

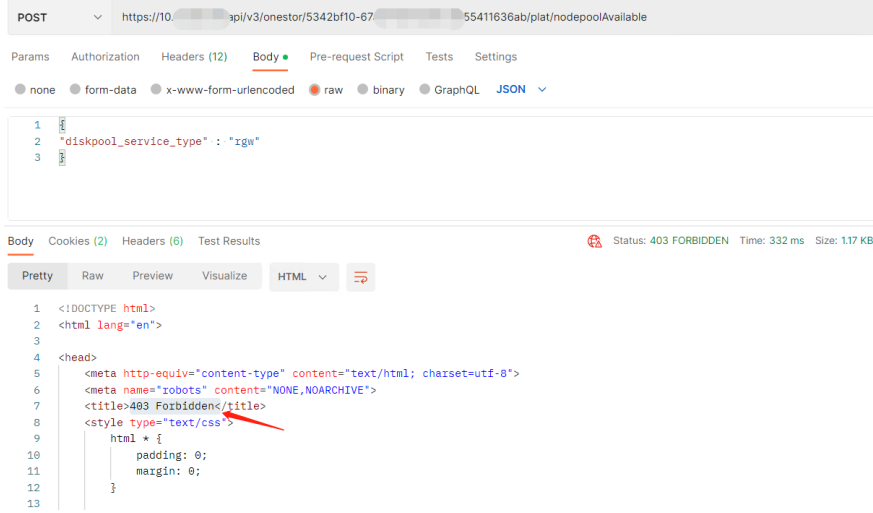
知 x10000 B50对接postman使用https POST报错403 Forbidden

存储配置 高成良 2023-03-31 发表

问题描述

x10000 B50对接postman使用https POST报错403 Forbidden，而同样的参数如果使用http URL可以成功

如下是报错示例：



POST https://10.10.10.10/api/v3/onestor/5342bf10-67-80-9e55411636ab/plat/nodepool/Available

Params Authorization Headers (12) Body Pre-request Script Tests Settings

none form-data x-www-form-urlencoded raw binary GraphQL JSON

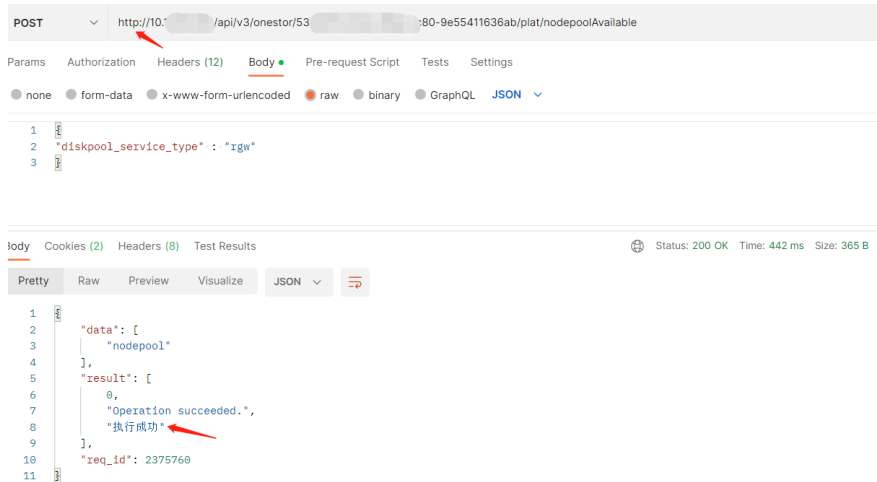
```
1 [{"diskpool_service_type": "rgw"}]
```

Body Cookies (2) Headers (6) Test Results Status: 403 FORBIDDEN Time: 332 ms Size: 117 KB

Pretty Raw Preview Visualize HTML

```
1 <!DOCTYPE html>
2 <html lang="en">
3
4 <head>
5   <meta http-equiv="content-type" content="text/html; charset=utf-8">
6   <meta name="robots" content="NONE,NOARCHIVE">
7   <title>403 Forbidden</title>
8   <style type="text/css">
9     html * {
10       padding: 0;
11       margin: 0;
12     }
13
```

相同的参数环境下，如果使用http URL可以成功：



POST http://10.10.10.10/api/v3/onestor/5342bf10-67-80-9e55411636ab/plat/nodepool/Available

Params Authorization Headers (12) Body Pre-request Script Tests Settings

none form-data x-www-form-urlencoded raw binary GraphQL JSON

```
1 [{"diskpool_service_type": "rgw"}]
```

Body Cookies (2) Headers (8) Test Results Status: 200 OK Time: 442 ms Size: 365 B

Pretty Raw Preview Visualize JSON

```
1 {
2   "data": [
3     "nodepool"
4   ],
5   "result": [
6     0,
7     "Operation succeeded.",
8     "执行成功"
9   ],
10  "req_id": 2375760
11 }
```

过程分析

经过测试，问题只发生在POST操作时，GET操作不管使用http或者https的URL都可以成功。

此问题可以在实验环境复现，详细报错如下：

```
<h1>Forbidden <span>(403)</span></h1>
```

```
<p>CSRF verification failed. Request aborted.</p>
```

```
<p>You are seeing this message because this HTTPS site requires a 'Referer header' to be sent by your Web browser, but none was sent. This header is required for security reasons, to ensure that your browser is not being hijacked by third parties.</p>
```

解决方法

在headers中添加如下Referer后问题解决。

key = Referer; 值 = https://管理IP/dsm

The screenshot displays a network request in a browser's developer tools. The request is a POST to the endpoint `https://10.10.10.10/api/v3/onestor/5342bf10-9e55411636ab/plat/nodepool/Available`. The 'Headers' tab is selected, showing several headers: 'Connection' (keep-alive), 'calamari_sessionid' (7n07nctvux2st0lbtr6s57h5juvktx0), 'X-XSRF-TOKEN' (GdrrI2XfQ53kwZ7zKawe46BYKu8smsFb), and 'Referer' (https://10.10.10.10/dsm). The 'Referer' header is highlighted with a red box. The 'Body' tab shows the response in JSON format, indicating a successful operation with a request ID of 2376672.

Key	Value	Description
Connection	keep-alive	
calamari_sessionid	7n07nctvux2st0lbtr6s57h5juvktx0	
X-XSRF-TOKEN	GdrrI2XfQ53kwZ7zKawe46BYKu8smsFb	
Referer	https://10.10.10.10/dsm	

```
1 {
2   "data": [
3     "nodepool"
4   ],
5   "result": [
6     0,
7     "Operation succeeded.",
8     "执行成功"
9   ],
10  "req_id": 2376672
11 }
```

