Uso di OpenAPI per ottenere informazioni sui certificati ISE su ISE 3.3

Sommario

Introduzione
Introduzione
<u>Prerequisiti</u>
Requisiti
Componenti usati
Configurazione
Esempio di rete
Configurazione su ISE
Esempi di Python
Ottieni Tutti I Certificati Di Sistema Di Un Nodo Specifico
Ottieni II Certificato Di Sistema Di Un Nodo Specifico In Base All'ID
Ottieni Elenco Di Tutti I Certificati Attendibili
Ottieni certificato di attendibilità per ID
Risoluzione dei problemi

Introduzione

In questo documento viene descritta la procedura per utilizzare openAPI per gestire il certificato Cisco Identity Services Engine (ISE).

Introduzione

Di fronte alla crescente complessità nella gestione e nella sicurezza della rete aziendale, Cisco ISE 3.1 introduce API in formato OpenAPI che semplificano la gestione del ciclo di vita dei certificati, offrendo un'interfaccia standardizzata e automatizzata per operazioni di certificazione efficienti e sicure, aiutando gli amministratori ad applicare procedure di sicurezza efficaci e a mantenere la conformità della rete.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati

- ISE 3.3
- Python 3.10.0

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Esempio di rete



Configurazione su ISE

Passaggio 1: Aggiungere un account amministratore Open API

Per aggiungere un amministratore API, selezionare Amministrazione -> Sistema -> Amministrazione -> Amministratori -> Utenti amministratori -> Aggiungi.

													-	
=	dentity Services I	Engine		Administration / System				- u	Q	⇔		I A		
щ	Bookmarks	Deployment Licensing	Certificate	s Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings				
5	Dashboard	Authentication	٨d	ministrat	ore									
15	Context Visibility	Authorization	> Au	ministrat	013						St	lected 0 T	otal 2 💈	3 @
*	Operations	Administrators	~ / Ed	+ Add	🛞 Change Status	🛛 Delete 🚺	Duplicate						All \sim	V
0	Policy	Admin Groups		Status	Name	Descriptio	on First Name	Last Name Email Ad	dress Admin Gro	oups				
A 0	Administration		0	Enabled	admin 😛	Default A	dmin User		Super Adr	min				
ñ.	Work Centers	Settings		Enabled	a ApiAdmin				ERS Admi	n				
?	Interactive Help													

Amministratore API

Fase 2: Abilitare Open API su ISE

Open API è disabilitato per impostazione predefinita su ISE. Per abilitarlo, selezionare Amministrazione > Sistema > Impostazioni API > Impostazioni servizio API. Attivate o disattivate le opzioni di Open API. Fare clic su Save (Salva).



```
Abilita OpenAPI
```

Passaggio 3: Esplora ISE open API

passare ad Amministrazione > Sistema > Impostazioni API > Panoramica. Fare clic sul collegamento Apri API.

≡	≡ dentity Services Engine				Administration / System					-	Q	۵ ۵	4	A	
Щ	Bookmarks	Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings				
== 18 火	Dashboard Context Visibility Operations	Client Provisionir FIPS Mode Security Settings Alarm Settings	na 1	API S	Settings API Service										
0	Policy	General MDM / U	JEM Settings	API Serv	rices Overvie	w									
20	Administration	Posture		> You can m Starting Ci	anage Cisco ISE sco ISE Release	nodes through two 3.1. new APIs are a	sets of API form vailable in the O	ats-External Restful Se conAPI format.	rvices (ERS) and OpenAPI.						
di.	Work Centers	Profiling		The ERS a Currently,	nd OpenAPI sen ERS APIs also o	vices are HTTPS-onl perate over port 906	y REST APIs that 0. However, port	operate over port 443 9060 might not be sup	oported for ERS APIs in late	r					
		Protocols		> Cisco ISE Both the A	releases. We ree PI services are	commend that you or disabled by default. E	nly use port 443 Enable the API se	for ERS APIs. arvices by clicking the o	corresponding toggle buttor	15					
?	Interactive Help	Endpoint Scripts		> To use eith	service Settings er API service,	i tab. you must have the El	RS-Admin or ER	S-Operator user group	assignment.						
	I	Proxy SMTP Server SMS Gateway System Time API Settings		For more in https://10. For openal 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 vi to/ers/sdk for ERS, click below: E Onen API, please vi to/api/swagger-ui/n	sit: visit: dox.html								



Esempi di Python

Ottieni Tutti I Certificati Di Sistema Di Un Nodo Specifico

L'API elenca tutti i certificati di un particolare nodo ISE.

Passaggio 1: Informazioni obbligatorie per una chiamata API.

Metodo	OTTIENI
URL	https:// <ise-pan-ip>/api/v1/certs/system- certificate/<ise-node-hostname></ise-node-hostname></ise-pan-ip>
Credenziali	Usa credenziali dell'account API aperto
Intestazioni	Accetta: application/json Content-Type: applicazione/json

Passaggio 2: Individuare l'URL utilizzato per recuperare i certificati di un particolare nodo ISE.

😝 Swa	BERCF. Select a definition	Certificates	×
Cisc	o ISE API - Certificates (IDD) (ASD) 33 82-44240apt/3/app-doc/*prop-Certificates		
Servers https://10	.106.33.92:44240 - Inferred Uri 🗸		
certs-	api-controller the certs API		~
Certif	icates		^
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)	Ň	× 🗎
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/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)	~ 🗎
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 Centificate		× 🗎
GET	/api/vl/certs/system-certificate/{hostName} Get all system certificates of a particular mode	,	
This API	supports filtering, sorting and pagination.		

URI API

Passaggio 3: Ecco l'esempio del Codice Python. Copiare e incollare il contenuto. Sostituire l'indirizzo IP, il nome utente e la password ISE. Salva come file Python da eseguire.

Verificare la buona connettività tra ISE e il dispositivo su cui è in esecuzione il codice Python.

<#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())
```

Di seguito è riportato l'esempio degli output previsti.

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

Ottieni II Certificato Di Sistema Di Un Nodo Specifico In Base All'ID

Questa API fornisce i dettagli di un certificato di sistema di un particolare nodo in base al nome host e all'ID specificati.

Passaggio 1: Informazioni obbligatorie per una chiamata API.

Metodo	OTTIENI
URL	https:// <ise-pan-ip>/api/v1/certs/system- certificate/<ise-node-hostname>/<id-of- Certificate></id-of- </ise-node-hostname></ise-pan-ip>
Credenziali	Usa credenziali dell'account API aperto
Intestazioni	Accetta: application/json Content-Type: applicazione/json

Passaggio 2: Individuare l'URL utilizzato per recuperare il certificato di un particolare nodo in base al nome host e all'ID specificati.

Cisco ISE API - Certificates	
Servers https://10.106.33.92:44240 - Inferred Uri	
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 Centificate 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 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)	/ 🗎
POST /api/vl/certs/renew-certificate Renew certificates of OCSP responder and Cisco ISE Messaging Service	/ 🚔
POST /spi/vl/certs/signed-certificate/bind Bind CA Signed Centificate	/ 🗎
GET /api/v1/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.	

URI API

Passaggio 3: Ecco l'esempio del Codice Python. Copiare e incollare il contenuto. Sostituire l'indirizzo IP, il nome utente e la password ISE. Salva come file Python da eseguire.

Verificare la buona connettività tra ISE e il dispositivo su cui è in esecuzione il codice Python.

<#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:")
```



Nota: I'ID deriva dagli output API al passaggio 3 di "Get All System Certificates Of A Particular Node", ad esempio, 5b5b28e4-2a51-495c-8413-610190e1070b è "Default self-signed saml server certificate - CN=SAML_ISE-DLC-CFME02-PSN.cisco.com".

Di seguito è riportato l'esempio degli output previsti.

Return Code: 200 Expected Outputs: {'response': {'id': '5b5b28e4-2a51-495c-8413-610190e1070b', 'friendlyName': 'Default self-signed saml server certificate - CN=SAML_ISE-DLC-CFME02

Ottieni Elenco Di Tutti I Certificati Attendibili

L'API elenca tutti i certificati attendibili del cluster ISE.

Passaggio 1: Informazioni obbligatorie per una chiamata API.

Metodo	OTTIENI
URL	https:// <ise-pan-ip>/api/v1/certs/trusted- certificate</ise-pan-ip>
Credenziali	Usa credenziali dell'account API aperto
Intestazioni	Accetta: application/json Content-Type: applicazione/json

Passaggio 2: individuare l'URL utilizzato per recuperare i certificati attendibili.

POST /api/vl/certs/certificate-signing-request/intermediate-ca Generate an intermediate CACSR (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 mode by ID	∨ ≜
PUT /api/vl/certs/system-certificate/{hostName}/{id} Update data for existing system certificate	∨ ≜
DELETE /api/vl/certs/system-certificate/{hostName}/{id} Delete System Certificate by ID and hostname	∨ ≜
POST /api/vl/certs/system-certificate/export Export a system certificate with a given a certificate ID	∨ ≜
POST /api/vl/certs/system-certificate/generate-selfsigned-certificate Generate self-signed certificate in Cisco ISE	∨ ≜
POST /api/vl/certs/system-certificate/import Import system certificate in Cisco ISE	∨ ≜
GET /api/vl/certs/trusted-certificate Oet list of all trusted certificates	^ ≜
This API supports Filtering, Sorting and Pagination.	
Filtering and Sorting are supported for the following attributes:	

URI API

Passaggio 3: Ecco l'esempio del Codice Python. Copiare e incollare il contenuto. Sostituire l'indirizzo IP, il nome utente e la password ISE. Salva come file Python da eseguire.

Verificare la buona connettività tra ISE e il dispositivo su cui è in esecuzione il codice Python.

<#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:")

Di seguito è riportato l'esempio degli output previsti.(Omesso)

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

Ottieni certificato di attendibilità per ID

Questa API consente di visualizzare i dettagli di un certificato di attendibilità in base a un determinato ID.

Passaggio 1: Informazioni obbligatorie per una chiamata API.

Metodo	OTTIENI
URL	https:// <ise-pan-ip>/api/v1/certs/trusted- certificate/<id-of-certificate></id-of-certificate></ise-pan-ip>
Credenziali	Usa credenziali dell'account API aperto
Intestazioni	Accetta: application/json Content-Type: applicazione/json

Passaggio 2: Individuare l'URL utilizzato per recuperare le informazioni sulla distribuzione.

Cisco ISE API - Certificates (100) (ASS) Input 156.33 32 442 Magav Shape-Genticates	
Servers https://10.106.33.92:44240 - Inferred Uri	
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)	- 🗎
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 GSR 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 enline 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 mode by ID	~ =
This API provides details of a system certificate of a particular node based on given hostname and ID.	

URI API

Passaggio 3: Ecco l'esempio del Codice Python. Copiare e incollare il contenuto. Sostituire l'indirizzo IP, il nome utente e la password ISE. Salva come file Python da eseguire.

Verificare la buona connettività tra ISE e il dispositivo su cui è in esecuzione il codice Python.

<#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:")



Nota: l'ID deriva dagli output API al passaggio 3 di "Get List Of All Trusted Certificates", ad esempio, 147d97cc-6ce9-43d7-9928-8cd0fa83e140 è "VeriSign Class 3 Public Primary Certification Authority".

Di seguito è riportato l'esempio degli output previsti.

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

Per risolvere i problemi relativi alle API aperte, impostare il livello di log per apiservicecomponent su DEBUGnella finestra di configurazione

del log di debug.

Per abilitare il debug, selezionare **Operations > Troubleshoot > Debug Wizard > Debug Log Configuration > ISE Node > apiservice.**

≡	dentity Services	Engine		Ot	perations / Troub	leshoot		📥 License Warning	Q	۵	0	٥	A
н	Bookmarks	Diagnostic Tools Download	Logs De	bug Wizard									
ा ह	Dashboard Context Visibility Operations	Debug Profile Configuration Debug Log Configuration	Node List	ug Level Co	onfiguration	1							3
-0	Policy		/ Edit	← Reset to Default	Log Filter Enable	Log Filter Disable					AI		7
8.	Administration			Component Name	A Log Level	Description	Log file Name	Log Filter					
ni.	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	cel -psc.log	Disabled					
			0	ca-service	INFO	CA Service messages	caservice.log	Disabled					

Debug del servizio API

Per scaricare i log di debug, selezionare Operations > Troubleshoot > Download Logs > ISE PAN Node > Debug Logs (Operazioni > Risoluzione dei problemi > Log di download > Nodo PAN ISE > Log di debug).

≡	dentity Services	Engine	e	Operations / Troubleshoot		License Warning	Q	۵	0	$\varphi \mid \varphi$	
Щ	Bookmarks	Diagn	nostic Tools Download Logs	Debug Wizard							
10	Dashboard		ISE-BGL-CFME01-PAN								
명	Context Visibility		ISE-BGL-CFME02-MNT	Delete 2 ^a Expand All <>Collapse	All						
*	Operations		ISE-DLC-CEME02-PSN	Debug Log Type	Log File	Description	Size				
0	Policy		ISE-RTP-CFME01-PAN	✓ Application Logs							î
8.	Administration		ISE-RTP-CFME02-MNT	> ad_agent (1) (100 KB)							_
ril.	Work Centers		x	> al-analytics (11) (52 KB) > apl-gateway (16) (124 KB)							
				🗸 api-service (13) (208 KB)							
?	Interactive Help				api-service (all logs)	API Service debug messages	208 KB				
					api-service.log		12 KB				
				0	api-service.log.2024-03-24-1		4.0 KB				
				0	api-service.log.2024-04-07-1		4.0 KB				
				-							

Scarica log di debug

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).