SPOGのPCCEコンポーネント証明書の管理

内容

概要 前提条件 要件 使用するコンポーネント 背景説明 新しいユーザインターフェイス – SPOG <u>SSL証明書のエクスポート</u> Administration Workstation(AW) Finesse Cisco ECE CUIC Cisco IDS ライブデータ **VVB** キーストアへのSSL証明書のインポート CVPコールサーバおよびレポートサーバ アドミンワークステーション Finesse、CUIC、Cisco idS、およびVVB FinesseとCUIC/LiveData間の証明書交換

概要

このドキュメントでは、Admin Workstation(AW)の自己署名SSL証明書をCustomer Voice Portal(CVP)、Finesse、Cisco Enterprise Chat and Email(ECE)、Cisco Unified Intelligence Center(CUIC)、Cisco Identity Service(idS)、およびVirtualized Voice Browser(VVB)にに交換する の方法について説明しますPackage Contact Center Enterprise(PCCE)Single Pane of Glass(SPOG)。

著者: Cisco TACエンジニア、Nagarajan ParamasivamおよびRobert Rogier

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。

- Packaged/Unified Contact Center Enterprises(PCCE/UCCE)
- VOSプラットフォーム
- •証明書管理
- •証明書キーストア

このドキュメントの情報は、次のコンポーネントに基づいています。

- •アドミンワークステーション(CCEADMIN/SPOG)
- CVP
- Finesse
- CUIC、IDS
- VVB
- Cisco ECE

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、初期(デフォルト)設定の状態から起動しています 。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。

PCCE PCCE

新しいユーザインターフェイス – SPOG

Packaged CCE 12.0には、他のコンタクトセンターアプリケーションに従った新しいユーザイン ターフェイスがあります。ユーザインターフェイスを使用すると、1つのアプリケーションでソリ ューションを設定できます。新しいUnified CCE Administration(https://<IP Address>/cceadmin)に サインインします。<IP Address>は、サイドAまたはサイドBのUnified CCE AWのアドレス、ま たはオプションの外部HDSのアドレスです。

このリリースでは、Unified CCE Administrationインターフェイスを使用して、次の設定を行うことができます。

- ・キャンペーン
- Courtesy Callback
- SIP サーバ グループ
- ファイル転送:ファイル転送は、プリンシパルAW(2000エージェント展開ではサイドA AW、4000エージェント展開および12000エージェント展開では設定AW)でのみ可能です。
- ルーティングパターン: Unified CVP Operations Consoleの着信番号パターンは、Unified CCE Administrationではルーティングパターンと呼ばれるようになりました。
- 場所: Unified CCE Administrationでは、ルーティングコードがサイトIDではなくロケーションプレフィックスになりました。
- デバイス設定:Unified CCE Administrationでは、次のデバイスを設定できます。CVPサーバ、 CVPレポートサーバ、VVB、Finesse、アイデンティティサービス(シングルサインオンのセットアップ)。
- チームリソース: Unified CCE Administrationでは、エージェントチームに次のリソースを定 義して関連付けることができます。コール変数のレイアウト、デスクトップレイアウト、電 話帳、ワークフロー、理由(受信不可、サインアウト、まとめ)
- •電子メールとチャット

SPOGを通じてシステムを管理する前に、Customer Voice Portal(CVP)、Finesse、Cisco Enterprise Chat and Email(ECE)、Cisco Unified Intelligence Center(CUIC)、Cisco Identity Service(idS)、Virtual Voice Browser(VVB)間)で証明書をを交換する必要がありますとAdmin

SSL証明書のエクスポート

Administration Workstation(AW)

ステップ1:AWサーバの<u>https://localhost URLにア</u>クセスし、サーバSSL証明書をダウンロードします。



ステップ2:証明書ウィンドウで、[Details]タブに移動し、[Copy To File]ボタンをクリックします。

	104.4	- 14
ferskin Seral nurder	17 10 et 40 Ja 33 50 fb 30 db	l
Sgnature algorithm Signature hash algorithm	\$4429675A \$14296	
Fald from	15 April 2018 15-41-20	
Laboret	anti-riag.com	14

ステップ3:Base-64 encoded X.509(CER)を選択し、証明書をローカルストレージに保存します。

 NATC & Local Dial (2) & Cold			- 63	Intel Ort
New P	Income in the local division of the local di	1 per	144	
Caretane .	229.031.010	International Constitution		3440
C AVE. at	10168-2019 (2.58	incutty CodPublic		1.000

Finesse

ステップ1:https://Finesseserver:8443/cmplatformにアクセス<u>し、tomcat証明書</u>をダウンロードします。



ステップ2:証明書ウィンドウで、[Details]タブに移動し、[Copy To File]ボタンをクリックします 。

ステップ3:[Base-64 encoded X.509 (CER)]を選択し、証明書をローカルストレージに保存します 。

	iterer .	 See extined	5pt	ia .
	- 100.00	to-on-intervision	Internetly Community	199
÷	G 446.cm	12-05-2010 (0.06	Security Continues -	240
in a	Ci maine	12 (3K-1011 Turk)	Second Development	110
	California -	0.08.200 0.08	Include Calificate	3 milet

Cisco ECE

ステップ1:<u>https://ECEWebServer</u>にアクセスし、サーバのSSL証明書をダウンロードします。



ステップ2:証明書ウィンドウで、[Details]タブに移動し、[Copy To File]ボタンをクリックします。

ステップ3:[Base-64 encoded X.509 (CER)]を選択し、証明書をローカルストレージに保存します。

Sau	Case-month And	Tet	104
12 APRIL OF	2010/02/02 12:08	Investment	198
and and and	5-34-3251 1238	heirty Catholas	110
14 ACEA	10.08.000 10.05	Renards Carefulate	1198.
12108.00	10.00.000.05.00	Salaria California	1.44

CUIC

ステップ1:https://CUICServer:8443/cmplatformにアクセス<u>し、tomcat証明書</u>をダウンロードしま す。



ステップ2:証明書ウィンドウで、[Details]タブに移動し、[Copy To File]ボタンをクリックします 。

ステップ3:[Base-64 encoded X.509 (CER)]を選択し、証明書をローカルストレージに保存します。

	NUME & LOUGHNERS & CAR.			1.0	Tabilit (set
	None -	interested.	100	10.0	
	C ANALM	10-09-009-03/06	Security Carttly also		110
	C AND on	10.49-301x19/W	Develop Carolinate		118
here:	CHOKAN	10 de - prime a con-	Density Destitution		118
	CF CHURNER	15.06.2019-06/01	Jacoby Cathlength		144
	The Poly of	10-09-0019 Talle	Security Centerple		218
	C2 Web.int	10-09-2019 (5-9)	Samely Carblook		218

Cisco IDS

ステップ1:https://IDSServer:8553/idsadmin/にアクセスし、tomcat証明書をダウンロードします。



ステップ2:証明書ウィンドウで、[Details]タブに移動し、[Copy To File]ボタンをクリックします。

ステップ3:[Base-64 encoded X.509 (CER)]を選択し、証明書をローカルストレージに保存します。

	tee .	The suffici	100	
	12 Addam	12-08-0819-10-08	terring Landson	3.68
etc -	LE ANNUA	11-00-001112-00	Security Calificate	3.488
inin 😳	To Oblance	11.46.2019.0017	Security Partness	1.48
	ing COCham	14-06-0214-0217	Second Laboration	0.00
	S 194.00	12-46-2010 12:00	Second General	248
	Top Phillippe	12-Decision inclusion	Include Cathlands	0.000
	CERTIFICATION - CONTRACTOR	15-00-2010-00/27	South California	248
	Car STALLE	15-06-0014-06/07	Investo Cardinani	110

ライブデータ

ステップ1:https://LiveDataServer:8444/cuic/gadget/LiveData/にアクセス<u>し、tomcat証明書</u>をダウ ンロードします。



ステップ2:証明書ウィンドウで、[Details]タブに移動し、[Copy To File]ボタンをクリックします。

ステップ3:[Base-64 encoded X.509 (CER)]を選択し、証明書をローカルストレージに保存します。

	NOPC & GORDARDO & Get		1.14	A Intelli
	tere *	Des worthat	1.04	line .
	C Antoniour	10/8-201-028	Security Contributes	140
	Contract of the second	121-061-0218-15-02	belong indiana.	3.448
de l	CE CECKINF	0.44.000.002	Jalaity Cattoola	148
	G CHOILine	01.08.0074.08.M	Annually (unifying	100
	Ci Phon. Lan	10-09-0715-01-04	Security Continues	198
	C276B.cm	10.05.275.018	Security Centilians	199
	C Chian	10-08-00144-00-07	Investigation in the second second	1.016
	(1) 000um	114.244-017	Industry Continues	140
	Gliveletaler	10-09-0233-00127	Intuity Detificate	100
	T2 Gradutation	Gal-2014-0032	Intelligite Contributes	140

VVB

o

ステップ1:https://VVBServer/appadmin/mainにアクセス<u>し、tomcat証明書</u>をダウンロードします



ステップ2:証明書ウィンドウで、[Details]タブに移動し、[Copy To File]ボタンをクリックします。

ステップ3:[Base-64 encoded X.509 (CER)]を選択し、証明書をローカルストレージに保存します。

	tere .	The wested	100	he
	Tel Allehow	to de larre hum	Terrori, Cardona	248
he i i	TH AND OF	12-18-20-1-12-12	Incompliants and	248
	T2 CHCa.m	10 de 2010 de 11	Incode Carolinate	0.68
	12 ORDere	100 ph 200 million	Incode Carthoute	148
	12 Hoaling	10.05.000 (10.00	Innets Cardoom	148
	Contration	10-04-0791538	Density Cariforni	1.08
	12 iOSecur	10.00.00000000	Taluth Cathline	148
	12 thile	to an internation	Design Tarritore	1.48
	Talandershare .	10.05-2019-06-07	Initial Cardinate	148.
	City Novelland Los	100 006 00010 00007	Security Carefronte	1.43
	12 Weiger	10.05-001010-010	Incode Carthology	1481
	C2 WHILE	10.00.000000000	Canada Cardonas	0.00

キーストアへのSSL証明書のインポート

CVPコールサーバおよびレポートサーバ

ステップ1:CVPサーバにログインし、AW CCE Admin証明書を**C:\cisco\cvp\conf\security**にコピーします。

	Tea PC & Local Date (1) & Chart & Cal	a used a secondar		+ 41	instantion
	fare 1	Descention	for.	24	
	C Heybers	19-08-2019-24-0	virting as		110
18	and a state	10-08-029-529	Investig Calification		1.454
internet.	Call and B	1.44.214.118	Second General		1.46

ステップ2:%**CVP_HOME%\conf\に移動し、**security.propertiesを開いてキーストアパスワードを コピーします。

		termine and the second se	Sale incident	Set.	1.4	
		and a	and strength	HINDING		148
-		Market and a second second				and any -
	10.	the Lat Annual Time Help		and the second second	1000	

ステップ3:コマンドプロンプトをadministratorとして開き、コマンド**cd** %CVP_HOME%\jre\binを実行します。 ステップ4:このコマンドを使用して、AW証明書をCVPサーバにインポートします。

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

Colling Of derivative bestern internet internet bestern 100 1000 and and all y derivative attention ADD allow management film to discussion and and

ステップ5:パスワードプロンプトで、security.propertiesからコピーしたパスワードを貼り付けます。

ステップ6:証明書を信頼**する**ためにyesと入力し、結果が**Certificate was added to keystoreであ** ることを確認します。



ステップ7:インポートの成功とともに警告が表示されます。これは、独自の形式であるキースト アが原因で、無視できます。

警告:

JCEKSキーストアは独自の形式を使用します。「keytool -importkeystore -srckeystore C:\Cisco\CVP\conf\security\.keystore -destkeystore C:\Cisco\CVP\conf\security\.keystore deststoretype pkcs12」を使用して、業界標準の形式であるPKCS12に移行することを推奨します 。

breing) De UER Annethre ann a prophotore farmat (11 ja reinnershiel ja signeta 65) Ald alich 25 an industry frankrika finnen alian "Anatol" (Appertantse ann Anna Criterian (Dirana Finner), Annatar (Anatol) (Appertantse anna Anatol)

アドミンワークステーション

ステップ1:AWサーバにログインし、管理者としてコマンドプロンプトを開きます。

ステップ2:C:\Program Files(x86)\Java\jre1.8.0_181\lib\security and ensure the cacerts file existに 移動します。

	Rana A.	Take resulting	7,00	in.
	a entry	10.04.2010.1010	Roa Automo-	
h	manufact	10-04-DPU Turk	. 104	110
-	maintenture	Think Jone 1978	COPPLEM .	110
	Ciere b	10.04.004.014	The .	114/9
	product .	10104-0010-0010	ARREST IN C.	140
	- manufacture and the	10.04.079.10.16	DOM: NO	0.01
	(an track globble)	2148-0111-011	RILCOM	
	In other in some	Trial data target	CONTRACTOR OF STREET, ST.	1.00

ステップ3:コ**マンドcd %JAVA_HOME%を入力し**て入力します。

C:\>ed xJA	UR_HOM	Ðκ	
C:\Program	Files	(x86)\Java\jre1.8.8	181)_

ステップ4:このコマンドを使用して、Finesse証明書をAWサーバにインポートします。

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

ステップ5:このキーツールを初めて使用するときは、パスワード**changeitを使用**して、証明書ス トアのパスワードを変更します。

ステップ6:キーストアの新しいパスワードを入力し、パスワードを確認するために再入力します 。

curity\cacerts Enter keystore password: New keystore password: Re-enter new keystore password:

ステップ7:証明書を信頼するために「yes」と入力し、結果「Certificate was added to keystore.



注:ステップ1 ~ 7は、他のすべてのFinesseノードとすべてのCUICノードでも繰り返す必要が あります

ステップ8:キーストアのパスワードが誤って入力された場合、またはリセットせずにステップを 実行した場合、この例外が発生すると予想されます。

この証明書を信頼しますか?[no]: あり

証明書がキーストアに追加されました

keytoolエラー:java.io.FiNotFoundException:.\lib\security\cacerts (指定されたパスが見つかりま せん)

キーストアのパスワードを入力: keytoolエラー:java.io.IO例外:キーストアが改ざんされているか、パスワードが正しくありませ ん

ステップ9:キーストアパスワードを変更するには、このコマンドを使用して、ステップ4から新 しいパスワードを使用して手順を再度再起動します。

keytool -storepasswd -keystore \lib\security\cacerts

A company of the second of the

ステップ10:インポートが成功したら、次のコマンドを使用してキーストアからの証明書を表示 します。

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

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



Finesse、CUIC、Cisco idS、およびVVB

ステップ1:FinesseサーバのOS管理ページにログインし、tomcat信頼でAW SSL証明書をアップロードします。

ステップ2:[OS Administration] > [Security] > [Certificate Management]に移動します。

and the local design of	-	7			
Arrent server	Acres,				
and a local					-
II BOTT	-161	Es	No.	(T) 122	-
<u>E</u>					eer-

ステップ3:[Upload Certificate\Certificate Chain]をクリックし、ドロップダウンから[tomcattrust]を選択します。

ステップ4:ローカルストレージの証明書ストアを参照し、[Upload]ボタンをクリックします。



ステップ5:手順を繰り返して、すべてのAWサーバ証明書をFinesseクラスタにアップロードします。

tomcat-trust

ステップ6:証明書の変更を有効にするには、tomcatサービスを再起動します。

ステップ7:CUIC、IDS、およびVVBでは、2 ~ 4の手順に従ってAW証明書をアップロードします。

FinesseとCUIC/LiveData間の証明書交換

ステップ1:Finesse、CUIC、およびLiveData証明書を別のフォルダに保存します。

	Nafit a lovel benitt a cas a have	lander		- 41	Course lines
	See. *	Des-voltes	140	line.	
	CO BACK OF	11-10-27-01-01	Second Contrasts		1100
	DOD: NOT	1.1-101-0210-02107	Internet Contractor		1.00
	Las Piloh casi	1244.4047348	Salating California		1.68
	101100.00	12,000,0000,0044	Investig-Contraste		198
	Tal to distance	11-08-22/9 (0.51	Security California		100
	() indiador	10.05.019.0001	Second Contrast		110

2:[Finesse][CUIC][LiveData OS Administration]ページにログインします。

ステップ3:[OS Administration] > [Security] > [Certificate Management]に移動します。

ステップ4:[Upload Certificate\Certificate Chain]をクリックし、ドロップダウンから[tomcat-trust]を選択します。

ステップ5:ローカルストレージ内の証明書ストアを参照し、次のように[いずれかのサーバ証明書]を選択し、[アップロード]ボタンをクリックします。

Finesseサーバ: Tomcat信頼としてのCUICおよびLiveData

CUICサーバの場合 – FinesseおよびLiveDataをtomcat信頼として

LiveData Server - Tomcat信頼としてのCUICおよびFinesse

注: tomcat-trust証明書をセカンダリノードにアップロードする必要はありません。これは 自動的に複製されます。

ステップ6:証明書の変更を有効にするために、各ノードでtomcatサービスを再起動します。