如何为FMC REST API交互生成身份验证令牌

简介

本文档介绍应用编程接口(API)管理员如何向Firepower管理中心(FMC)进行身份验证、生成令牌并将其用于任何进一步的API交互。

先决条件

要求

Cisco 建议您了解以下主题：

- Firepower管理中心(FMC)功能和配置。(配置指南)
- 了解各种REST API调用。(什么是REST API?)
- 查看《FMC API快速入门指南》。

使用的组件

- 支持REST API（版本6.1或更高版本）且已启用REST API的Firepower管理中心。
- REST客户端，如Postman、Python脚本、CURL等

背景信息

REST API越来越受欢迎，因为网络管理员可以使用轻量级可编程方法来配置和管理其网络。
FMC支持使用任何REST客户端以及使用内置API资源管理器进行配置和管理。

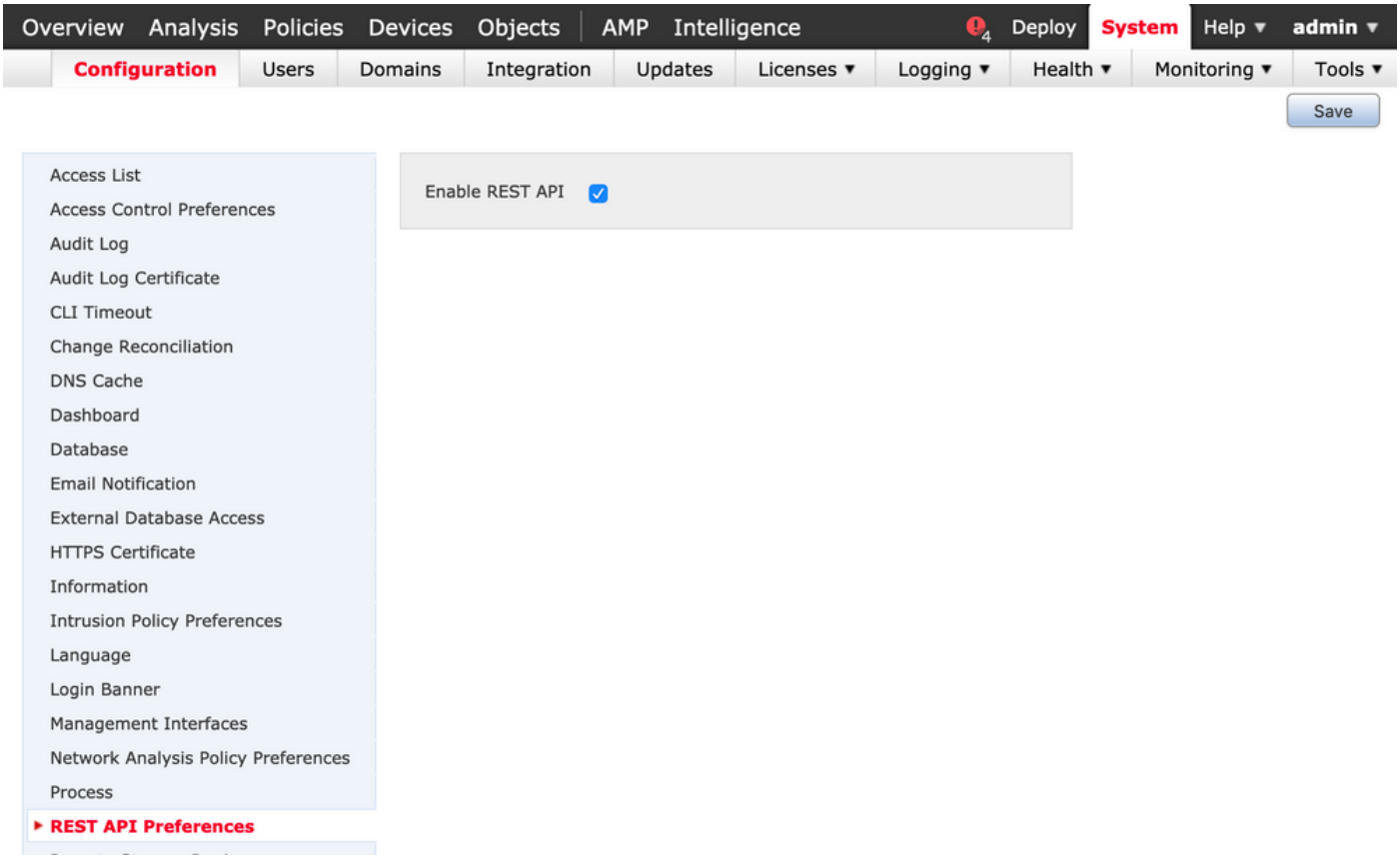
配置

在FMC上启用REST API

步骤1.导航至**System > Configuration > REST API Preferences > Enable REST API。**

步骤2.选中启**用REST API复**选框。

步骤3.单**击保**存，**启用**REST API时显示“保存成功”对话框，如图所示：



在FMC上创建用户

在FMC上使用API基础设施的最佳做法是将UI用户和脚本用户分开。有关各种用户角色的了解以及创建新用户的指南，请参阅《FMC用户帐户指南》。

请求身份验证令牌的步骤

步骤1.打开**REST API**客户端。

步骤2.将客户端设置为执行POST命令，URL:https://<management_center_IP_or_name>/api/fmc_platform/v1/auth/generatetoken。

步骤3.将用户名和密码作为基本身份验证报头。POST正文应为空。

例如，使用Python的身份验证请求：

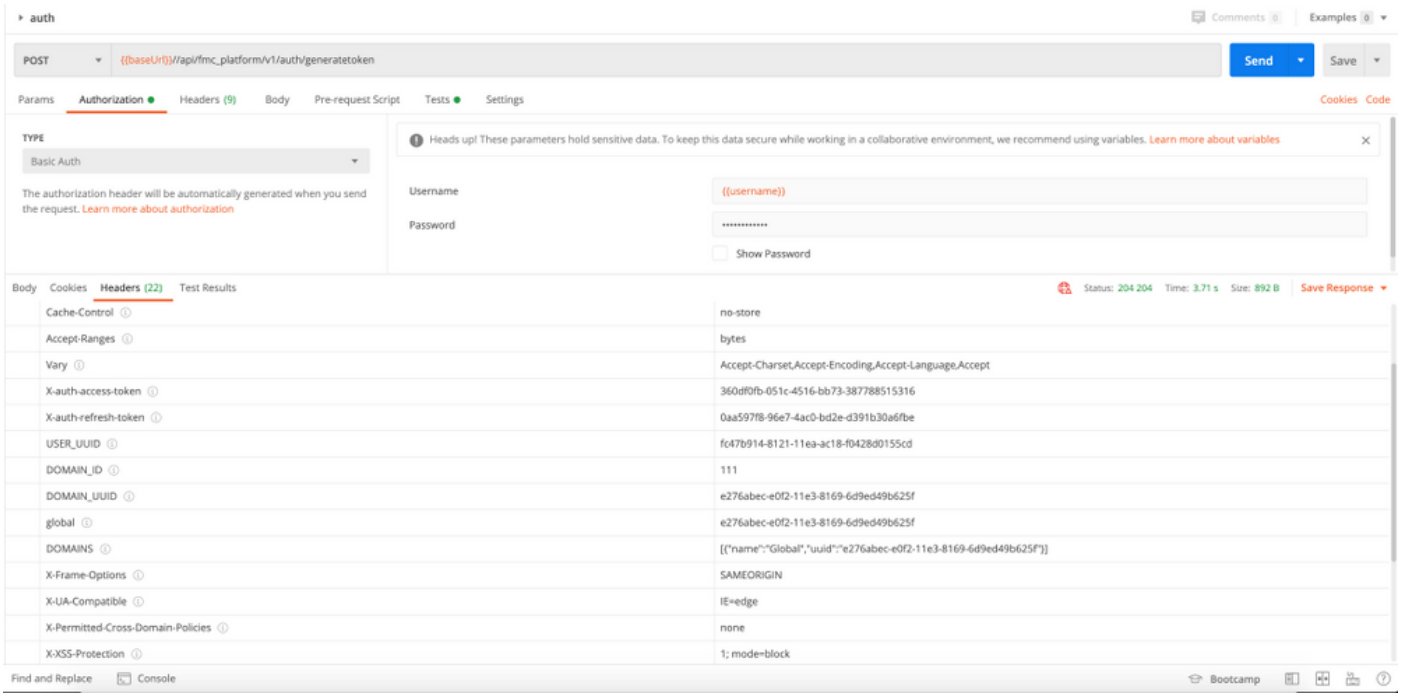
```
import requests url = "https://10.10.10.1//api/fmc_platform/v1/auth/generatetoken" payload = {}
headers = { 'Authorization': 'Basic Y2lzY291c2VyOmNpc2NwYXBpdXNlcg==' } response =
requests.request("POST", url, headers=headers, data = payload, verify=False)
print(response.headers)
```

使用CURL的身份验证请求的另一个示例：

```
$ 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
```

如图所示，来自基于GUI的客户端（如Postman）的示例：



发送后续API请求

> **注意**：您在输出中看到的是响应报头，而不是响应正文。实际响应正文为空。 需要提取的重要报头信息**是X-auth-access-token、X-auth-refresh-token和DOMAIN_UUID。**

成功向FMC进行身份验证并提取令牌后，您需要利用以下信息来获取更多API请求：

- 将报头X-auth-access-token**<authentication token value>作为**请求的一部分添加。
- 在刷新令牌的请求中添**加报头X-auth-access-token**<authentication token value>**和X-auth-refresh-token<refresh token value>**。
- 在向服务器发出的所有REST请求中，使用身份验证令牌中的Domain_UUID。

使用此报头信息，您可以使用REST API成功与FMC交互。

排除常见问题

- 为身份验证发送的POST请求和响应正文为空。您需要在请求报头中传递基本身份验证参数。所有令牌信息都通过响应报头返回。
- 使用REST客户端时，可能会看到与SSL证书问题相关的错误，原因是自签名证书。您可以根据您使用的客户端关闭此验证。
- 用户凭证不能同时用于REST API和GUI接口，如果同时用于两者，则用户将注销而不发出警告。
- FMC REST API身份验证令牌的有效期为30分钟，最多可刷新三次。