Como gerar um token de autenticação para interações de API REST do FMC

Introduction

Este documento descreve como um administrador de API (Application Programming Interface, interface de programação de aplicativos) pode se autenticar no Firepower Management Center (FMC), gerar tokens e usá-los para quaisquer outras interações de API.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Recursos e configuração do Firepower Management Center (FMC). (Guia de configuração)
- Entendendo várias chamadas de API REST. (O que são APIs REST?)
- Revisão do Guia de Início Rápido da API do FMC.

Componentes Utilizados

- Firepower Management Center que suporta APIs REST (versão 6.1 ou superior) com API REST ativada.
- Clientes REST como Postman, scripts Python, CURL etc.

Informações de Apoio

As APIs REST são cada vez mais populares devido à abordagem programável leve que os gerentes de rede podem usar para configurar e gerenciar suas redes. O FMC suporta configuração e gerenciamento usando qualquer cliente REST e também usando o explorador de API interno.

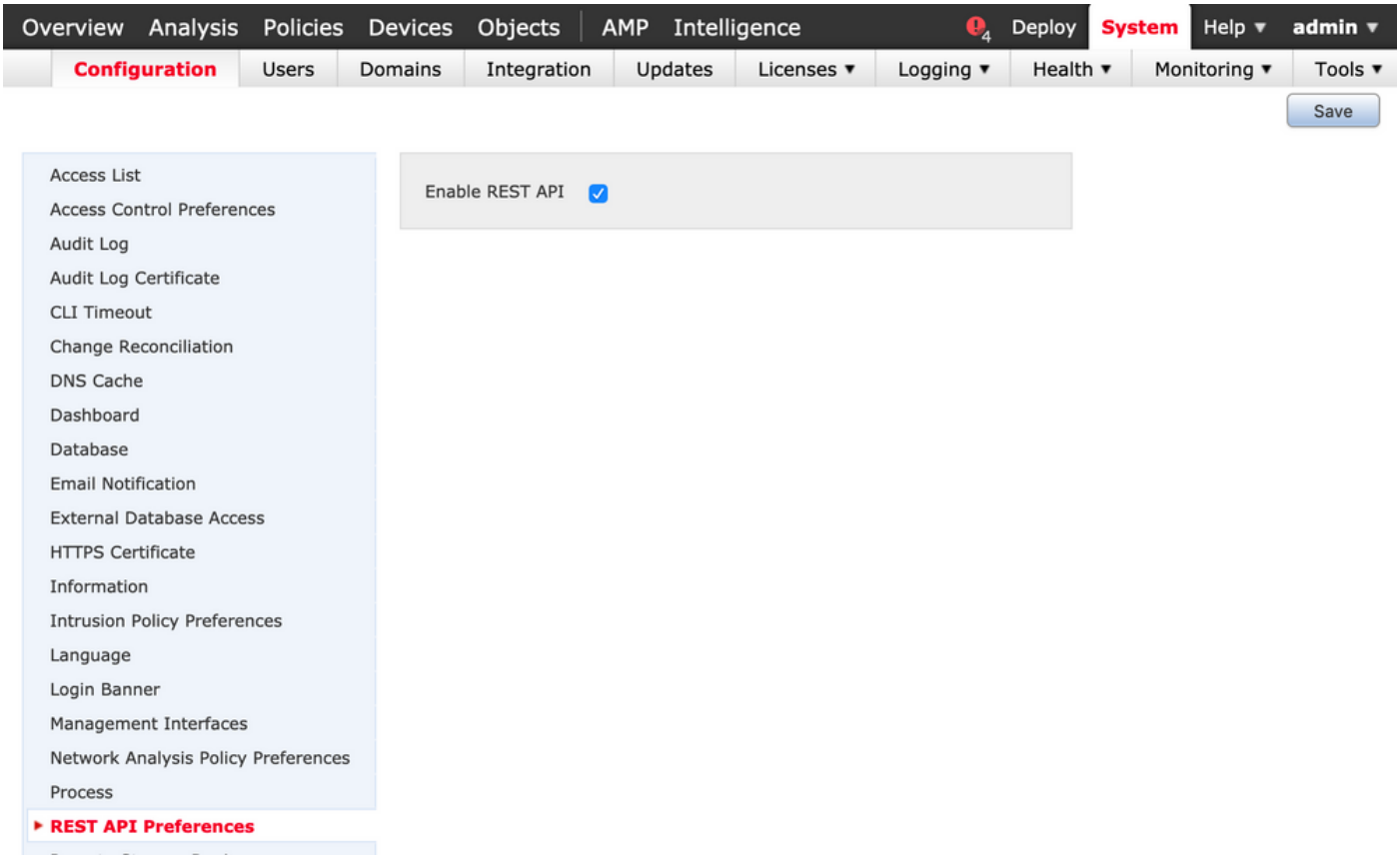
Configurar

Ativação da API REST no FMC

Etapa 1. Navegue até **System** > **Configuration** > **REST API Preferences** > Enable **REST API.**

Etapa 2. Marque a caixa de seleção **Habilitar API REST**.

Etapa 3. Clique em **Salvar,** uma caixa de diálogo **Salvar com Êxito** será exibida quando a API REST estiver habilitada, como mostrado na imagem:



Criando um usuário no FMC

Como prática recomendada para usar a infraestrutura de API no FMC é manter os usuários de interface de usuário e usuários de script separados. Consulte o Guia de Contas de Usuário do FMC para obter informações sobre várias funções de usuário e as diretrizes para a criação de um novo usuário.

Etapas para solicitar um token de autenticação

Etapa 1. Abra seu **REST API Client**.

Etapa 2. Defina o cliente para fazer um comando POST, URL: https://<management_center_IP_or_name>/api/fmc_platform/v1/auth/geneatetoken.

Etapa 3. Inclua o nome de usuário e a senha como um cabeçalho de autenticação básica. O corpo do **POST** deve estar em branco.

Por exemplo, uma solicitação de autenticação usando Python:

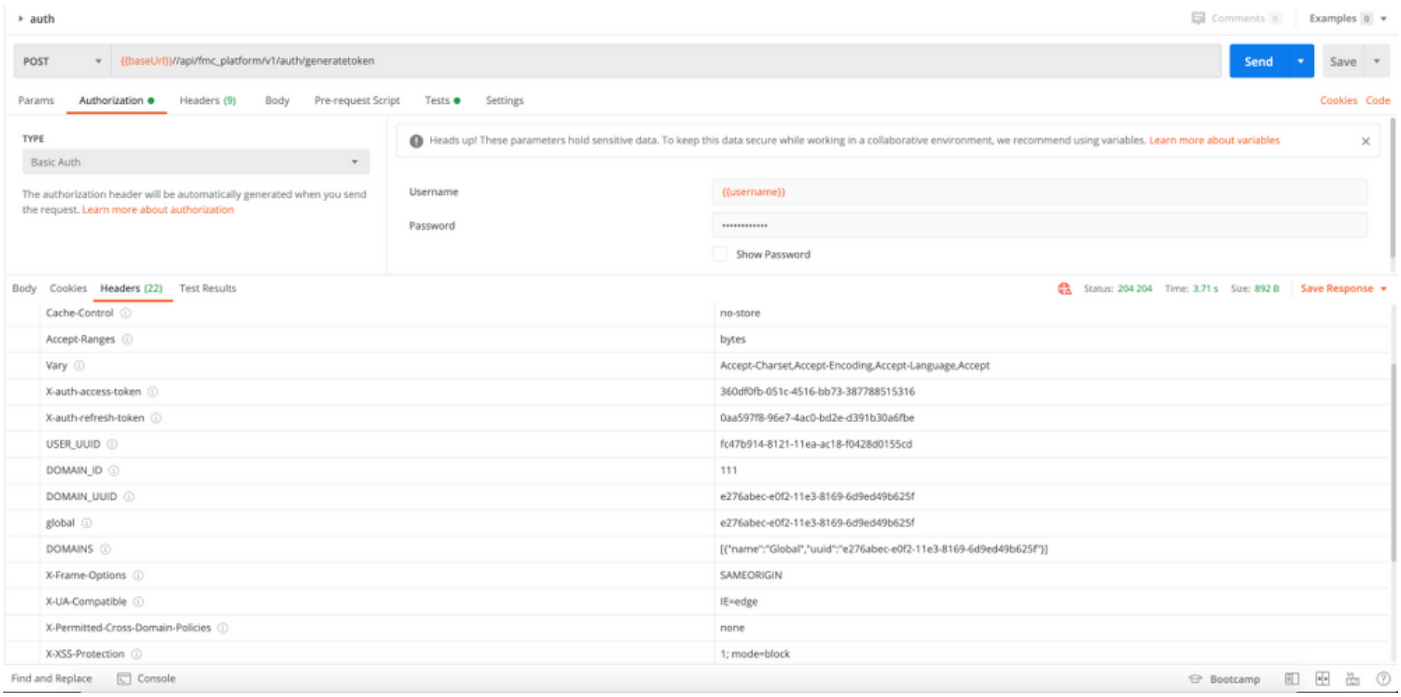
```
import requests url = "https://10.10.10.1//api/fmc_platform/v1/auth/generatetoken" payload = {}
headers = { 'Authorization': 'Basic Y2lzY291c2VyOmNpc2NwYXBpdXNlcg==' } response =
requests.request("POST", url, headers=headers, data = payload, verify=False)
print(response.headers)
```

Outro exemplo de uma solicitação de autenticação usando 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
```

Exemplo de um cliente baseado em GUI como o Postman, como mostrado na imagem:



Enviando solicitações de API subsequentes

> **Note**: O que você vê na saída são os cabeçalhos de resposta e não o corpo de resposta. O corpo da resposta real está em branco. As informações importantes do cabeçalho que precisam ser extraídas são **X-auth-access-token**, **X-auth-refresh-token** e **DOMAIN_UUID**.

Depois de ter autenticado com êxito o FMC e extraído os tokens, para obter mais solicitações de API, você precisa aproveitar as informações abaixo:

- Adicione o cabeçalho X-auth-access-token **<authentication token value>** como parte da solicitação.
- Adicione os cabeçalhos X-auth-access-token **<authentication token value>** e X-auth-refresh-token **<refresh token value>** em solicitações para atualizar o token.
- Use o Domain_UUID do token de autenticação em todas as solicitações REST para o servidor.

Com essas informações de cabeçalho, você pode interagir com o FMC usando APIs REST.

Solucionar problemas comuns

- O corpo da solicitação e da resposta do POST enviado para a autenticação está em branco. Você precisa passar os parâmetros básicos de autenticação no cabeçalho da solicitação. Todas as informações do token são retornadas através dos cabeçalhos de resposta.

- Ao usar o cliente REST, você pode ver erros relacionados ao problema de certificado SSL devido a um certificado autoassinado. Você pode desativar essa validação dependendo do cliente que está usando.
- As credenciais do usuário não podem ser usadas para interfaces REST API e GUI simultaneamente, e o usuário será desconectado sem aviso se for usado para ambos.
- Os tokens de autenticação da API REST do FMC são válidos por 30 minutos e podem ser atualizados até três vezes.