

Recuperare le API dei ruoli utente ESA tramite l'API Privilegi

Sommario

[Introduzione](#)

[Ambiente](#)

[Risoluzione](#)

[Interpreta la risposta](#)

[Contenuto correlato](#)

[Problema](#)

[Causa](#)

[Risultato previsto](#)

[Risoluzione](#)

[Procedura](#)

[Output di esempio](#)

Introduzione

In questo documento viene descritto come recuperare le informazioni sui privilegi per il ruolo ESA autenticato utilizzando l'endpoint `/esa/api/v2.0/login/privilegi`.

Ambiente

- Python 3.x
- Libreria richieste Python installata
- Email Security Appliance (ESA) con il servizio API abilitato sull'interfaccia di gestione e con la porta API configurata

Risoluzione

1. Verificare che il servizio API ESA sia abilitato sull'interfaccia di gestione.
2. Confermare la porta API configurata sull'ESA e utilizzare lo stesso valore di porta nello script.
3. Ottenere un valore di intestazione Authorization e un cookie di sessione ESA valido per l'account utilizzato per chiamare l'API.

4. Se necessario, installare la dipendenza richiesta:

```
pip install requests
```

5. Aggiornare la variabile di script (indirizzo IP ESA, porta API e valori di autenticazione), quindi eseguire lo script.

 Nota: Usare la porta API configurata sull'ESA. Mantenere la coerenza del valore della porta sullo script e sugli eventuali screenshot.

Interpreta la risposta

La risposta `/login/privilegi` rappresenta i privilegi concessi alla sessione autenticata. Utilizzare l'elenco dei privilegi restituito per determinare quali risorse e operazioni API sono disponibili per il ruolo utente corrente.

Nel payload JSON, esaminare `data.privilegi`. Ogni voce elenca un percorso di risorsa e i metodi HTTP consentiti per tale risorsa.

Contenuto correlato

2) Installare le richieste (per impostazione predefinita non è installato con Python). Eseguire questo comando dal prompt dei comandi:

```
pip install requests
```

Le richieste consentono di inviare richieste HTTP da Python.

3) `pprint` è incluso con Python (libreria standard). Non è richiesta alcuna installazione.

Il modulo `pprint` fornisce una capacità di stampare strutture dati Python arbitrarie in un formato che può essere utilizzato come input per l'interprete e visualizzarle in un formato leggibile. Questo modulo è facoltativo. Lo script può utilizzare invece `print`; tuttavia, l'output è meno leggibile.

JSON NON deve essere installato separatamente perché fa parte della libreria standard.

Problema

Determinare quali API Cisco Email Security Appliance (ESA) sono accessibili al ruolo utente autenticato.

Causa

L'accesso alle API sull'ESA è controllato dai privilegi assegnati alla sessione e al ruolo autenticati. L'endpoint `/esa/api/v2.0/login/privilegi` restituisce l'elenco dei privilegi validi, in modo che sia possibile determinare quali risorse API e metodi HTTP sono consentiti per l'utente corrente.

Risultato previsto

Una richiesta GET riuscita a `/esa/api/v2.0/login/privilegi` restituisce HTTP 200 OK e un payload JSON in cui sono elencati i privilegi (accesso API) disponibili per la sessione autenticata. Esaminare il file JSON restituito per identificare le risorse API e le operazioni consentite per il ruolo.

Risoluzione

Procedura

```
import requests
import json
import pprint

url = "https://192.0.2.10:6080/esa/api/v2.0/login/privileges"
headers = {
    "Authorization": "Basic <BASE64_BASIC_AUTH>",
    "Cookie": "<SESSION_COOKIE>"
}

response = requests.request("GET", url, headers=headers, verify=True)
json_string = json.loads(response.content)
pprint.pprint(json_string)
```

Output di esempio

Output di esempio:

```
{
  "data": {
    "privileges": [
      {
        "resource": "/esa/api/v2.0/login/privileges",
        "methods": ["GET"]
      }
    ]
  }
}
```

Esaminare la lista dei privilegi per identificare le risorse API e i metodi HTTP consentiti per la sessione autenticata.

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).