How to troubleshoot common HTTP error code

Last updated by | Ruoyu Li | Jan 16, 2023 at 1:18 AM PST

Contents

Issue Symptom

You usually see below errors reported from pipeline activities.

```
Message=Http request failed with client error, status code 400 BadRequest, please check your activity settings. If you configured a base Url that includes pat
Request URL: https://some-site.com/folder1/relativeURL.
```

```
Details Rest call failed with client error, status code 401 Unauthorized, please check your activity settings.
Request URL: https://some-site.com/someapi. Response: {'Message':'Authorization has been denied for this request.'} Activity ID: xxxxx
```

In essential, these are all HTTP error status. So you need to troubleshoot it using general HTTP knowledge.

Note: This TSG applies to **Web activity**, **HTTP/REST/OData connectors** of copy or lookup activity.

General Guidance

1. Use Postman to reproduce

For such scenario, ADF components acts like a HTTP client. A basic idea is to test using other HTTP client (e.g. Postman tool). **If you can repro using other tool, then it's an issue outside ADF.**

2. SHIR + Fiddler

If it only happened in ADF activity and it runs via SHIR, then we could install Fiddler on SHIR VM to capture **HTTPS** traffic when reproducing the issue.

We have shared some case study with details on how to analyze Fiddler trace as in this TSG and this TSG.

3. Leverage HTTP echo service

For some specific issue (e.g. you want to verify if the URL got truncated due to some constraint), you could leverage some HTTP echo service like postman-echo.com ↗ to test.

Special Note: as it is a 3rd party HTTP server, please DO NOT pass any customer data like credential in HTTP request to avoid any compliance issue.

Common troublesooting steps for different HTTP error codes

400: Bad Request

Usually it's due to the HTTP request is in bad syntax. You need to check **request header/request body/URL path** etc.

401: Unauthorized

Authentication Issue usually due to **incorrect authentication info** or **authentication failure**. You need to understand basic authentication/Azure AD Oauth authentication/Windows authentication etc and do some auth related investigation.

From past cases, we observed some 401 errors got fixed when customer **changed to the correct auth type** and **using correct credentials**.

403: Forbidden

Similar to 401 but 401 is an auth error while 403 is more related with **permission denied**. Usually you need to check whether the account used has sufficient permission to specific URL. Switch to some 'admin' accounts sometimes can help you to quickly narrow down and fix it.

500: Internal Server Error, 502: Bad Gateway, 503: Service Unavailable

Error status started with 5XX are all server errors. You need to check who owns the service (other Microsoft HTTP service endpoint/ HTTP server owned by customer) and collaborate with support from corresponding teams.