使用OpenAPI檢索ISE 3.3上的ISE策略資訊

目錄
<u>必要條件</u>
<u>採用元件</u>
<u>背景資訊</u>
<u>設定</u>
網路圖表 一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一
ISE上的配置
Python示例
<u>Device Admin -策略集清單</u>
<u>裝置管理-獲取身份驗證規則</u>
<u>裝置管理-獲取授權規則</u>
網路訪問-策略集清單
網路訪問 <u>-獲</u> 取身份驗證規則
網路訪問-獲取授權規則
疑難排解

簡介

本檔案介紹使用OpenAPI來管理網際網路的程式 思科身分辨識服務引擎(ISE) 政策。

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。

背景資訊

從Cisco ISE 3.1開始,新的API以OpenAPI格式提供。管理策略透過增強互操作性、提高自動化效率、增強安全性、促進創新和降低成本,最佳化了網路安全和管理。此策略允許ISE與其他系統無 縫整合,實現自動配置和管理,提供精細的訪問控制,鼓勵第三方創新,並簡化管理流程,從而降 低維護成本並提高總體投資回報。

設定

網路圖表



ISE上的配置

步驟 1.新增anOpenAPI 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 E	Ingine				Administra	tion / System				Q & Ø	Q Q
н	Bookmarks	Deployment Licensing	Cer	tificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access Settings		
23	Dashboard	Authentication		Adm	inietrat							
망	Context Visibility	Authorization	>	Aum	mistrati	015					Selected 0, Total 2	0 A
×	Operations	Administrators	Ŷ	0 Edit	+ Add	🛞 Change Status	🖗 Delete 🚺 Du	plicate			And the second s	uv V
.0	Policy	Admin Users Admin Groups			Status	Name	Description	First Name	Last Name Email A	ddress Admin Groups		
80	Administration			0	Enabled	yadmin	Default Admir	n User		Super Admin		
di.	Work Centers	Settings	>		Enabled	a ApiAdmin				ERS Admin		
?	Interactive Help											

API管理

步驟 2.在ISE上啟用OpenAPI。

預設情況下,在ISE上停用開放式API。若要啟用它,請導覽至 Administration > System > Settings > API Settings > API Service Settings.切換OpenAPI選項按一下 儲存.

Ξ	dentity Services I	Engine				Administrat	tion / Systen	n		_	License Warning	Q	۵	0	Ф А
Щ	Bookmarks	Deployment L	Licensing C	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings				
	Bookmarks Dashboard Context Visibility Operations Policy Administration Work Centers Interactive Help	Client Provisioning FIPS Mode Security Settings Alarm Settings General MDM / UEM Pesture Profiling Protocols Endpoint Scripts Proxy SMTP Server SMS Gateway Sottem Time	I Settings	API Se	API Service API Service Copen API (Re rvice Settir ERS (Read) Open API (Re Open API (Re	API G os Settings API G Ings for Primary A Ing for All Other N Ing for All Other N	Upgrade	n Node	Backup o kestore	Admin Access	settings				
		API Settings Data Connect		✓ CSRF (Check (only	for ERS Setting	s)								
		Network Success D	Diagnostics >	 Enable Disable 	CSRF Check	for Enhanced Securit IS Request (compatit	y (Not compatibl	le with pre ISE 2.3 Clier ents older than ISE 2.3)	nts)						
		DHCP & DNS Service Max Sessions Light Data Distribute Endpoint Replication	es on									Rese	t		Save

啟用OpenAPI

o

步驟 3.探索ISE OpenAPI。

導覽至 Administration > System > Settings > API Settings > Overview.按一下OpenAPI以訪問連結

	ahalia Identity Services E	Engine	Administration / System		Q	۵ ۵	Q	R	
н	Bookmarks	Deployment Licensing	ificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin A	ccess Settings					
22	Dashboard	Client Provisioning							
망	Context Visibility	FIPS Mode Security Settings	API Settings						
×	Operations	Alarm Settings	Overview API Service Settings API Gateway Settings						
U	Policy	General MDM / UEM Settings	API Services Overview						
20	Administration	Posture	You can manage Cisco ISE nodes through two sets of API formats—External Restful Services (ERS) and OpenAPI. Starting Cisco ISE Release 3.1, new APIs are available in the OpenAPI format. 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						
đ	Work Centers	Profiling							
		Protocols	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 Scripts	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 API Settings	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 Err more information on ISE Onen ADI: clease visit: https://10.106.33.92.44240/api/swagger-ui/index.html						

訪問OpenAPI

Python示例

Device Admin -策略集清單

此API檢索裝置管理策略集資訊。

步驟 1.API呼叫所需的資訊。

方法	取得
URL	https:// <ise-pan-ip>/api/v1/policy/device-</ise-pan-ip>

	admin/policy-set
憑證	使用OpenAPI帳戶憑據。
標頭	接受 : application/json Content-Type : application/json

步驟 2.找到用於檢索裝置管理策略集資訊的URL。

Harrow Swagger.	Select a definition Policy	×	
Cisco ISE API - Policy (III) (III)			
Servers https://10.106.33.92:44240 - Inferred Uri 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		^	
GET /api/vl/policy/device-admin/policy-set Device Admin - List of policy sets.		^ ≜	
Device Admin - List of policy sets.			

API URI

步驟 3.這是Python代碼的一個示例。 複製並貼上內容。替換ISE IP、使用者名稱和密碼。儲存為要 執行的python檔案。

確保ISE和運行Python代碼示例的裝置之間的良好連線。

<#root>

from requests.auth import HTTPBasicAuth import requests

requests.packages.urllib3.disable_warnings()

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

url = "

https://10.106.33.92/api/v1/policy/device-admin/policy-set

...

headers = $\{$

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

}

basicAuth = HTTPBasicAuth(

```
)
response = requests.get(url=url, auth=basicAuth, headers=headers, verify=False)
print("Return Code:")
print(response.status_code)
print("Expected Outputs:")
print(response.json())
```

這是預期輸出的示例。

"ApiAdmin", "Admin123"

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

D裝置管理員-獲取身份驗證規則

此API檢索特定策略集的身份驗證規則。

步驟 1.API呼叫所需的資訊。

方法	取得
URL	https:// <ise-pan-ip>/api/v1/policy/device- admin/policy-set/<策略集的ID>/authentication</ise-pan-ip>
憑證	使用OpenAPI帳戶憑據。
標頭	接受 : application/json Content-Type : application/json

步驟 2.找到用於檢索身份驗證規則資訊的URL。

	Here Swagger	Select a definition	Policy ~	
	Cisco ISE API - Policy (IDD) (ASS) https://10.106.33.82.44240aev/slage-decs?groupe=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		~	
	Device Administration - Authorization Global Exception Rules		~	
	Device Administration - Authentication Rules		^	
	GET /api/v1/policy/device-admin/policy-set/{policyId}/authentication Device Admin - Get authentication	tion rules.	∧ ≙]
	Device Admin - Get authentication rules.			

API URI

步驟 3.這是Python代碼的一個示例。 複製並貼上內容。替換ISE IP、使用者名稱和密碼。儲存為要 執行的python檔案。

確保ISE和運行Python代碼示例的裝置之間的良好連線。

<#root>

from requests.auth import HTTPBasicAuth import requests

requests.packages.urllib3.disable_warnings()

if __name__ == "__main__":

url = "

https://10.106.33.92/api/v1/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:")
```



註:ID來自裝置管理第3步-策略集清單中的API輸出。例如,41ed8579-429b-42a8-879e-61861cb82bbf是TACACS預設策略集。

這是預期輸出的示例。

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

裝置管理-獲取授權規則

此API檢索特定策略集的授權規則。

步驟 1.API呼叫所需的資訊。

方法	取得
URL	https:// <ise-pan-ip>/api/v1/policy/device- admin/policy-set/<策略集ID>/authorization</ise-pan-ip>
憑證	使用OpenAPI帳戶憑據。
標頭	接受 : application/json Content-Type : application/json

步驟 2.找到用於檢索授權規則資訊的URL。

Cisco ISE API - Policy 600 000

Servers https://10.106.33.92:44240 - Inferred Url 🗸	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	~
Device Administration - Authorization Global Exception Rules	~
Device Administration - Authentication Rules	~
Device Administration - Authorization Rules	^
GET /api/vl/policy/device-admin/policy-set/{policyId}/authorization Device Admin - Get authorization rules.	<u>^ ≜</u>

API URI

步驟 3.這是Python代碼的一個示例。 複製並貼上內容。替換ISE IP、使用者名稱和密碼。儲存為要 執行的python檔案。

確保ISE和運行Python代碼示例的裝置之間的良好連線。

<#root>

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

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

" 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來自裝置管理第3步-策略集清單中的API輸出。例如,41ed8579-429b-42a8-879e-61861cb82bbf是TACACS預設策略集。

這是預期輸出的示例。

Return Code: 200 Expected Outputs:

{'version': '1.0.0', 'response': [{'rule': {'default': True, 'id': '39d9f546-e58c-4f79-9856-c0a244b8a2ae', 'name': 'Default', 'hitCounts': 0, 'rank': 0, 'state': 'enable': 'enable': 'local terms' ('local terms') 'local terms') 'local terms' ('local terms') 'local terms' ('local terms') 'local terms') 'local terms' ('local terms') 'local terms') 'local terms' ('local terms') 'local terms') 'loc

網路訪問-策略集清單

此API檢索ISE部署的網路訪問策略集。

步驟 1.API呼叫所需的資訊。

方法	取得
URL	https:// <ise-pan-ip>/api/v1/policy/network- access/policy-set</ise-pan-ip>
憑證	使用OpenAPI帳戶憑據。
標頭	接受 : application/json Content-Type : application/json

步驟 2.查詢用於檢索特定ISE節點資訊的URL。

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

API URI

步驟 3.這是Python代碼的一個示例。 複製並貼上內容。替換ISE IP、使用者名稱和密碼。儲存為要 執行的python檔案。

確保ISE和運行Python代碼示例的裝置之間的良好連線。

<#root>

from requests.auth import HTTPBasicAuth import requests

requests.packages.urllib3.disable_warnings()

if __name__ == "__main__":

url = "

https://10.106.33.92/api/v1/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)
```

這是預期輸出的示例。

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

網路訪問-獲取身份驗證規則

此API檢索特定策略集的身份驗證規則。

步驟 1.API呼叫所需的資訊。

方法	取得
URL	https:// <ise-pan-ip>/api/v1/policy/network- access/policy-set/<id-of-policy- Set>/authentication</id-of-policy- </ise-pan-ip>
憑證	使用OpenAPI帳戶憑據。
標頭	接受 : application/json Content-Type : application/json

步驟 2.找到用於檢索身份驗證規則資訊的URL。

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

API URI

步驟 3.這是Python代碼的一個示例。 複製並貼上內容。替換ISE IP、使用者名稱和密碼。儲存為要 執行的python檔案。

確保ISE和運行Python代碼示例的裝置之間的良好連線。

<#root>

from requests.auth import HTTPBasicAuth import requests

requests.packages.urllib3.disable_warnings()

if _____name___ == "____main___":

```
url = "
https://10.106.33.92/api/v1/policy/network-access/policy-set/ba7la417-4a48-4411-8bc3-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())
```



註:ID來自網路訪問-策略集清單步驟3中的API輸出。例如, ba71a417-4a48-4411-8bc3-

d5df9b115769是BGL_CFME02-FMC。

這是預期輸出的示例。

Return Code: 200 Expected Outputs: {'version': '1.0.0', 'response': [{'rule': {'default': True, 'id': '03875777-6c98-4114-a72e-a3e1651e533a', 'name': 'Default': 'Default': '04875777-6c98-4114-a72e-a3e1651e533a', 'name': 'Default': '048875777-6c98-4114-a72e-a3e1651e533a', 'name': 'Default': 'Default'

網路訪問-獲取授權規則

此API檢索特定策略集的授權規則。

步驟 1.API呼叫所需的資訊。

方法	取得
URL	https:// <ise-pan-ip>/api/v1/policy/network- access/policy-set/<策略集ID>/authorization</ise-pan-ip>
憑證	使用OpenAPI帳戶憑據。
標頭	接受 : application/json Content-Type : application/json

步驟 2.找到用於檢索授權規則資訊的URL。

Networ	k Access - Authorization Rules	^
GET	/api/v1/policy/network-access/policy-set/{policyId}/authorization Network Access - Get authorization rules.	^ ≜
Network Acc	cess - Get authorization rules.	

API URI

步驟 3.這是Python代碼的一個示例。 複製並貼上內容。替換ISE IP、使用者名稱和密碼。儲存為要 執行的python檔案。

確保ISE和運行Python代碼示例的裝置之間的良好連線。

<#root>

from requests.auth import HTTPBasicAuth import requests

requests.packages.urllib3.disable_warnings()

if _____name___ == "____main___":

```
url = "
https://10.106.33.92/api/v1/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())
```



注意:ID來自網路訪問-策略集清單的步驟3中的API輸出。例如,ba71a417-4a48-4411-8bc3-d5df9b115769是BGL_CFME02-FMC。

這是預期輸出的示例。

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

疑難排解

若要疑難排解與OpenAPI相關的問題,請在偵錯日誌組態視窗中將theapiservicecomponent的記錄 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> apiservice。

≡	dentity Services	Engine		Op	oerations / Trou	bleshoot		License Warning	Q	۵	0	۵	A
н	Bookmarks	Diagnostic Tools Download Lo	ogs Del	bug Wizard									
≣ ≓ड %	Dashboard Context Visibility Operations	Debug Profile Configuration Debug Log Configuration	Node List) ISE-BOL-CEMEOI-PAN Ug Level Co	onfiguratio	n						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					
-fil	Work Centers		0	accessfilter	INFO	RBAC resource access filter	ise-psc.log	Disabled				í	
			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					
			•	apiservice	DEBUG	ISE API Service logs	apl-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服務調試

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

≡	dentity Services I	Engine			Оре	erations / Troubleshoot		🔺 License Warning	Q Q	0	$\phi \mid \phi$
Ц	Bookmarks	Diagno	ostic Tools	Download Logs	Debug Wizard						
-	Dashboard		ISE-BO	GL-CFME01-PAN							
명	Context Visibility		ISE-BO	GL-CFME02-MNT	Delete 2 ^a Expand Al	I SPCollapse All					
×	Operations		SE-DI	LC-CFME01-PSN	Debug Log Type	Log File	Description	Size			
	Policy		ISE-DI	LC-CFME02-PSN	V Application Logs						^
80	Administration		ISE-RT	TP-CFME01-PAN	> ad_agent (1) (100 KE	3)					
1	Work Centers		< C	Þ	> ai-analytics (11) (52	K8)					- 11
					> api-gateway (16) (12	44 KB) 3 KB)					
?	Interactive Help					api-service (all logs)	API Service debug messages	208 KB			
						api-service.log		12 KB			
						api-service.log.2024-03	1-24-1	4.0 KB			
						api-service.log.2024-04	1-07-1	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)。