OpenAPIを使用したISE 3.3でのISE証明書情報 の取得

内容

 はじめに

 茸屋

 前提条件

 要件

 使用するコンポーネント

 設定

 ネットワーク図

 ISEでの設定

 Pythonの例

 特定のノードのすべてのシステム証明書を取得する

 特定のノードのすべてのシステム証明書を取得する

 すべての信頼できる証明書の一覧を取得する

 しによる信頼証明書の取得

はじめに

このドキュメントでは、openAPIを使用してCisco Identity Services Engine(ISE)証明書を管理する手順について説明します。

背景

企業ネットワークのセキュリティと管理がますます複雑化する中、Cisco ISE 3.1では、証明書ラ イフサイクル管理を合理化するOpenAPI形式のAPIを導入し、効率的で安全な証明書操作のため の標準化および自動化されたインターフェイスを提供して、管理者が強力なセキュリティ対策を 実施し、ネットワークコンプライアンスを維持できるようにします。

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。

- Cisco Identity Services Engine (ISE)
- REST API
- Python

使用するコンポーネント

- ISE 3.3
- Python 3.10.0

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。

設定

ネットワーク図



ISEでの 設定

ステップ1:Open API adminアカウントを追加します。

API管理者を追加するには、Administration -> System -> Administration -> Administrators -> Admin Users -> Addの順に移動します。

≡	dentity Services	Engine		Administration / System						A (lcense Warning	Q	۵	0	φ	8		
щ	Bookmarks	Deployment Licensing	Cer	rtificates	Logging	Maintenance	Upgrade	Health	Checks	Backup & R	estore	Admin Access	Settings					
5	Dashboard	Authentication		Adm	inistrat	ore												
15	Context Visibility	Authorization	>	Aum	แกรแลแ	515								5	elected (Total 2	a	ക
*	Operations	Administrators	~	0 Edit	+ Add	Change Status	Delete	Duplicate								,	u ~	V
0	Policy	Admin Users Admin Groups			Status	Name	Descrip	tion	First Name	Last Name	Email Addr	ess Admin Gr	oups					
20	Administration				Enabled	admin 😝	Default	Admin User				Super Ad	min					
rili.	Work Centers	Settings	>		Enabled	a ApiAdmin						ERS Adm	in					
?	Interactive Help																	

API管理者

ステップ2:ISEでOpen APIを有効にする

ISEでは、オープンAPIはデフォルトで無効になっています。これを有効にするには、 Administration > System > API Settings > API Service Settingsの順に移動します。Open APIオプ ションを切り替えます。[Save] をクリックします。



OpenAPIの有効化

ステップ3:ISEオープンAPIを調べる

Administration > System > API Settings > Overviewの順に移動します。「APIを開く」をクリック します。

≡	diale Identity Services	Engine			Administration / System							Q	۵ (A A	
Щ	Bookmarks	Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings					
	Dashboard	Client Provisioni	ng													
망	Context Visibility	FIPS Mode Security Setting	5	API S	API Service	a Settings API G	ateway Settings									
0	Policy	Alarm Settings General MDM /	UEM Settings	API Serv	ices Overvie											
8.	Administration	Posture		> You can m	an manage Cisco ISE nodes through two sets of API formats-External Restful Services (ERS) and OpenAPI.											
đ	Work Centers	Profiling		The ERS a Currently,	CISCO DEL Revelase 3.1, new APIS are available in the UppenAPI format. § and OpenAPI services are HTTPS-only REST APIs that operate over port 443. IN EPS APIs also poerate over one 90 600 However port 9060 million to the supported for EPS APIs in later											
		Protocols		> Cisco ISE Both the A	eleases. We ree PI services are	commend that you on disabled by default. E	ly use port 443 nable the API se	for ERS APIs. ervices by clicking the c	corresponding toggle buttor	15						
?	Interactive Help	Endpoint Script	5	> To use eith	Service Settings er API service,	i tab. you must have the ER	S-Admin or ERS	-Operator user group	assignment.							
		Proxy SMTP Server SMS Gateway System Time API Settings		For more in https://10. For opena ERS_V1 For more in https://10.	nformation on IS 106.33.92:4424 pi documention nformation on IS 106.33.92:4424	E ERS API, please vis to/ers/sdk for ERS, click below: ECOneo API, please v to/api/swagger-ui/inc 125.426	sit: dox.html									

OpenAPIにアクセス

Pythonの例

特定のノードのすべてのシステム証明書を取得する

APIは、特定のISEノードのすべての証明書をリストします。

ステップ1:APIコールに必要な情報。

メソッド	GET
URL	https:// <ise-pan-ip>/api/v1/certs/system- certificate/<ise-node-hostname></ise-node-hostname></ise-pan-ip>
Credentials	Open APIアカウントの資格情報を使用する
ヘッダー	受け入れ:application/json Content-Type:application/json

ステップ2:特定のISEノードの証明書を取得するために使用されるURLを特定します。

How Select a definition Certificates	×	
Cisco ISE API - Certificates (IDD) (AS) https://10.106.33.92.4424/https//Japi-docr/typoup-Certificates		
Servers https://10.106.33.92:44240 - Inferred Url v		
certs-api-controller the certs API	~	
Certificates	^	
CET /api/vl/certs/certificate-signing-request Get all Certificate Signing Requests from PAN	∨ ≜	
POST /api/vl/certs/certificate-signing-request Generate a Certificate Signing Request (CSR)	∨ ≜	
CET /api/vl/certs/certificate-signing-request/{hostName}/{id} Get the certificate signing request for a given ID	∨ ≜	
DELETE /api/vl/certs/certificate-signing-request/{hostName}/{id} Delete the certificate signing request for a given ID	∨ ≜	
CET /api/v1/certs/certificate-signing-request/export/{hostname}/{id} Export a CSR for a given CSR ID and hostname	∨ ≜	
POST /api/v1/certs/certificate-signing-request/intermediate-ca Generate an Intermediate CA CSR (certificate signing request)	✓ ≜	
POST /api/v1/certs/ise-root-ca/regenerate Regenerate entire internal CA certificate chain including root CA on the primary PAN and subordinate CAs on the PSNs (Applicable only for in	itemal CA service) 🗸 🗎	
POST /api/v1/certs/renew-certificate Ranew certificates of OCSP responder and Cisco ISE Messaging Service	✓ ≜	
POST /api/v1/certs/signed-certificate/bind Bind CA Signed Certificate	✓ ≜	
CET /api/vl/certs/system-certificate/{hostName} Set all system certificates of a particular node	^ ≜	
This API supports filtering, sorting and pagination.		

API URI(API URI)

ステップ3:Pythonコードの例を次に示します。コンテンツをコピーして貼り付けます。ISEのIP、 ユーザ名、パスワードを置き換えます。実行するPythonファイルとして保存します。

ISEとPythonコード例を実行しているデバイスの間の接続が良好であることを確認します。

<#root>

from requests.auth import HTTPBasicAuth import requests

requests.packages.urllib3.disable_warnings()

if _____name___ == "____main___":

url = "

https://10.106.33.92/api/v1/certs/system-certificate/ISE-DLC-CFME02-PSN

••

```
headers = {
    "Accept": "application/json", "Content-Type": "application/json"
    basicAuth = HTTPBasicAuth(
    "ApiAdmin", "Admin123"
)
    response = requests.get(url=url, auth=basicAuth, headers=headers, verify=False)
    print("Return Code:")
    print(response.status_code)
    print("Expected Outputs:")
    print(response.json())
```

次に、予想される出力の例を示します。

Return Code: 200 Expected Outputs: {'response': [{'id': '5b5b28e4-2a51-495c-8413-610190e1070b', 'friendlyName': 'Default self-signed saml server certificate - CN=SAML_ISE-DLC-CFME0

特定のノードのシステム証明書をIDで取得する

このAPIは、指定されたホスト名とIDに基づいて、特定のノードのシステム証明書の詳細を提供します。

ステップ1:APIコールに必要な情報。

メソッド	GET
URL	https:// <ise-pan-ip>/api/v1/certs/system- certificate/<ise-node-hostname>/<id-of- Certificate></id-of- </ise-node-hostname></ise-pan-ip>
Credentials	Open APIアカウントの資格情報を使用する
ヘッダー	受け入れ:application/json Content-Type:application/json

ステップ2:指定されたホスト名とIDに基づいて特定のノードの証明書を取得するために使用されるURLを見つけます。

Cisco ISE API - Certificates (ISB) (CSB) Hegeuri 101 33 92 424 Wagev Step-does tyroup-Centrales		
Servers https://10.106.33.92:44240 - Inferred Url v		
certs-api-controller the certs API	~	
Certificates	^	
GET /api/vl/certs/certificate-signing-request Get all Certificate Signing Requests from PAN	✓ ≜	
POST /api/vl/certs/certificate-signing-request Generate a Certificate Signing Request (CSR)	 ✓ ≜ 	
GET /api/vl/certs/certificate-signing-request/{hostName}/{id} Get the certificate signing request for a given ID	∨ ≜	
DELETE /api/vl/certs/certificate-signing-request/{hostName}/{id} Delete the certificate signing request for a given ID	 ✓ ≜ 	
GET /api/vl/certs/certificate-signing-request/export/{hostname}/{id} Export a CSR for a given CSR ID and hostname	∨ ≜	
POST /api/v1/certs/certificate-signing-request/intermediate-ca Generate an intermediate CA CSR (certificate signing request)	 ✓ ≜ 	
POST /api/vl/certs/ise-root-ca/regenerate Regenerate entire internal CA certificate chain including root CA on the primary PAN and subordinate CAs on the PSNs (Applicable only for internal CA service)	✓ ≜	
POST /api/vl/certs/renew-certificate Renew certificates of OCSP responder and Cisco ISE Messaging Service	✓ ≜	
POST /api/vl/certs/signed-certificate/bind Bind CA Signed Certificate	 ✓ ≜ 	
GET /api/vl/certs/system-certificate/{hostName} Get all system certificates of a particular node	 → 	
GET /api/vl/certs/system-certificate/{hostName}/{id} Get system certificate of a particular node by ID	<u>∧</u> ≜	
This API provides details of a system certificate of a particular node based on given hostname and ID.		

API URI(API URI)

ステップ3:ここはPythonコードの例です。コンテンツをコピーして貼り付けます。ISEのIP、ユ ーザ名、パスワードを置き換えます。実行するPythonファイルとして保存します。

ISEとPythonコード例を実行しているデバイスの間の接続が良好であることを確認します。

<#root>

from requests.auth import HTTPBasicAuth import requests requests.packages.urllib3.disable_warnings() if __name__ == "__main__": url = "

https://10.106.33.92/api/v1/certs/system-certificate/ISE-DLC-CFME02-PSN/5b5b28e4-2a51-495c-8413-610190e2

" headers = {

"Accept": "application/json", "Content-Type": "application/json"

} basicAuth = HTTPBasicAuth(

"ApiAdmin", "Admin123"

) response = requests.get(url=url, auth=basicAuth, headers=headers, verify=False) print("Return Code:")



注:このIDは、「特定のノードのすべてのシステム証明書の取得」のステップ3のAPI出 力からのものです。たとえば、5b5b28e4-2a51-495c-8413-610190e1070bは「デフォル トの自己署名証明書 – CN=SAML_ISE-DLC-CFME02-PSN.cisco.com」です。

次に、予想される出力の例を示します。

Return Code: 200 Expected Outputs:

{'response': {'id': '5b5b28e4-2a51-495c-8413-610190e1070b', 'friendlyName': 'Default self-signed saml server certificate - CN=SAML_ISE-DLC-CFME02

すべての信頼できる証明書の一覧を取得する

APIは、ISEクラスタのすべての信頼できる証明書をリストします。

メソッド	GET
URL	https:// <ise-pan-ip>/api/v1/certs/trusted- certificate(信頼できる証明書)</ise-pan-ip>
Credentials	Open APIアカウントの資格情報を使用する
ヘッダー	受け入れ:application/json Content-Type:application/json

ステップ2:信頼できる証明書を取得するために使用されるURLを見つけます。

POST /api/vl/certs/certificate-signing-request/intermediate-ca Generate an intermediate CA CSR (certificate signing request)	\sim	1
POST /api/vl/certs/ise-root-ca/regenerate entire internal CA certificate chain including root CA on the primary PAN and subordinate CAs on the PSNs (Applicable only for internal CA service)	\sim	-
POST /api/vl/certs/renew-certificate Renew certificates of OCSP responder and Cisco ISE Messaging Service	\sim	1
POST /api/vl/certs/signed-certificate/bind Bind CA Signed Certificate	\sim	1
GET /api/vl/certs/system-certificate/{hostName} Get all system certificates of a particular node	\sim	-
GET /api/vl/certs/system-certificate/{hostName}/{id} Get system certificate of a particular node by ID	\sim	1
PUT /api/vl/certs/system-certificate/{hostName}/{id} Update data for existing system certificate	\sim	â
DELETE /api/vl/certs/system-certificate/{hostName}/{id} Delete System Certificate by ID and hostname	\sim	â
POST /api/v1/certs/system-certificate/export Export a system certificate with a given a certificate ID	\sim	-
POST /api/v1/certs/system-certificate/generate-selfsigned-certificate Generate self-signed certificate in Cisco ISE	\sim	â
POST /api/vl/certs/system-certificate/import Import system certificate in Claco ISE	\sim	-
GET /api/vl/certs/trusted-certificate Get list of all busked certificates	^	-
This API supports Filtering, Sorting and Pagination.		
Filtering and Sorting are supported for the following attributes:		
foreign (vanie vanie vanie vanie		
• IssuedPo • IssuedPy		
vade-foll super-fold Date Format sympholic Add HH mm ss Superioritid Date Format Sympholic Control (Strength Contro) (Strength Control (Strength Control (Strength Control (Streng)		
expiratedcubae expiratedcubae supported Date Format: yyyy-MM-dd HR mm as		
supported coperators: LC) Net (c) and L1 fallus // fallus		
Supported Operators: EQ, NEQ		
Note: ISE internal CA certificates will not be exported.		

API URI(API URI)

ステップ3:ここはPythonコードの例です。コンテンツをコピーして貼り付けます。ISEのIP、ユ ーザ名、パスワードを置き換えます。実行するPythonファイルとして保存します。

ISEとPythonコード例を実行しているデバイスの間の接続が良好であることを確認します。

<#root>

from requests.auth import HTTPBasicAuth import requests requests.packages.urllib3.disable_warnings() if __name__ == "__main__": url = "

https://10.106.33.92/api/v1/certs/trusted-certificate

```
" headers = {
```

"Accept": "application/json", "Content-Type": "application/json"

} basicAuth = HTTPBasicAuth(

"ApiAdmin", "Admin123"

) response = requests.get(url=url, auth=basicAuth, headers=headers, verify=False) print("Return Code:")

想定される出力例を以下に示します(略)。

Return Code:

200

Expected Outputs:

{'response': [{'id': '147d97cc-6ce9-43d7-9928-8cd0fa83e140', 'friendlyName': 'VeriSign Class 3 Public Primary Certification Authority', 'subject': 'CN=Veri

IDによる信頼証明書の取得

このAPIは、指定されたIDに基づいて信頼証明書の詳細を表示できます。

ステップ1:APIコールに必要な情報。

メソッド	GET
URL	https:// <ise-pan-ip>/api/v1/certs/trusted- certificate/<id-of-certificate></id-of-certificate></ise-pan-ip>
Credentials	Open APIアカウントの資格情報を使用する
ヘッダー	受け入れ:application/json Content-Type:application/json

手順2:展開情報の取得に使用するURLを見つけます。

Cisco ISE API - Certificates (ICO) (ASS) https://10.106.33.92.442.40/ape//Step-doc/fprup-Certificates		
Servers https://10.106.33.92:44240 - Inferred Uri		
certs-api-controller the certs API	~	
Certificates	^	
GET /api/v1/certs/certificate-signing-request Get all Certificate Signing Requests from PAN	× 🗎	
POST /api/vl/certs/certificate-signing-request Generate a Certificate Signing Request (CSR)	~ ≙)
GET /api/v1/certs/certificate-signing-request/{hostName}/{id} Get the certificate signing request for a given	ID 🗸 🗎)
DELETE /api/v1/certs/certificate-signing-request/{hostName}/{id} Delete the certificate signing request for a given by	ven ID 🗸 🔪	
GET /api/v1/certs/certificate-signing-request/export/{hostname}/{id} Export a CSR for a given CSR ID	and hostname \checkmark \cong	
POST /api/v1/certs/certificate-signing-request/intermediate-ca Generate an Intermediate CA CSR (confilca	e signing request) 🗸 🗎)
POST /api/v1/certs/ise-root-ca/regenerate Regenerate entire internal CA certificate chain including root CA on the prime	iny PAN and subordinate CAs on the PSNs (Applicable only for internal CA service) $$	
POST /api/v1/certs/renew-certificate Renew certificates of OCSP responder and Claco ISE Messaging Service	✓ [≜]	
POST /api/vl/certs/signed-certificate/bind Bind CA Signed Certificate	✓ â)
OET /api/vl/certs/system-certificate/{hostName}. Get all system certificates of a particular node	~ ≜	
GET /api/v1/certs/system-certificate/{hostName}/{id} Get system certificate of a particular node by ID	^ ≜	
This API provides details of a system certificate of a particular node based on given hostname and ID.		

ステップ3:ここはPythonコードの例です。コンテンツをコピーして貼り付けます。ISEのIP、ユ ーザ名、パスワードを置き換えます。実行するPythonファイルとして保存します。

ISEとPythonコード例を実行しているデバイスの間の接続が良好であることを確認します。

<#root>

from requests.auth import HTTPBasicAuth import requests.packages.urllib3.disable_warnings() if __name__ == "__main__": url = "

https://10.106.33.92/api/v1/certs/trusted-certificate/147d97cc-6ce9-43d7-9928-8cd0fa83e140

" headers = $\{$

"Accept": "application/json", "Content-Type": "application/json"

} basicAuth = HTTPBasicAuth(

"ApiAdmin", "Admin123"

) response = requests.get(url=url, auth=basicAuth, headers=headers, verify=False) print("Return Code:")



注:このIDは、「すべての信頼できる証明書のリストの取得」のステップ3のAPI出力からのものです。たとえば、 147d97cc-6ce9-43d7-9928-8cd0fa83e140は、「VeriSign Class 3 Public Primary Certification Authority」です。

次に、予想される出力の例を示します。

Return Code: 200 Expected Outputs: {'response': {'id': '147d97cc-6ce9-43d7-9928-8cd0fa83e140', 'friendlyName': 'VeriSign Class 3 Public Primary Certification Code: 200 Expected Outputs: {'response': {'id': '147d97cc-6ce9-43d7-9928-8cd0fa83e140', 'friendlyName': 'VeriSign Class 3 Public Primary Certification Code: 200 Expected Outputs: {'response': {'id': '147d97cc-6ce9-43d7-9928-8cd0fa83e140', 'friendlyName': 'VeriSign Class 3 Public Primary Certification Code: 200 Expected Outputs: {'response': {'id': '147d97cc-6ce9-43d7-9928-8cd0fa83e140', 'friendlyName': 'VeriSign Class 3 Public Primary Certification Code: 200 Expected Outputs: {'response': {'id': '147d97cc-6ce9-43d7-9928-8cd0fa83e140', 'friendlyName': 'VeriSign Class 3 Public Primary Certification Code: 200 Expected Outputs: {'response': {'respon

トラブルシュート

オープンAPIに関連する問題をトラブルシューティングするには、デバッグログ設定ウィンドウでtheapiservicecomponentのログレ ベルをDEBUGに設定します。

デバッグを有効にするには、Operations -> Troubleshoot -> Debug Wizard -> Debug Log Configuration -> ISE Node -> apiserviceの 順に移動します。

≡	dentity Services	Engine	Operations / Troubleshoot						Q	۵	0	٩	A
н	Bookmarks	Diagnostic Tools Download Lo	ogs Del	bug Wizard									
태 명 ※	Dashboard Context Visibility Operations	Debug Profile Configuration Debug Log Configuration	Node List Debi	ug Level Co	meld.com	1						6	3
0	Policy		0 Edit	🕁 Reset to Default	Log Filter Enable	Log Filter Disable					AI	~ 5	7
80	Administration			Component Name	∧ Log Level	Description	Log file Name	Log Filter					
nii:	Work Centers		0	accessfilter	INFO	RBAC resource access filter	ise-psc.log	Disabled					1
			0	Active Directory	WARN	Active Directory client internal messages	ad_agent.log						
?	Interactive Help		0	admin-ca	INFO	CA Service admin messages	ise-psc.log	Disabled					
			0	admin-infra	INFO	infrastructure action messages	ise-psc.log	Disabled					
			0	admin-license	INFO	License admin messages	ise-psc.log	Disabled					
			0	ai-analytics	INFO	AI Analytics	ai-analytics.log	Disabled					
			0	anc	INFO	Adaptive Network Control (ANC) debug	ise-psc.log	Disabled					
			0	api-gateway	INFO	API Gateway native objects logs	api-gateway.log	Disabled					
			0	apiservice	DEBUG	ISE API Service logs	api-service.log	Disabled					
			0	bootstrap-wizard	INFO	Bootstrap wizard messages Save Can	-psc.log	Disabled					
			0	ca-service	INFO	CA Service messages	caservice.log	Disabled					

APIサービスのデバッグ

デバッグログをダウンロードするには、Operations -> Troubleshoot -> Download Logs -> ISE PAN Node -> Debug Logsの順に移動 します。

≡	dentity Services	Engine	9			Operations / Trou	ıbleshoot		🔺 License Warning	Q	۵	0	$\varphi \mid \varphi$
Ц	Bookmarks	Diagn	ostic Tools	Download Logs	Debug Wi	zard							
53	Dashboard		ISE-B	GL-CFME01-PAN									
망	Context Visibility		ISE-B	GL-CFME02-MNT	Delete	e [®] Expand All ≤>Collapse	All	Barra da da					
*	Operations		E ISE-D	C-CEME02-PSN	Deb	ug Log Type	Log File	Description	Size				
0	Policy		ISE-R	TP-CFME01-PAN	✓ Applica	ition Logs							
20	Administration		ISE-R	TP-CFME02-MNT	> 1	ad_agent (1) (100 KB)							
-fili	Work Centers		×			ai-analytics (11) (52 KB) api-gateway (16) (124 KB)							
					× 1	api-service (13) (208 KB)		1					
?	Interactive Help						api-service (all logs)	API Service debug messages	208 KB				
							api-service.log		12 KB				
							api-service.log.2024-03-24-1		4.0 KB				
							api-service.log.2024-04-07-1		4.0 KB				
					1								

デバッグログのダウンロード

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。