

ESA User Role API's ophalen met behulp van de Privileges API

Inhoud

[Inleiding](#)

[milieu](#)

[resolutie](#)

[Interpreteer het antwoord](#)

[Gerelateerde inhoud](#)

[uitgifte](#)

[Oorzaak](#)

[verwacht resultaat](#)

[resolutie](#)

[Procedure](#)

[Voorbeelduitvoer](#)

Inleiding

In dit document wordt beschreven hoe u privilegegegevens voor de geverifieerde ESA-rol kunt ophalen met behulp van het eindpunt `/esa/api/v2.0/login/privileges`.

milieu

- Python 3.x
- Python vraagt bibliotheek geïnstalleerd
- Email Security Appliance (ESA) met de API-service ingeschakeld op de beheerinterface en met de API-poort geconfigureerd

resolutie

1. Bevestig dat de ESA API-service is ingeschakeld op de beheerinterface.
2. Bevestig de geconfigureerde API-poort op de ESA en gebruik dezelfde poortwaarde in het script.
3. Verkrijg een Authorisation header-waarde en een geldige ESA-sessiecookie voor het account dat wordt gebruikt om de API aan te roepen.

4. Installeer indien nodig de vereiste afhankelijkheid:

```
pip install requests
```

5. Werk de scriptvariabele (ESR IP-adres, API-poort en verificatiewaarden) bij en voer het script vervolgens uit.

 **Opmerking:** Gebruik de API-poort die is geconfigureerd op de ESA. Houd de poortwaarde consistent in het script en eventuele screenshots.

Interpreteer het antwoord

Het antwoord/login/privileges vertegenwoordigt de privileges die aan de geverifieerde sessie zijn toegekend. Gebruik de teruggestuurde privilege lijst om te bepalen welke API resources en bewerkingen beschikbaar zijn voor de huidige gebruikersrol.

Controleer in de JSON-payload `data.privileges`. Elk item geeft een resource pad en de toegestane HTTP-methoden voor die resource.

Gerelateerde inhoud

2) Installeer aanvragen (het is niet standaard geïnstalleerd met Python). Voer deze opdracht uit via een opdrachtprompt:

```
pip install requests
```

verzoeken staat het verzenden van HTTP-verzoeken van Python toe.

3) Print is inbegrepen bij Python (standaard bibliotheek). Installatie is niet nodig.

De `printmodule` biedt een mogelijkheid om willekeurige Python-gegevensstructuren behoorlijk af te drukken in een vorm die kan worden gebruikt als invoer voor de interpreter en deze in een leesbaar formaat weer te geven. Deze module is optioneel. Het script kan in plaats daarvan afdrukken gebruiken; de uitvoer is echter minder leesbaar.

JSON hoeft NIET apart te worden geïnstalleerd omdat het deel uitmaakt van de standaardbibliotheek.

uitgifte

Bepaal welke API's van Cisco Email Security Appliance (ESA) toegankelijk zijn voor de geverifieerde gebruikersrol.

Oorzaak

API-toegang op de ESA wordt beheerst door de bevoegdheden die zijn toegewezen aan de geverifieerde sessie en rol. Het eindpunt `/esa/api/v2.0/login/privileges` retourneert de lijst met effectieve privileges, zodat u kunt bepalen welke API-bronnen en HTTP-methoden zijn toegestaan voor de huidige gebruiker.

verwacht resultaat

Een succesvol GET-verzoek aan `/esa/api/v2.0/login/privileges` retourneert HTTP 200 OK en een JSON-payload met de privileges (API-toegang) die beschikbaar zijn voor de geverifieerde sessie. Controleer de teruggestuurde JSON om de toegestane API-bronnen en -bewerkingen voor die rol te identificeren.

resolutie

Procedure

```
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)
```

Voorbeelduitvoer

Voorbeeld uitvoer:

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

Controleer de lijst met bevoegdheden om te bepalen welke API-bronnen en HTTP-methoden zijn toegestaan voor de geverifieerde sessie.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.