使用OpenAPI檢索ISE 3.3上的ISE證書資訊

目錄	
<u>背景</u>	
<u>必要條件</u>	
<u>需求</u>	
<u>採用元件</u>	
<u>設定</u>	
網路圖表	
<u>ISE上的配置</u>	
<u>Python示例</u>	
<u>取得特定節點的所有系統憑證</u>	
按ID取得特定節點的系統憑證	
<u>取得所有信任憑證的清單</u>	
透過ID獲取信任證書	
<u>疑難排解</u>	

簡介

本檔案介紹使用openAPI管理思科身分辨識服務引擎(ISE)憑證的程式。

背景

面對企業網路安全和管理日益成長的複雜性,思科ISE 3.1引入了OpenAPI格式的API,簡化了證書 生命週期管理,提供標準化和自動化介面以實現高效安全的證書操作,幫助管理員實施強大的安全 實踐並保持網路合規性。

必要條件

需求

思科建議您瞭解以下主題:

- 思科身分辨識服務引擎(ISE)
- REST API
- Python

採用元件

- ISE 3.3
- Python 3.10.0

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

設定

網路圖表



ISE上的配置

第1步:增加打開API admin帳戶

要增加API管理員,請導航到管理>系統>管理員訪問許可權>管理員>管理員使用者>增加。

≡	dentity Services I	Engine				Administra	ation / System			Le Ue	ense Warning	Q (۵ ۵	Q	۹
Ц	Bookmarks	Deployment I	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restor	re Admin Access	Settings				
5	Dashboard	Authentication		Ada											
망	Context Visibility	Authorization		Adn	ninistrat	ors									da.
×	Operations	Administrators		/ D Edit	+ Add	🛞 Change Status	Delete 🗍 Dur	licate				Select	ed 0 Total 2	NIV 1	87 V
U	Policy	Admin Users		0	Status	Name	Description	First Name	Last Name Ema	il Address Admin Grou	ips				
20	Administration			0	Enabled	y admin	Default Admir	User		Super Admi	in				
nii.	Work Centers	Settings			Enabled	a ApiAdmin				ERS Admin					
(?)	Interactive Help														

API管理

第2步:在ISE上啟用開放式API

預設情況下,在ISE上停用開放式API。要啟用該功能,請導航到管理>系統>設定> API設定> API服 務設定。切換「開啟API」選項。按一下Save。

≡	diale Identity Services	Engine				Administrat	tion / Syster	n		_	License Warning	Q	۵ (୭ ଦ	2 A
щ	Bookmarks	Deployment Lice	nsing Ce	ertificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings				
	Einer Trovisioning Cleant Provisioning I'D Subbadd First Made Sociarty Visibility Sociarty Settings Aturn Settings Curview Betwer Aturn Settings Curview API Service Settings Aturn Settings Overview Betwer Policy Proticing Proticing Proticing First (Read/Write) Proticing First (Read/Write) Proticing First (Read/Write) Protice Setting for All Other Nodes Protice Setting for All Other Nodes Proty Enservice Sign Greany First (Read) Proty Enservice Setting for All Other Nodes Proty Enservice Sign Greany First (Read) Proty Enservice Setting for All Other Nodes Proty Enservice Sign Greany First (Read) Proty Enservice Setting for All Other Nodes Proty Enservice Sign Greany Open API (Read) Sign Greany Context (only for ERS Settings) Or CSRF Check (only for ERS Settings) Or Lable CSRF Check for Enhanced Security (Not compatible with pre ISE 2.3 Clients) O Instable CSRF Check Set For ERS Request (compatible with pre ISE 2.3 Clients)														
		DHCP & DNS Services Max Sessions Light Data Distribution Endpoint Replication										Rese	t	SI	ave

啟用OpenAPI

第3步:探索ISE開放式API

導航到管理>系統>設定> API設定>概述。點選打開API訪問連結。

≡	diale Identity Services I	Engine				Administra	tion / Syster	n		A	lcense Warning	Q	۵ ۵	Q Q		
Щ	Bookmarks	Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings					
- 55	Dashboard	Client Provisioni	ing													
명	Context Visibility	FIPS Mode Security Setting	5	API S	Settings											
×	Operations	Alarm Settings		Overview	API Service	Settings API G	ateway Settings									
0	Policy	General MDM /	UEM Settings	API Ser	vices Overvie	w										
80	Administration	Posture		> You can n Starting C	anage Cisco ISE isco ISE Release	nodes through two s	ets of API forma	ts-External Restful Ser	vices (ERS) and OpenAPI.							
đ	Work Centers	Profiling		The ERS a Currently,	The ERS and OpenAPI services are HTTPS-only REST APIs that operate over port 443. Currently, ERS APIs also operate over port 9060. However, port 9060 might not be supported for ERS APIs in later											
		Protocols		> Cisco ISE Both the A	Cisco ISE releases. We recommend that you only use port 443 for ERS APIs. Both the API services are disabled by default. Enable the API services by clicking the corresponding toggle buttons											
?	Interactive Help	Endpoint Script	ts	> To use eit	In the API service Settings tab. To use either API service, you must have the ERS-Admin or ERS-Operator user group assignment.											
		Proxy SMTP Server SMS Gateway System Time		For more information on ISE ERS API, please visit: https://10.106.33.92:44240/ers/sdk For openapi documention for ERS, click below: ERS_V1												
		Data Connect				ERS API										

訪問OpenAPI

Python示例

取得特定節點的所有系統憑證

API列出特定ISE節點的所有證書。

第1步:API呼叫的必要資訊。

方法	取得
URL	https:// <ise-pan-ip>/api/v1/certs/system- certificate/<ise-node-hostname></ise-node-hostname></ise-pan-ip>

憑證	使用Open API帳戶慿據
標頭	接受:application/json Content-Type: application/json

第2步:查詢用於檢索特定ISE節點證書的URL。

Select a definition Certificates	Υ.	
Cisco ISE API - Certificates (IDD) (ASS) https://10.106.33.82-44240egv/Jage-does/tyroup-Certificates		
Servers https://10.106.33.92:44240 - Inferred Uri 🗸		
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)	∨ ≜	
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	∨ ≜	
GET /api/vl/certs/certificate-signing-request/export/{hostname}/{id} Export a CSR for a given CSR ID and hostname	✓ ≜	
POST /api/vl/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)	ice) 🗸 🗎	
POST /api/vi/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	^ ≜	
This API supports filtering, sorting and pagination.		

API URI

第3步:以下是Python代碼的示例。複製並貼上內容。替換ISE IP、使用者名稱和密碼。另存為要執 行的python檔案。

確保ISE與運行python代碼示例的裝置之間保持良好的連線。

<#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())
```

以下是預期輸出的範例。

Return Code:

200

Expected Outputs:

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

按ID取得特定節點的系統憑證

此API根據給定的主機名和ID提供特定節點的系統證書的詳細資訊。

第1步:API呼叫的必要資訊。

方法	取得
URL	https:// <ise-pan-ip>/api/v1/certs/system- certificate/<ise-node-hostname>/<id-of- Certificate></id-of- </ise-node-hostname></ise-pan-ip>
憑證	使用Open API帳戶憑據
標頭	接受:application/json Content-Type: application/json

第2步:根據給定的主機名和ID查詢用於檢索特定節點證書的URL。

Cisco ISE API - Certificates CSS CSS	
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 bootname	/ 🗎
POST /api/vl/certs/certificate-signing-request/intermediate-ca Generate an intermediate CA CSR (certificate signing request)	/ 🚔
POST /api/vl/certs/ise-root-cs/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	/ 🚔
OET /api/vl/certs/system-certificate/{hostName} Get all system certificates of a particular node	× 🚔
OET /api/vl/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.	

API URI

第3步:以下是Python代碼的示例。複製並貼上內容。替換ISE IP、使用者名稱和密碼。另存為要執 行的python檔案。

確保ISE與運行python代碼示例的裝置之間保持良好的連線。

<#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:")



註:ID來自「獲取特定節點的所有系統證書」步驟3中的API輸出,例如,5b5b28e4-2a51-495c-8413-610190e1070b為「預設自簽名saml伺服器證書- CN=SAML_ISE-DLC-CFME02-PSN.cisco.com」。

以下是預期輸出的範例。

Return Code: 200 Expected Outputs:

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

取得所有信任憑證的清單

API列出ISE集群的所有受信任證書。

第1步:API呼叫的必要資訊。

方法	取得
URL	https:// <ise-pan-ip>/api/v1/certs/trusted- certificate</ise-pan-ip>
憑證	使用Open API帳戶憑據
標頭	接受:application/json Content-Type: application/json

第2步:查詢用於檢索受信任證書的URL。

POST /api/vl/certs/certificate-si	gning-request/intermediate-ca Generate an intermediate CA CSR (certificate signing request)	\sim	-
POST /api/vl/certs/ise-root-ca/re	generate 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-certific	ate Renew certificates of OCSP responder and Cisco ISE Messaging Service	\sim	-
POST /api/vl/certs/signed-certifi	cate/bind Bind CA Signed Certificate	\sim	â
GET /api/vl/certs/system-certifi	cate/{hostName} Get all system certificates of a particular node	\sim	ŵ
GET /api/vl/certs/system-certifi	cate/{hostName}/{id} Get system certificate of a particular node by ID	\sim	ŵ
PUT /api/v1/certs/system-certifi	cate/{hostName}/{id} Update data for existing system certificate	\sim	-
DELETE /api/vl/certs/system-certifi	cate/{hostName}/{id} Delete System Certificate by ID and hostname	\sim	ŵ
POST /api/v1/certs/system-certifi	cate/export Export a system certificate with a given a certificate ID	\sim	ŵ
POST /api/vl/certs/system-certifi	cate/generate-selfsigned-certificate Generate self-signed certificate in Cisco ISE	\sim	ŵ
POST /api/v1/certs/system-certifi	cate/import Import system certificate in Claco ISE	\sim	ŵ
GET /api/v1/certs/trusted-certif	icate Get list of all trusted certificates	^	ŵ
This API supports Filtering, Sorting and Pagination.			
Filtering and Sorting are supported for the following • transfyrkame • subject • subject • subject • subject of the format: yyyy-AM-dd HH rmm • supported Operators: EO, NEO, OT and LT • supported Operators: EO, NEO, OT and LT • status • Allowed Values: enabled, disabled • Supported Operators: EO, NEO, • Allowed Values: enabled, disabled • Supported Operators: EO, NEO,	athributes: 55 55		

API URI

第3步:以下是Python代碼的示例。複製並貼上內容。替換ISE IP、使用者名稱和密碼。另存為要執 行的python檔案。

確保ISE與運行python代碼示例的裝置之間保持良好的連線。

<#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:")

以下是預期輸出的範例。(省略)

Return Code:

200

Expected Outputs:

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

透過ID獲取信任證書

此API可根據給定ID顯示信任證書的詳細資訊。

第1步:API呼叫的必要資訊。

方法	取得
URL	https:// <ise-pan-ip>/api/v1/certs/trusted- certificate/<id-of-certificate></id-of-certificate></ise-pan-ip>
憑證	使用Open API帳戶憑據
標頭	接受:application/json Content-Type: application/json

第2步:查詢用於檢索部署資訊的URL。

Cisco ISE API - Certificates (100) (755) https://to.101.33.92.442.40apev/3ap-doceTypruge-Certificates	
Servers https://10.106.33.92:44240 - Inferred Url 🗸	
certs-api-controller the certs API	~
Certificates	^
CET /api/vl/certs/certificate-signing-request Get all Certificate Signing Requests from PAN	~ ≞
POST /api/v1/certs/certificate-signing-request Generate a Certificate Signing Request (CSR)	\sim \triangleq
GET /api/v1/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	✓ â
GET /spi/vl/certs/certificate-signing-request/export/{hostname}/{id} Export a CSR for a given CSR ID and hostname	✓ ≜
POST /api/vl/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 PS	SNs (Applicable only for internal CA service) 🗸 🔒
POST /api/v1/certs/renew-certificate Renew certificates of OCSP responder and Cisco ISE Messaging Service	~ ≜
POST /api/vl/certs/signed-certificate/bind Bind CA Signed Certificate	~ ≜
CET /api/vl/certs/system-certificate/{hostName} Get all system certificates of a particular node	~ ≙
CET /api/vl/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.	

API URI

第3步:以下是Python代碼的示例。複製並貼上內容。替換ISE IP、使用者名稱和密碼。另存為要執 行的python檔案。

確保ISE與運行python代碼示例的裝置之間保持良好的連線。

<#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/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:")



註:ID來自「獲取所有受信任證書清單」第3步中的API輸出,例如,147d97cc-6ce9-43d7-9928-8cd0fa83e140是「VeriSign 3類公共主要證書頒發機構」。

以下是預期輸出的範例。

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

若要疑難排解與開放式API相關的問題,請在偵錯日誌組態視窗中將theapiservicecomponent的日誌層級設定為DEBUG。

要啟用調試,請導航到操作>故障排除>調試嚮導>調試日誌配置> ISE節點>裝置服務。

≡	abala Identity Services	Engine		Operations / Troubleshoot						License Warning	Q	۵	0	٩	A
н	Bookmarks	Diagnostic Tools	Download Logs	Deb	oug Wizard										
≣ ⊮ %	Dashboard Context Visibility Operations	Debug Profile Configuration	tion N	ode List 3 Debu	ISE-BOL-CFME01-PAN.S	neid.c	om guratior	ı						6	3
0	Policy		0	/ Edit	← Reset to Default	Log	Filter Enable	Log Filter Disable					ÂI		7
20	Administration				Component Name	\sim	Log Level	Description	Log file Name	Log Filter					
nii.	Work Centers			0	accessfilter		INFO	RBAC resource access filter	ise-psc.log	Disabled					-
				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	Al 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					
				•	apiservice		DEBUG	ISE API Service logs	api-service.log	Disabled					
				0	bootstrap-wizard		INFO	Bootstrap wizard messages Save I Can	cel -psc.log	Disabled					
				0	ca-service		INFO	CA Service messages	caservice.log	Disabled					

API服務調試

要下載調試日誌,請導航到操作>故障排除>下載日誌> ISE PAN節點>調試日誌。

≡	dentity Services	Engine	9			Operat	tions / Trou	bleshoot		License Warning	Q	۵	0	Q	R
Щ	Bookmarks	Diagn	iostic Tools	Download Logs	Debug Wiz	ard									
	Dashboard		ISE-BO	GL-CFME01-PAN			-								
15	Context Visibility		ISE-BO	SL-CFME02-MNT	Delete	2 ⁸ Expand All	< ? Collapse A	31							
*	Operations		ISE-DI	C-CEME02-PSN	Debug	g Log Type		Log File	Description	Size					
0	Policy		ISE-RT	FP-CFME01-PAN	✓ Application	on Logs								î	
8.	Administration		ISE-RT	FP-CFME02-MNT	> ad	_agent (1) (100 KB)									
ก็เ	Work Centers		<	,	> ai-	analytics (11) (52 KB) i-gateway (16) (124 KB	0								
					\lor ap	i-service (13) (208 KB)									
?	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					
					-										

下載調試日誌

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。