Hoe u verificatieToken voor FMC REST API-interacties kunt genereren

Inleiding

In dit document wordt beschreven hoe een API-beheerder (Application programmeur Interface) kan authenticeren aan Firepower Management Center (FMC), penningen genereren en gebruiken voor elke verdere API-interactie.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Firepower Management Center (FMC) functies en configuratie. (Config-handleiding)
- Het begrip van verschillende REST API-oproepen. (Wat zijn REST API's?)
- Review of the FMC API Quick Start Guide.

Gebruikte componenten

- Firepower Management Center dat REST API's (versie 6.1 of hoger) ondersteunt met REST API ingeschakeld.
- REST klanten zoals Postman, Python scripts, CURL, etc.

Achtergrondinformatie

REST API's zijn steeds populairder vanwege de lichtgewicht programmeerbare benadering die netwerkbeheerders kunnen gebruiken om hun netwerken te configureren en te beheren. FMC ondersteunt configuratie en beheer met behulp van elke REST-client en ook met behulp van de ingebouwde API-verkenner.

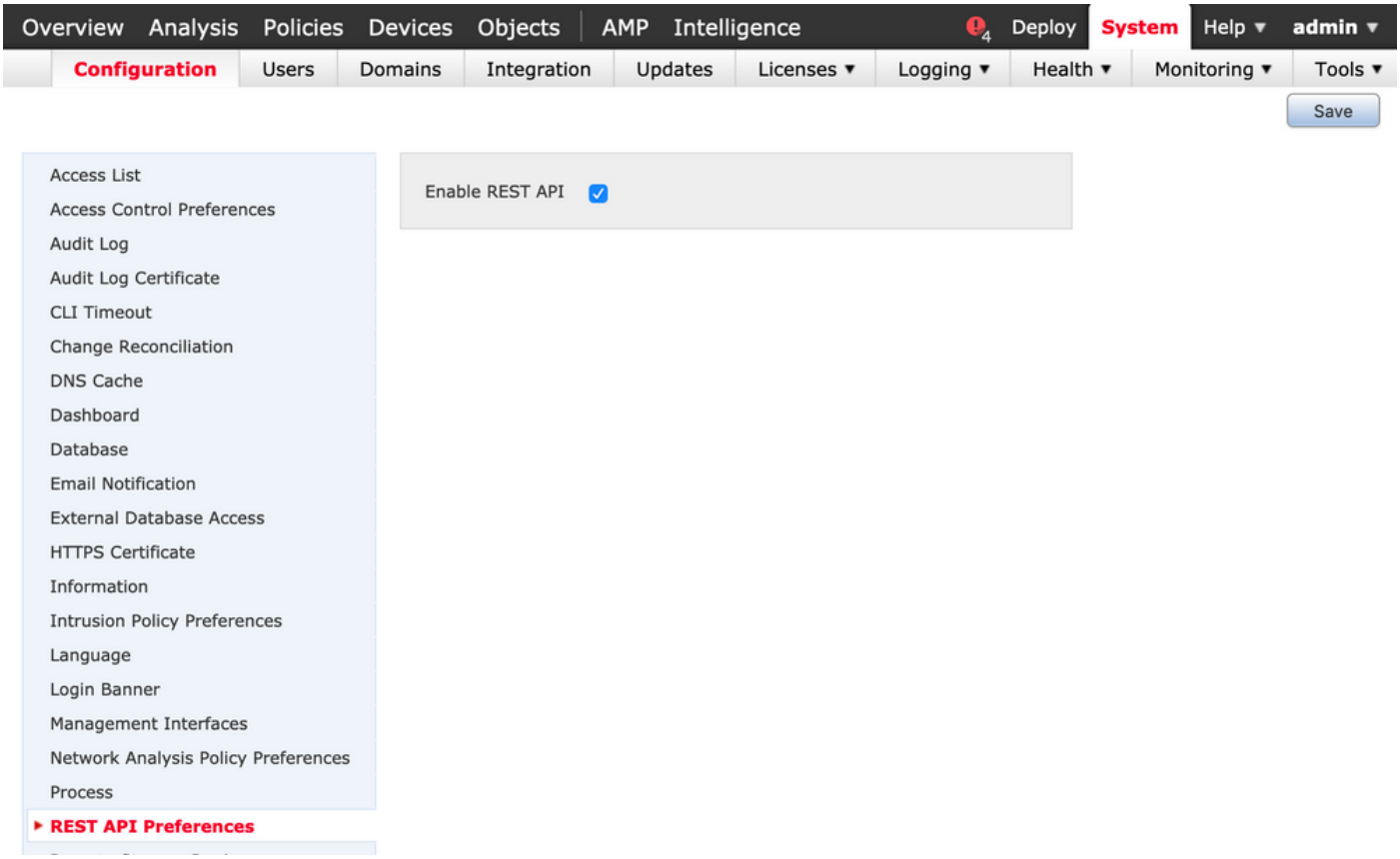
Configureren

REST API inschakelen op FMC

Stap 1 . Navigeer naar **System>Configuration>REST API-voorkeuren>REST API** inschakelen.

Stap 2. Controleer het selectieteken **REST API inschakelen**.

Stap 3. Klik op **Opslaan,** een dialoogvenster Opslaan **en** geslaagd wordt weergegeven wanneer de REST API is ingeschakeld, zoals in de afbeelding:



Een gebruiker op FMC maken

Als beste praktijk om de API infrastructuur op FMC te gebruiken is gebruikers UI en script gebruikers gescheiden te houden. Raadpleeg de gebruikersrekeningen voor de FMC-gids voor het begrip van verschillende gebruikersrollen en de richtlijnen voor het maken van een nieuwe gebruiker.

Stappen om een verificatietoken aan te vragen

Stap 1 . Open uw **REST API-client**.

Stap 2 . Stel de client in om een POST-opdracht te maken, URL: <management_center_IP_or_name>/api/fmc_platform/v1/auth/generatetoken.

Stap 3. Voeg de gebruikersnaam en het wachtwoord toe als een basisauthenticatieheader. Het **POST** lichaam moet leeg zijn.

Bijvoorbeeld een verificatieaanvraag waarbij Python wordt gebruikt:

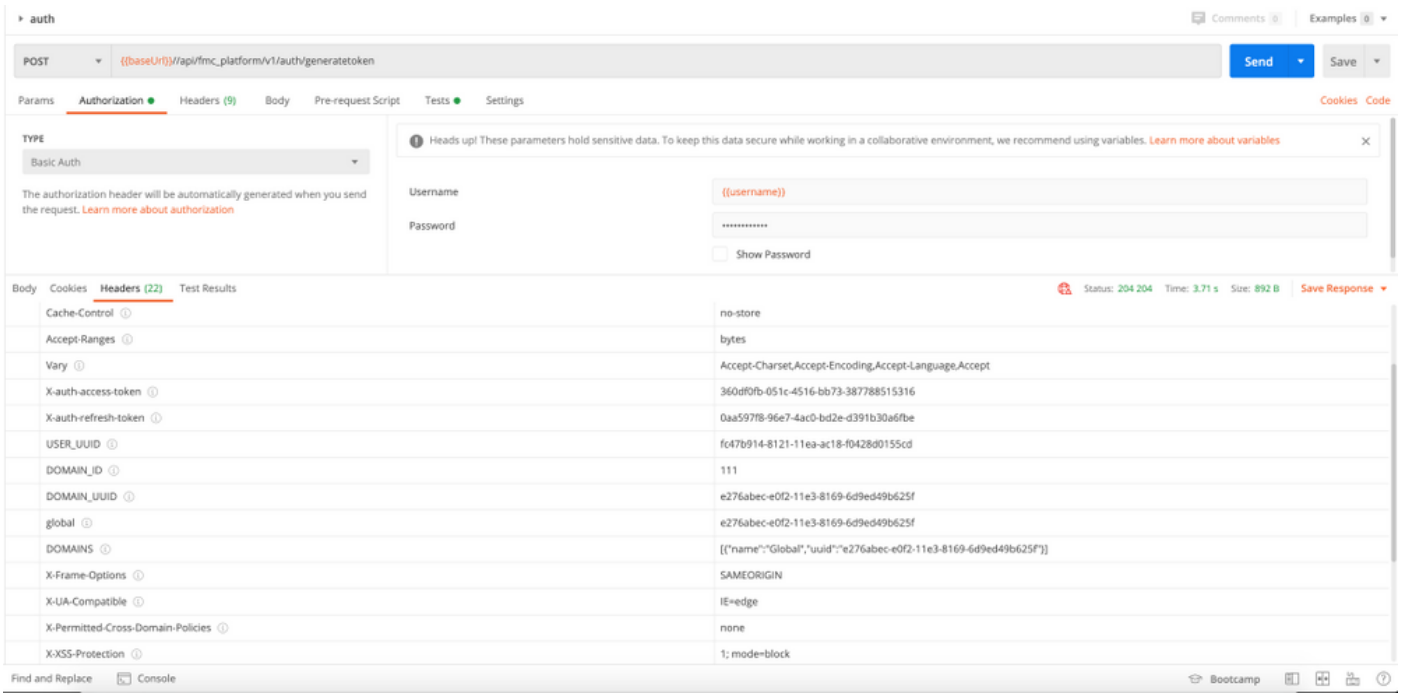
```
import requests url = "https://10.10.10.1//api/fmc_platform/v1/auth/generatetoken" payload = {}
headers = { 'Authorization': 'Basic Y2lzY291c2VyOmNpc2NwYXBpdXNlcg==' } response =
requests.request("POST", url, headers=headers, data = payload, verify=False)
print(response.headers)
```

Een ander voorbeeld van een verificatieaanvraag met behulp van 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
```

Voorbeeld van een op GUI gebaseerde cliënt zoals Postman, zoals getoond in de afbeelding:



Volgende API-aanvragen verzenden

> Opmerking: Wat je ziet in de output zijn de responskoppen en niet het responslichaam. Het responsorgaan is leeg. De belangrijke header-informatie die moet worden geëxtraheerd is **X-auth-access-token**, **X-auth-verfrissing-token** en **DOMAIN_UID**.

Zodra u voor FMC succesvol heeft geauthenticeerd en de tokens hebt geëxtraheerd, moet u voor verdere API-verzoeken om onderstaande informatie gebruiken:

- Voeg de kop X-auth-access-token toe **<verificatie-token waarde>**als deel van het verzoek.
- Voeg de kopregels X-auth-access-token toe **<verificatie-token>** en X-auth-verfrissing-token **<verfrissing-token>**in verzoeken om het token op te frissen.
- Gebruik Domain_UID van het authenticatiemenk in alle REST-verzoeken aan de server.

Met deze header informatie kunt u met succes met FMC communiceren met REST API's.

Problemen oplossen

- De aanvraag- en antwoordinstantie van de POST die voor de authenticatie wordt verzonden, is leeg. U moet de basisauthenticatieparameters doorgeven in de header van het verzoek. Alle token informatie wordt via de responskop teruggegeven.

- Wanneer u de REST-client gebruikt, kunt u fouten zien die te maken hebben met het SSL-

certificeringsprobleem door een zelfondertekend certificaat. U kunt deze validatie uitzetten afhankelijk van de client die u gebruikt.

- De gebruikersreferenties kunnen niet tegelijkertijd worden gebruikt voor REST API en GUI-interfaces, en de gebruiker zal zonder waarschuwing worden aangemeld als deze voor beide interfaces wordt gebruikt.
- De FMC REST API-verificatiepenningen zijn geldig voor 30 minuten en kunnen tot drie keer worden bijgewerkt.