CCE 12.6ソリューションでのCA署名付き証明書の実装

内容

概要 前提条件 要件 <u>使用するコンポーネント</u> バックグラウンド 手順 CCE Windowsベースのサーバ <u>1. CSRの生成</u> 2. CA署名付き証明書の取得 3. CA署名付き証明書のアップロード 4. CA署名付き証明書のIISへのバインド 5. Diagnostic PorticoへのCA署名付き証明書のバインド 6. Javaキーストアへのルートおよび中間証明書のインポート CVPソリューション <u>1. FQDNを使用した証明書の生成</u> 2. CSRの生成 3. CA署名付き証明書の取得 4. CA署名付き証明書のインポート VOSサーバ 1. CSR証明書の生成 2. CA署名付き証明書の取得 3.アプリケーション証明書とルート証明書のアップロード 確認 トラブルシュート 関連情報

概要

このドキュメントでは、Cisco Contact Center Enterprise(CCE)ソリューションで認証局(CA)署名 付き証明書を実装する方法について説明します。

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。

- ・ Unified Contact Center Enterprise(UCCE)リリース12.6.2
- ・ Package Contact Center Enterprise リリース12.6.2
- ・ Customer Voice Portal(CVP)リリース12.6.2
- Cisco Virtualized Voice Browser(VVB)
- Cisco CVP Operations and Administration Console(OAMP)
- Cisco Unified Intelligence Center (CUIC)
- Cisco Unified Communications Manager (CUCM)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- PCCE 12.6.2
- CVP 12.6.2
- Cisco VVB 12.6.2
- Finesss 12.6.2 (2015年9月)
- CUIC 12.6.2
- Windows 2019

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、クリアな(デフォルト)設定で作業を開始していま 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。

バックグラウンド

証明書は、クライアントとサーバ間の認証で通信が安全であることを保証するために使用されま す。ユーザはCAから証明書を購入するか、自己署名証明書を使用できます。

自己署名証明書(名前が示すように)は、認証局によって署名されるのではなく、IDが証明され る同じエンティティによって署名されます。自己署名証明書は、CA証明書ほど安全とは見なされ ませんが、多くのアプリケーションでデフォルトで使用されます。

Package Contact Center Enterprise(PCCE)ソリューションバージョン12.xでは、ソリューション のすべてのコンポーネントが、プリンシパルAdmin Workstation(AW)サーバでホストされるSingle Pane of Glass(SPOG)によって制御されます。

PCCE 12.5(1)バージョンのSecurity Management Compliance(SRC)により、SPOGとソリューション内の他のコンポーネント間のすべての通信は、セキュアHTTPプロトコルを介して行われます。

このドキュメントでは、セキュアなHTTP通信のためにCCEソリューションでCA署名付き証明書 を実装するために必要な手順について詳しく説明します。その他のUCCEセキュリティの考慮事 項については、『<u>UCCEセキュリティガイドライン</u>』を参照してください。

セキュアHTTPとは異なる、その他のCVPのセキュア通信については、『CVP Configuration Guide: <u>CVP Security Guidelines</u>』のセキュリティガイドラインを参照してください。

注:このドキュメントは、CCEバージョン12.6にのみ適用されます。他のバージョンへのリンクについては、「関連情報」のセクションを参照してください。

手順

CCE Windowsベースのサーバ

1. CSRの生成

この手順では、インターネットインフォメーションサービス(IIS)マネージャから証明書署名要求 (CSR)を生成する方法について説明します。

ステップ1: Windowsにログインし、Control Panel > Administrative Tools > Internet Information Services (IIS) Managerの順に選択します。

ステップ2.[接続]ウィンドウで、サーバー名をクリックします。サーバのホーム・ペインが表示されます。

Connections							
0,- 🗐 Ź 9 ,	PC 🧌 PC	CEAWA H	ome				
Start Page PCCEAWA (PCCERCDN/pcceadmin)	Filter		• 19 Go - 1	Show All	Group by:		
		•					A
	Connection Strings	SMTP E-mail					
	15			100 C	_		
		2	0	TP2	48	2	
	Authentic_	Compression	Default Document	Directory Browsing	Error Pages	Handler Mappings	
			5	3		1	
	HTTP Redirect	HTTP Respon	ISAPI and CGI Restri	BAPI Fites	Logging	MME Types	-
	4		8		2		
	Modules	Output Caching	Request Filtering	Server Certificates	Worker Processes		
	Manageme	nt				~ ^	
			貆				
	Configurat	Feature	Shared				v

手順3:IIS領域で、Server Certificatesをダブルクリックします。



ステップ4.ActionsペインでCreate Certificate Requestをクリックします。

File View Help				
Connections	Gamma Castillan	i au		Actions
Q 🔛 (🖄) 🖗.	Server Cerunca	0.5		Import
Start Page PCCLAIRA (PCCIRCDW pcceadmin)	Use this feature to request and m websites configured for 25L	anage certificates that the Web ser	ver can use with	Complete Certificate Request
	Filter + 17	Go - 🖓 Show All Group by:		Create Domain Cettificate
	Name *	Issued To	based By	Create Self-Signed Certificate
	Cisca ICM Diagnostic Framew	PCCEARAPCCORCONCISION.	PCCEANA.PCCERCE	Enable Automatic Rebind of
	Cisca ICM SSL Certificate	PCCLANA.PCCDRCDN.cisco.c.	PCCEANA.PCCERCI	Renewed Centificate Proto Pro

ステップ 5: Request Certificateダイアログボックスで、次の操作を行います。

表示されたフィールドに必要な情報を指定し、Nextをクリックします。

Request Certificate		?	x
Distinguished Na	me Properties		
Specify the required information official names and they cannot	n for the certificate. State/province and City/locality must be specified as contain abbreviations.		
Common name:	pcceawa.pccercdn.cisco.com		
Organization:	Cisco		
Organizational unit:	CX		
City/locality	RCDN		
State/province:	TX		
Country/region:	US v		
	Previous Next Finish	Cancel	

Cryptographic service providerドロップダウンリストで、デフォルト設定を残します。

Bit lengthドロップダウンリストから、2048を選択します。

Request Certificate	7	x
Cryptographic Service Provider Properties		
Select a cryptographic service provider and a bit length. The bit length of the encryption key determines to certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater to length may decrease performance. Cryptographic service provider: Microsoft RSA SChannel Cryptographic Provider v Bit length: 2048	he it	
Previous Next Finish	Cancel	

手順 6:証明書要求のファイル名を指定して、Finishをクリックします。

Request Certificate	?	x
File Name		
Specify the file name for the certificate request. This information can be sent to a certification authority for signing. Specify a file name for the certificate request: PCCEAW.PCCERCDN.cisco.com	r	
Previous Next Finish	Cancel	

2. CA署名付き証明書の取得

ステップ1:CAで証明書に署名します。

注:CAが使用する証明書テンプレートにクライアント認証とサーバ認証が含まれていること を確認してください。

ステップ 2: CA署名付き証明書を認証局(ルート、アプリケーション、および中間(存在する場合))から取得します。

3. CA署名付き証明書のアップロード

ステップ1: Windowsにログインし、Control Panel > Administrative Tools > Internet Information Services (IIS) Managerの順に選択します。



ステップ2.[接続]ウィンドウで、サーバー名をクリックします。



手順3:IIS領域で、Server Certificatesをダブルクリックします。



ステップ4.ActionsペインでComplete Certificate Requestをクリックします。

File Vew Help				
Connections	Server Certifica	tes		Actions
W. Mail 121 (M. Wij Start Pape > Nij PCCEARA (PCCERCON proceedmin)	Use this feature to request and movebolies configured for SSL.	anage certificates that the Web se (Go - 😨 Show All Group By:	ver can use with	Conte Cetificate Report Conte Cetificate Report Conste Domain Cetificate
	Name CocciCM Diagnostic Frames CocciCM SSL Certificate	Issued To PCCLANA.PCCDR.CDN.cisco.c. PCCLANA.PCCDR.CDN.cisco.c.	Issued By PCCEANA.PCCIRCI PCCEANA.PCCIRCI	Orate Self-Signed Certificate Enable Automatic Rebind of Renewed Certificate Phase Help

ステップ5:Complete Certificate Requestダイアログボックスで、次のフィールドに値を入力します。

[File name which contains the certification authority response]フィールドで、[...]ボタンをクリックします。

署名されたアプリケーション証明書が保存されている場所を参照し、[開く]をクリックします。

注:これが2-Tier CA実装であり、ルート証明書がまだサーバ証明書ストアにない場合は、 署名付き証明書をインポートする前に、ルートをWindowsストアにアップロードする必要が あります。ルートCAをWindowsストア「<u>Microsoft - Installing the Trusted Root Certificate</u>」 にアップロードする必要がある場合は、このドキュメントを参照してください。

[フレンドリ名]フィールドに、サーバーの完全修飾ドメイン名(FQDN)または任意の有効な名前を

入力します。Select a certificate store for the new certificateドロップダウンがPersonalのままであることを確認します。

Specify Certificate Authority Response Complete a previously created certificate request by retrieving the file that contains the certificate authority's response		
Complete a previously created certificate request by retrieving the file that contains the certificate authority's		
File name containing the certification authority's response: C:\Certificates\PCCEAWcertnew.cer Friendly name: PCCEAWA.pccercdn.cisco.com Select a certificate store for the new certificate: Personal v		
	nrel	_

ステップ6:[OK]をクリックして証明書をアップロードします。

証明書のアップロードが成功すると、証明書が[サーバ証明書]ペインに表示されます。

🐂 Internet Information Services (IS) Manager				_ 0 X
(a a) *] + PCCLARA +				₩ ≈ § 0 •
File Vew Help				
Connections Q. • [2] [2] [2] Q. • [2] Start Page > [2] PCCLARIA (PCCDRCDW proceedmin)	Server Certificates Use this feature to request and manage cer websites configured for SSL Filter • 17 Co 5	tificates that the Web server can		Actions Import. Courte Certificate Request. Complete Certificate Request. Courte Domain Certificate.
	Nama Cisco ICM Diagnostic Pramawork servi Cisco ICM SS. Certificate PCCDARK gccarcolis cisco.com	Insued To PODEANALPOCERCEN.cover.c. PODEANALPOCERCEN.cover.c. proseeus.prosecde.cisco.com	PCCLANAP PCCLANAP PCCLANAP PCCLANAP	Create Self-Signed Certificate Enable Automatic Rabind of Research Certificate Photo

4. CA署名付き証明書のIISへのバインド

この手順では、IISマネージャでCA署名付き証明書をバインドする方法について説明します。

ステップ1: Windowsにログインし、Control Panel > Administrative Tools > Internet Information Services (IIS) Managerの順に選択します。



ステップ2.Connectionsペインで、<server_name> > Sites > Default Web Siteの順に選択します。

🍞 Internet Information Services (IS) Manager			-	0	ж
😥 + PCCEANA + Stes + Default Web Ste	1			= 9	
File View Help					
Connections Q. • • • • • • • • • • • • • • • • • • •	Default Web Site Home	Actions Edit Pr Edit SP Ender Binder View V Manage W C Restart	te p	e rei echories	
	Strings.	 Stat Stap Brown Br	e Websi 1980 (ke 1980 (ke)) (ke 1980 (ke)) (ke 1980 (ke)) (ke 1980 (ke)) (ke)) (ke)) (ke) (ke)) (ke)) (ke	te tel tel tel tel	

手順3:[操作]ウィンドウで、[バインド…]をクリックします。



ステップ4.httpsと入力し、ポート443をクリックして、Edit...をクリックします。

File View Help					
Connections		Conference and	Chailenne.		Actions
Q,- 🔛 🙇 😥	Stellindep:	Default Wet	site Home	7 X	Diplore Edit Permissions
PECEARIA (PECEREDNycon Pecearia Peols Peols Peols Peols Peols Peols Peols	Type Host Name http: htt	Pot P Address 80 * 440	Binding Informa	Add Edk Remove Browse	Edit Site Enderge Basic Settings Verw Applications Verw Virtual Directories Verw Virtual Directories Verw Virtual Directories Setting Setting Browne Website Browne Website
		Cutput Request	SZI, Settings t View	Close	Booke 100 (Ktp) Booke 100 (Ktp) Advanced Settings Configure Limits Help
Part 1					en

ステップ5:SSL証明書のドロップダウンリストから、前の手順で指定したフレンドリ名と同じ名前を持つ証明書を選択します。

Ny Internet Information Services (IS) Manager	= 0 X
Ge PCCEANA + Stes + Default Web Ste +	🖬 🖂 🔒 🖷 •
File View Help	
Connections Default Web Site Home	Actions
Q: 2 2 9. Estate	A Depice
v S POCLANA (PCCIRCOM prox	Lot Permissions
Application Pools Type Host Name Post IP Address Binding Informa. Add.	Endog.
S Default Web Ster Maps 447	Tasic Settings.
Remove	View Applications View Midstel View Internation
Edit Ster Binding	Manane Website
Ter Pattern Int	2 Restart
https://www.aligned.wy	▶ Sat
Hod name	· 300
	C Browse "40 (Http)
Require Server Name Indication	Erowse (443 (https)
	Advanced Settings
SS, cetificate	Configure
PCCLAstA.gozerodn.ckos.com v Select View	6 145
OK Cented u	
The Section New 100 Content New	
Ready	۹.

ステップ 6 : [OK] をクリックします。

ステップ7: Start > Run > services.mscの順に移動し、IIS Admin Serviceを再起動します。

Q, Services					- 0	×
File Action View	Help					
🕈 🕈 📷 🖬 🖄	🕞 🖩 🕾 🕨 🖬 🔂					
Q, Senices (Local)	 Services (Local) 	·				
	Apache Tomcat 9	Name	Description	Status	Statup Type	Log n
		Q, Hyper V Data Exchange Service	Provides a mechanism to exchange data betwee		Manual (Trip	Los
	Stop the service	Q. Hyper-V-Guest Service Interface	Provides an interface for the Hyper-V host to int		Manual (Trip	Los I
	Easted the service	Q Hyper V Guest Shutdown Senice	Provides a mechanism to shut down the operati		Manual (Trip	Los I
		Q Hyper-Y Heartbeat Service	Monitors the state of this virtual machine by rep		Manual (Trip	1.0
	Descriptions	Q Hyper-Y PowerShell Direct Service	Provides a mechanism to manage virtual machi		Manual (Dig.,	Los I
	Agenthe Terricat \$10 Server -	Q Hyper-Villemote Desistop Virtuelastio	Provides a platform for communication betwee		Manual (Trig.,	101-1
	http://fomcat.apache.org/fomcat/	Q Hyper-V Time Synchronization Service	Synchronizes the system time of this virtual mac		Manual (Trip.,	Local D
		All Hyper Vitelame Shadow Copy Reput	Coordinates the communications that are requir		Manual (Trip	100
		TS Admin Service	Enables this server to administer the IS metabas	Renning	Automatic	Les 📕
		Contrast Autor Press Caying Modules	The REECT service heats the Internet Key Excha-	Renning	Automatic (T.,	Los I
		Queteractive Services Detection	Enables user notification of user input for intera		Disabled	tei 🛛
		Quinternet Connection Sharing (ICS)	Provides network address translation, addressin		Disabled	Los I
		Q. P Helper	Provides turnel connectivity using IPv6 transitio	Surviva .	Automatic	1.04
		Q:Puec Policy Agent	Internet Protocol security (Poec) supports netw	Rendered	Manual (Trip	Ne
		ADC Proxy Server service (KPS)	KDC Proxy Server service runs on edge servers to		Manual	No
		Quiterelies for Distributed Transaction C	Coordinates transactions between the Distribute		Manual (Trip-	Ne

5. Diagnostic PorticoへのCA署名付き証明書のバインド

この手順では、Diagnostic PorticoでCA署名付き証明書をバインドする方法について説明します。

ステップ1:コマンドプロンプトを開きます([管理者として実行])。

ステップ2.Diagnostic Porticoホームフォルダに移動します。次のコマンドを実行します。

手順 3 : Diagnostic Porticoにバインドされている現在の証明書を削除します。次のコマンドを実行します。

DiagFwCertMgr /task:UnbindCert

c:\icm\serviceability\diagnostics\bin>_

ステップ4.署名付き証明書を開き、[拇印]フィールドのハッシュコンテンツ(スペースなし)をコ ピーします。

注:ハッシュコンテンツの先頭または末尾から隠し文字を削除してください。Notepad++な どのエディタを使用すると、これらの隠し文字を識別できます。

Certificate	×
General Details Certification Path	
Show: <all></all>	
FieldValueAuthority Key IdentifierKeyID=03 2f 51 02 27 8c c7 3CRL Distribution Points[1]CRL Distribution Point: DistrAuthority Information Access[1]Authority Info Access: AccCertificate Template Inform[1]Authority Info Access: AccApplication Policies[1]Application Certificate PolicKey UsageDigital Signature, Key EncipherThumbprint algorithmsha1Thumbprint97 93 74 00 99 19 53 d6 4e 0b c5 6e c4 4c 196 36 dc 4b cb	^ ≡
Edit Properties Copy to File	

ステップ 5:次のコマンドを実行して、ハッシュの内容を貼り付けます。

::\icm\serviceability\diagnostics\bin>DiagFwCertMgr /task:BindCertFromStore /certhash:97937400991953d64e0bc56ec44cbd9636 ic4bcb

::\icm\serviceability\diagnostics\bin>_

証明書のバインドが成功すると、「The certificate binding is VALID」というメッセージが表示さ れます。

手順 6 : 証明書のバインドが正常に行われたかどうかを検証します。次のコマンドを実行します。

DiagFwCertMgr /task:ValidateCertBinding

::\icm\serviceability\diagnostics\bin>DiagFwCertMgr /task:ValidateCertBinding Cisco Unified ICM/CCE Diagnostic Framework Certificate Manager Executing Task: 'ValidateCertBinding' Read port number from service configuration file: '7890' ATTEMPTING TO VALIDATE CERTIFICATE BINDING WITH WINDOWS HTTP SERVICE Binding IP Address: '0.0.0.0:7890' Attempting to query HTTP service for SSL certificate binding Found a certificate binding on 0.0.0.0:7890 Attempting to locate this certificate in the Local Computer certificate store Trying to look up certificate: 97937400991953D64E0BC56EC44CBD9636DC4BCB Local Computer Personal certificate store was opened successfully Certificate requested found in store Certificate store was closed successfully The certificate binding is VALID <u>Certificate hash stored in service registry matches certificate used by service</u> ALL TASKS FOR VALIDATING CERTIFICATE BINDING COMPLETED SUCCESSFULLY

c:\icm\serviceability\diagnostics\bin>____

注:DiagFwCertMgrはデフォルトでポート7890を使用します。

証明書のバインドが成功すると、「The certificate binding is VALID」というメッセージが表示されます。

手順7: Diagnostic Frameworkサービスを再起動します。次のコマンドを実行します。

net stop DiagFwSvc
net start DiagFwSvc

診断フレームワークが正常に再起動すると、アプリケーションの起動時に証明書エラー警告が表示されません。

6. Javaキーストアへのルートおよび中間証明書のインポート

注意:作業を開始する前に、キーストアをバックアップし、管理者としてJavaホームから コマンドを実行する必要があります。

ステップ1:Javaキーツールがホストされている場所を確認するためにJavaホームパスを知ります 。Javaホームパスを見つける方法はいくつかあります。

オプション1:CLIコマンド: echo %CCE_JAVA_HOME%

C:\>echo %CCE_JAVA_HOME% C:\Program Files (x86)\OpenJDK\jre-8.0.272.10-hotspot

オプション2:図に示すように、高度なシステム設定を使用して手動で

🗸 T 🔤 > Control Par	hei > System and Security > System		~ 0	Search Control Panel
trol Panel Home	System Properties ×			
ice Manager	Computer Name Hardware Advanced Remote			
note settings		Environment Variables		
anced system settings	You must be logged on as an Administrator to make most of these changes.			
ancea system settings	Performance	User variables for Administrator	r	
	Visual effects, processor scheduling, memory usage, and virtual memory	Mariaka	Mahara .	
	Cottineer	Variable	Value	
	Settings	3 Path TEMP	C:\Users\Administrator\AppData\Local\Microsoft\WindowsAp	ops;
	User Profiles	TMP	C:\Users\Administrator\AppData\Local\Temp	
	Desktop settings related to your sign-in		c. (outs) (commission of pponta (cocar) remp	
		1		
	Settings			
	Statup and Recovery			
	System startup, system failure, and debugging information		New	Edit Delete
	Settings	System variables		
		Variable	Value	
	Environment vanables	CCE_JAVA_HOME	C:\Program Files (x86)\OpenJDK\jre-8.0.272.10-hotspot	
		COMPLUS_ProtAPI_ProfilerC.	EnableV2Profiler	
	OK Cancel Apply	ComSpec	C:\Windows\system32\cmd.exe	
		COR_ENABLE_PROFILING	1	
		COR_PROFILER	AppDynamics.AgentProfiler	
		CORECUR PROFILER	AnnDunamics AgentProfiler	
		CORECER PROFILER	ADDUVNAMICS.AdentProfiler	
			New	Edit Delete
			L	OK Cancel

ステップ 2: ICMとOpenJDKの両方のパス<ICM install directory>\ssl\ および %CCE_JAVA_HOME%\lib\security\cacertsからcacertsファイルをバックアップします。 これらは 別の場所にコピーできます。

ステップ3:管理者としてコマンドウィンドウを開き、次のコマンドを実行します。

cd %CCE_JAVA_HOME%\bin keytool.exe -keystore <ICM install directory>\ssl\cacerts -trustcacerts -import -file <path where the R keytool.exe -keystore %CCE_JAVA_HOME%\lib\security\cacerts -trustcacerts -import -file <path where the

注:必要な特定の証明書は、証明書の署名に使用するCAによって異なります。パブリック CAの一般的な2層CAでは、内部CAよりもセキュリティが高いため、ルート証明書と中間証 明書の両方をインポートする必要があります。中間証明書がないスタンドアロンCA(通常 はラボまたはよりシンプルな内部CAで見られる)では、ルート証明書をインポートするだ けで済みます。System CLIは引き続きOpenJDKキーストアを使用するため、ルート証明書 と中間証明書をICMとOpenJDKキーストアの両方にインポートする必要があります。

CVPソリューション

1. FQDNを使用した証明書の生成

この手順では、Web Service Manager(WSM)、Voice XML(VXML)、Call Server and Operations Management(OAMP)サービスのFQDNを使用して証明書を生成する方法について説明します。

注:CVPをインストールする場合、証明書名にはサーバの名前のみが含まれ、FQDNは含ま れないため、証明書を再生成する必要があります。

注意:作業を開始する前に、次の操作を行う必要があります。 1.管理者としてコマンドウィンドウを開きます。 2.12.6.2の場合、キーストアパスワードを識別するには、%CVP_HOME%\binフォルダに移動し、DecryptKeystoreUtil.batファイルを実行します。 3.12.6.1の場合、キーストアパスワードを識別するには、more %CVP_HOME%\conf\security.propertiesコマンドを実行します。 4.このパスワードは、keytoolコマンドを実行するときに必要です。 5.%CVP_HOME%\conf\security\ディレクトリから、copy .keystore backup.keystoreコマン ドを実行します。

CVPサーバ

ステップ1:CVPサーバの証明書を削除するには、次のコマンドを実行します。

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -a
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -a
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -a

プロンプトが表示されたら、キーストアのパスワードを入力します。

ステップ2:WSM証明書を生成するには、次のコマンドを実行します。

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypai

プロンプトが表示されたら、キーストアのパスワードを入力します。

注:デフォルトでは、証明書は2年間生成されます。-validity XXXXを使用して、証明書が再 生成される有効期限を設定します。そうでない場合、証明書は90日間有効であり、この時 間の前にCAによって署名される必要があります。これらの証明書のほとんどでは、3 ~ 5年 は妥当な検証期間である必要があります。

標準的な有効性の入力を次に示します。

1年	365
----	-----

2年	730
三年	1095
4年	1460
五年	1895
十年	3650

注意:12.5以降の証明書は、SHA 256、キーサイズ2048、および暗号化アルゴリズムRSAで ある必要があります。これらのパラメータを使用して、次の値を設定します。-keyalg RSAおよび – keysize 2048。CVPキーストアコマンドには – storetype JCEKSパラメータを 含めることが重要です。これを行わないと、証明書、キー、またはキーストアが破損する可 能性があります。

質問に対して、サーバのFQDNを指定します。最初と最後の名前は何ですか。



次の質問に答えてください。

組織ユニットの名前は何ですか。

[不明]: <OUを指定>

組織の名前は何ですか。

[不明]: <組織名を指定>

市区町村の名前は何ですか。

[不明]: <都市/地域の名前を指定>

都道府県の名前は何ですか。

[不明]: <都道府県の名前を指定>

このユニットの2文字の国番号は何ですか。

[不明]: <2文字の国番号を指定>

次の2つの入力にyesを指定します。

ステップ3:vxml_certificateとcallserver_certificateに対して同じ手順を実行します。

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypai
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypai

CVP レポート サーバ

ステップ1:WSMとReporting Serverの証明書を削除するには、次のコマンドを実行します。

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -a
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -a

プロンプトが表示されたら、キーストアのパスワードを入力します。

ステップ2:WSM証明書を生成するには、次のコマンドを実行します。

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypai

プロンプトが表示されたら、キーストアのパスワードを入力します。

クエリのサーバのFQDNとして名と姓を指定し、CVPサーバで行った手順と同じ手順を続行しま す。

ステップ3: callserver_certificateに対して同じ手順を実行します。

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypai

プロンプトが表示されたら、キーストアのパスワードを入力します。

CVP OAMP(UCCE導入)

PCCEソリューションバージョン12.xでは、ソリューションのすべてのコンポーネントがSPOGに よって制御され、OAMPがインストールされていないため、これらの手順が必要になるのは UCCE導入ソリューションだけです。

ステップ1:WSMとOAMPサーバの証明書を削除するには、次のコマンドを実行します。

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -a
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -a

プロンプトが表示されたら、キーストアのパスワードを入力します。

ステップ2:WSM証明書を生成するには、次のコマンドを実行します。

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypai

プロンプトが表示されたら、キーストアのパスワードを入力します。

クエリのサーバのFQDNとして名と姓を指定し、CVPサーバで行った手順と同じ手順を続行しま す。

ステップ3: oamp_certificateに対して同じ手順を実行します。

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypai

プロンプトが表示されたら、キーストアのパスワードを入力します。

2. CSRの生成

注:RFC5280準拠のブラウザでは、各証明書にサブジェクトの別名(SAN)が含まれている必 要があります。これは、CSRの生成時にSANで – extパラメータを使用して実行できます。

サブジェクト代替名

-extパラメータを使用すると、特定の拡張子を指定できます。この例では、サーバの完全修飾ド メイン名(FQDN)とlocalhostを使用して、サブジェクト代替名(SAN)を追加します。追加のSANフ ィールドは、カンマ区切り値として追加できます。

有効なSANタイプは次のとおりです。

-ext san=dns:mycvp.mydomain.com,dns:localhost

CVPサーバ

ステップ1:エイリアスの証明書要求を生成します。次のコマンドを実行し、ファイル (wsm_certificateなど)に保存します。

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -

プロンプトが表示されたら、キーストアのパスワードを入力します。

ステップ2:vxml_certificateとcallserver_certificateに対して同じ手順を実行します。

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -

プロンプトが表示されたら、キーストアのパスワードを入力します。

CVP レポート サーバ

ステップ1:エイリアスの証明書要求を生成します。次のコマンドを実行し、ファイル (wsmreport_certificateなど)に保存します。

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -

プロンプトが表示されたら、キーストアのパスワードを入力します。

ステップ2: callserver_certificateに対して同じ手順を実行します。

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -

プロンプトが表示されたら、キーストアのパスワードを入力します。

CVP OAMP(UCCE導入のみ)

ステップ1:エイリアスの証明書要求を生成します。次のコマンドを実行し、ファイル (wsmoamp_certificateなど)に保存します。

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -

プロンプトが表示されたら、キーストアのパスワードを入力します。

ステップ2: oamp_certificateに対して同じ手順を実行します。

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -

プロンプトが表示されたら、キーストアのパスワードを入力します。

3. CA署名付き証明書の取得

ステップ 1: CA上の証明書に署名します(CVPサーバの場合はWSM、CallserverおよびVXMLサ ーバ、CVP OAMPサーバの場合はWSMおよびOAMP、CVPレポートサーバの場合はWSMおよび Callserver)。

ステップ2:CA認証局からアプリケーション証明書とルート証明書をダウンロードします。

ステップ3:ルート証明書とCA署名付き証明書を各サーバのフォルダ %CVP_HOME%\conf\security\にコピーします。

4. CA署名付き証明書のインポート

これらの手順をCVPソリューションのすべてのサーバに適用します。 CA署名付き証明書をイン ポートする必要があるのは、そのサーバ上のコンポーネントの証明書だけです。

ステップ1:ルート証明書をインポートします。次のコマンドを実行します。

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -t

プロンプトが表示されたら、キーストアのパスワードを入力します。Trust this certificateプロン プトで、Yesと入力します。

中間証明書がある場合は、次のコマンドを実行します。

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -t

プロンプトが表示されたら、キーストアのパスワードを入力します。Trust this certificateプロン プトで、Yesと入力します。

ステップ 2:そのサーバ証明書用のCA署名付きWSMをインポートします(CVP、Reporting、お よびOAMP)。次のコマンドを実行します。

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -t

プロンプトが表示されたら、キーストアのパスワードを入力します。Trust this certificateプロン プトで、Yesと入力します。

ステップ 3:CVPサーバとレポートサーバで、Callserver CA署名付き証明書をインポートします 。次のコマンドを実行します。

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -t

プロンプトが表示されたら、キーストアのパスワードを入力します。Trust this certificateプロン プトで、Yesと入力します。

ステップ 4:CVPサーバで、VXMLサーバのCA署名付き証明書をインポートします。次のコマン ドを実行します。

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -t

プロンプトが表示されたら、キーストアのパスワードを入力します。Trust this certificateプロン プトで、Yesと入力します。

ステップ 5:CVP OAMPサーバ(UCCEのみ)で、OAMPサーバCA署名付き証明書をインポート します。次のコマンドを実行します。

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -t

プロンプトが表示されたら、キーストアのパスワードを入力します。Trust this certificateプロン プトで、Yesと入力します。 注:UCCEの導入では、CSRの生成時に指定したFQDNを使用して、CVP OAMP内のサーバ (CVPレポート、CVPサーバなど)を追加してください。

VOSサーバ

1. CSR証明書の生成

この手順では、Cisco Voice Operating System(VOS)ベースのプラットフォームからTomcat CSR証明書を生成する方法について説明します。

このプロセスは、次のようなVOSベースのアプリケーションに適用できます。

- Finesse
- ・ CUIC \ライブデータ(LD) \アイデンティティサーバ(IDS)
- クラウド接続
- Cisco VVB

ステップ1: Cisco Unified Communications Operating System Administrationページ (https://FQDN :<8443または443>/cmplatform)に移動します。

ステップ2: Security > Certificate Managementの順に移動し、Generate CSRを選択します。

Show - Settings - Secu	rty = Software Upgrades = Services = Heb =
Certificate List	
Cenerate Sett-signed	Upload Certificate/Certificate chain
Certificate List	
Find Certificate List where	Certificate v begins with v Find Clear Filter I w
	No active query. Please enter your search criteria using the options above.
Generate Self-signed	Upload Certificate/Certificate chain Generate CSR

ステップ3:CSR証明書が生成されたら、ウィンドウを閉じてDownload CSRを選択します。

Show * Settings * Security * Software Upgrades * Services * Help *
Certificate List
💽 Generale Self-signed 🖓 Upload Certificate Certificate chain 💽 Generale CSR 🛐 Download CSR
Certificate List
Find Certificate List where Certificate 🗠 begins with 🗠 Find Clear Filter 💠 🚥
No active query. Please enter your search oriteria using the options above.
Generate Self-signed Upload Certificate/Certificate chain Generate CSR Download CSR

ステップ4:証明書の目的がtomcatであることを確認し、Download CSRをクリックします。

Download Certificate Signing Request - Mozilla Firefox	-	×
🛛 🔓 https://10.201.224.234/cmplatform/certificateDownloadNewCsr.do		 ≡
Download Certificate Signing Request		
Download CSR 🖳 Close		
Status Certificate names not listed below do not have a corresponding CSR Download Certificate Signing Request Certificate Purpose* tomcat Download CSR Close ··································		
<		>

ステップ 5:Save Fileをクリックします。ファイルはDownloadフォルダに保存されます。



2. CA署名付き証明書の取得

ステップ1:CAにエクスポートされたtomcat証明書に署名します。

ステップ2:CA認証局から認証されたアプリケーションとルートをダウンロードします。

3.アプリケーション証明書とルート証明書のアップロード

ステップ1: Cisco Unified Communications Operating System Administrationページ (<u>https://FQDN</u>:<8443または443>/cmplatform)に移動します。

ステップ 2: Security > Certificate Managementの順に移動し、Upload Certificate/Certificate chainを選択します。



ステップ 3: Upload certificate/Certificate chainウィンドウのcertificate purposeフィールドで tomcat-trustを選択し、ルート証明書をアップロードします。

Upload Certificate/Certificate chain			
Upload 🖳 Close			
- Status			
Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster			
Upload Certificate/Certificate chain			
Certificate Purpose*	tomcat-trust		
Description(friendly name)			
Upload File	Choose File No file chosen		
Upload Close			

ステップ4:中間証明書(存在する場合)をtomcat-trustとしてアップロードします。

ステップ 5: Upload certificate/Certificate chainウィンドウで、Certificate Purposeフィールドで now tomcatを選択し、アプリケーションCA署名付き証明書をアップロードします。

ι	Jpload Certificate/Certifica	te chain				
1	Upload 🖳 Close					
	Status Status Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster					
ľ	Certificate Purpose*	tomcat				
I	Description(friendly name)	Self-signed certificate				
	Upload File	Browse No file selected.				
1	Upload Close i • indicates required item.					
1			3			

手順6:サーバをリブートすると、

確認

サーバをリブートした後、次の手順を実行してCA署名付き実装を確認します。

ステップ1:Webブラウザを開き、キャッシュをクリアします。

ステップ2:ブラウザを閉じて、もう一度開きます。

ここで、CA署名付き証明書を開始するための証明書スイッチが表示され、証明書が自己署名であるため信頼できないことを示すメッセージがブラウザウィンドウに表示されなくなります。

トラブルシュート

このガイドには、CA署名付き証明書の実装をトラブルシューティングする手順はありません。

関連情報

- <u>CVP設定ガイド セキュリティ</u>
- <u>UCCEセキュリティガイド</u>
- <u>PCCE管理ガイド</u>
- Exchange PCCE自己署名証明書 PCCE 12.5

- Exchange UCCE自己署名証明書 UCCE 12.5
- Exchange PCCE自己署名証明書 PCCE 12.6
- Exchange UCCE自己署名証明書 UCCE 12.6
- 証明書交換ユーティリティ
- ・ <u>テクニカル サポートとドキュメント Cisco Systems</u>

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。