)
```

Eingabe des Keystore-Kennworts: Tastaturfehler: java.io.IOException: Keystore wurde manipuliert, oder das Kennwort war falsch.

Schritt 9: Um das Keystore-Kennwort zu ändern, verwenden Sie diesen Befehl, und starten Sie das Verfahren erneut mit dem neuen Kennwort von Schritt 4 aus.

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

Er-Orogene Film (officience)er(3.6,900 bepter) -renequired -layeree -clifford participaniers protect harders parametri for harders parametri for harders parametri for harders parametri

Schritt 10: Verwenden Sie nach dem erfolgreichen Import diesen Befehl, um das Zertifikat vom Keystore anzuzeigen.

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

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



Finesse, CUIC, Cisco IDS und VVB

Schritt 1: Melden Sie sich auf der Verwaltungsseite für das Betriebssystem des Finesse-Servers an, und laden Sie die AW SSL-Zertifikate in die Vertrauenswürdigkeit von Tomcat hoch.

Schritt 2: Navigieren Sie zu Betriebssystemverwaltung > Sicherheit > Zertifikatsverwaltung.

and the latest local plane in the same			A Designation		
Arrent State	No.				

Schritt 3: Klicken Sie auf Upload Certificate\Certificate Chain, und wählen Sie in der Dropdown-Liste die Option tomcat-trust aus.

Schritt 4: Durchsuchen Sie den Zertifikatsspeicher im lokalen Speicher, und klicken Sie auf die Schaltfläche Upload (Hochladen).



Schritt 5: Wiederholen Sie die Schritte, um das gesamte AW-Serverzertifikat in das Finesse-Cluster hochzuladen.

Hinweis: Es ist nicht erforderlich, das Zertifikat "tomcat-trust" in den sekundären Knoten hochzuladen. Dies wird automatisch repliziert.

Schritt 6: Starten Sie den Tomcat-Dienst neu, damit die Zertifikatänderungen wirksam werden.

Schritt 7: In CUIC, IDS und VVB folgen Sie den Schritten von 2 bis 4 und laden das AW-Zertifikat hoch.

Zertifikataustausch zwischen Finesse und CUIC/LiveData

Schritt 1: Bewahren Sie die Zertifikate Finesse, CUIC und LiveData in einem separaten Ordner auf.

	Nov. *	Data-readilities	tum .	line.	
	(QUALAN)	this present	Second Contrady		inst.
60 -	Distance.	14-08-0218-0227	Investor Contribution		1.00
-	Lat Planced	1244-01419-014	Second Links		1.000
	1100.00	12.05.00 0.04	Investig-Cellificate		1.00
	California and a second second	11-08-209-0031	Searcy Latinum		100
	The instant or	10.00.000.0001	Desiry Contrast		1.00

Schritt 2: Melden Sie sich bei der Seite Finesse, CUIC und LiveData OS Administration an.

Schritt 3: Navigieren Sie zu Betriebssystemverwaltung > Sicherheit > Zertifikatsverwaltung.

Schritt 4: Klicken Sie auf Upload Certificate\Certificate Chain, und wählen Sie in der Dropdown-Liste die Option tomcat-trust aus.

Schritt 5: Durchsuchen Sie den Zertifikatsspeicher im lokalen Speicher, und wählen Sie "Entweder-Server-Zertifikat" wie unten aus, und klicken Sie dann auf die Schaltfläche Hochladen.

In Finesse Server - CUIC und LiveData als Tomcat Trust

In CUIC Server - Finesse und LiveData als tomcat trust

In LiveData Server - CUIC und Finesse als Tomcat Trust

Hinweis: Es ist nicht erforderlich, das Zertifikat "tomcat-trust" in den sekundären Knoten hochzuladen. Dies wird automatisch repliziert.

Schritt 6: Starten Sie den Tomcat-Dienst für jeden Knoten neu, damit die Zertifikatänderungen wirksam werden.