FMC REST APIインタラクション用の認証トークンの生成方法

概要

このドキュメントでは、アプリケーションプログラミングインターフェイス(API)管理者がFirepower Management Center(FMC)に対して認証を行い、トークンを生成し、その後のAPIインタラクションに使用する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Firepower Management Center(FMC)の機能と設定。(設定ガイド)
- 各種のREST APIコールについて。(REST APIとは)
- FMC APIクイックスタートガイドの復習。

使用するコンポーネント

- REST APIを有効にした状態でREST API（バージョン6.1以降）をサポートするFirepower Management Center(FMC)。
- Postman、Pythonスクリプト、CURLなどのRESTクライアント

背景説明

ネットワークマネージャがネットワークの設定と管理に使用できる軽量でプログラム可能なアプローチにより、REST APIの普及が進んでいます。FMCは、任意のRESTクライアントを使用し、組み込みのAPIエクスプローラを使用して、設定と管理をサポートします。

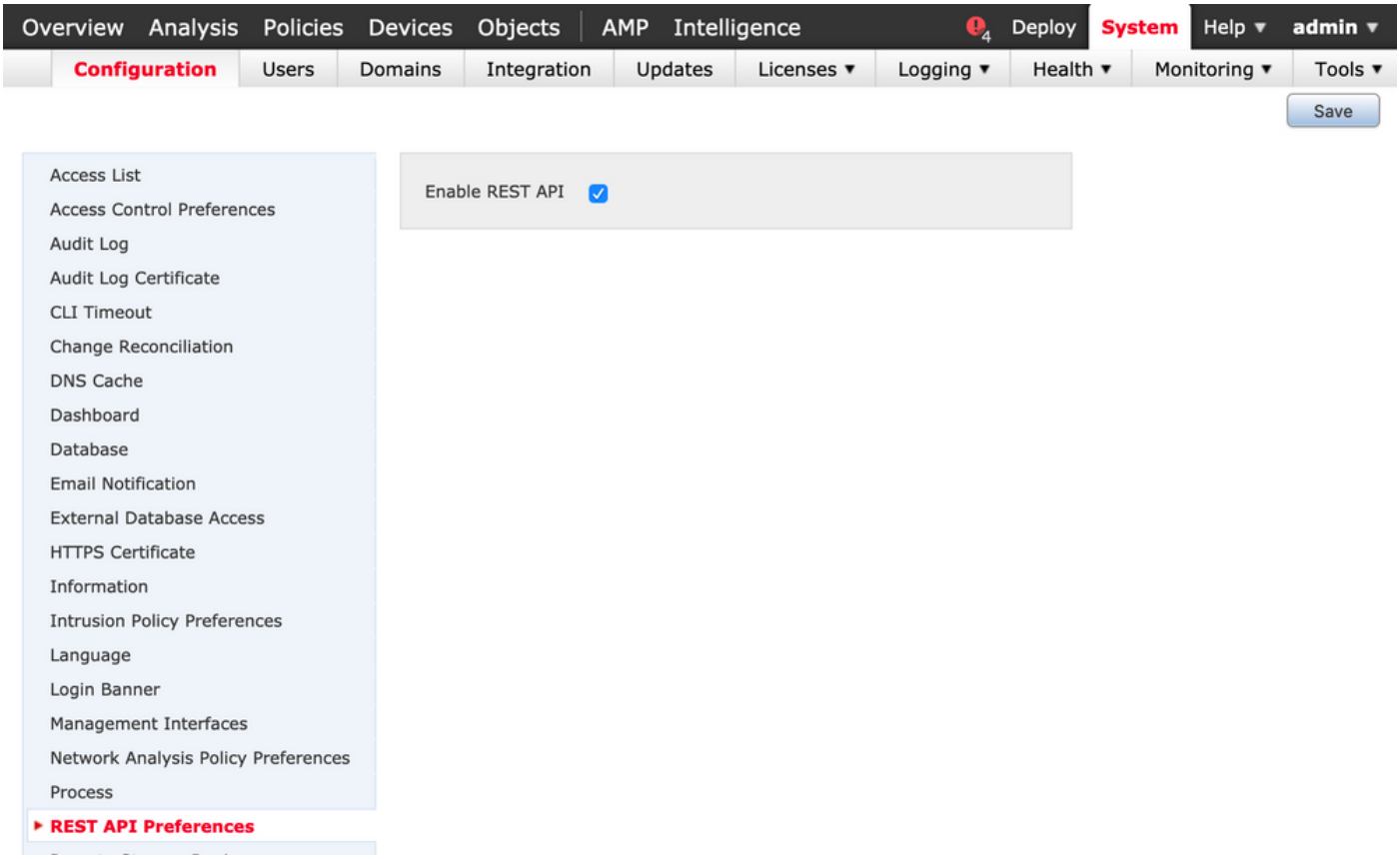
設定

FMCでのREST APIの有効化

ステップ1:[System] > [Configuration] > [REST API Preferences] > [Enable **REST API]**に移動します。

ステップ2:[Enable REST API]チェックボックスを**オン**にします。

ステップ3:図に示すように**REST APIが有効**な場合、[Save Successful]ダイアログボックスが表示されます。



FMCでのユーザの作成

FMCでAPIインフラストラクチャを使用するベストプラクティスは、UIユーザとスクリプトユーザを分離することです。さまざまなユーザーの役割と新しいユーザーを作成する際のガイドラインについては、『FMC用ユーザーアカウント』ガイドを参照してください。

認証トークンを要求する手順

ステップ1:REST APIクライアントを開きます。

ステップ2:POSTコマンドを実行するようにクライアントを設定します。
URL:https://<management_center_IP_or_name>/api/fmc_platform/v1/auth/generatetoken。

ステップ3：基本認証ヘッダーとしてユーザ名とパスワードを含めます。POST本文**は空白**である必要があります。

たとえば、Pythonを使用した認証要求：

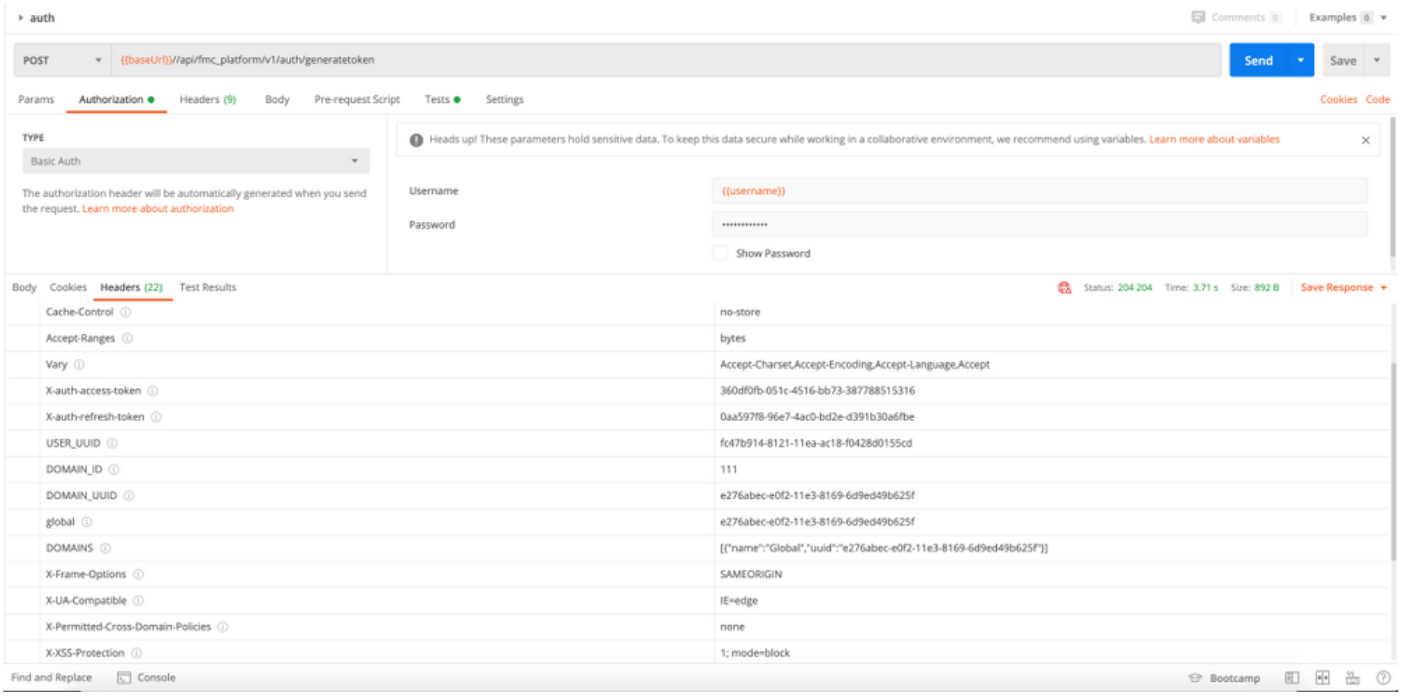
```
import requests url = "https://10.10.10.1//api/fmc_platform/v1/auth/generatetoken" payload = {}
headers = { 'Authorization': 'Basic Y2lzY291c2VyOmNpc2NwYXBpdXNlcg==' } response =
requests.request("POST", url, headers=headers, data = payload, verify=False)
print(response.headers)
```

CURLを使用した認証要求の別の例：

```
$ 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

図に示すように、PostmanのようなGUIベースのクライアントからの例：



後続のAPI要求の送信

> **注**：出力に表示されるのは、応答ヘッダーであり、応答の本文ではありません。実際の応答本文は空白です。 抽出する必要がある重要なヘッダー情報は、**X-auth-access-token**、**X-auth-refresh-token**、**DOMAIN_UUIDです**。

FMCに対して正常に認証され、トークンが抽出されたら、さらにAPI要求を行うために、次の情報を活用する必要があります。

- ヘッダーX-auth-access-token **<authentication token value>を要求**の一部として追加します。
- X-auth-access-token **<authentication token value>**ヘッダーとX-auth-refresh-token **<refresh token value>ヘッダーを追加して、トークンを更新する要求を**行います。
- サーバへのすべてのREST要求で認証トークンのDomain_UUIDを使用します。

このヘッダー情報を使用すると、REST APIを使用してFMCと正常に対話できます。

一般的な問題のトラブルシューティング

- 認証のために送信されたPOSTの要求と応答の本文が空白です。要求ヘッダーの基本認証パラメータを渡す必要があります。すべてのトークン情報は、応答ヘッダーを介して返されます。

- RESTクライアントを使用すると、自己署名証明書が原因でSSL証明書の問題に関連するエラーが表示されることがあります。この検証は、使用しているクライアントに応じてオフにで

きます。

- ユーザクレデンシャルは、REST APIとGUIの両方のインターフェイスに同時に使用することはできません。両方に使用すると、警告なしでユーザがログアウトされます。

- FMC REST API認証トークンは30分間有効で、最大3回更新できます。