Come generare il token di autenticazione per le interazioni dell'API REST di FMC

Introduzione

In questo documento viene descritto come un amministratore API (Application Programming Interface) può eseguire l'autenticazione in Firepower Management Center (FMC), generare token e utilizzarli per ulteriori interazioni API.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Caratteristiche e configurazione di Firepower Management Center (FMC). (Guida di configurazione)
- Informazioni su varie chiamate all'API REST. (Che cosa sono le API REST?)
- Revisione della Guida introduttiva all'API di FMC.

Componenti usati

- Firepower Management Center che supporta le API REST (versione 6.1 o successiva) con l'API REST abilitata.
- Client REST come Postman, script Python, CURL, ecc.

Premesse

Le API REST sono sempre più diffuse a causa dell'approccio programmabile leggero che i gestori di rete possono utilizzare per configurare e gestire le loro reti. FMC supporta la configurazione e la gestione utilizzando qualsiasi client REST e utilizzando inoltre l'API explorer integrato.

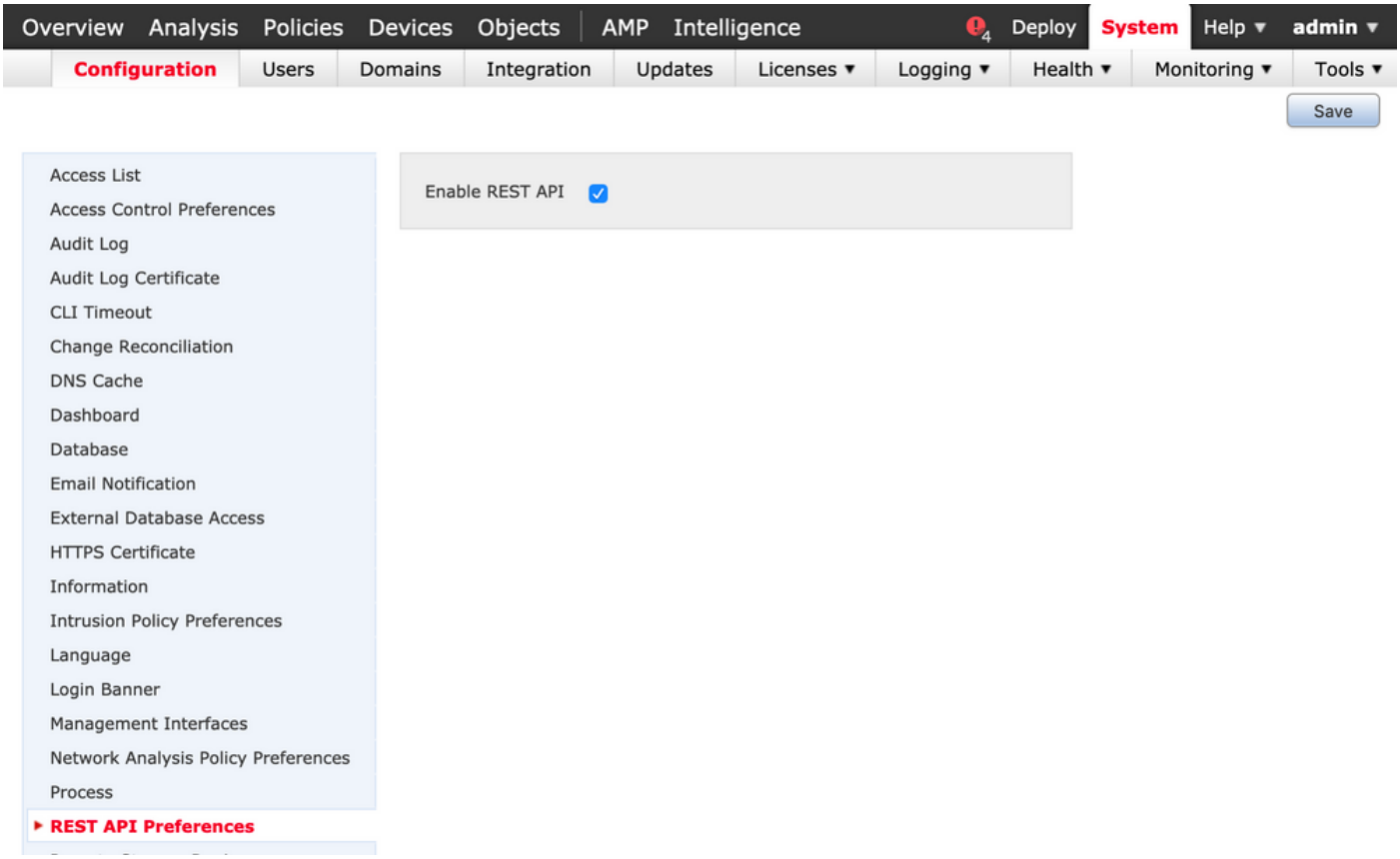
Configurazione

Abilitazione dell'API REST in FMC

Passaggio 1. Passare a **Sistema>Configurazione>Preferenze API REST>**Abilita **API REST.**

Passaggio 2. Selezionare la casella di controllo **Abilita API REST**.

Passaggio 3. Fare clic su **Save.** Viene visualizzata una finestra di dialogo **Save Successful** quando l'API REST è abilitata, come mostrato nell'immagine:



Creazione di un utente in FMC

Èconsigliabile utilizzare l'infrastruttura API in FMC per tenere separati gli utenti dell'interfaccia utente e gli utenti di script. Per informazioni sui vari ruoli utente e sulle linee guida per la creazione di un nuovo utente, fare riferimento alla Guida agli account utente per FMC.

Procedura per richiedere un token di autenticazione

Passaggio 1. Aprire il **client API REST**.

Passaggio 2. Impostare il client per creare un comando POST URL: https://<management_center_IP_or_name>/api/fmc_platform/v1/auth/generatetoken.

Passaggio 3. Includere il nome utente e la password come intestazione di autenticazione di base. Il corpo **POST** deve essere vuoto.

Ad esempio, una richiesta di autenticazione tramite Python:

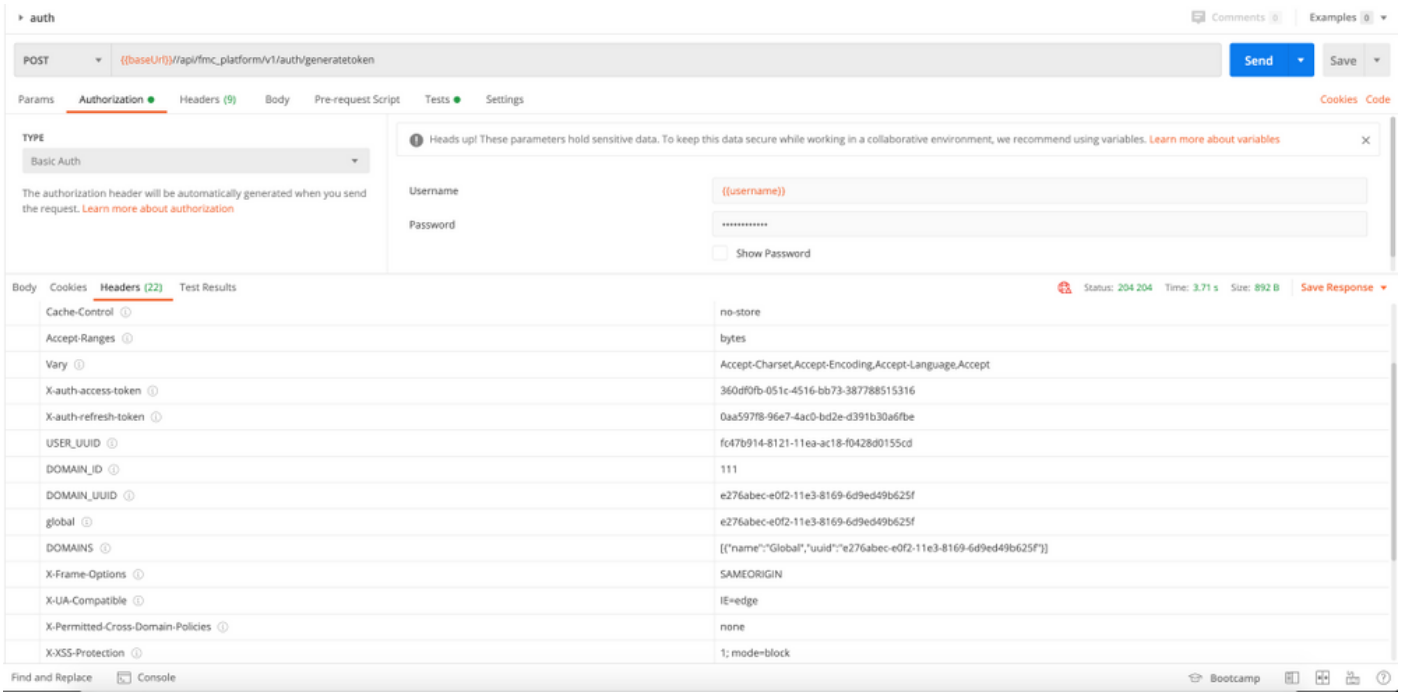
```
import requests url = "https://10.10.10.1//api/fmc_platform/v1/auth/generatetoken" payload = {}
headers = { 'Authorization': 'Basic Y2lzY291c2VyOmNpc2NwYXBpdXNlcg==' } response =
requests.request("POST", url, headers=headers, data = payload, verify=False)
print(response.headers)
```

Di seguito è riportato un altro esempio di richiesta di autenticazione tramite 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

Esempio da un client basato su GUI come Postman, come mostrato nell'immagine:



Invio di richieste API successive

> **Nota:** Nell'output vengono visualizzate le intestazioni di risposta e non il corpo della risposta. Il corpo effettivo della risposta è vuoto. Le informazioni importanti dell'intestazione da estrarre sono **X-auth-access-token**, **X-auth-refresh-token** e **DOMAIN_UUID**.

Dopo aver eseguito l'autenticazione a FMC ed estratto i token, per ulteriori richieste API è necessario utilizzare le informazioni seguenti:

- Aggiungere l'intestazione X-auth-access-token **<authentication token value>** come parte della richiesta.
- Aggiungere le intestazioni X-auth-access-token **<authentication token value>** e X-auth-refresh-token **<refresh token value>** nelle richieste di aggiornamento del token.
- Utilizzare Domain_UUID dal token di autenticazione in tutte le richieste REST inviate al server.

Con queste informazioni di intestazione è possibile interagire con il FMC utilizzando le API REST.

Risoluzione dei problemi comuni

- Il corpo della richiesta e della risposta del POST inviato per l'autenticazione è vuoto. È necessario passare i parametri di autenticazione di base nell'intestazione della richiesta. Tutte le informazioni sul token vengono restituite tramite le intestazioni di risposta.

- Quando si utilizza il client REST, è possibile che vengano visualizzati errori correlati al problema del certificato SSL a causa di un certificato autofirmato. È possibile disattivare questa convalida a seconda del client in uso.
- Le credenziali utente non possono essere utilizzate contemporaneamente per entrambe le interfacce API REST e GUI e l'utente verrà disconnesso senza avviso se utilizzato per entrambe.
- I token di autenticazione dell'API REST di FMC sono validi per 30 minuti e possono essere aggiornati fino a tre volte.