Generieren von Authentifizierungstoken für FMC REST API-Interaktionen

Einführung

In diesem Dokument wird beschrieben, wie sich ein Administrator der Application Programming Interface (API) beim FirePOWER Management Center (FMC) authentifizieren, Token generieren und für weitere API-Interaktionen verwenden kann.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- FirePOWER Management Center (FMC) - Funktionen und Konfiguration (Konfigurationsanleitung)
- Verstehen verschiedener REST API-Aufrufe. (Was sind REST-APIs?)
- Lesen Sie die FMC API Quick Start Guide.

Verwendete Komponenten

- FirePOWER Management Center unterstützt REST-APIs (Version 6.1 oder höher) mit aktivierter REST-API.
- REST-Clients wie Postman, Python-Scripts, CURL usw.

Hintergrundinformationen

REST-APIs sind aufgrund des einfachen programmierbaren Ansatzes, den Netzwerkmanager zur Konfiguration und Verwaltung ihrer Netzwerke verwenden können, zunehmend beliebt. FMC unterstützt die Konfiguration und Verwaltung über jeden REST-Client und den integrierten API-Explorer.

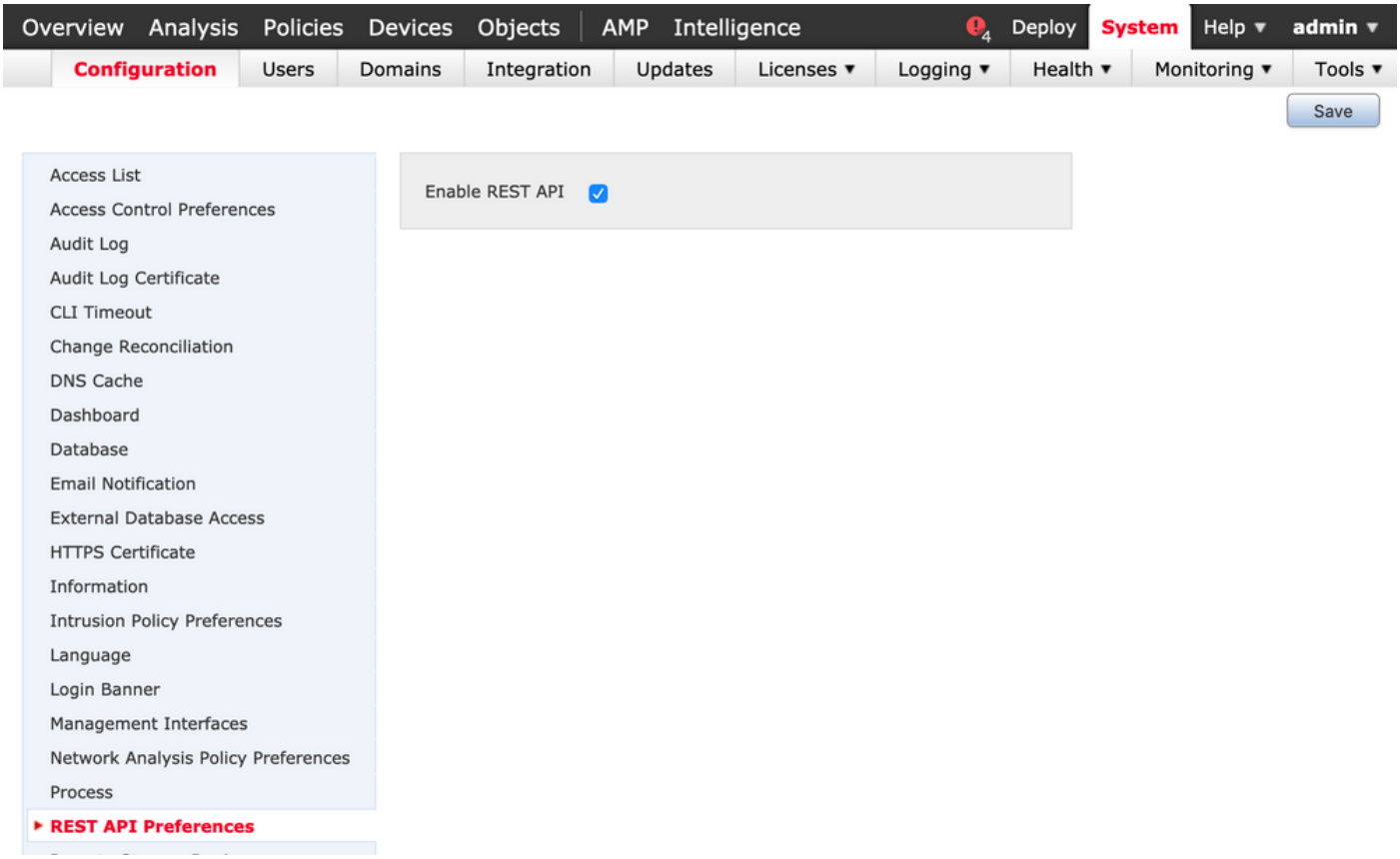
Konfigurieren

Aktivieren der REST-API auf FMC

Schritt 1: Navigieren Sie zu **System>Configuration>REST API Preferences>**Enable **REST API.**

Schritt 2: Aktivieren Sie das Kontrollkästchen **REST-API aktivieren**.

Schritt 3: Klicken Sie auf **Speichern,** ein Dialogfeld **Erfolgreich speichern** wird angezeigt, wenn die REST-API aktiviert ist, wie im Bild gezeigt:



Erstellen eines Benutzers auf FMC

Die Verwendung der API-Infrastruktur auf dem FMC hat sich bewährt, weil Benutzer der Benutzeroberfläche und Skripteuser getrennt bleiben. Informationen zu verschiedenen Benutzerrollen und Richtlinien zum Erstellen eines neuen Benutzers finden Sie im FMC-Handbuch für Benutzerkonten.

Schritte zum Anfordern eines Authentifizierungstokens

Schritt 1: Öffnen Sie Ihren **REST API-Client**.

Schritt 2: Legen Sie fest, dass der Client den POST-Befehl URL ausführt: https://<management_center_IP_or_name>/api/fmc_platform/v1/auth/generatetoken.

Schritt 3: Integrieren Sie den Benutzernamen und das Kennwort als einfachen Authentifizierungs-Header. Der **POST-**Text sollte leer sein.

Beispielsweise eine Authentifizierungsanforderung mit Python:

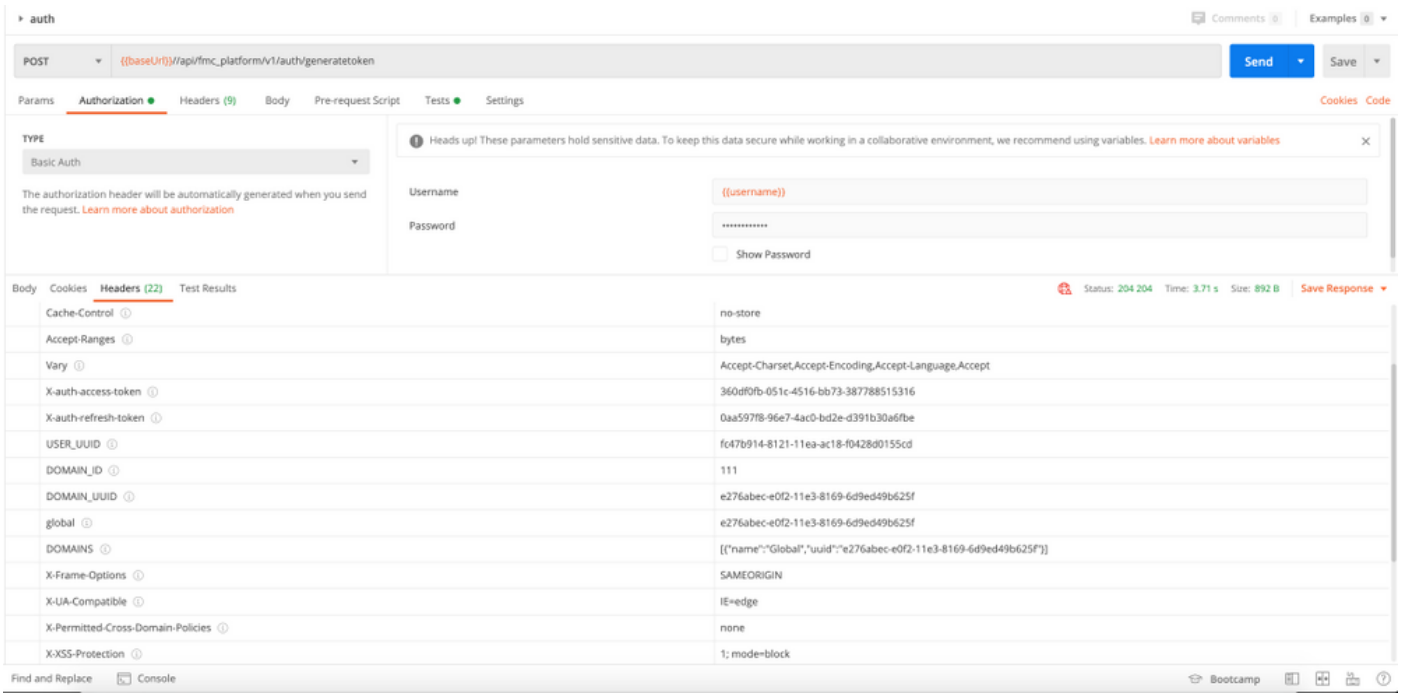
```
import requests url = "https://10.10.10.1//api/fmc_platform/v1/auth/generatetoken" payload = {}
headers = { 'Authorization': 'Basic Y2lzY291c2VyOmNpc2NwYXBpdXNlcg==' } response =
requests.request("POST", url, headers=headers, data = payload, verify=False)
print(response.headers)
```

Ein weiteres Beispiel für eine Authentifizierungsanfrage mit CURL:

```
$ curl --request POST 'https://10.10.10.1/api/fmc_platform/v1/auth/generatetoken' --header
'Authorization: Basic Y2lzY291c2VyOmNpc2NwYXBpdXNlcg==' -k -i HTTP/1.1 204 204 Date: Tue, 11 Aug
2020 02:54:06 GMT Server: Apache Strict-Transport-Security: max-age=31536000; includeSubDomains
```

```
Cache-Control: no-store Accept-Ranges: bytes Vary: Accept-Charset,Accept-Encoding,Accept-
Language,Accept X-auth-access-token: aa6f8326-0a0c-4f48-9d85-7a920c0fdca5 X-auth-refresh-token:
674e87d1-1572-4cd1-b86d-3abec04ca59d USER_UUID: fc47b914-8121-11ea-ac18-f0428d0155cd DOMAIN_ID:
111 DOMAIN_UUID: e276abec-e0f2-11e3-8169-6d9ed49b625f global: e276abec-e0f2-11e3-8169-
6d9ed49b625f DOMAINS: [{"name":"Global","uuid":"e276abec-e0f2-11e3-8169-6d9ed49b625f"}] X-Frame-
Options: SAMEORIGIN X-UA-Compatible: IE=edge X-Permitted-Cross-Domain-Policies: none X-XSS-
Protection: 1; mode=block Referrer-Policy: same-origin Content-Security-Policy: base-uri 'self'
X-Content-Type-Options: nosniff
```

Beispiel aus einem GUI-basierten Client wie Postman, wie im Bild gezeigt:



Senden nachfolgender API-Anfragen

> **Hinweis**: In der Ausgabe sehen Sie die Antwortheader und nicht den Antworttext. Der tatsächliche Ansprechtext ist leer. Die wichtigsten Headerinformationen, die extrahiert werden müssen, sind **X-auth-access-token**, **X-auth-fresh-token** und **DOMAIN_UUID**.

Nachdem Sie sich erfolgreich beim FMC authentifiziert und die Token extrahiert haben, müssen Sie für weitere API-Anfragen die folgenden Informationen nutzen:

- Fügen Sie den Header X-auth-access-token **<authentication token value>** als Teil der Anforderung hinzu.
- Fügen Sie die Header X-auth-access-token **<authentication token value>** und X-auth-fresh-token **<update token value>** in Anforderungen zur Aktualisierung des Tokens hinzu.
- Verwenden Sie die Domain_UUID aus dem Authentifizierungstoken aller REST-Anforderungen an den Server.

Mit diesen Headerinformationen können Sie mithilfe von REST-APIs erfolgreich mit dem FMC interagieren.

Fehlerbehebung bei häufig auftretenden Problemen

- Der Anforderungs- und Antworttext des für die Authentifizierung gesendeten POST-Tests ist leer. Sie müssen die grundlegenden Authentifizierungsparameter im Anforderungsheader

übergeben. Alle Tokeninformationen werden über die Antwortheader zurückgegeben.

- Wenn Sie den REST-Client verwenden, können aufgrund eines selbstsignierten Zertifikats Fehler im Zusammenhang mit dem SSL-Zertifikatproblem auftreten. Sie können diese Validierung je nach dem verwendeten Client deaktivieren.

- Die Benutzeranmeldeinformationen können nicht gleichzeitig für die REST-API und die GUI-Schnittstellen verwendet werden, und der Benutzer wird ohne Vorwarnung abgemeldet, wenn er für beide Schnittstellen verwendet wird.

- Die Authentifizierungs-Token für die FMC REST API sind 30 Minuten gültig und können bis zu dreimal aktualisiert werden.