Comment générer un jeton d'authentification pour les interactions FMC REST API

Introduction

Ce document décrit comment un administrateur d'interface de programmation d'application (API) peut s'authentifier auprès de Firepower Management Center (FMC), générer des jetons et les utiliser pour d'autres interactions API.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Fonctionnalités et configuration de Firepower Management Center (FMC). (Guide de configuration)
- Compréhension des divers appels de l'API REST. (Que sont les API REST ?)
- Révision du Guide de démarrage rapide de l'API FMC.

Composants utilisés

- Firepower Management Center qui prend en charge les API REST (version 6.1 ou ultérieure) avec l'API REST activée.
- REST clients comme Postman, scripts Python, CURL, etc.

Informations générales

Les API REST sont de plus en plus populaires en raison de l'approche programmable légère que les administrateurs réseau peuvent utiliser pour configurer et gérer leurs réseaux. FMC prend en charge la configuration et la gestion à l'aide de tout client REST et de l'explorateur d'API intégré.

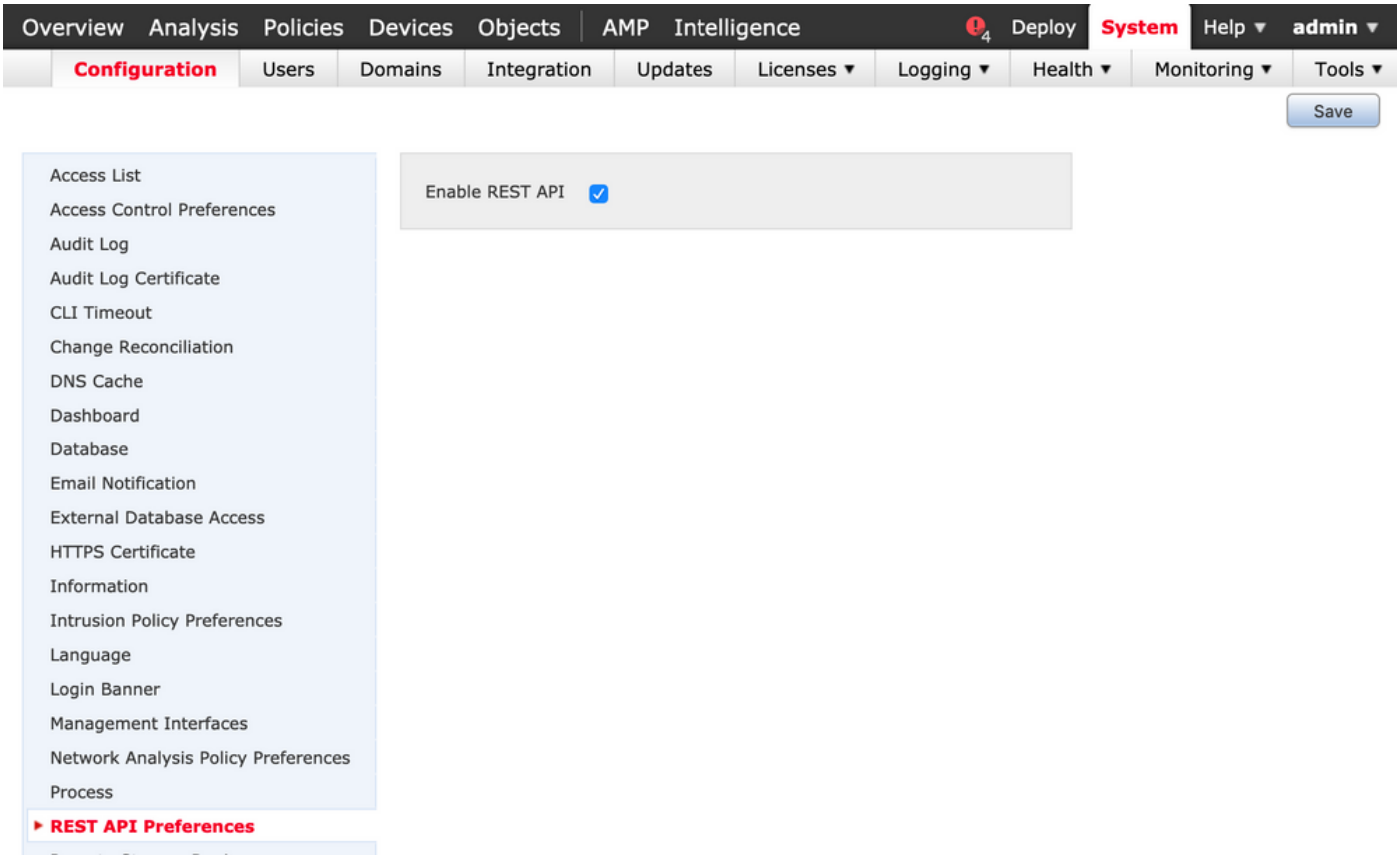
Configurer

Activation de l'API REST sur FMC

Étape 1. Accédez à System>Configuration>REST API Preferences>Enable REST API.

Étape 2. Cochez la case Enable REST API.

Étape 3. Cliquez sur Save, une boîte de dialogue Save Successful s'affiche lorsque l'API REST est activée, comme illustré dans l'image :



Création d'un utilisateur sur FMC

La meilleure pratique d'utilisation de l'infrastructure d'API sur FMC consiste à séparer les utilisateurs d'interface utilisateur et les utilisateurs de script. Reportez-vous au Guide des comptes d'utilisateurs pour FMC pour la compréhension des différents rôles d'utilisateur et les directives pour créer un nouvel utilisateur.

Étapes pour demander un jeton d'authentification

Étape 1. Ouvrez votre client REST API.

Étape 2. Configurez le client pour exécuter une commande POST, URL : https://<management_center_IP_or_name>/api/fmc_platform/v1/auth/generatetoken.

Étape 3. Incluez le nom d'utilisateur et le mot de passe comme en-tête d'authentification de base. Le corps POST doit être vide.

Par exemple, une requête d'authentification utilisant Python :

```
import requests
url = "https://10.10.10.1//api/fmc_platform/v1/auth/generatetoken"

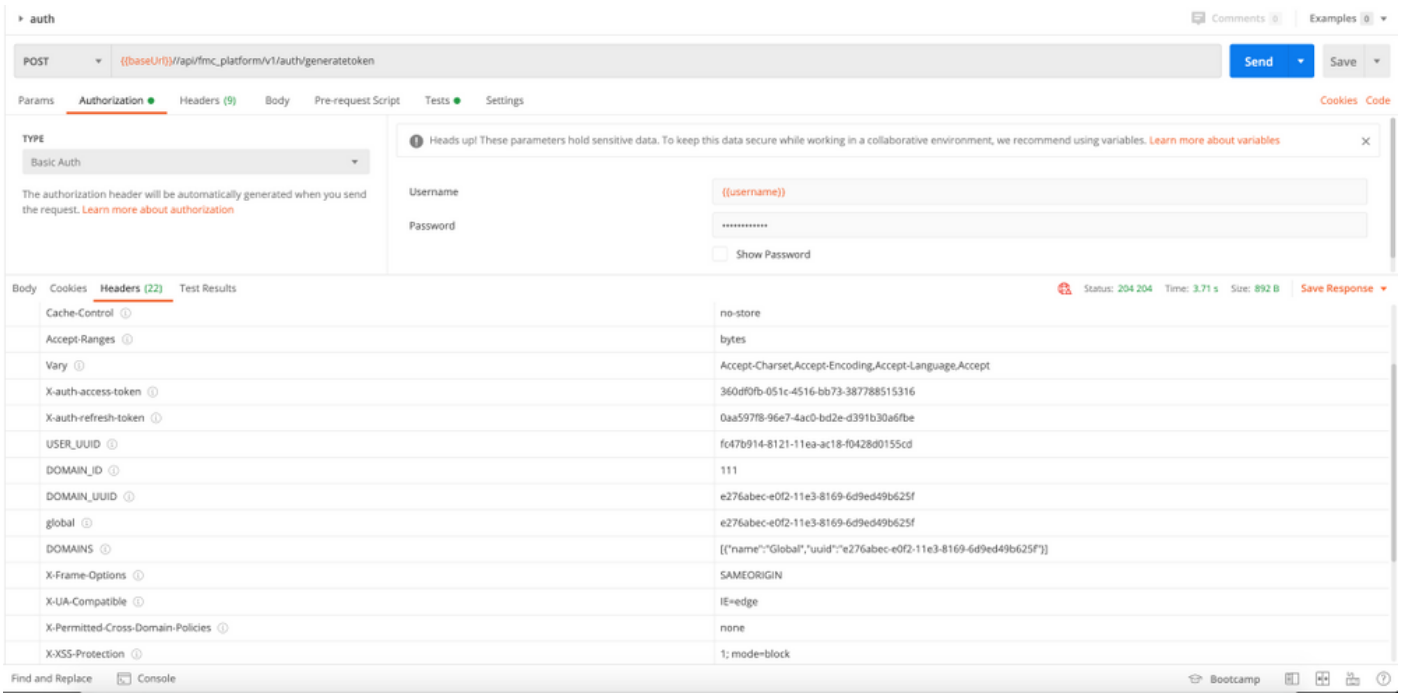
payload = {}
headers = {
'Authorization': 'Basic Y2lzY291c2VyOmNpc2NwYXBpdXNlcg=='
}
```

```
response = requests.request("POST", url, headers=headers, data = payload, verify=False)
print(response.headers)
```

Autre exemple de demande d'authentification utilisant CURL :

```
$ curl --request POST 'https://10.10.10.1/api/fmc_platform/v1/auth/generatetoken' --header 'Authorizati
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
```

Exemple à partir d'un client basé sur une interface graphique utilisateur comme Postman, comme illustré dans l'image :



Envoi des demandes API suivantes

Remarque : Ce que vous voyez dans le résultat sont les en-têtes de réponse et non le corps de réponse. Le corps de réponse réel est vide. Les informations d'en-tête importantes qui doivent être extraites sont X-auth-access-token, X-auth-refresh-token, et DOMAIN_UUID.

Une fois que vous vous êtes authentifié avec succès auprès de FMC et que vous avez extrait les jetons, vous devez exploiter les informations ci-dessous pour d'autres demandes d'API :

- Ajoutez l'en-tête X-auth-access-token <authentication token value> dans le cadre de la requête.
- Ajoutez les en-têtes X-auth-access-token <authentication token value> et X-auth-refresh-token <refresh token value> dans les demandes d'actualisation du jeton.
- Utilisez le Domain_UUID du jeton d'authentification dans toutes les requêtes REST adressées au serveur.

Grâce à ces informations d'en-tête, vous pouvez interagir avec le FMC à l'aide des API REST.

Résoudre les problèmes courants

- Le corps de la requête et de la réponse du POST envoyé pour l'authentification est vide. Vous devez passer les paramètres d'authentification de base dans l'en-tête de la demande. Toutes les informations de jeton sont renvoyées via les en-têtes de réponse.
- Lors de l'utilisation du client REST, vous pouvez voir des erreurs liées au problème de certificat SSL en raison d'un certificat auto-signé. Vous pouvez désactiver cette validation en fonction du client que vous utilisez.
- Les informations d'identification de l'utilisateur ne peuvent pas être utilisées simultanément pour les interfaces REST API et GUI, et l'utilisateur sera déconnecté sans avertissement s'il est utilisé pour les deux.
- Les jetons d'authentification de l'API REST FMC sont valides pendant 30 minutes et peuvent être actualisés jusqu'à trois fois.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.