Web-Activity-Failure-when-using-expired-SSL-TLS-certificates

Last updated by | Veena Pachauri | Mar 16, 2023 at 1:49 AM PDT

Web Activity Failure when using expired SSL/TLS certificates

Contents

Issue

Web Activity Failure when using expired SSL/TLS certificates.

This issue is observed when the WEB Activity keeps on failing either intermittently or consistently with the below error.

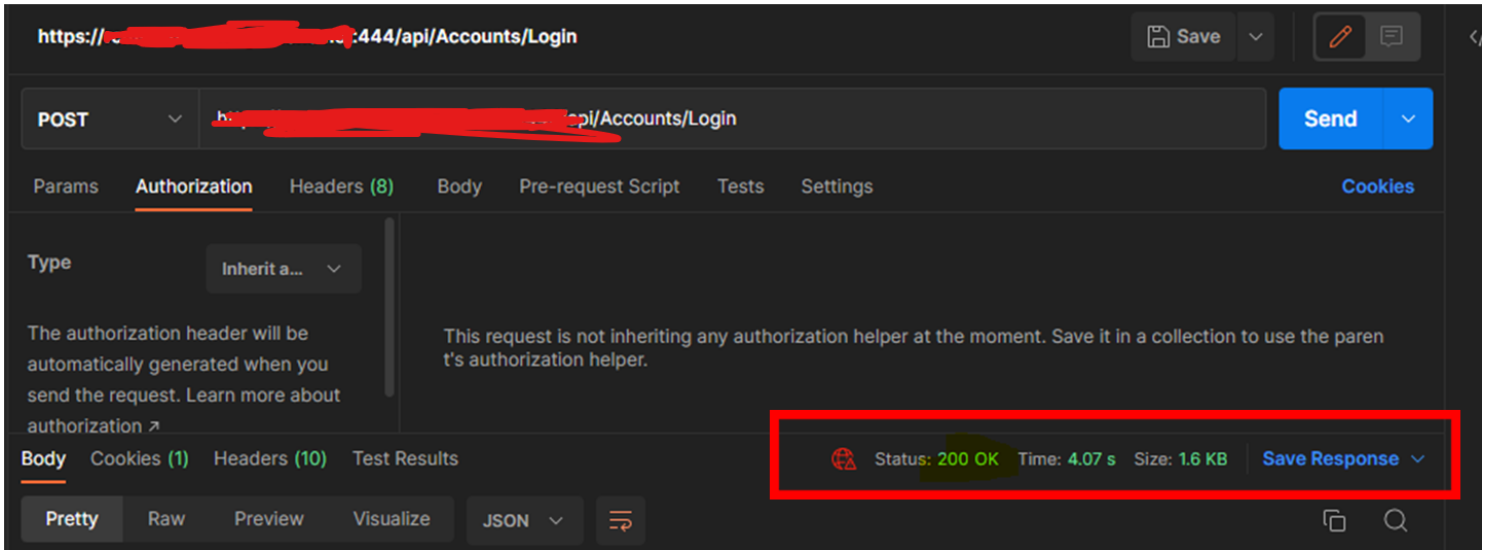
Response status code: 'NA - Unknown'. More details: Exception message: 'NA - Unknown [ClientSideException] An error occurred while sending the request.'. **The request didn't reach the server from client. This could happen because of an underlying issue such as network connectivity, a DNS failure, a server certificate validation, or a timeout**.

Troubleshooting

1] Look into the CustomLogEvent and it would show a web activity failure with status NA – unknown:

```
2023-01-05 08:01:02.8842276 <LogProperties><Text>ExecuteWebActivityAsync: invoking POST on https://rcm-zones-integrations.net:444/api/Accounts/Login, in datafactory zones-datafactoryV2-uat, region eu</Text></LogProperties>
2023-01-05 08:01:02.8842606 <LogProperties><Text>WriteAsync start</Text></LogProperties>
2023-01-05 08:01:02.8842902 <LogProperties><Text>WriteAsync: Generating body for method POST</Text></LogProperties>
2023-01-05 08:01:02.8843340 <LogProperties><Text>WriteAsync: Invoking endpoint - https://rcm-zones-integrations.net:444/api/Accounts/Login</Text></LogProperties>
2023-01-05 08:01:02.9146228 <LogProperties><Text>GetStateFromExceptionType: Processing exception of type ClientSideException with status NA - Unknown</Text></LogProperties>
2023-01-05 08:01:02.9146708 <LogProperties><Text>StartAsync failed. Extracting internal message. An error occurred while sending the request.</Text><FunctionName></FunctionName><FunctionParameter></FunctionParameter></LogProperties>
```

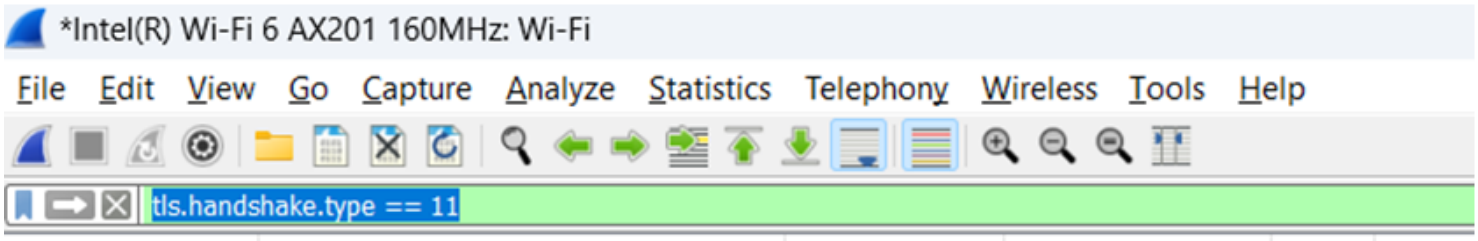
2] Check if we are able to reach the server endpoint through the POSTMAN, It should show the **status: 200 OK** means we are able to reach the endpoint from the POSTMAN. See below snippet



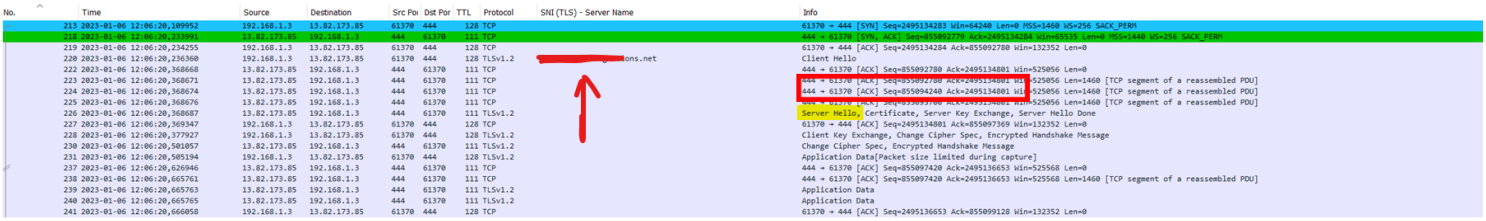
3] Take a network trace with Wireshark while replicating the issue using POSTMAN (if we are able to reach the server through POSTMAN) from endpoint while Wireshark was running:

4] Filter network trace using the below command :

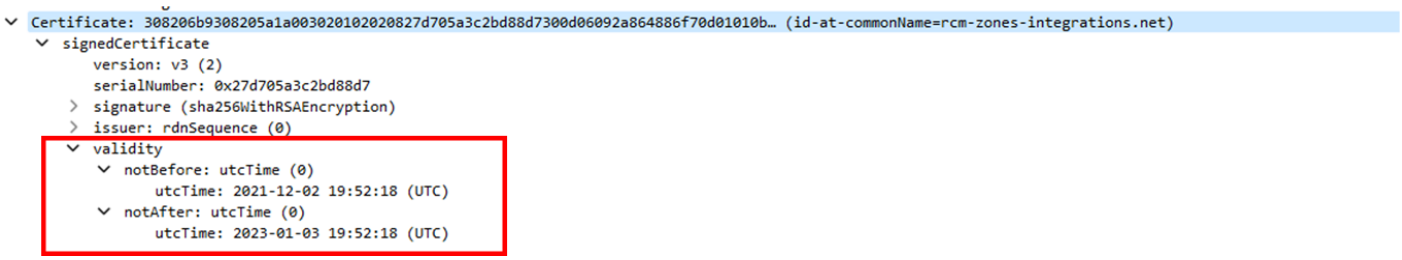
tls.handshake.type == 11



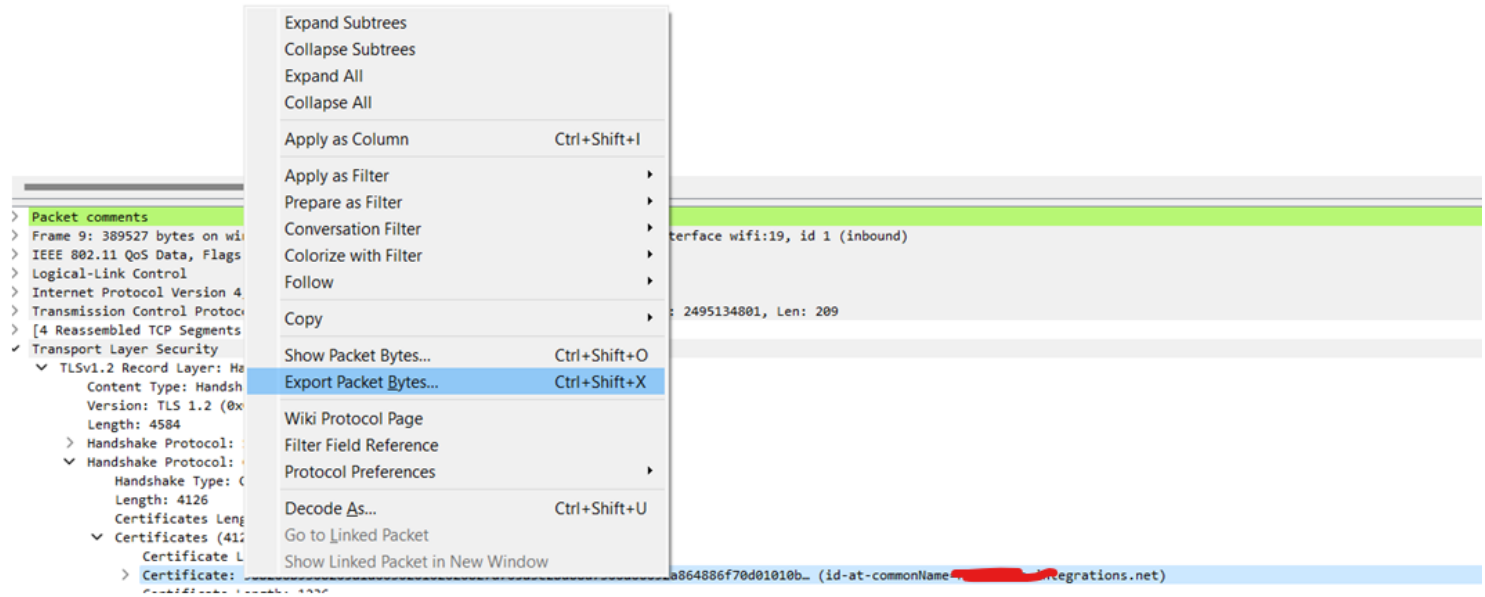
Example as below :



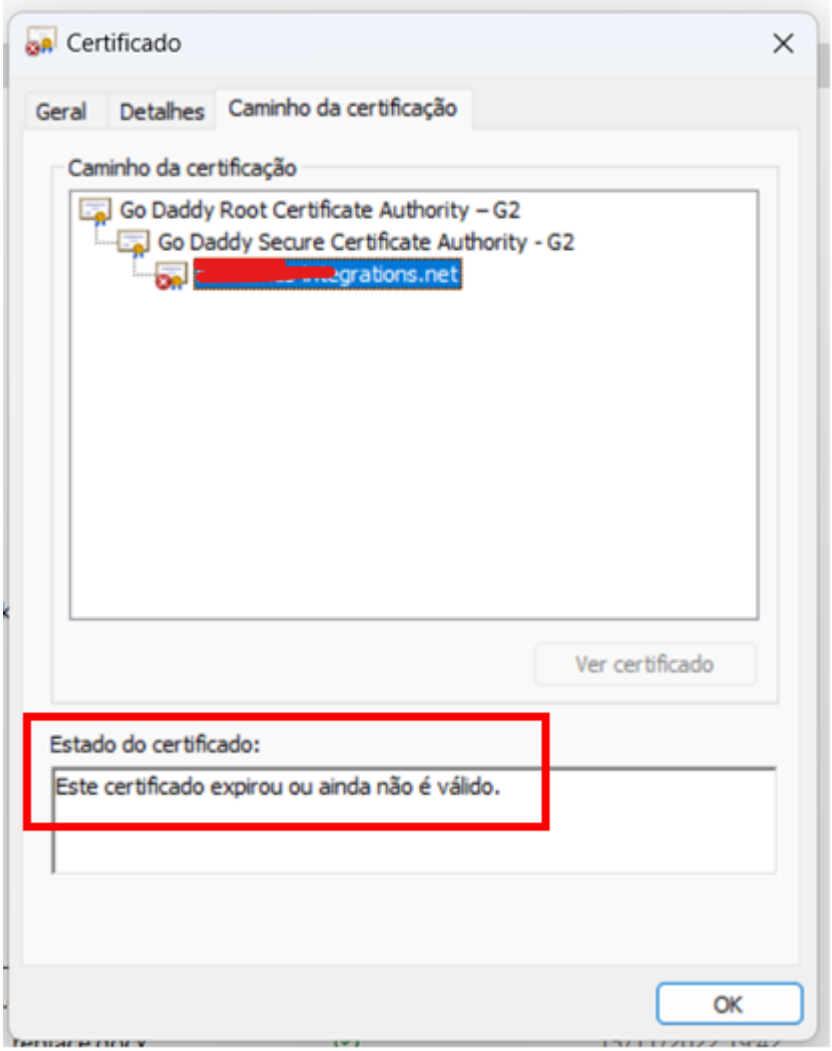
This will show all server certificates in the network trace. Then, you should select the correct SNI used by the https endpoint. See for the Server Name (SNI). Then, in the packet details pane, Server Hello, we can find the certificate validity:



Or, if you select the same packet and perform an export packet Bytes in Wireshark

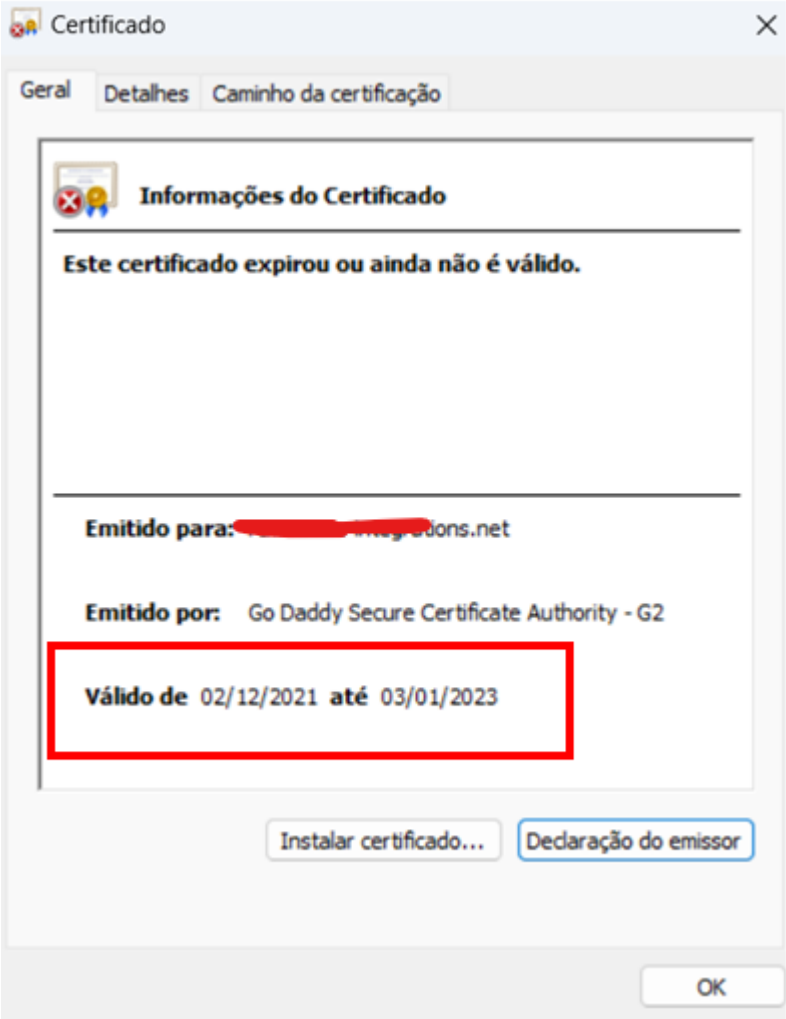


And save it as test.crt file type. You will be able to open the certificate:



On top, we have a message saying the certificate is not valid or the certificate is expired.

Then, you can see the certificate validation:



Which is not valid after 03-01-2023, 19:52:18 UTC. And in this example, the pipelines started to fail at: 3rd January 2023 at 08:00 PM UTC time.

Cause

The validation from ADF to HTTP server was failing due to the expired certificates at the server end and leading to our WEB activity failure.

Resolution (Recommended)

Recommended As we can confirm that the server-side certificate is expired, recommend customer to renew their certificates.

**NOTE: ** Once, certificates are valid, the issue would be resolved.

Workaround (Non-recommended)

We can disable certificate validation from the settings pane of the Web activity of the pipeline, but disabling the certificate validation means the data is not encrypted. This is something not recommended until you are connected to a trusted server that does not use a standard CA cert.

NOTE: Let the customer know about the risk of disabling the certificate validation if cx or SE is going forward with the workaround of disabling the cert validation.

Refer: https://learn.microsoft.com/en-us/azure/data-factory/control-flow-web-activity#type-properties

disableCertValidation	Removes server side certificate validation (not recommended unless you are connecting to a trusted server that does not use a standard CA cert).	Allowed values are false (default) and true.	No

- **Reviewer:** Veena Pachauri
- **Keywords:** Web Activity

How good have you found this content?