

APIs für ESA-Benutzerrollen mit der Privileges-API abrufen

Inhalt

[Einleitung](#)

[Umwelt](#)

[Auflösung](#)

[Interpretieren der Antwort](#)

[Verwandte Inhalte](#)

[Problem](#)

[Ursache](#)

[Erwartetes Ergebnis](#)

[Auflösung](#)

[Vorgehensweise](#)

[Beispielausgabe](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie mithilfe des Endpunkts `/esa/api/v2.0/login/privilegien` Berechtigungsinformationen für die authentifizierte ESA-Rolle abrufen.

Umwelt

- Python 3.x
- Python-Anforderungsbibliothek installiert
- E-Mail Security Appliance (ESA) mit aktiviertem API-Service über die Verwaltungsschnittstelle und konfiguriertem API-Port

Auflösung

1. Vergewissern Sie sich, dass der ESA API-Dienst auf der Verwaltungsschnittstelle aktiviert ist.
2. Bestätigen Sie den konfigurierten API-Port auf der ESA, und verwenden Sie denselben Port-Wert im Skript.

3. Rufen Sie einen Autorisierungs-Headerwert und ein gültiges ESA-Sitzungscookie für das Konto ab, das zum Aufrufen der API verwendet wird.
4. Installieren Sie ggf. die erforderliche Abhängigkeit:

```
pip install requests
```
5. Aktualisieren Sie die Skriptvariable (ESA-IP-Adresse, API-Port und Authentifizierungswerte), und führen Sie dann das Skript aus.

 Anmerkung: Verwenden Sie den auf der ESA konfigurierten API-Port. Halten Sie den Port-Wert im gesamten Skript und in allen Screenshots gleich.

Interpretieren der Antwort

Die Antwort `/login/privileges` stellt die Berechtigungen dar, die für die authentifizierte Sitzung erteilt wurden. Ermitteln Sie anhand der zurückgegebenen Berechtigungsliste, welche API-Ressourcen und -Vorgänge für die aktuelle Benutzerrolle verfügbar sind.

Überprüfen Sie in der JSON-Payload `data.privileges`. Jeder Eintrag listet einen Ressourcenpfad und die zulässigen HTTP-Methoden für diese Ressource auf.

Verwandte Inhalte

2) Install Requests (es wird standardmäßig nicht mit Python installiert). Führen Sie diesen Befehl an einer Eingabeaufforderung aus:

```
pip install requests
```

-Anfragen können HTTP-Anfragen von Python senden.

3) Druck ist im Lieferumfang von Python (Standardbibliothek) enthalten. Es ist keine Installation erforderlich.

Das Druckmodul bietet die Möglichkeit, beliebige Python-Datenstrukturen in einer Form hübsch zu drucken, die als Eingabe für den Interpreter verwendet werden kann, und sie in einem lesbaren Format anzuzeigen. Dieses Modul ist optional. Stattdessen kann das Skript `print` verwenden. Die Ausgabe ist jedoch weniger lesbar.

JSON muss NICHT separat installiert werden, da es Teil der Standardbibliothek ist.

Problem

Legen Sie fest, auf welche APIs der Cisco E-Mail Security Appliance (ESA) die authentifizierte Benutzerrolle zugreifen kann.

Ursache

Der API-Zugriff auf der ESA wird durch die Berechtigungen gesteuert, die der authentifizierten Sitzung und Rolle zugewiesen sind. Der Endpunkt `/esa/api/v2.0/login/privileges` gibt die Liste der effektiven Berechtigungen zurück, sodass Sie bestimmen können, welche API-Ressourcen und HTTP-Methoden für den aktuellen Benutzer zulässig sind.

Erwartetes Ergebnis

Eine erfolgreiche GET-Anforderung an `/esa/api/v2.0/login/privileges` gibt HTTP 200 OK und eine JSON-Nutzlast zurück, die die für die authentifizierte Sitzung verfügbaren Berechtigungen (API-Zugriff) auflistet. Überprüfen Sie den zurückgegebenen JSON, um die zulässigen API-Ressourcen und -Vorgänge für diese Rolle zu identifizieren.

Auflösung

Vorgehensweise

```
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)
```

Beispielausgabe

Beispiel:

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

Überprüfen Sie die Liste der Berechtigungen, um festzustellen, welche API-Ressourcen und HTTP-Methoden für die authentifizierte Sitzung zulässig sind.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.