Connect to Git Repository failed due to different tenant

Last updated by | Jackie Huang | Jan 4, 2022 at 12:24 AM PST

Connect to Git Repository failed due to different tenant

Tuesday, February 25, 2020
10:33 AM

Background: Sometimes we encounter Authentication issues like HTTP status 401. Especially when customer have multiple tenants with guest account, this could make things more complicated.

How to use it:

1. For almost every request, there is a field in header containing the access token.

2. Then just paste the token into https://jwt.io/ and the token will be decoded.

JWT

Debugger | Libraries | Introduction | Ask | Get a T-shirt!

Crafted by Auth0

ALGORITHM

Encoded PASTE A TOKEN HERE

ITjIViiwiaWOiJUXNTgXMDU0MTC4LCJuTiii1UjL
1ODEwNTQxNzgsImV4cCI6MTU4MTA1ODA3OCwiYWN
yIjoiMSIsImFpbyI6IjQyTmdZT0JydVhCTm9qLyt
3cTVtVDcrN0RWeHp2cWt6Nmhtw1WVrZks3djc0TmI
5WjZCRUEiLCJhbXIiOlsicHdkIiwicnNhIl0sImF
wcGlkIjoiMTZmOWI4ZTktZDIwYi00NWExLWFiOWU
tZGIyZTgyNTQ1MDhiIiwiYXBwaWRhY3IiOiIwIiw
iZGV2aWNlaWQiOiJmZWJkN2YzMi01YmFjLTQ2MjY
tYWJlNi05YzJlNzc2YjI1ZTYiLCJmYW1pbHlfbmF
tZSI6IkR0YW5hbGrc2htaSIsImdpdmVuX25hbWU
iOiJFY2hpcHV0dHVyIiwiaXBhZGRyIjoiMTI1LjI
yLjE5My4xNDgiLCJuYW1lIjoiRWNoaXB1dHR1ciB
EaGFuYWxha3NobWkiLCJvaWQiOiJkYzY0NzYxOS0
3MTNjLTRhZWUtODAyNi1mYzUwNGY4YzJlMWEiLCJ
vbnByZW1fc2lkIjoiUy0xLTUtMjEtMjY2NzQ5OTQ
wLTE2Mzc5NjQ0NDQtOTI5NzAxMDAwLTM5MzE0MjU
iLCJwdWlkIjoiMTAwMzIwMDA2RTA0NzEzQSIsInN
jcCI6InVzZXJfaW1wZXJzb25hdGlvbiIsInN1YiI
6InhQcy1qR0F1Q1UyMnpLdFY4bktR0RpaDFySmx
QbVNrTEFMNGdRdXryRjgiLCJ0aWQiOiI2M2NlN2Q
1OS0yZjNlLTQyY2QtYThjYy1iZTc2NGNmZjVlYjY
iLCJ1bmlxdWVfbmFtZSI6ImVjaGlwdXR0dXIuZEB

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{}
```

PAYLOAD: DATA

```
{
  "aud": "499b84ac-1321-427f-aa17-267ca6975798",
  "iss": "https://sts.windows.net/63ce7d59-2f3e-42cd-a8cc-
be764cff5eb6/",
  "iat": 1581054178,
  "nbf": 1581054178,
  "exp": 1581058078,
  "acr": "1",
  "aio":
"42NgYOBruXBNoj/+wq5mT7+7DVxzvqkz6hm1ekfK7v74Nb9Z6BEA",
  "amr": [
    "pwd",
    "rsa"
  ],
  "appid": "16f9b8e9-d20b-45a1-ab9e-db2e8254508b",
  "appidacr": "0",
  "deviceid": "febd7f32-5bac-4626-abe6-9c2e766b25e6",
  "family_name": "████████",
  "given_name": "████████",
  "ipaddr": "125.22.193.148",
  "name": "████████████████",
  "oid": "dc647619-713c-4aee-8026-fc504f8c2e1a",
  "onprem_sid": "S-1-5-21-266749940-1637964444-929701000-
3931425",
  "puid": "100320006E04713A"
```

Real case reference:

In this case customer needs to access their DevOps using ADF portal as client. This user has her original tenant while she is also a guest user in another guest tenant. The DevOps she want to visit is in guest tenant. We see requests to DevOps failed with **401** but all user permission has been checked without any issue.

For this customer's account, it has been invited to tenant (83beff02-9d00-472b-94ef-6ca23e448cfb) as a guest.

Original Tenant	63ce7d59-2f3e-42cd-a8cc-be764cff5eb6	Guest Tenant	83beff02-9d00-472b-94ef-6ca23e448cfb	
User Principal Name (UPN)	xxxxxxxx.d_ixxxxxxs.com	User Principal Name (UPN)	xxxxxxxx.d_ixxxxxxs.com#EXT#@bigcorporate.onmicrosoft.com	
Object ID	dc647619-713c-4aee-8026-fc504f8c2e1a	Object ID	f43dfaf6-3c5b-40cb-9c59-3a8aa1502fe6	

Both the target ADF and DevOps are in guest tenant.

I setup similar environment, where ADF & DevOps also in guest tenant.

Then we compared the two access tokens in collected Fiddler traces when trying to access Azure DevOps Service.

Working scenario in my lab test	Failed scenario, in customer's environment

```
{
    "aud": "499b84ac-1321-427f-aa17-267ca6975798",
    "iss": "https://sts.windows.net/6d5653e0-            b10d-
3389e0f18cee/",
    "iat": 1582101730,
    "nbf": 1582101730,
    "exp": 1582105630,
    "acr": "1",
    "aio":
"AXQAi/80AAAAYNHtveswuhk1YOSEUnsgAb/UEIMaEJFvEiudUgZNuRxQk
WN2PVQCcx4ajCD4Y4              1oUD99
hJLuRDWPXMejcBjpSM/16PF0vbphmD7M1MqPz4QOf4Qm03w==",
    "altsecid": "5::1003BFFD953F54BD",
    "amr": [
      "pwd",
      "rsa"
    ],
    "appid": "16f9b8e9-d20b-45a1-ab9e-db2e8254508b",
    "appidacr": "0",
    "email": "ruoyu.li@microsoft.com",
    "idp": "https://sts.windows.net/72f988bf-      )1ab-
2d7cd011db47/",
    "ipaddr": "121.235.137.170",
    "name": "Ruoyu Li",
    "oid": "0ef7855c-7b0b-465f-be3c-ef7927fb9497",
    "puid": "100320009BFD1FB1",
    "scp": "user_impersonation",
    "sub": "ER0Dx12z83sdb1SSm1HQd2hgkYBu1q7Ce5o_azPh2AE",
    "tid": "6d5653e0-793a-4906-b10d-3389e0f18cee",
    "unique_name": "ruoyu.li@microsoft.com",
    "uti": "K2-kYATKG0anrVQlcfxZAQ",
    "ver": "1.0"
}
```

guest tenant

original tenant

```
{
    "aud": "499b84ac-1321-427f-aa17-267ca6975798",
    "iss": "https://sts.windows.net/63ce7d59-2f3e-42cd-a8cc-
be764cff5eb6/",
    "iat": 1581054178,
    "nbf": 1581054178,
    "exp": 1581058078,
    "acr": "1",
    "aio":
"42NgYOBruXBNoj/+wq5mT7+7DVxzvqkz6hm1ekfK7v74Nb9Z6BEA",
    "amr": [
      "pwd",
      "rsa"
    ],
    "appid": "16f9b8e9-d20b-45a1-ab9e-db2e8254508b",
    "appidacr": "0",
    "deviceid": "febd7f32-5bac-4626-abe6-9c2e766b25e6",
    "family_name": "Dhanalakshmi",
    "given_name": "Echiputtur",
    "ipaddr": "125.22.193.148",
    "name": "Echiputtur Dhanalakshmi",
    "oid": "dc647619-713c-4aee-8026-fc504f8c2e1a",
    "onprem_sid": "S-1-5-21-266749940-1637964444-929701000-
3931425",
    "puid": "100320006E04713A",
    "scp": "user_impersonation",
    "sub": "xPs-jGAuBU22zKtV8nKMGDih1rJlPmSkLAL4gQuwrF8",
    "tid": "63ce7d59-2f3e-42cd-a8cc-be764cff5eb6",
    "unique_name": "e          .d@ad.       .com",
    "upn": "e          .d@ad.       .com",
    "uti": "o5N8nr3HsUmGpvTl1HRHAA",
    "ver": "1.0"
}
```

In my scenario, even **it successfully recognized my original tenant, but correctly requested token from the guest tenant**, and then use the token to visit DevOps in guest tenant. This is normal behavior and expected result.

In customer's scenario, the **token** was obtained from the **original** tenant, but ADF is in **guest** tenant and trying to use this token to visit **DevOps** in **guest** tenant. This is not the expected behavior. Customer should use the token issued from guest tenant instead.

Finally, we figured out that we need to explicitly specify the Azure Active Directory to be customer's **guest tenant, the one same as their DevOps**, so it can correct the token obtain behavior and use the correct tenant.

Repository settings

Enter Git repository information to be associated with your Data Fact
testADFruoli

Repository type *

    Azure DevOps Git

Select a different directory ✓

Azure Active Directory *

    Martin Test

    Martin Test   ← Please select your guest tenant here.

    Microsoft

Created with Microsoft OneNote 2016.

How good have you found this content?