Uso di OpenAPI per recuperare le informazioni sulle policy ISE su ISE 3.3

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Premesse
Configurazione
Esempio di rete
Configurazione su ISE
Esempi di Python
Amministratore Del Dispositivo - Elenco Di Set Di Criteri
Amministrazione dispositivi - Ottieni regole di autenticazione
Amministrazione dispositivi - Ottieni regole di autorizzazione
Accesso Alla Rete - Elenco Di Set Di Criteri
Accesso di rete - Ottieni regole di autenticazione
Accesso di rete - Ottieni regole di autorizzazione
Risoluzione dei problemi

Introduzione

Questo documento descrive la procedura per l'utilizzo di OpenAPI per la gestione Cisco Identity Services Engine (ISE) Policy.

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.

Premesse

Da Cisco ISE 3.1 in poi, le nuove API sono disponibili in formato OpenAPI. La policy di gestione ottimizza la sicurezza e la gestione della rete migliorando l'interoperabilità, migliorando l'efficienza dell'automazione, rafforzando la sicurezza, promuovendo l'innovazione e riducendo i costi. Questa politica consente ad ISE di integrarsi facilmente con altri sistemi, ottenere una configurazione e una gestione automatizzate, fornire un controllo granulare dell'accesso, incoraggiare l'innovazione di terze parti e semplificare i processi di gestione, riducendo in tal modo i costi di manutenzione e aumentando il ritorno complessivo sull'investimento.

Configurazione



Configurazione su ISE

Passaggio 1. Aggiungere un account amministratore OpenAPI.

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

≡	≡ dentity Services Engine					Administration / System				📥 License Warning	Q	۵	0	0 2	۹		
Щ	Bookmarks	Deployment Licensing	Cert	tificates	Logging	Maintenance	Upgrade	Health	Checks	Backup & Rest	tore Admin A	ccess Settings					
	Dashboard	Authentication		Adm	inistrat	oro											
명	Context Visibility	Authorization	>	Aum	mistrat	015							2.4	in the d	Tini O	a a	
*	Operations	Administrators	~	0 Edit	+ Add	🛞 Change Status	Delete	Duplicate					540	ected 0	All	~ 7	
.0	Policy	Admin Users		0	Status	Name	Descrip	otion	First Name	Last Name Er	mail Address	Admin Groups					
80	Administration			0	Enabled	😛 ədmin	Default	Admin User				Super Admin					
-file	Work Centers	Settings	>		Enabled	a ApiAdmin						ERS Admin					
?	Interactive Help																

Amministratore API

Passaggio 2. Abilitare OpenAPI su ISE.

Open API è disabilitato per impostazione predefinita su ISE. Per attivarlo, passare a Amministrazione > Sistema > Impostazioni > Impostazioni API > Impostazioni servizio API. Attivate o disattivate le opzioni di OpenAPI. Fare clic su Salva.

≡ dirate Identity Services Engine	Administration / System	🔺 License Warning 🛛 🖓 🎯 🗘 🞗
Bookmarks Deployment Licensing	Certificates Logging Maintenance Upgrade Health Checks Backup & Restore	Admin Access Settings
Image: Dashboard Client Provisioning. Context Visibility FIPS Mode Security Settings Security Settings Operations Alarm Settings Policy General MDM / UEM Settings Administration Pesture Image: Work Centers Profiling	API Settings Overview API Service Settings API Gateway Settings ~ API Service Settings for Primary Administration Node ERS (Read/Write) Open API (Read/Write)	
Interactive Help Endpoint Scripts Prosy SMTP Server SMS Gateway Surger Tom	 API Service Setting for All Other Nodes ERS (Read) Open API (Read) 	
API Settings Data Connect Network Success Diagnostics DHCP & DNS Services Max Sessions Light Data Distribution Endpoint Replication	 CSRF Check (only for ERS Settings) Enable CSRF Check for Enhanced Security (Not compatible with pre ISE 2.3 Clients) Disable CSRF For ERS Request (compatible with ERS clients older than ISE 2.3) 	Reset Save

Abilita OpenAPI

Passaggio 3. Scopri ISE OpenAPI.

Passa a Amministrazione > Sistema > Impostazioni > Impostazioni API > Panoramica. Fare clic su OpenAPI per visitare il collegamento.

≡	diale Identity Services I	Engine				Administra	tion / Syster	•				Q	۵	0	Q A
н	Bookmarks	Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings				
	Dashboard	Client Provisioni	ng		ettinas										
18 X	Context Visibility Operations	Security Settings		Overview	API Servic	e Settings API G	ateway Settings								
-0	Policy	General MDM / I	JEM Settings	API Serv	ices Overvie	w									
80	Administration	Posture		> You can m Starting Ci	anage Cisco ISE sco ISE Release	nodes through two s 3.1, new APIs are av	ets of API form railable in the O	ets-External Restful Se benAPI format.	rvices (ERS) and OpenAPI.						
-fil	Work Centers	Profiling		Currently, Cisco ISE	nd OpenAPI ser ERS APIs also o releases. We re	vices are HTTPS-only perate over port 9060 commend that you on	REST APIs that D. However, port Iv use port 443	operate over port 443 9060 might not be sup for ERS APIs.	pported for ERS APIs in late	r					
		Protocols		> Both the A	PI services are	disabled by default. E	nable the API se	ervices by clicking the o	corresponding toggle buttor	ns					
?	Interactive Help	Endpoint Script	•	> To use eith	er API service,	you must have the ER	S-Admin or ERS	Operator user group	assignment.						
		Proxy SMTP Server		For more in https://10. For openag	nformation on IS 106.33.92:4424 pi documention	SE ERS API, please vis 40/ers/sdk for ERS, click below:	sit:								
	I	System Time API Settings Data Connect		For more in https://10.	formation on 15 106.33.92:442	E Onen API, niease v 40/api/swagger-ui/inc 183.495	isir lox.html								

Visita OpenAPI

Esempi di Python

Amministratore Del Dispositivo - Elenco Di Set Di Criteri

Questa API recupera le informazioni sui set di criteri di amministrazione del dispositivo.

Passaggio 1. Informazioni necessarie per una chiamata API.

Metodo	OTTIENI
URL	https:// <ise-pan-ip>/api/v1/policy/device- admin/policy-set</ise-pan-ip>
Credenziali	Utilizzare le credenziali dell'account OpenAPI.
Intestazioni	Accetta : application/json Content-Type : application/json

Passaggio 2. Individuare l'URL utilizzato per recuperare le informazioni sui set di criteri di amministrazione del dispositivo.

H Swagger.	Select a definition Policy	
Cisco ISE API - Policy (ISO) (ISO) https://10.106.33.92-42404ppv3/spi-docs/tyroup-Policy		
Servers https://10.106.33.92:44240 - Inferred Url V	Authorize 🔒	
device-admin-api-controller the device-admin API	~	
network-access-api-controller the network-access API	~	
Device Administration - Command Sets	~	
Device Administration - Conditions	~	
Device Administration - Dictionary Attributes List	~	
Device Administration - Identity Stores	~	
Device Administration - Network Conditions	~	
Device Administration - Policy Sets	^	
CET /api/vl/policy/device-admin/policy-set Device Admin - List of policy sets.	^ ≜	
Device Admin - List of policy sets.		

URI API

Passaggio 3. Questo è un esempio di codice Python. Copiare e incollare il contenuto. Sostituire l'ISE IP, il nome utente e la password. Salvare come file Python da eseguire.

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

<#root>

from requests.auth import HTTPBasicAuth import requests

requests.packages.urllib3.disable_warnings()

if __name__ == "__main__":

```
https://10.106.33.92/api/v1/policy/device-admin/policy-set
"
    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())

Questo è l'esempio degli output previsti.

Return Code: 200 Expected Outputs: {'version': '1.0.0', 'response': [{'default': True, 'id': '41ed8579-429b-42a8-879e-61861cb82bbf', 'name': 'Default', 'descr

DDevice Admin - Ottieni regole di autenticazione

Questa API recupera le regole di autenticazione di un set di criteri specifico.

Passaggio 1. Informazioni necessarie per una chiamata API.

Metodo	OTTIENI
URL	https:// <ise-pan-ip>/api/v1/policy/device- admin/policy-set/<id-of-policy- Set>/authentication</id-of-policy- </ise-pan-ip>
Credenziali	Utilizzare le credenziali dell'account OpenAPI.
Intestazioni	Accetta : application/json Content-Type : application/json

Passaggio 2. Individuare l'URL utilizzato per recuperare le informazioni sulle regole di autenticazione.

	H Swagger.	Select a definition	licy	~
	Cisco ISE API - Policy (0.0.3) (0.1.3) https://to.100.3.3.92.442404ee/decifyree-Peley			
	Servers https://10.106.33.92:44240 - Inferred Url V		Authorize	a
	device-admin-api-controller the device-admin API			~
	network-access-api-controller the network-access API			~
	Device Administration - Command Sets			~
	Device Administration - Conditions			~
	Device Administration - Dictionary Attributes List			~
	Device Administration - Identity Stores			~
	Device Administration - Network Conditions			~
	Device Administration - Policy Sets			\sim
	Device Administration - Authorization Global Exception Rules			~
	Device Administration - Authentication Rules			^
	CET /api/vl/policy/device-admin/policy-set/{policyId}/authentication	ation rules.	,	× ≜
	Device Admin - Get authentication rules.			

URI API

Passaggio 3. Questo è un esempio di codice Python. Copiare e incollare il contenuto. Sostituire l'ISE IP, il nome utente e la password. Salvare come file Python da eseguire.

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

<#root>

```
from requests.auth import HTTPBasicAuth
import requests
requests.packages.urllib3.disable_warnings()
if _____name___ == "____main___":
 url = "
https://10.106.33.92/api/v1/policy/device-admin/policy-set/41ed8579-429b-42a8-879e-61861cb82bbf/authent:
...
    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())



Nota: l'ID deriva dagli output API al passaggio 3 di Device Admin - List Of Policy Sets. Ad esempio, 41ed8579-429b-42a8-879e-61861cb82bbf è impostato come criterio predefinito di TACACS.

Questo è l'esempio degli output previsti.

Return Code: 200 Expected Outputs: {'version': '1.0.0', 'response': [{'rule': {'default': True, 'id': '73461597-0133-45ce-b4cb-6511ce56f262', 'name': 'Default': 'True, 'Name': 'Default': 'True, 'Name': 'Default': 'True, 'Name': 'True, '

Amministrazione dispositivi - Ottieni regole di autorizzazione

Questa API recupera le regole di autorizzazione di un set di criteri specifico.

Passaggio 1. Informazioni necessarie per una chiamata API.

Metodo	OTTIENI
URL	https:// <ise-pan-ip>/api/v1/policy/device- admin/policy-set/<id-of-policy- Set>/authorization</id-of-policy- </ise-pan-ip>
Credenziali	Utilizzare le credenziali dell'account OpenAPI.
Intestazioni	Accetta : application/json Content-Type : application/json

Passaggio 2. Individuare l'URL utilizzato per recuperare le informazioni sulla regola di autorizzazione.

Cis	SCO ISE API - Policy (100) (100) 10 105 33 92 442401egiv/34ge-decr/group-Policy		
Server: http:	s s://10.106.33.92:44240 - Inferred Urt	Authorize 🔒	
de	vice-admin-api-controller the device-admin API	~	
net	twork-access-api-controller the network-access API	~	
De	vice Administration - Command Sets	~	
De	vice Administration - Conditions	~	
De	vice Administration - Dictionary Attributes List	~	
De	vice Administration - Identity Stores	~	
De	vice Administration - Network Conditions	~	
De	vice Administration - Policy Sets	~	
De	vice Administration - Authorization Global Exception Rules	~	
De	vice Administration - Authentication Rules	~	
De	vice Administration - Authorization Rules	^	
G	/api/vl/policy/device-admin/policy-set/{policyId}/authorization Device Admin - Get authorization rules.	^ ≞	
Der	vice Admin - Get authorization rules.		

URI API

Passaggio 3. Questo è un esempio di codice Python. Copiare e incollare il contenuto. Sostituire l'ISE IP, il nome utente e la password. Salvare come file Python da eseguire.

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

<#root>

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

https://10.106.33.92/api/v1/policy/device-admin/policy-set/41ed8579-429b-42a8-879e-61861cb82bbf/authoriz

```
" 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 Device Admin - List Of Policy Sets. Ad esempio, 41ed8579-429b-42a8-879e-61861cb82bbf è impostato come criterio predefinito di TACACS.

Questo è l'esempio degli output previsti.

Return Code: 200

Accesso Alla Rete - Elenco Di Set Di Criteri

Questa API recupera i set di criteri di accesso alla rete delle distribuzioni ISE.

Passaggio 1. Informazioni necessarie per una chiamata API.

Metodo	OTTIENI
URL	https:// <ise-pan-ip>/api/v1/policy/network- access/policy-set</ise-pan-ip>
Credenziali	Utilizzare le credenziali dell'account OpenAPI.
Intestazioni	Accetta : application/json Content-Type : application/json

Passaggio 2. Individuare l'URL utilizzato per recuperare le informazioni specifiche del nodo ISE.

Network Access - Policy Sets					
GET	/api/v1/policy/network-access/policy-set Network Access - List of policy sets.	^ ≜			
Get all ne	twork access policy sets.				

URI API

Passaggio 3. Questo è un esempio di codice Python. Copiare e incollare il contenuto. Sostituire l'ISE IP, il nome utente e la password. Salvare come file Python da eseguire.

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

<#root>

from requests.auth import HTTPBasicAuth import requests

requests.packages.urllib3.disable_warnings()

```
if _____name___ == "____main___":
```

url = "

https://10.106.33.92/api/v1/policy/network-access/policy-set

"

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())
```

Questo è l'esempio degli output previsti.

Return Code: 200 Expected Outputs: {'version': '1.0.0', 'response': [{'default': False, 'id': 'ba71a417-4a48-4411-8bc3-d5df9b115769', 'name': 'BGL_CFME0

Accesso di rete - Ottieni regole di autenticazione

Questa API recupera le regole di autenticazione di un set di criteri specifico.

Passaggio 1. Informazioni necessarie per una chiamata API.

Metodo	OTTIENI
URL	https:// <ise-pan-ip>/api/v1/policy/network- access/policy-set/<id-of-policy- Set>/authentication</id-of-policy- </ise-pan-ip>
Credenziali	Utilizzare le credenziali dell'account OpenAPI.
Intestazioni	Accetta : application/json Content-Type : application/json

Passaggio 2. Individuare l'URL utilizzato per recuperare le informazioni sulla regola di autenticazione.

N	Network Access - Authentication Rules	^
	GET /api/vl/policy/network-access/policy-set/{policyId}/authentication Network Access - Get authentication rules.	^ ≜
	Network Access - Get authentication rules.	

URI API

Passaggio 3. Questo è un esempio di codice Python. Copiare e incollare il contenuto. Sostituire l'ISE IP, il nome utente e la password. Salvare come file Python da eseguire.

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

<#root>

```
from requests.auth import HTTPBasicAuth
import requests
requests.packages.urllib3.disable_warnings()
if _____name___ == "____main___":
 url = "
https://10.106.33.92/api/v1/policy/network-access/policy-set/ba71a417-4a48-4411-8bc3-d5df9b115769/auther
...
    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())
```



Nota: l'ID deriva dagli output API al passaggio 3 di Accesso alla rete - Elenco di set di criteri. Ad esempio, ba71a417-4a48-4411-8bc3-d5df9b115769 è BGL_CFME02-FMC.

Questo è l'esempio degli output previsti.

Return Code: 200 Expected Outputs: {'version': '1.0.0', 'response': [{'rule': {'default': True, 'id': '03875777-6c98-4114-a72e-a3e1651e533a', 'name': 'Default': 'Default':

Accesso di rete - Ottieni regole di autorizzazione

Questa API recupera le regole di autorizzazione di un set di criteri specifico.

Passaggio 1. Informazioni necessarie per una chiamata API.

Metodo	OTTIENI
URL	https:// <ise-pan-ip>/api/v1/policy/network-</ise-pan-ip>

	access/policy-set/ <id-of-policy- Set>/authorization</id-of-policy-
Credenziali	Utilizzare le credenziali dell'account OpenAPI.
Intestazioni	Accetta : application/json Content-Type : application/json

Passaggio 2. Individuare l'URL utilizzato per recuperare le informazioni sulla regola di autorizzazione.

Network Access - Authorization Rules	^
GET /api/vl/policy/network-access/policy-set/{policyId}/authorization Network Access - Ge	t authorization rules.
Network Access - Get authorization rules.	

URI API

Passaggio 3. Questo è un esempio di codice Python. Copiare e incollare il contenuto. Sostituire l'ISE IP, il nome utente e la password. Salvare come file Python da eseguire.

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

<#root>

```
from requests.auth import HTTPBasicAuth
import requests
requests.packages.urllib3.disable_warnings()
if _____name___ == "____main___":
 url = "
https://10.106.33.92/api/v1/policy/network-access/policy-set/ba71a417-4a48-4411-8bc3-d5df9b115769/author
...
    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())
```



Nota: l'ID deriva dagli output API al passaggio 3 di Accesso alla rete - Elenco di set di criteri. Ad esempio, ba71a417-4a48-4411-8bc3-d5df9b115769 è BGL_CFME02-FMC.

Questo è l'esempio degli output previsti.

Return Code: 200 Expected Outputs: {'version': '1.0.0', 'response': [{'rule': {'default': False, 'id': 'bc67a4e5-9000-4645-9d75-7c2403ca22ac', 'name': 'FMC A

Risoluzione dei problemi

Per risolvere i problemi relativi alle OpenAPI, 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			Op	erati	ions / Troub	leshoot		License Warning	Q	۵	0	٩	R ا
н	Bookmarks	Diagnostic Tools	Download Logs	Del	bug Wizard										
ा ह	Dashboard Context Visibility Operations	Debug Profile Configuratio	ation	Node List Debu	ug Level Co	nfi	guration								3
0	Policy			0 Edit	Seset to Default	Log	Filter Enable	Log Filter Disable					All	v 1	7
8.	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					^
				0	Active Directory		WARN	Active Directory client internal messages	ad_agent.log						L
?	Interactive Help			0	admin-ca		INFO	CA Service admin messages	ise-psc.log	Disabled					L
				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	- C	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					

Debug del servizio API

Per scaricare il file di 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	Ð		Operati	ons / Troubleshoot		🔺 License Warning	Q	۵	0	$\varphi \mid \varphi$
Ц	Bookmarks	Diagn	nostic Tools Download	js Debug W	lizard							
55	Dashboard		ISE-BGL-CFME01-PA									
망	Context Visibility		ISE-BGL-CFME02-MM	Delet	ℓ ∠ ³ Expand All	<>Collapse All	Bread Mar	0 1				
*	Operations		ISE-DLC-CEME02-PS	De	oug Log Type	Log File	Description	Size				
0	Policy		ISE-RTP-CFME01-PA		ation Logs							
8.	Administration		ISE-RTP-CFME02-MM	>	ad_agent (1) (100 KB)							_
ñ	Work Centers		K.		ai-analytics (11) (52 KB) api-gateway (16) (124 KB)							
?	Interactive Help				api-service (13) (208 KB)	api-service (all logs)	API Service debug messages	208 KB				
						api-service.log		12 KB				
						api-service.log.2024-0	3-24-1	4.0 KB				
						api-service.log.2024-0	4-07-1	4.0 KB				
			1	-								

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).