Solving some failing transfers to NET2 using CERN and BNL FTS services

Eduardo Bach

The clues

BNL FTS

INFO Wed, 21 Jun 2023 09:56:57 -0400; Will attempt retrieval of macaroon for source
INFO Wed, 21 Jun 2023 09:56:57 -0400; Will attempt retrieval of macaroon for destination
INFO Wed, 21 Jun 2023 09:56:57 -0400; Failed to retrieve macaroon for destination: Could not retrieve token for davs://atn12.data.net2.mghpcc.org:2880/hiro/DAVS/test/2023/06/21/09/56/BNL_1/user.HironoriIto.MICH.Load_001.000 [last failed attempt: Macaroon request failed: (Neon): SSL handshake failed: sslv3 alert certificate unknown]
INFO Wed, 21 Jun 2023 09:56:57 -0400; Transfer accepted
INFO Wed, 21 Jun 2023 09:56:57 -0400; Proxy: /tmp/x509up_h11825090104134366411_fbcfd8b4885435d3
INFO Wed, 21 Jun 2023 09:56:57 -0400; VO: atlas
INFO Wed, 21 Jun 2023 09:56:57 -0400; Job id: 79d1372e-103b-11ee-95f7-b49691292f84
INFO Wed, 21 Jun 2023 09:56:57 -0400; File id: 1749542006
INFO Wed, 21 Jun 2023 09:56:57 -0400; Source url: davs://dcgftp.usatlas.bnl.gov:443/pnfs/usatlas.bnl.gov/BNLT0D1/hiro/DAVS/2/user.HironoriIto.MICH.Load_001.000
INFO Wed, 21 Jun 2023 09:56:57 -0400; Dest url: davs://atn12.data.net2.mghpcc.org:2880/hiro/DAVS/test/2023/06/21/09/56/BNL_1/user.HironoriIto.MICH.Load_001.000
INFO Wed, 21 Jun 2023 09:56:57 -0400; Overwrite enabled: 0
INFO Wed, 21 Jun 2023 09:56:57 -0400; Disable delegation: 0
INFO Wed, 21 Jun 2023 09:56:57 -0400; Disable local streaming: 0
INFO Wed, 21 Jun 2023 09:56:57 -0400; Evict source file: 0
INFO Wed, 21 Jun 2023 09:56:57 -0400; Dest space token:
INFO Wed, 21 Jun 2023 09:56:57 -0400; Source space token:
INFO Wed, 21 Jun 2023 09:56:57 -0400; Checksum:
INFO Wed, 21 Jun 2023 09:56:57 -0400; Checksum enabled: No checksum comparison
INFO Wed, 21 Jun 2023 09:56:57 -0400; User filesize: 0
INFO Wed, 21 Jun 2023 09:56:57 -0400; File metadata:
INFO Wed, 21 Jun 2023 09:56:57 -0400; Job metadata: {\"auth_method\":?\"certificate\"}
INFO Wed, 21 Jun 2023 09:56:57 -0400; Bringonline token:
INFO Wed, 21 Jun 2023 09:56:57 -0400; UDT: 0
INFO Wed, 21 Jun 2023 09:56:57 -0400; BDII:lcg-bdii.cern.ch:2170
INFO Wed, 21 Jun 2023 09:56:57 -0400; Source token issuer:
INFO Wed, 21 Jun 2023 09:56:57 -0400; Destination token issuer:
INFO Wed, 21 Jun 2023 09:56:57 -0400; Report on the destination tape file: 0
INFO Wed, 21 Jun 2023 09:56:57 -0400; Third Party TURL protocol list: https;root;gsiftp
INFO Wed, 21 Jun 2023 09:56:57 -0400; Getting source file size
INFO Wed, 21 Jun 2023 09:56:57 -0400; File size: 3600000000
INFO Wed, 21 Jun 2023 09:56:57 -0400; Checking existence of destination file
ERR Wed, 21 Jun 2023 09:56:57 -0400; **Non recoverable error: [13] Result (Neon): SSL handshake failed: sslv3 alert certificate unknown after 1 attempts**

CERN FTS

INFO Mon, 03 Jul 2023 21:41:14 +0200; Configured to skip retrieval of SE-issued tokens. Retrieval delegated to downstream Gfal2 client
INFO Mon, 03 Jul 2023 21:41:14 +0200; Transfer accepted
INFO Mon, 03 Jul 2023 21:41:14 +0200; Proxy: /tmp/x509up_h2519077123857950514_4846fbc9df3edf22
INFO Mon, 03 Jul 2023 21:41:14 +0200; VO: atlas
INFO Mon, 03 Jul 2023 21:41:14 +0200; Job id: 90ff820a-19d9-11ee-a8ef-fa163ec6a1a1
INFO Mon, 03 Jul 2023 21:41:14 +0200; File id: 1773482938
INFO Mon, 03 Jul 2023 21:41:14 +0200; Source url: davs://dcgftp.usatlas.bnl.gov:443/pnfs/usatlas.bnl.gov/BNLT0D1/hiro/DAVS/2/user.HironoriIto.MICH.Load_001.000
INFO Mon, 03 Jul 2023 21:41:14 +0200; Dest url: davs://atn12.data.net2.mghpcc.org:2880/bach/user.HironoriIto.MICH.Load_001.000
….
INFO Mon, 03 Jul 2023 21:41:14 +0200; Davix: > POST /pnfs/usatlas.bnl.gov/BNLT0D1/hiro/DAVS/2/user.HironoriIto.MICH.Load_001.000 HTTP/1.1
INFO Mon, 03 Jul 2023 21:41:14 +0200; Davix: > Host: dcgftp.usatlas.bnl.gov
INFO Mon, 03 Jul 2023 21:41:14 +0200; Davix: > Accept: */*
INFO Mon, 03 Jul 2023 21:41:14 +0200; Davix: > Content-Type: application/macaroon-request
…
INFO Mon, 03 Jul 2023 21:41:14 +0200; Davix: > Accept: */*
INFO Mon, 03 Jul 2023 21:41:14 +0200; Davix: > Depth: 0
INFO Mon, 03 Jul 2023 21:41:14 +0200; Davix: > ClientInfo: job-id=90ff820a-19d9-11ee-a8ef-fa163ec6a1a1;file-id=1773482938;retry=0
INFO Mon, 03 Jul 2023 21:41:14 +0200; Davix: > Authorization: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
INFO Mon, 03 Jul 2023 21:41:14 +0200; Davix: > User-Agent: libdavix/0.8.4 libcurl/7.69.0-DEV
INFO Mon, 03 Jul 2023 21:41:15 +0200; Davix:
INFO Mon, 03 Jul 2023 21:41:15 +0200; Davix: < HTTP/1.1 207 Multi-status
INFO Mon, 03 Jul 2023 21:41:15 +0200; Davix: < Date: Mon, 03 Jul 2023 19:41:14 GMT
INFO Mon, 03 Jul 2023 21:41:15 +0200; Davix: < X-Content-Type-Options: nosniff
INFO Mon, 03 Jul 2023 21:41:15 +0200; Davix: < X-Frame-Options: SAMEORIGIN
INFO Mon, 03 Jul 2023 21:41:15 +0200; Davix: < X-XSS-Protection: 1; mode=block
INFO Mon, 03 Jul 2023 21:41:15 +0200; Davix: < Server: dCache/8.2.15
INFO Mon, 03 Jul 2023 21:41:15 +0200; Davix: < Content-Security-Policy: default-src 'none' ; img-src 'self' data: ; style-src 'self' 'unsafe-inline' ; script-src 'self'; font-src 'self'
INFO Mon, 03 Jul 2023 21:41:15 +0200; Davix: < Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
INFO Mon, 03 Jul 2023 21:41:15 +0200; Davix: < Referrer-Policy: strict-origin-when-cross-origin
INFO Mon, 03 Jul 2023 21:41:15 +0200; Davix: < Content-Type: application/xml; charset=utf-8
INFO Mon, 03 Jul 2023 21:41:15 +0200; Davix: < DAV: 1, 2
INFO Mon, 03 Jul 2023 21:41:15 +0200; Davix: < Transfer-Encoding: chunked
INFO Mon, 03 Jul 2023 21:41:15 +0200; File size: 3600000000
INFO Mon, 03 Jul 2023 21:41:15 +0200; Checking existence of destination file
INFO Mon, 03 Jul 2023 21:41:15 +0200; **(SEToken) Error during token retrieval: Macaroon request failed: curl error (35): SSL connect error**
INFO Mon, 03 Jul 2023 21:41:15 +0200; (SEToken) Could not retrieve any token for davs://atn12.data.net2.mghpcc.org:2880/bach/user.HironoriIto.MICH.Load_001.000
INFO Mon, 03 Jul 2023 21:41:15 +0200; Davix: Negative result for operation: curl error (35): SSL connect error. After 1 retry
ERR Mon, 03 Jul 2023 21:41:15 +0200; Non recoverable error: [13] Result curl error (35): SSL connect error after 1 attempts

Te error can not be easily reproduced manually in lxplus

Manually retrieving Macaroons from NET2 works using gfal and curl

```
$ export X509_USER_PROXY=/tmp/x509up_u$(id -u)
$ export CAPATH="/cvmfs/grid.cern.ch/etc/grid-security/certificates
$ curl [--include,--fail] --location --key ${X509_USER_PROXY}  --cert ${X509_USER_PROXY}  --cacert ${X509_USER_PROXY}  --capath ${CAPATH} -X POST
-H 'Content-Type: application/macaroon-request' https://atn12.data.net2.mghpcc.org:2880/bach/
{
    "macaroon": "MDAxY2xvY2…",
    "uri": {
        "targetWithMacaroon": "https://atn12.data.net2.mghpcc.org:2880/bach?authz=MDAxY2xvY2…",
        "baseWithMacaroon": "https://atn12.data.net2.mghpcc.org:2880/?authz=MDAxY2xvY2…",
        "target": "https://atn12.data.net2.mghpcc.org:2880/bach/",
        "base": "https://atn12.data.net2.mghpcc.org:2880/"
    }
}

$ gfal-token davs://atn12.data.net2.mghpcc.org:2880/bach/
MDAxY2xvY2F…
```

Also, manual transfers from lxplus using gfal-copy, davix-put and curl, all worked.

dCache did not show errors in info log level

Only in debug log level because it was doing what it was told by the new Alma9 security standards in the file

/etc/crypto-policies/back-ends/java.config

jdk.certpath.disabledAlgorithms=MD2, SHA1, MD5, DSA, RSA keySize < 2048

```
05 Jul 2023 09:53:15 (WebDAV-S-atn12) []
DecryptedEndPoint@316b6b6f{l=/69.16.45.212:2880,r=/128.142.194.106:45934,OPEN,fill=-,flush=-,to=92/300000} stored flush exception
javax.net.ssl.SSLHandshakeException: Certificates do not conform to algorithm constraints
    at java.base/sun.security.ssl.Alert.createSSLException(Alert.java:131)
    at java.base/sun.security.ssl.TransportContext.fatal(TransportContext.java:360)
    at java.base/sun.security.ssl.TransportContext.fatal(TransportContext.java:303)
    at java.base/sun.security.ssl.TransportContext.fatal(TransportContext.java:298)
    at java.base/sun.security.ssl.CertificateMessage$T12CertificateConsumer.checkClientCerts(CertificateMessage.java:700)
    at java.base/sun.security.ssl.CertificateMessage$T12CertificateConsumer.onCertificate(CertificateMessage.java:411)
    at java.base/sun.security.ssl.CertificateMessage$T12CertificateConsumer.consume(CertificateMessage.java:375)
    at java.base/sun.security.ssl.SSLHandshake.consume(SSLHandshake.java:392)
    at java.base/sun.security.ssl.HandshakeContext.dispatch(HandshakeContext.java:443)
    …
Caused by: java.security.cert.CertPathValidatorException: Algorithm constraints check failed on signature algorithm: SHA1withRSA
    at java.base/sun.security.provider.certpath.AlgorithmChecker.check(AlgorithmChecker.java:237)
    at java.base/sun.security.ssl.AbstractTrustManagerWrapper.checkAlgorithmConstraints(SSLContextImpl.java:1661)
    ... 29 common frames omitted
```

Solution(s)

- You can add exceptions in the file /etc/crypto-policies/back-ends/java.config
- Or disable the include of this file entirely, setting the variable security.useSystemPropertiesFile=false
  In the file
  /etc/java/java-11-openjdk/java-11-openjdk-11.0.19.0.7-4.el9.alma.x86_64/conf/security/java.security

- May also worked, not tested.
  update-crypto-policies --set LEGACY