Configurazione di Postman per l'esecuzione di API su vManage

Sommario

[Introduzione](#)
[Requisiti di sistema](#)
[Premesse](#)
[Configurazione di Postman per l'esecuzione delle API](#)
[Passaggio 1. Aprire Postman e creare una nuova richiesta HTTP.](#)
[Passaggio 2. Eseguire l'autenticazione con le credenziali di nome utente e password per vManage.](#)
[Passaggio 3. Richiedi un token](#)
[Passaggio 4. Procedere per eseguire un'altra API in vManage.](#)
[Passaggio 5. Chiudi la sessione](#)
[Esecuzione di chiamate API in un ambiente automatizzato](#)
[Come salvare il token in una variabile?](#)
[Come cancellare il cookie SESSIONID per le nuove sessioni?](#)
[Modalità d'uso di Collection Runner](#)

Introduzione

In questo documento viene descritto come eseguire le API (Application Programming Interfaces) con Postman.

Requisiti di sistema

- Postman installato
- Accesso a vManage e alle credenziali di nome utente e password

Nota: se non hai Postman, scaricalo da https://www.postman.com/downloads/

Premesse

I verbi HTTP primari o più comunemente utilizzati (o metodi, come vengono chiamati correttamente) sono POST, GET, PUT, PATCH e DELETE.

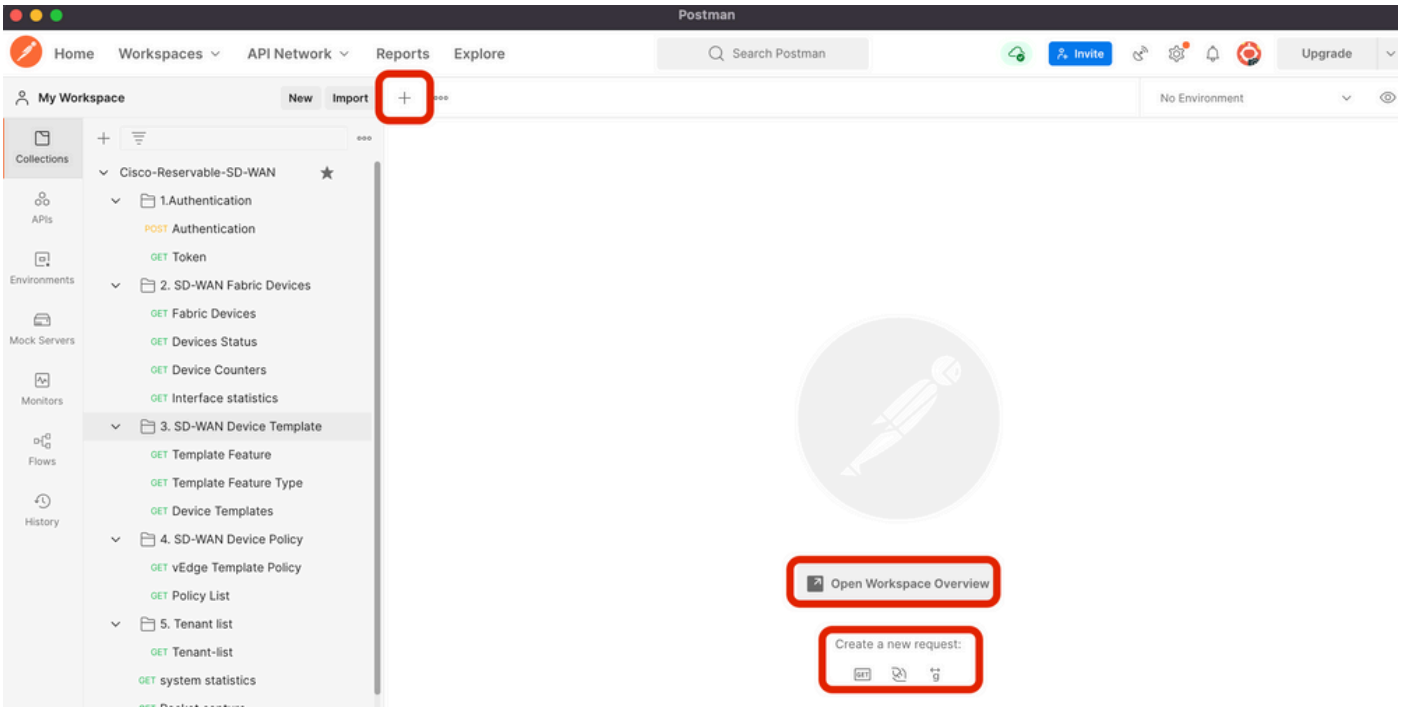
Corrispondono rispettivamente alle operazioni di creazione, lettura, aggiornamento ed eliminazione (o CRUD).

Ci sono anche molti altri verbi, ma sono utilizzati meno frequentemente. Di questi metodi meno frequenti, OPTIONS e HEAD sono utilizzati più spesso di altri.

Configurazione di Postman per l'esecuzione delle API

Passaggio 1. Aprire Postman e creare una nuova richiesta HTTP.

Èpossibile creare nuove richieste HTTP facendo clic su una delle opzioni evidenziate.



Crea una nuova richiesta HTTP.

Passaggio 2. Eseguire l'autenticazione con le credenziali di nome utente e password per vManage.

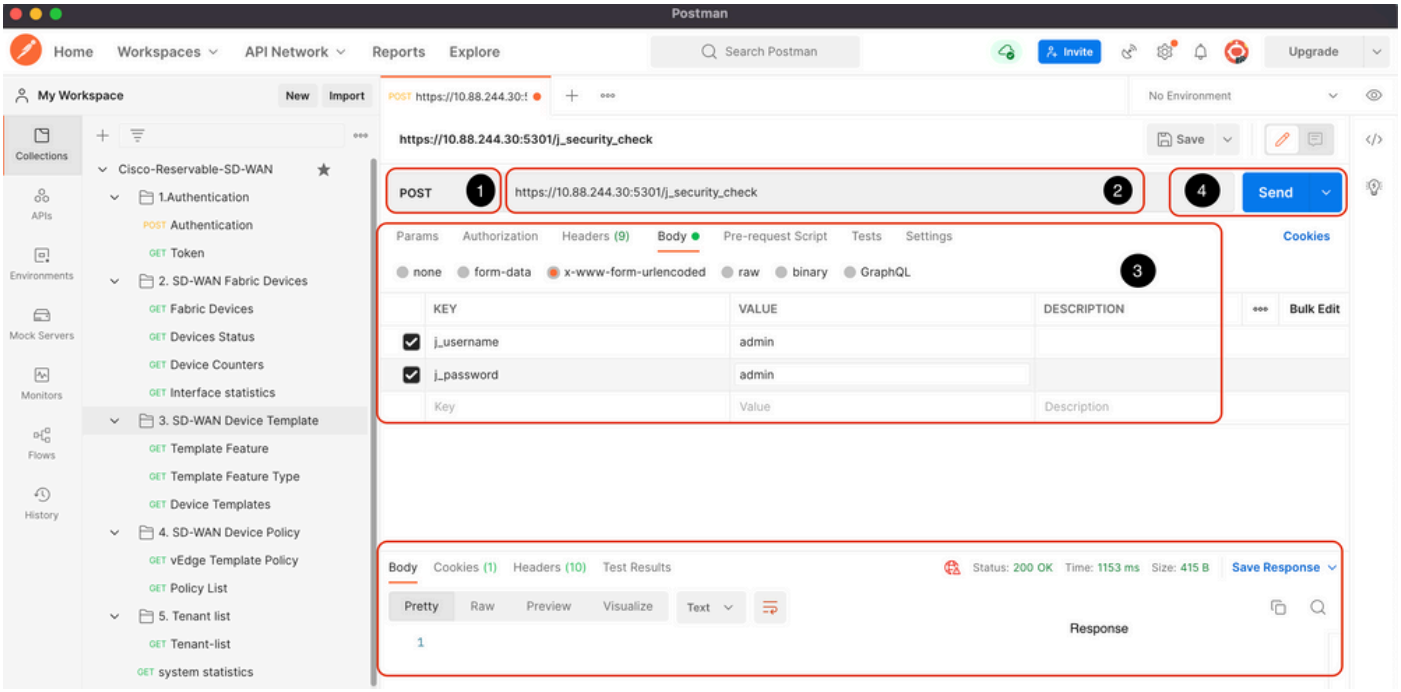
Crea un'altra richiesta HTTP.

1. Selezionare **POST** come verbo HTTP.
2. Aggiungere https://<vmanage-ip>/j_security_checkaccanto a POST.
3. Fate clic su **Body** e aggiungete come parametri **KEY j_username** e **j_password** rispettivamente con i relativi valori.
4. Fare clic su **Invia.**

Nota: nell'esempio, l'indirizzo IP di vManage è 10.88.244.30 e la porta è 5301

Nota: come valori di nome utente e password, utilizziamo admin.

Completare i parametri in Postman.



Autenticazione vManage.

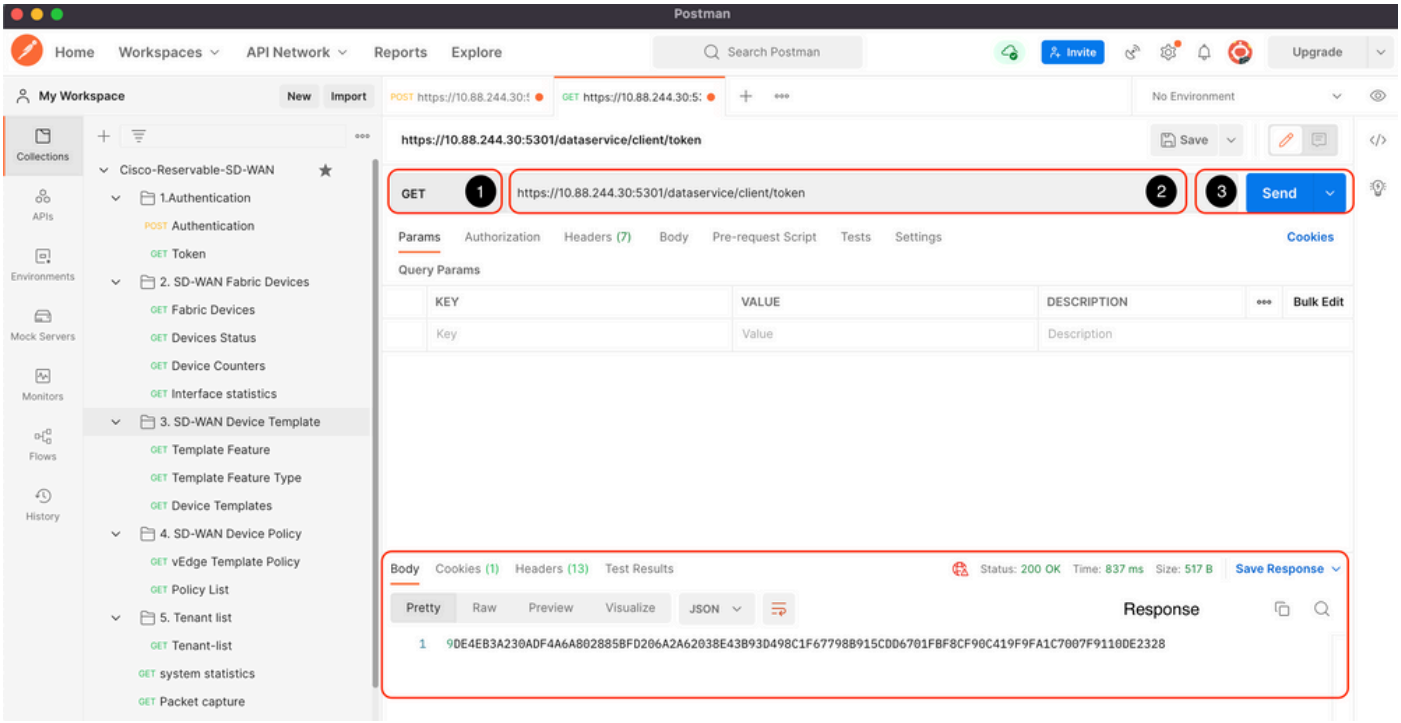
Attenzione: la risposta di questa chiamata API deve essere vuota

Passaggio 3. Richiedi un token

1. Selezionare **GET** come verbo HTTP.
2. Aggiungere i dettagli della chiamata API accanto a GET https://<vmanage-ip>/dataservice/client/token
3. Fare clic su **Invia**

Nota: a partire dalla versione 19.2.1 di vManage, è stato reso obbligatorio che un utente che ha eseguito l'accesso invii un token X-XSRG-TOKEN o CSRF per ogni operazione POST/PUT/DELETE tramite chiamata API.

Una volta eseguita la chiamata API, si ottiene una stringa di risposta nel corpo. Salvate quella stringa. L'immagine mostra l'output in Postman.



Richiedi un token per vManage

Avviso: se non si ottiene un token come mostrato nell'immagine, ripetere il passaggio.

Passaggio 4. Procedere per eseguire un'altra API in vManage.

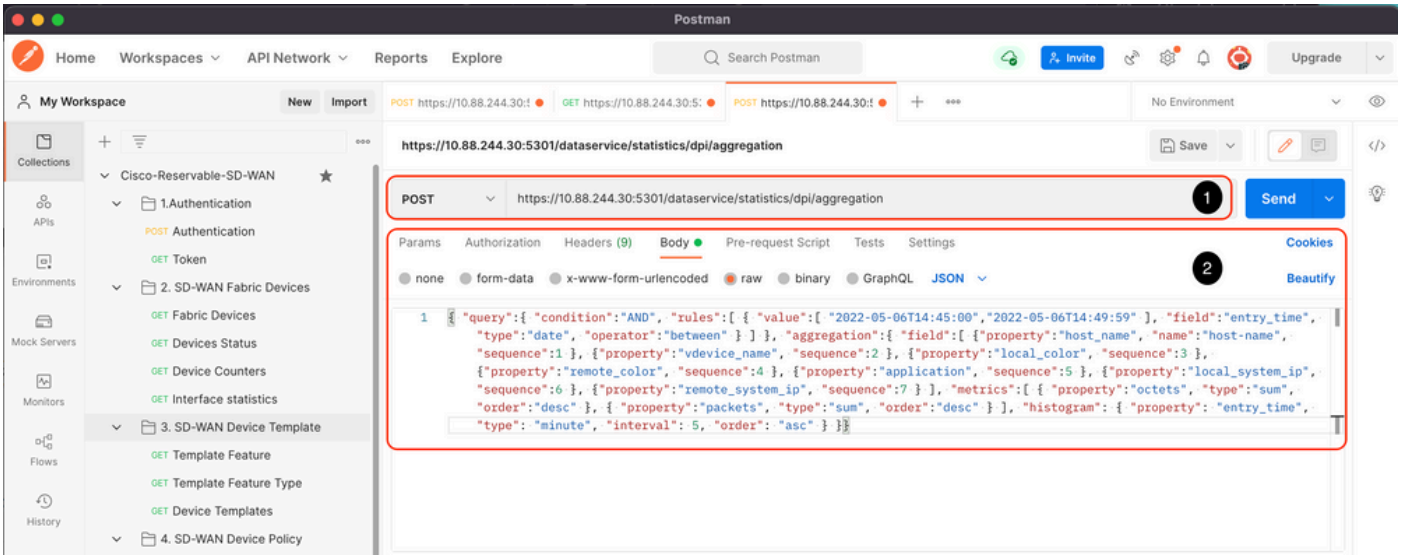
Questo esempio comporta una richiesta POST

1. Selezionare la chiamata API da eseguire, nel caso specifico `https:///dataservice/statistics/dpi/aggregation`

   Suggerimento: per esplorare altre chiamate API, visitare il sito Web all'indirizzo https://vmanage-ip:port/apidocs

2. Raccogliere il corpo della chiamata API.

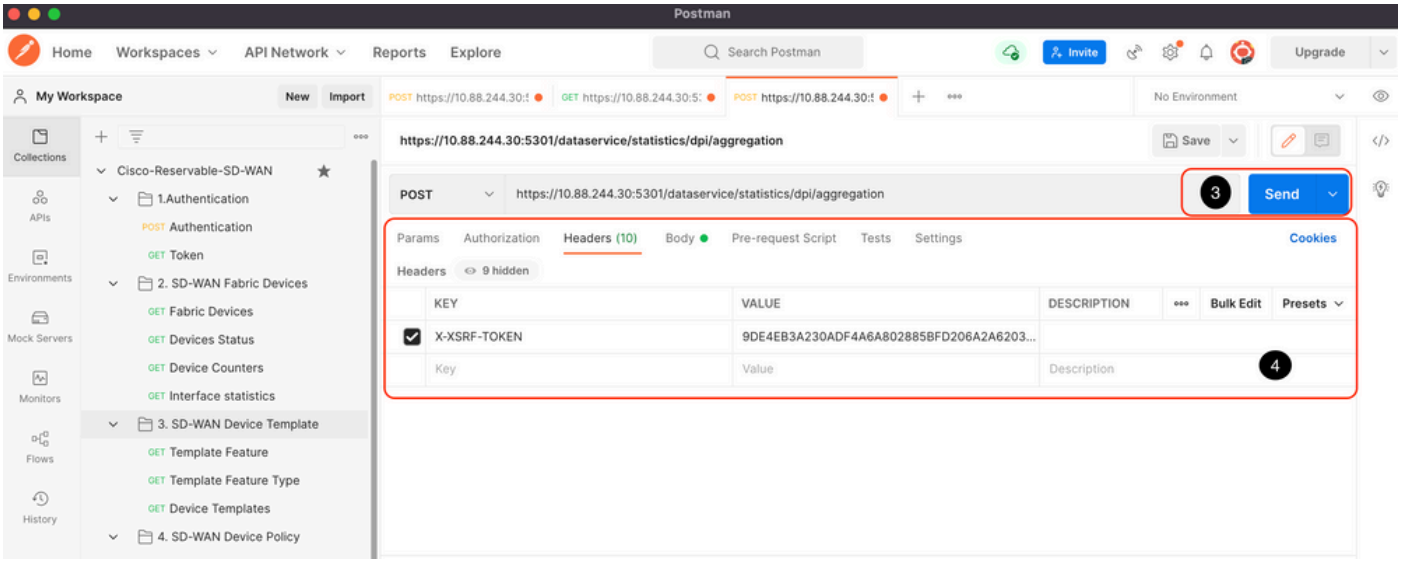
   Nota: questa chiamata API contiene un corpo in formato JSON



3. Fare clic su **Header** e aggiungere come **chiave** la stringa **X-XSRF-TOKEN** come valore.

4. Fare clic su **Invia.**

L'immagine mostra come deve apparire la chiamata API.



Chiamata API di aggregazione DPI.

Passaggio 5. Chiudi la sessione

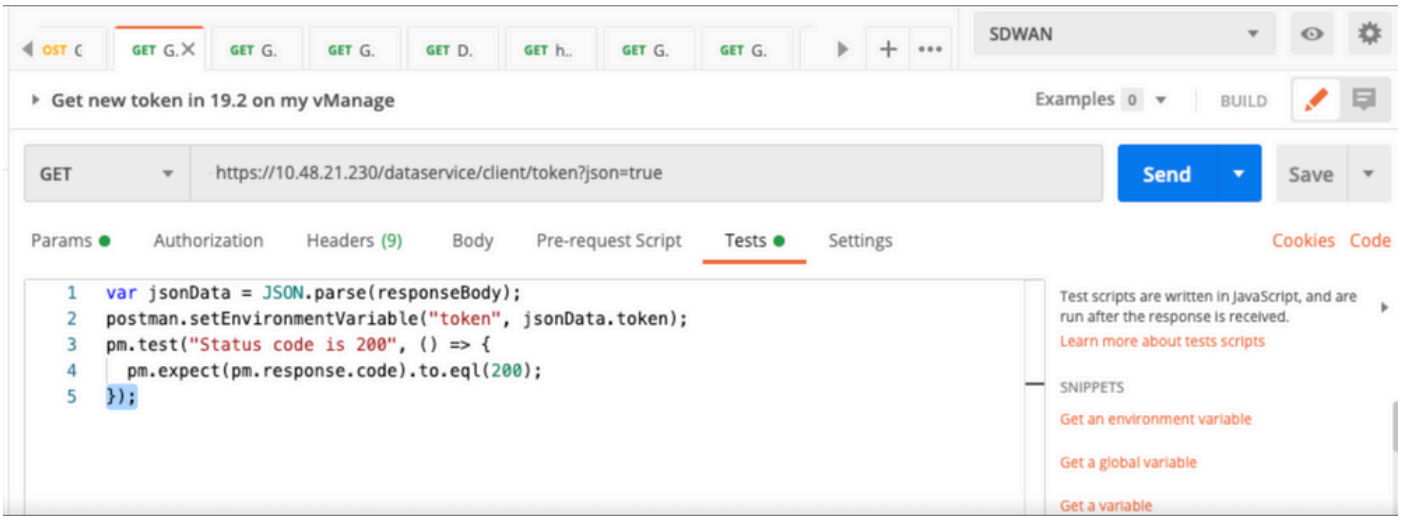
Dopo aver recuperato tutte le informazioni necessarie da vManage e/o dai dispositivi, liberare le risorse di vManage ed eliminare la possibilità per utenti malintenzionati di utilizzare la sessione.

Esecuzione di chiamate API in un ambiente automatizzato

Salva cookie e variabili da utilizzare nelle chiamate API successive

Come salvare il token in una variabile?

Salvare il token in una variabile per un successivo riutilizzo.



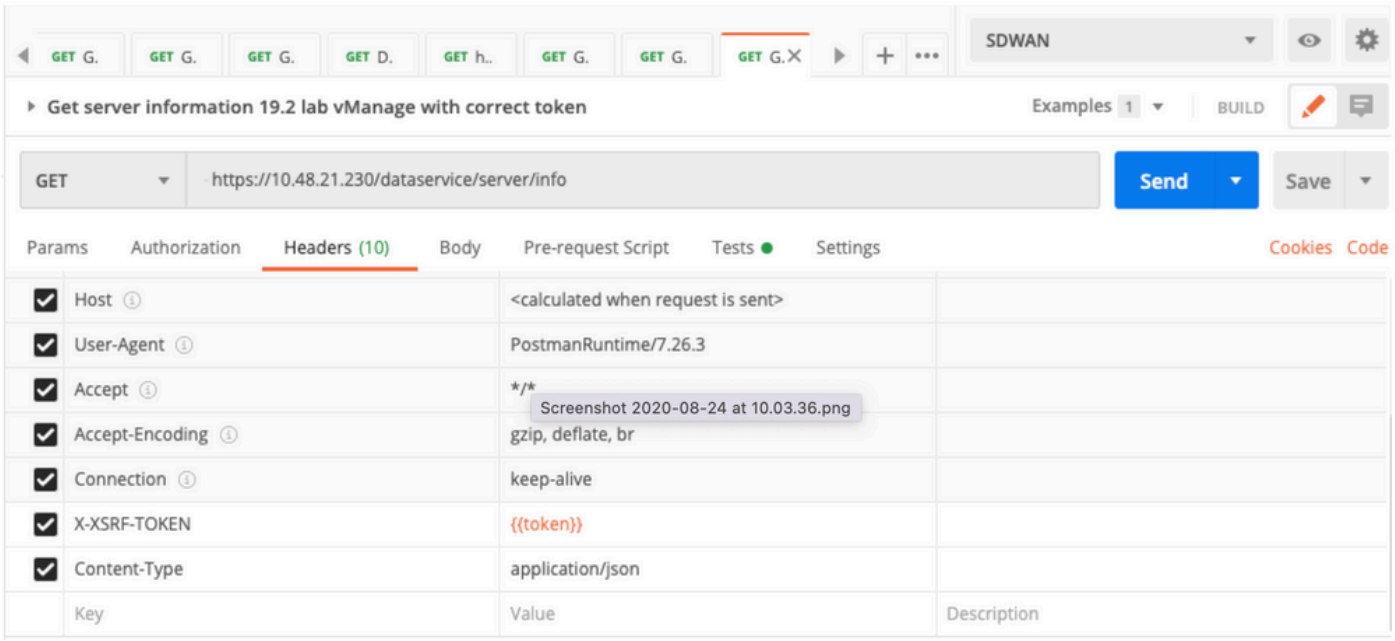
Salva il token in una variabile

Quando il token viene richiesto in formato JSON, archiviarlo. Utilizzare la scheda **Test** e incollare

le righe visualizzate.

```
var jsonData = JSON.parse(responseBody);
postman.setEnvironmentVariable("token", jsonData.token);
```

In seguito, qualsiasi chiamata API può utilizzare una variabile token.

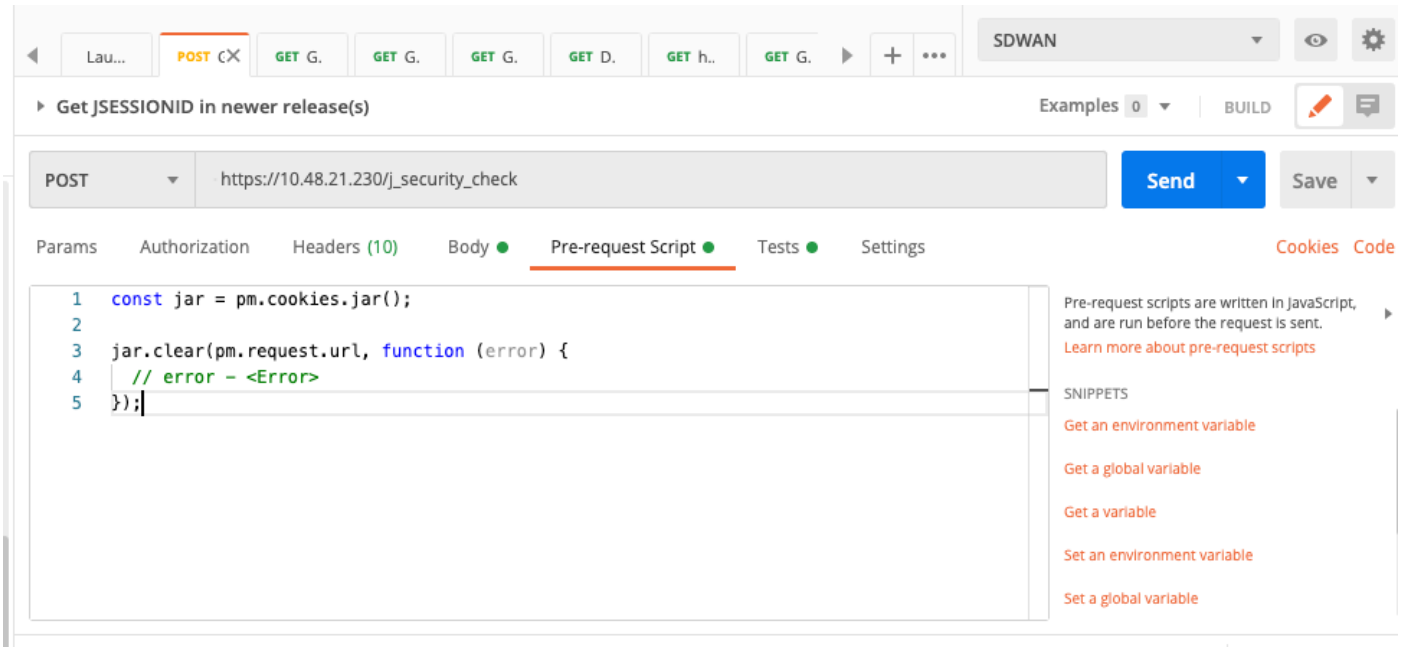


Utilizza la variabile token

Come cancellare il cookie SESSIONID per le nuove sessioni?

Ogni volta che si esegue la chiamata API per uscire, utilizzare JSESSIONID.

Non è possibile utilizzare un'autenticazione di base come nelle versioni precedenti. Al contrario, forniamo solo le credenziali e salviamo l'ID nel nostro cookie. Prima di questo, possiamo utilizzare un pre-test per cancellare tutti o specifici cookie.



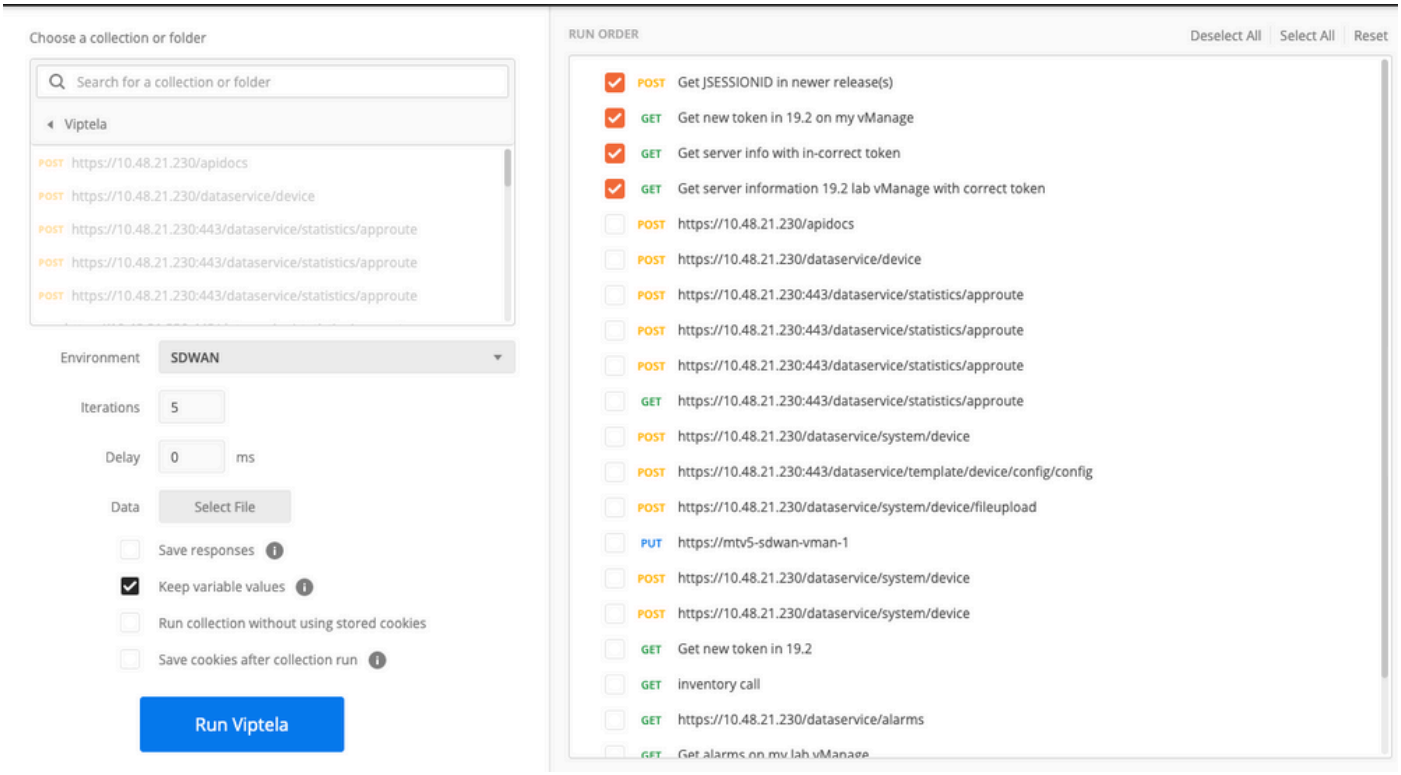
Cancella cookie

Ciò avviene tramite il codice inserito nello script di pre-richiesta.

Modalità d'uso di Collection Runner

Ora che si dispone di un ambiente in cui è possibile eseguire le sessioni e salvare i dati specifici di ciascuna sessione, è possibile eseguire una sequenza di chiamate utilizzando Collection Runner.

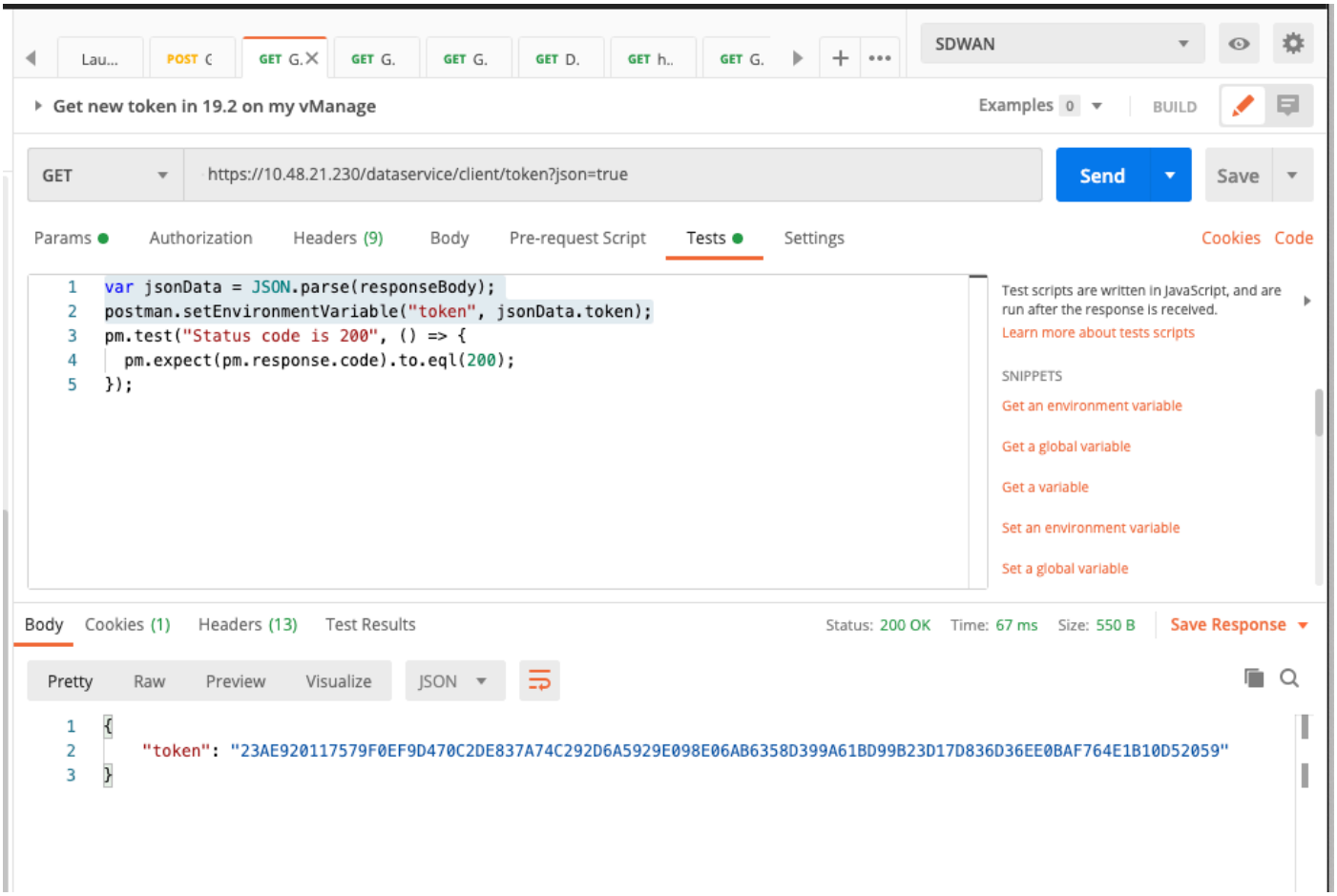
Selezionare l'ordine degli eventi che si desidera ripetere, selezionare il conteggio ripetizioni in modo che Postman possa eseguire le chiamate API, il numero di volte selezionato con i risultati per esecuzione.



Esecuzione raccolta

Dalla "libreria" di chiamata, metterli in un certo ordine per ottenere un flusso/ordine specifico da eseguire.

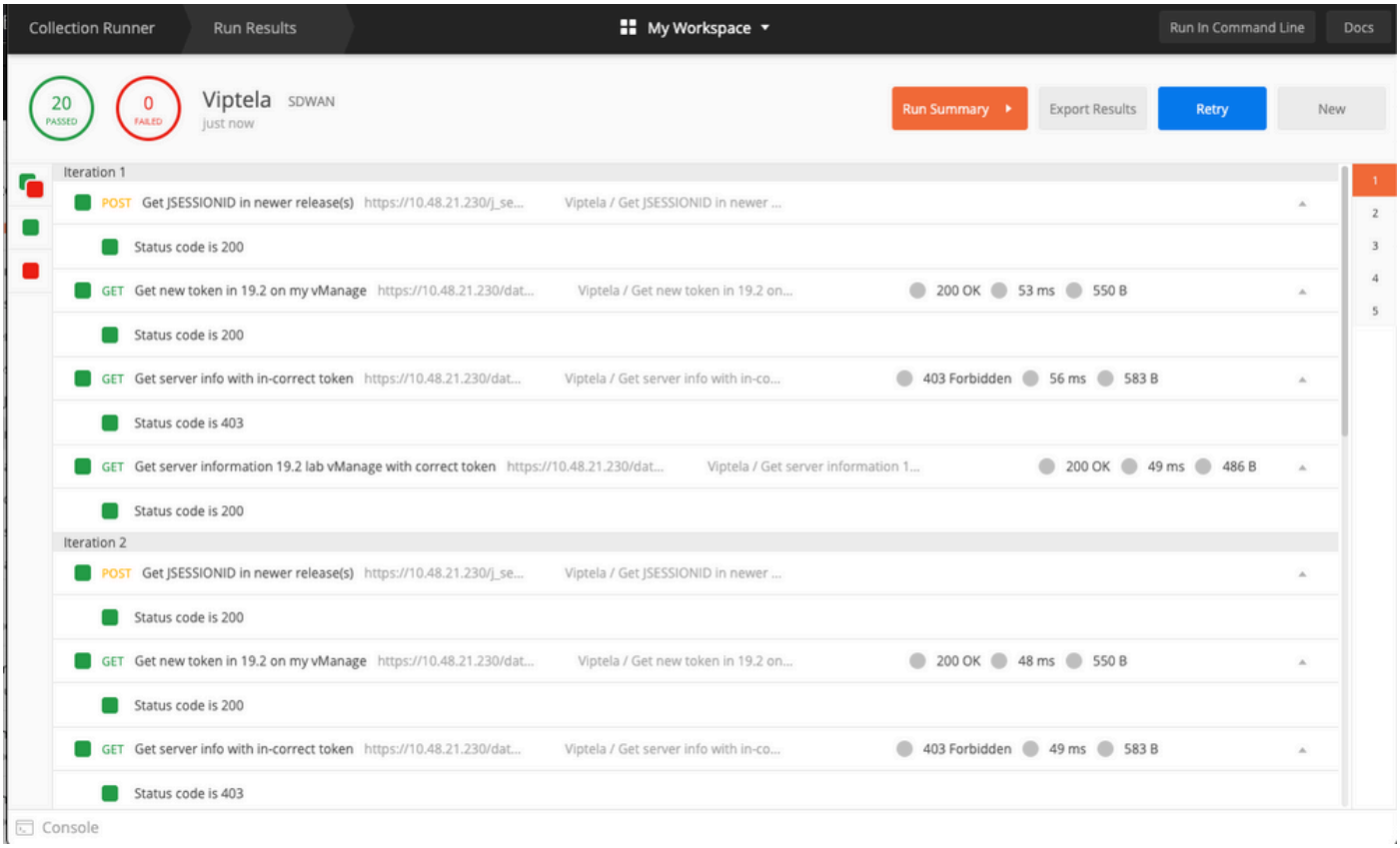
Inserite un risultato e verificate se ottenete 200 OK o un altro valore come risposta e trattatelo come superata o fallita.



Verifica codice di risposta

```
pm.test("Status code is 200", () => {
 pm.expect(pm.response.code).to.eql(200);
});
```

Poi possiamo vedere passare o fallire nelle nostre corse.



Esecuzione automatica

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).