ISEでのサードパーティCA署名付き証明書のイ ンストール

内容
<u>はじめに</u>
前提条件
<u>要件</u>
<u>使用するコンポーネント</u>
<u>背景説明</u>
<u>設定</u>
<u>ステップ1:証明書署名要求(CSR)の生成</u>
<u>ステップ2: 新しい証明書チェーンをインポートします。</u>
<u>確認</u>
トラブルシュート
<u>dot1x認証中にサプリカントがISEローカルサーバ証明書を信頼しない</u>
<u>ISE証明書チェーンは正しいが、認証中にエンドポイントがISEサーバ証明書を拒否する</u>
<u>関連情報</u>

はじめに

このドキュメントでは、サードパーティの認証局(CA)によって署名された証明書をCisco Identity Services Engine(ISE)にインストールする方法について説明します。

前提条件

要件

Basic Public Key Infrastructureに関する基本的な知識があることが推奨されます。

使用するコンポーネント

このドキュメントの情報は、Cisco Identity Services Engine(ISE)リリース3.0に基づくものです。 同じ設定がリリース2.Xにも適用されます

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。

背景説明

このプロセスは、最終的な証明書ロール(EAP認証、ポータル、管理者、およびpxGrid)に関係 なく同じです。

設定

ステップ1:証明書署名要求(CSR)の生成

CSRを生成するには、Administration > Certificates > Certificate Signing Requestsの順に移動し、 Generate Certificate Signing Requests (CSR)をクリックします。

Certificate Management \checkmark System Certificates	Certificate Signing Requests	~
Trusted Certificates	Generate Certificate Signing Requests (CSR)	
OCSP Client Profile	A Certificate Signing Requests (CSRs) must be sent to and signed by an external author	rity. Click
Certificate Signing Requests	request has been signed, click "bind" to bind the request to the signed certificate issued	by that au
Certificate Periodic Check Se	🔍 View 🛧 Export 👘 Delete Bind Certificate	
Certificate Authority >	Friendly Name Certificate S	ubject

- 1. Usageセクションで、ドロップダウンメニューから使用するロールを選択します。証明書が 複数のロールに使用されている場合は、[多用途]を選択できます。証明書が生成されてから も、必要に応じてロールを変更できます。
- 2. 証明書を生成できるノードを選択します。
- 3. 必要な情報を入力します(組織単位、組織、市区町村、都道府県、国)。
- ◆ 注:Common Name(CN)フィールドで、ISEはノードの完全修飾ドメイン名(FQDN)を自動的 に入力します。

ワイルドカード:

- ワイルドカード証明書を生成する場合は、Allow Wildcard Certificatesボックスにチェックマ ークを入れます。
- 証明書がEAP認証に使用される場合、Windowsサプリカントはサーバ証明書を拒否するため、サブジェクトCNフィールドに*記号を入れないでください。
- サプリカントでValidate Server Identityが無効になっている場合でも、CNフィールドに*が あると、SSLハンドシェイクが失敗する可能性があります。

- 代わりに、汎用FQDNをCNフィールドで使用し、次にサブジェクト代替名(SAN)のDNS名 フィールドでを使用すること*.domain.comができます。
- ◆ 注:一部の認証局(CA)は、CSRにワイルドカード(*)が存在しなくても、証明書のCNにワイ ルドカードを自動的に追加できます。このシナリオでは、このアクションを防ぐために特別 な要求を発行する必要があります。

個々のサーバ証明書 CSR の例

Usage

Certificate(s) will be used	for Multi-Use	You can use a single certificate for multiple services, but doing so is not a recommended practice. Rather, you should obtain individual certificates specifically for each service (for example, one certificate each for Guest Portals,
Allow Wildcard Certificate	s 🗌 ϳ	EAP, and pxGrid).
Node(s)		
Generate CSR's for these N	lodes:	
Node	CSR Friendly Name	
abtomar30	abtomar30#Multi-Use	e
Subject		
Common Name (CN) \$FQDN\$		<u>(</u>)
Organizational Unit (OU) Cisco TAC		<u>(</u>)
Organization (O) Cisco		(i)
City (L) Bangalore		
State (ST) Karnataka		
Country (C) IN		
Subject Alternative Name (S	(AN)	
IP Address	✓ 10.106.120.87	- + 0
* Key type		
RSA	× (i)	

ワイルドカード CSR の例

Isage			×
Certificate(s) will be used for	Multi-Use	\sim	You can use a single certificate for multiple services, but doing so is not a recommended
			practice. Rather, you should obtain individual certificates specifically for each service (for example, one certificate each for Guest Portals,
Allow Wildcard Certificates 🗸	0		EAP, and pxGrid).
Subject			
Common Name (CN) Mycluster.mydomain,com		<u>(</u>)	
Organizational Unit (OU) Cisco TAC		<u>(</u>)	
Organization (O) Cisco		<u>(</u>)	
City (L) Bangalore			
State (ST) Karnataka			
Country (C) IN			
Subject Alternative Name (SAN)			
IP Address	✓ 10.106.120.87		- +
DNS Name	✓ *.mydomain.com		- + 0
* Key type			
RSA	✓ (i)		

◆ 注:各導入ノードのIPアドレスをSANフィールドに追加すると、IPアドレスを使用してサー バにアクセスする際に証明書の警告が表示されるのを回避できます。

CSRが作成されると、ISEにポップアップウィンドウが表示され、CSRをエクスポートするオプ ションが表示されます。エクスポートした後、このファイルは署名のためにCAに送信する必要 Successfully generated CSR(s) 🔽

Certificate Signing request(s) generated:

abtomar30.abtomar.local#Multi-Use

Click Export to download CSR(s) or OK to return to list of CSR(s) screen



ステップ2:新しい証明書チェーンをインポートします。

認証局(CA)は、完全な証明書チェーン(ルート/中間)とともに署名付きサーバ証明書を返します 。証明書を受け取ったら、次の手順を実行して証明書をISEサーバにインポートします。

- 1. CAから提供されたルートおよび(または)中間証明書をインポートするには、 Administration > Certificates > Trusted Certificatesの順に移動します。
- 2. Importをクリックし、ルート証明書または中間証明書(あるいはその両方)を選択し、送信 に適用される関連するチェックボックスを選択します。
- 3. サーバ証明書をインポートするには、Administration > Certificates > Certificate Signing Requestsの順に移動します。
- 4. 前に作成した CSR を選択してから、[Bind Certificate] をクリックします。
- 5. 新しい証明書の場所を選択すると、ISEはデータベースに作成および保存された秘密キーに 証明書をバインドします。

◇ 注:この証明書に対して管理者ロールが選択されている場合、特定のISEサーバサービスが 再起動します。

▲ 注意:インポートされた証明書が展開のプライマリ管理ノード用であり、管理者ロールが選択されている場合、すべてのノードのサービスが次々に再起動されます。これは予期された動作であり、このアクティビティを実行するにはダウンタイムが推奨されます。

~

確認

照明書をインポートする際に管理ロールを選択した場合は、ブラウザに管理ページを読み込むこ とによって、新しい証明書を検証できます。チェーンが正しく構築されていて、証明書チェーン がブラウザで信頼されている限り、ブラウザは新しい管理証明書を信頼する必要があります。

	P - ■ C G Identity Services Engine ×
General Details Certification Path Certification path Certification path abtomar-WIN-231PNBS4IPH-CA abtomar30.abtomar.local	
	Identity Services Engine
View Certificate	Username
Certificate status: This certificate is OK.	Password
OK	
	Problems logging in?

© 2020 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S and certain other countries. Cisco ISE I View third-party licenses and notices

さらに詳しく検証するには、ブラウザで南京錠シンボルを選択し、証明書パスに完全なチェーン が含まれていて、そのチェーンがマシンで信頼されていることを確認します。これは、サーバが 完全なチェーンを渡したことを直接示すことにはなりませんが、ブラウザがローカルの信頼スト アに基づいてサーバ証明書を信頼できることを示します。

トラブルシュート

dot1x認証中にサプリカントがISEローカルサーバ証明書を信頼しない

SSL ハンドシェーク プロセス中に ISE が完全な証明書チェーンを渡していることを確認します。

サーバ証明書を必要とするEAP方式(PEAP)と[サーバIDの検証]を選択した場合、サプリカントは認証プロセスの一部としてローカル信頼ストアにある証明書を使用して証明書チェーンを検証し

ます。SSLハンドシェイクプロセスの一部として、ISEは自身の証明書を提示し、チェーンに含ま れるルート証明書や中間証明書も提示します。チェーンが完全でないと、サプリカントはサーバ ID を検証できません。証明書チェーンがクライアントに返されていることを確認するには、次の 手順を実行します。

- 1. 認証中にISE(TCPDump)からキャプチャを取得するには、Operations > Diagnostic Tools > General Tools > TCP Dumpの順に移動します。
- Wiresharkでキャプチャをダウンロードして開き、フィルタssl.handshake.certificatesを適用 して、アクセスチャレンジを見つけます。
- 3. 選択したら、Expand Radius Protocol > Attribute Value Pairs > EAP-Message Last segment > Extensible Authentication Protocol > Secure Sockets Layer > Certificate > Certificatesの順に選択します。

以下に、キャプチャした証明書チェーンの例を示します。

Eile Ed	Elle Edit View Go Capture Analyze Statistics Telephony Tools Internals Help					
0 0	🗶 🗮 🖉 (🗎 🗎 🗶 😂 (🔍 🔶)	+ 🖕 7 🛓 🗐 🗐 🍳 Q Q 🖄	🗑 🖻 🥵 🗱 💢			
Filter	ssUhandshake.certificates	 Expression 	Clear Apply	Save		
No.	Time	Source	Destination	Protocol Length Info		
33	4 13:59:41.137274	14.36.157.20	14.36.157.21	TLSv1.2 992 Server Hello, Certificate, Server Hello Done		
85	7 13:59:53.158063	14.36.157.21	14.36.154.5	RADIUS 1178 Access-Challenge(11) (id=198, 1=1136)		
86	0 13:59:53.193912	14.36.157.21	14.36.154.5	RADIUS 1174 Access-Challenge(11) (id=199, 1=1132)		
- 86	2 13:59:53.213715	14.36.157.21	14.36.154.5	RADIUS 1174 Access-Challenge(11) (id=200, 1=1132)		
86	4 13:59:53.231653	14.36.157.21	14.36.154.5	RADIUS 301 Access-Challenge(11) (1d=201, 1=259)		
120	5 14:00:01.253698	14.36.157.20	14.36.157.21	TLSv1.2 992 Server Hello, Certificate, Server Hello Done		
4				11		
00.4	<pre>AVP: 1=255 t=EAP-Message(/9 </pre>	9) Segment[1]				
в,	<pre>WP: 1=255 t=EAP-Message(/S</pre>	9) Segment[2]				
	<pre>WP: I=255 t=EAP-Message(/5 WP: 1 355 t EAP-Message(/5)</pre>	Segment[3]				
8.0	EAD forement	9) Last segment[4]				
	Extensible Authentication	Protocol				
	Code: Request (1)	Protocor				
	Code: Request (I)					
	le off					
	Ungen, INIZ Type: Protected FAP (FAP-PFAP) (2%)					
	EAP-TLS Flags: 0xc0					
	FAD-TIS Frage: 0x00					
	[4 EAP-TLS Fragments (3)	141 bytes): #857(1002), #860	(1002), #862(100)	2), #864(135)]		
	Secure Sockets Layer					
	III TLSv1 Record Layer: Ha	indshake Protocol: Server Hel	10			
	□ TLSv1 Record Layer: Ha	undshake Protocol: Certificat	te			
	Content Type: Handsh	ake (22)				
	Version: TLS 1.0 (0x	0301)				
	Length: 3048					
	B Handshake Protocol: Certificate					
	Handshake Type: Certificate (11)					
	Length: 3044					
	Certificates Length: 3041					
	Certificates (3041)	bytes)				
	Certificate Lengt	h: 1656				
	E Certificaté (id-a	t-commonNane=TORISE20A.rtpaa	a.net,id-at-orga	nizationalunitwame=RTPAAA,id-at-organizationName=CISCO,id-at-localityName=R1		
	Certificate Length: 13/9					
	E Certificate (id-a	t-commonwane=rtpaaa-ca,dc=rt	paaa,oc=net)			
Ι.	I ILSVI RECORD Layer: Handshake Protocol: Server Hello Done					

チェーンが不完全な場合は、ISE Administration > Certificates > Trusted Certificatesの順に移動し 、ルート証明書および(または)中間証明書が存在することを確認します。証明書チェーンが正 常に渡された場合は、ここで説明する方法を使用して、チェーン自体が有効であることを確認す る必要があります。

各証明書(サーバ、中間、およびルート)を開き、各証明書のSubject Key Identifier(SKI)を、チェーン内の次の証明書のAuthority Key Identifier(AKI)と照合して、信頼のチェーンを確認します。

証明書チェーンの例。

Certificate 25	Certificate 25	Certificate 25
General Details Certification Path	General Details Certification Path	General Details Certification Path
Show <all></all>	Show <all></all>	Show <all></all>
Field Value A	Field Value ^	Field Value *
Public key RSA (2048 88s)	CA Version V0.0	Public key RSA (4096 Bits)
ESubject Key Identifier da 39 a3 ee 5e 6b 4b 0d 32 55 bf ef 95 6	Subject Key Identifier fe 34 ca 8d 22 9b 6e d7 a6 86 11 cl 18 1.	Key Usage Digital Signature, Certificate Signing, Off-I
Enhanced Key Usage Server Authentication (1.3.6.1.5.5.7.3.1)	E Certificate Templat SubCA	Subject Key Ident 52 2e e5 2c 38 29 66 da 81 19 11 70 74 00
Subject Alternative IP Address=14.36.157.21	Authority Key Identif KeyID=52 2e e5 2c 38 29 d6 da 81 19 11	CA Version V0.0
Authority Key Identi KeyID=fe 34 ca 8d 22 9b 6e d7 a6 86 11	CRL Distribution Pol [1]CRL Distribution Point: Distribution Pol	Basic Constraints Subject Type=CA, Path Length Constraint= ::
CRL Distribution Pol [1]CRL Distribution Point: Distribution Pol	Authority Informatio [1] Authority Info Access: Access Method	Thumbprint algori sha1
Authority Informati [1] Authority Info Access: Access Method +	Key Usage Digital Signature, Certificate Signing, Off-L +	Thumbprint cb 24 48 a5 30 11 72 a3 da 9e 31 d1 f3 f6 +
•	· · · · · · · · · · · · · · · · · · ·	€
A3	1/3	V3
		-
Edit Properties Copy to File	Edit Properties Copy to File	Edit Properties Copy to File
Learn more about <u>certificate details</u>	Learn more about certificate details	Learn more about certificate details
OK	OK	OK

ISE証明書チェーンは正しいが、認証中にエンドポイントがISEサーバ証明書を拒否 する

SSLハンドシェイク中にISEが完全な証明書チェーンを提示し、サプリカントが引き続き証明書チ ェーンを拒否する場合は、次の手順で、ルート証明書および(または)中間証明書がクライアン トのローカル信頼ストアにあることを確認します。

Windowsデバイスからこれを確認するには、mmc.exe File > Add-Remove Snap-inに移動します 。Available snap-ins列からCertificatesを選択し、Addをクリックします。使用している認証タイ プ(ユーザまたはマシン)に応じて、My user accountまたはcomputer accountのいずれかを選択 し、OKをクリックします。

コンソールビューでTrusted Root Certification AuthoritiesとIntermediate Certification Authoritiesを 選択し、ローカルの信頼ストアにルート証明書と中間証明書が存在することを確認します。

Sile Action View Favorites Window Help ← ⇒ 2 □ □ □ 0 → 0 □					
Console Root	Issued To	Issued By	Expiration	Intended Purpo	Friendly Name
 Certificates - Current User Personal Trusted Root Certification Authorities Certificates Enterprise Trust Intermediate Certification Authorities Certificate Revocation List Certificates Certificates Active Directory User Object Trusted Publishers 	AddTrust External CA Root Baltimore CyberTrust Root Certum CA Cisco Root CA 2048 Cisco Root CA M1 Class 2 Primary CA Class 3 Public Primary Ce COMODO RSA Certificati COpyright (c) 1997 Micro	AddTrust External CA Root Baltimore CyberTrust Root Certum CA Cisco Root CA 2048 Cisco Root CA M1 Class 2 Primary CA Class 3 Public Primary Certi COMODO RSA Certificatio Copyright (c) 1997 Microso	5/30/2020 5/12/2025 6/11/2027 5/14/2029 11/18/2033 7/6/2019 8/1/2028 1/18/2038 12/30/1999	Server Authenti Server Authenti Server Authenti <all> <all> Secure Email, S Secure Email, C Server Authenti Time Stamping</all></all>	USERTrust Baltimore Cybe Certum <none> <none> CertPlus Class 2 VeriSign Class 3 COMODO Microsoft Time</none></none>
Certificates Intrusted Certificates Intrusted Certification Authorities Intrusted People Other People Certificate Enrollment Requests Intrusted Roots	DigiCert Assured ID Root DigiCert Global Root CA DigiCert High Assurance DST Root CA X3 DST Root CA X3 DST Root Certification	DigiCert Assured ID Root C DigiCert Global Root CA DigiCert High Assurance E DST Root CA X3 DST Root CA X3 Entrust Root Certification	11/9/2031 11/9/2031 11/9/2031 9/30/2021 9/30/2021 11/27/2026	Server Authenti Server Authenti Server Authenti Secure Email, S <all> Server Authenti</all>	DigiCert DigiCert DIgiCert DST Root CA X3 <none> Fotoust</none>

これがサーバIDチェックの問題であることを確認する簡単な方法として、サプリカントプロファ イル設定でValidate Server Certificateのチェックマークを外して、もう一度テストします。

Connection Security	When connecting:	
Security type: WPA2-Enterprise	Connect to these servers:	_
Encryption type: AES	Trusted Root Certification Authorities:]
	AddTrust External CA Root	٦
	Baltimore CyberTrust Root	
Choose a network authentication method:	Certum CA	1
Microsoft: Protected EAP (PEAP)	Cisco Root CA 2048	
Indebola Protected Lis (i Lis)	Cisco Root CA M1	
Remember my credentials for this connection each	Class 2 Primary CA	
time I'm logged on	Class 3 Public Primary Certification Authority	
	COMORO DEL CUMPLICA Labora	

関連情報

- <u>Cisco Identity Services Engine 管理者ガイド リリース 3.0</u>
- シスコのテクニカルサポートとダウンロード

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。