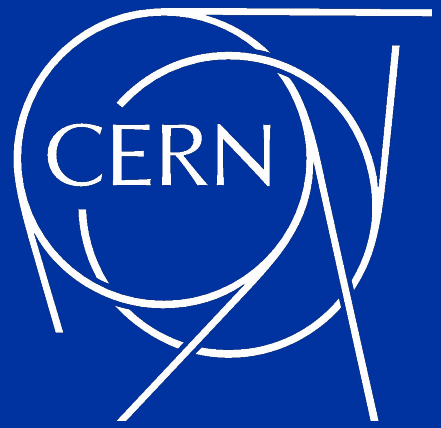


XrdHttp and XrdHttpTPC
The 12-Month Diff

Presented by Cedric Caffy

XRootD workshop 2026 - 2026-09-18

Outline

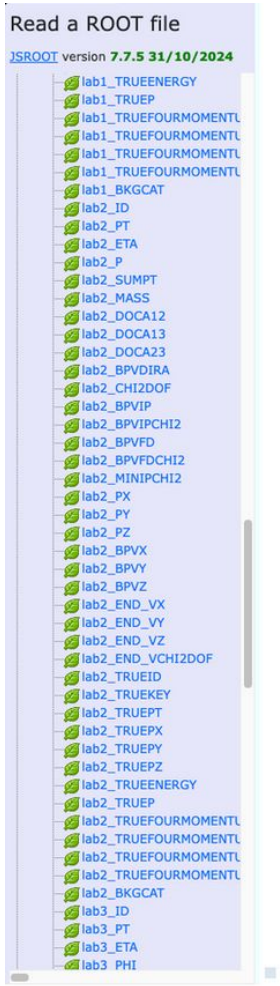
- A new use-case from LHCb: web-browser friendly access to EOS
  - CORS plugin
  - XRootD HTTP Proxy setup
- WLCG HTTP Third Party Copy data integrity check
- Out-Of-Memory kill on XRootD EOS+CTA clusters after the end of Run 3

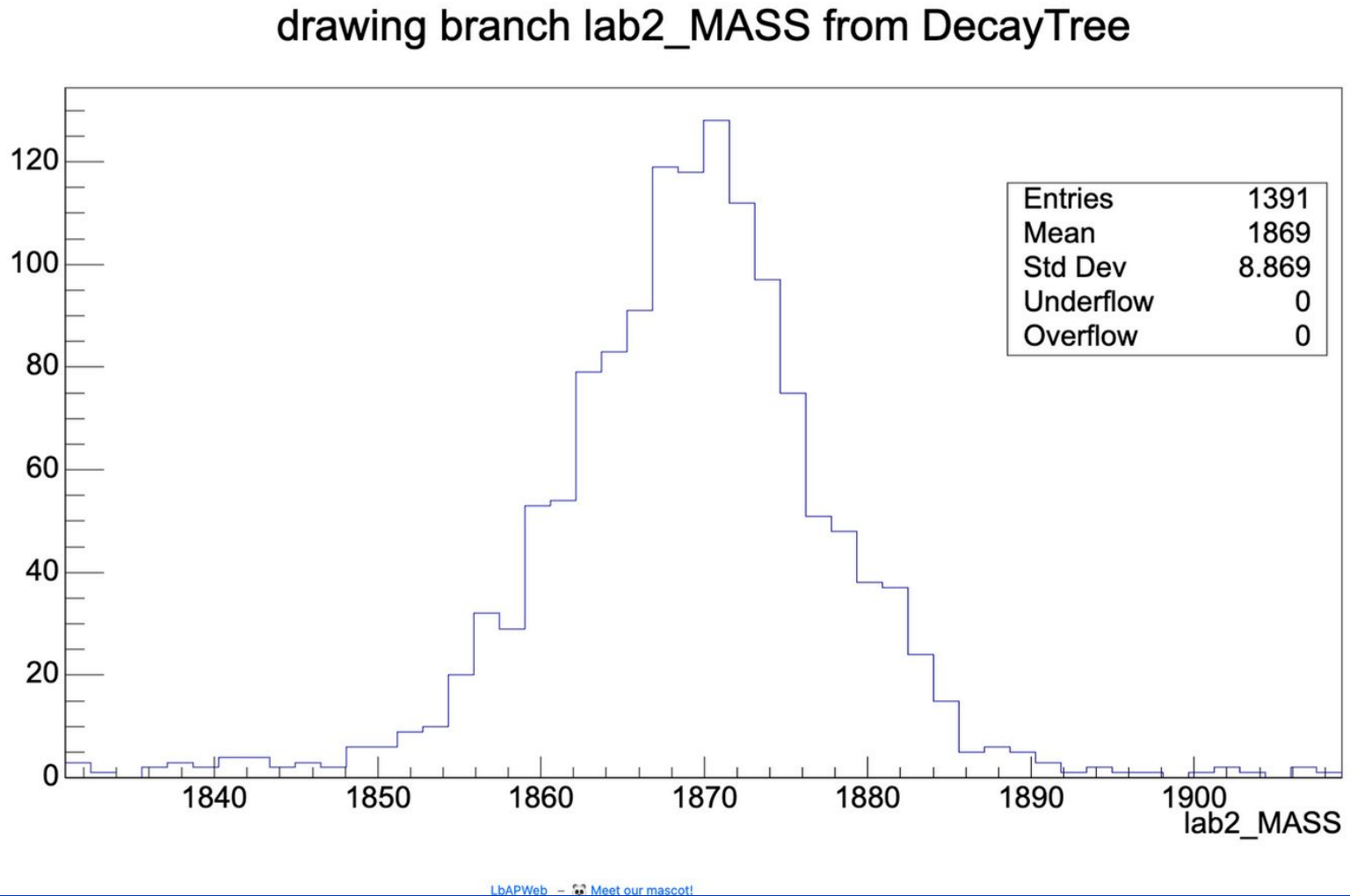
Use-case

Web-browser based physics analysis interactive view (JSROOT)

Use-case

Web-browser based physics analysis interactive view (JSROOT)





Use-case

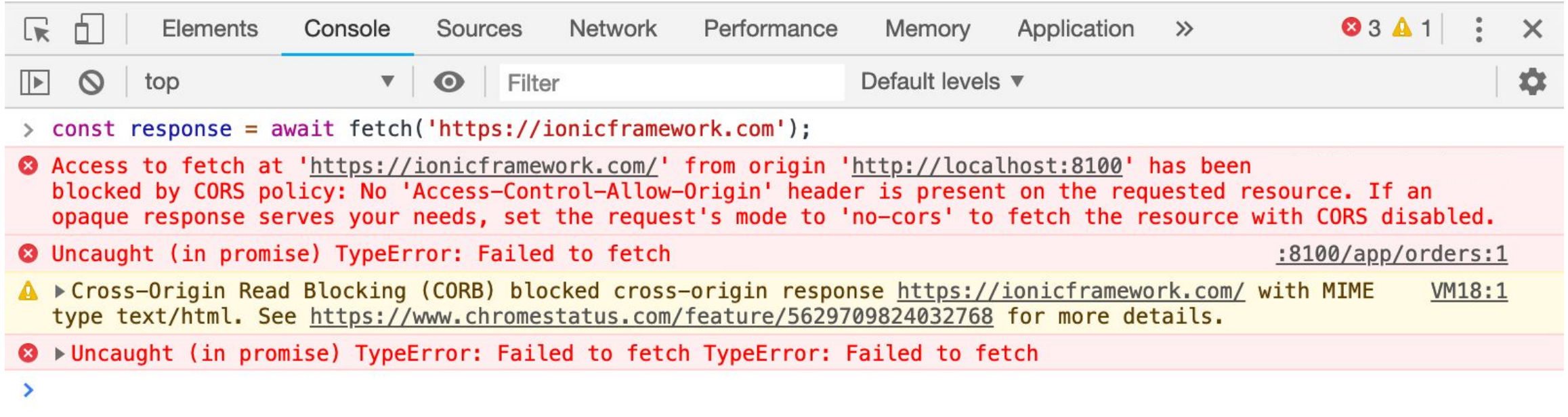
Web-browser based physics analysis interactive view (JSROOT)

- Publicly-trusted access
  - Users should not need to install CERN CA files on web browsers

Web-browser security features

Web-browser security features

CORS - Cross Origin Resource Sharing



Web-browser security features

HTTPS to HTTP redirection: Forbidden

Web-browser security features

Summary

- CORS
- Redirection to HTTP

XRootD HTTP CORS plugin
Cross Origin Resource Sharing

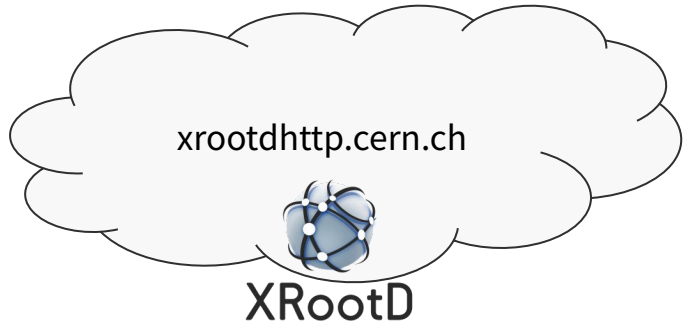
CORS Plugin

Use case

- CORS allows controlled access to resources from a different origin

CORS Plugin

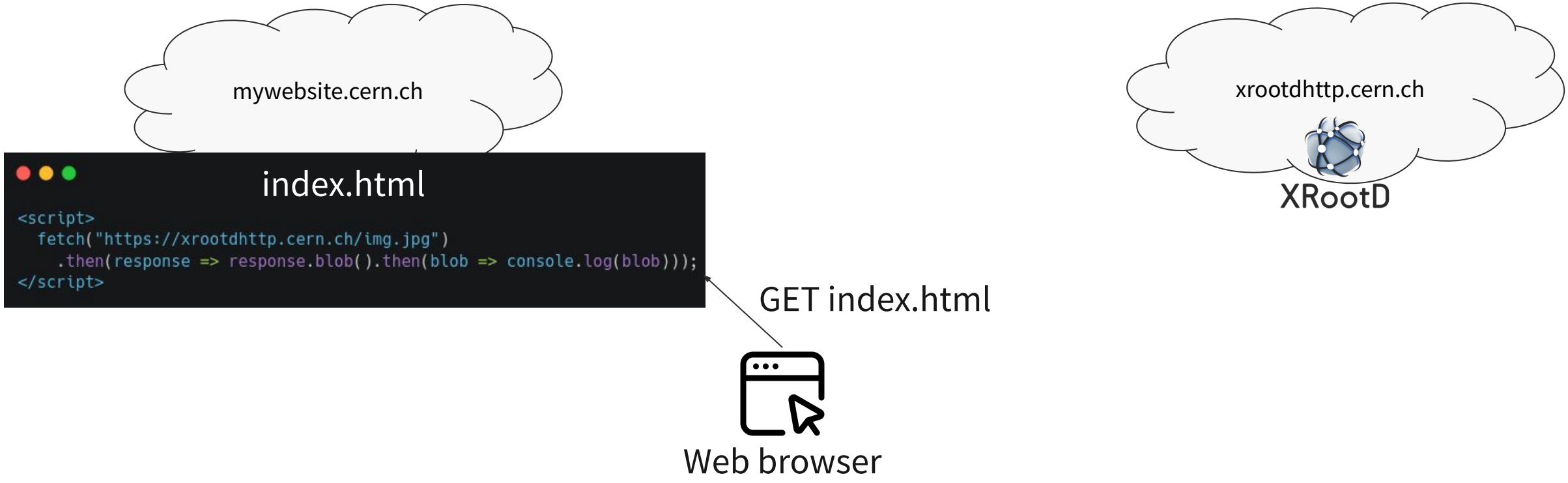
Example



Web browser

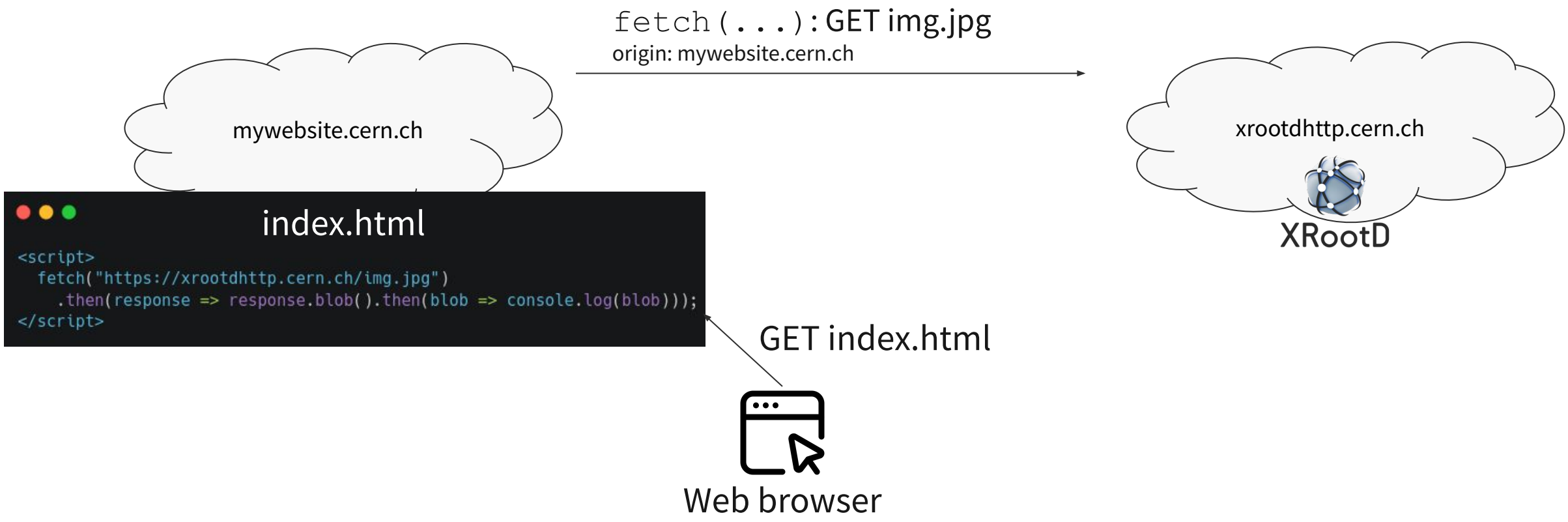
CORS Plugin

Example



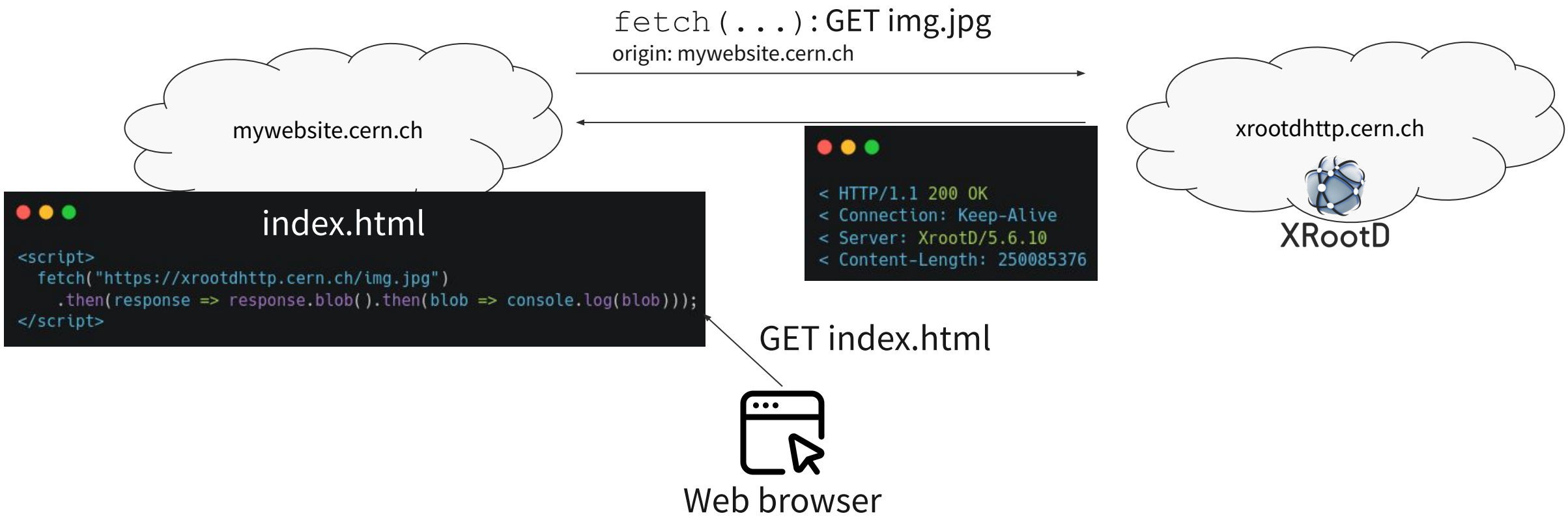
CORS Plugin

Example



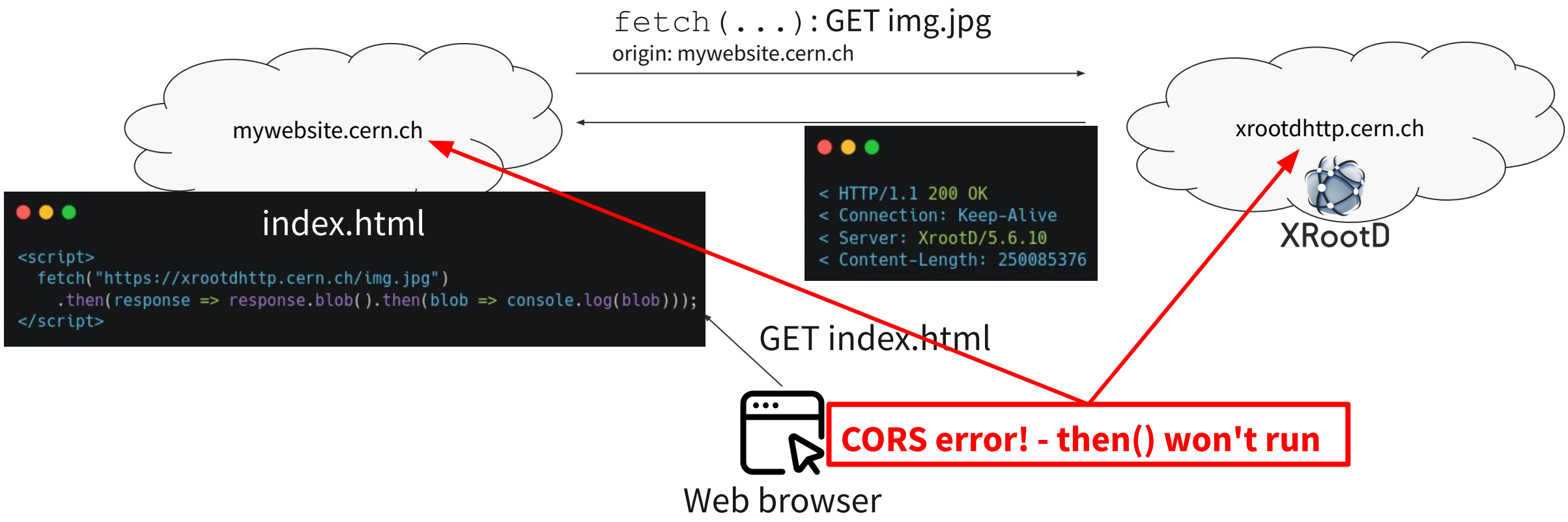
CORS Plugin

Example



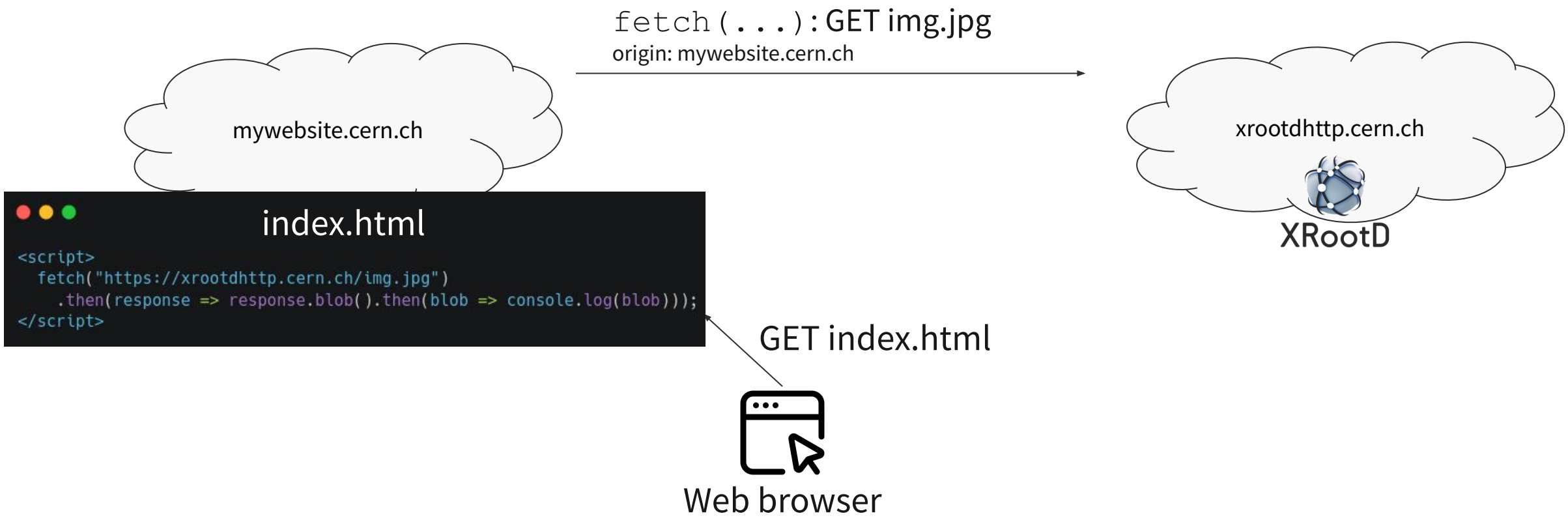
CORS Plugin

Example



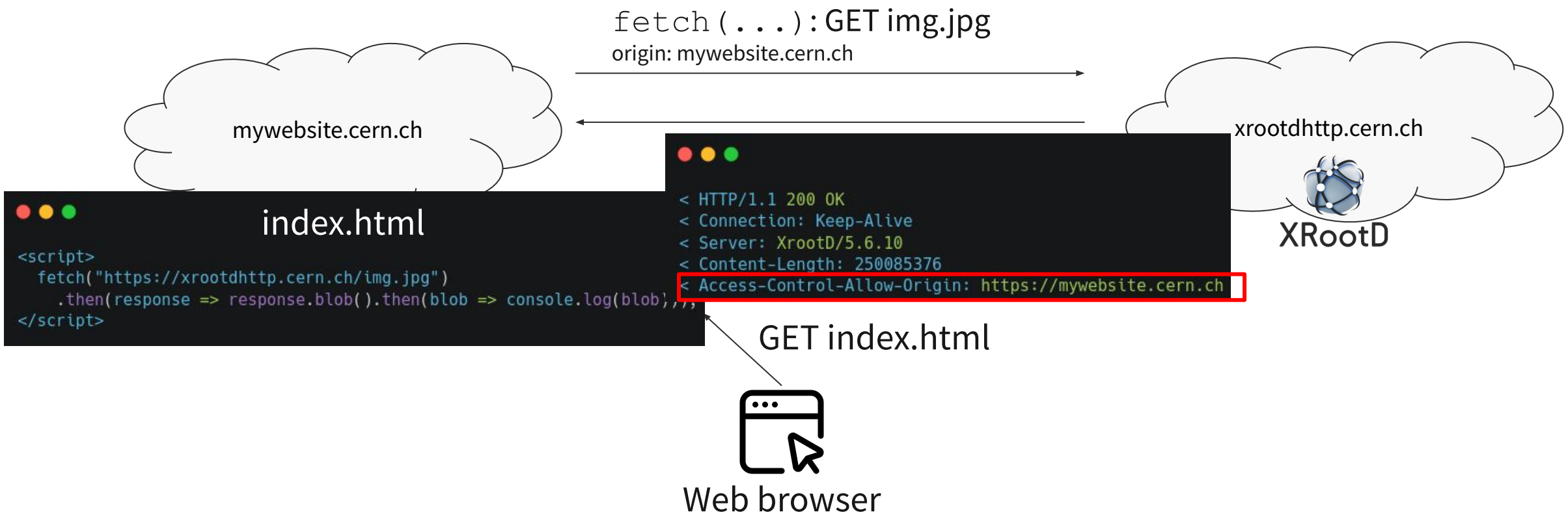
CORS Plugin

Example



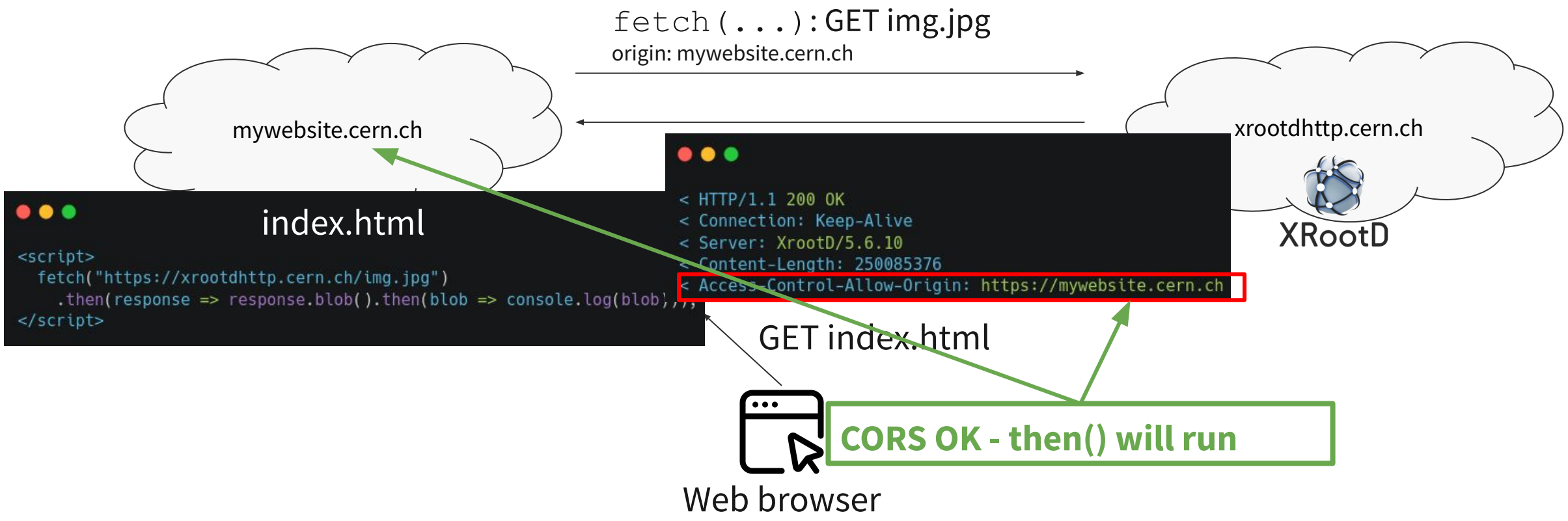
CORS Plugin

Example



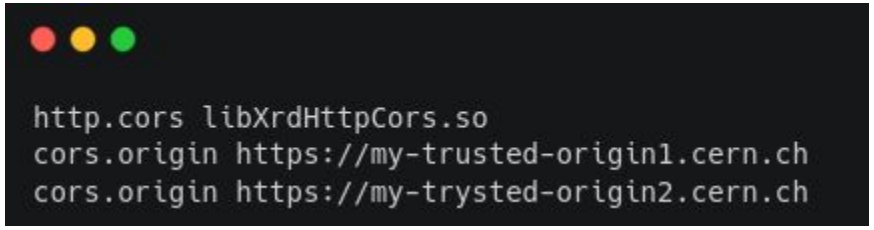
CORS Plugin

Example



CORS Plugin

Configuration



Requirements

Web-browser security features - Summary

- CORS → OK
- Redirection to HTTP → NOK

Extra requirement

"No need to install Site-specific-CA on client web-browsers" → NOK

How to do it

A new XRootD server

How to do it

XRootD

A new XRootD server

- HTTP(S) enabled

How to do it

A new XRootD server

- HTTP(S) enabled
- CORS plugin configured → JS fetch(...) can work

How to do it

A new XRootD server

- HTTP(S) enabled
- CORS plugin configured → JS fetch(...) can work
- Sectigo certificate → no need to install site-specific CA on browser

How to do it

A new XRootD server

- HTTP(S) enabled
- CORS plugin configured → JS fetch(...) can work
- Sectigo certificate → no need to install site-specific CA on browser
- Behave as a proxy in front of the storage cluster (EOS)

How to do it

A new XRootD server

- HTTP(S) enabled
- CORS plugin configured → JS fetch(...) can work
- Sectigo certificate → no need to install site-specific CA on browser
- Behave as a proxy in front of the storage cluster (EOS)
  - No client redirection to read files from the storage cluster
  - Authenticates with SSS (Simple Shared Secrets)
  - Forwards users credentials to EOS

How to do it

A new XRootD server

```
all.role  proxy server
all.export  /eos/ readonly
xrd.protocol  XrdHttp:8443 libXrdHttp.so
ofs.osslib  libXrdPss.so
pss.origin  eoslhcb.cern.ch:1094
pss.persona  client noverify
xrd.tls  /etc/grid-security/daemon/proxycert.pem /etc/grid-security/daemon/proxykey.pem
xrd.tlsca  certdir /etc/grid-security/certificates
http.secxtractor  libXrdVoms.so
http.gridmap  /etc/grid-security/grid-mapfile
http.header2cgi  Authorization authz
http.tlsclientauth  off
http.cors  libXrdHttpCors.so
cors.origin  https://lhcb-productions.web.cern.ch https://lhcbdiracx.app.cern.ch
https://lhcbdiracx-cert.app.cern.ch
```

How to do it

A new XRootD server

```
all.role  proxy server
all.export  /eos/ readonly
xrd.protocol  XrdHttp:8443 libXrdHttp.so
ofs.osslib  libXrdPss.so
pss.origin  eoslhcb.cern.ch:1094
pss.persona  client noverify
xrd.tls  /etc/grid-security/daemon/proxycert.pem /etc/grid-security/daemon/proxykey.pem
xrd.tlsca  certdir /etc/grid-security/certificates
http.secxtractor  libXrdVoms.so
http.gridmap  /etc/grid-security/grid-mapfile
http.header2cgi  Authorization authz
http.tlsclientauth  off
http.cors  libXrdHttpCors.so
cors.origin  https://lhcb-productions.web.cern.ch https://lhcbdiracx.app.cern.ch
https://lhcbdiracx-cert.app.cern.ch
```

How to do it

A new XRootD server

```
all.role  proxy server
all.export  /eos/ readonly
xrd.protocol  XrdHttp:8443 libXrdHttp.so
ofs.osslib  libXrdPss.so
pss.origin  eoslhcb.cern.ch:1094
pss.persona  client noverify
xrd.tls  /etc/grid-security/daemon/proxycert.pem /etc/grid-security/daemon/proxykey.pem
xrd.tlsca  certdir /etc/grid-security/certificates
http.secxtractor  libXrdVoms.so
http.gridmap  /etc/grid-security/grid-mapfile
http.header2cgi  Authorization authz
http.tlsclientauth  off
http.cors  libXrdHttpCors.so
cors.origin  https://lhcb-productions.web.cern.ch https://lhcbdiracx.app.cern.ch
https://lhcbdiracx-cert.app.cern.ch
```

Enable HTTP

How to do it

A new XRootD server

```
all.role  proxy server
all.export  /eos/ readonly
xrd.protocol  XrdHttp:8443 libXrdHttp.so
ofs.osslib  libXrdPss.so
pss.origin  eoslhcb.cern.ch:1094
pss.persona  client noverify
xrd.tls  /etc/grid-security/daemon/proxycert.pem /etc/grid-security/daemon/proxykey.pem
xrd.tlsca  certdir /etc/grid-security/certificates
http.secxtractor  libXrdVoms.so
http.gridmap  /etc/grid-security/grid-mapfile
http.header2cgi  Authorization authz
http.tlsclientauth  off
http.cors  libXrdHttpCors.so
cors.origin  https://lhcb-productions.web.cern.ch https://lhcbdiracx.app.cern.ch
https://lhcbdiracx-cert.app.cern.ch
```

Enable HTTP

Proxy library

How to do it

A new XRootD server

```
all.role  proxy server
all.export  /eos/ readonly
xrd.protocol  XrdHttp:8443 libXrdHttp.so
ofs.osslib  libXrdPss.so
pss.origin  eoslhcb.cern.ch:1094
pss.persona  client noverify
xrd.tls  /etc/grid-security/daemon/proxycert.pem /etc/grid-security/daemon/proxykey.pem
xrd.tlsca  certdir /etc/grid-security/certificates
http.secxtractor  libXrdVoms.so
http.gridmap  /etc/grid-security/grid-mapfile
http.header2cgi  Authorization authz
http.tlsclientauth  off
http.cors  libXrdHttpCors.so
cors.origin  https://lhcb-productions.web.cern.ch https://lhcbdiracx.app.cern.ch
https://lhcbdiracx-cert.app.cern.ch
```

Enable HTTP

Proxy library

How to do it

A new XRootD server

```
all.role  proxy server
all.export  /eos/ readonly
xrd.protocol  XrdHttp:8443 libXrdHttp.so
ofs.osslib  libXrdPss.so
pss.origin  eoslhcb.cern.ch:1094
pss.persona  client noverify
xrd.tls  /etc/grid-security/daemon/proxycert.pem /etc/grid-security/daemon/proxykey.pem
xrd.tlsca  certdir /etc/grid-security/certificates
http.secxtractor  libXrdVoms.so
http.gridmap  /etc/grid-security/grid-mapfile
http.header2cgi  Authorization authz
http.tlsclientauth  off
http.cors  libXrdHttpCors.so
cors.origin  https://lhcb-productions.web.cern.ch https://lhcbdiracx.app.cern.ch
https://lhcbdiracx-cert.app.cern.ch
```

Enable HTTP

Proxy library

SECTIGO®

Forward token credentials to the MGM

How to do it

A new XRootD server

```
all.role  proxy server
all.export  /eos/ readonly
xrd.protocol  XrdHttp:8443 libXrdHttp.so
ofs.osslib  libXrdPss.so
pss.origin  eoslhcb.cern.ch:1094
pss.persona  client noverify
xrd.tls  /etc/grid-security/daemon/proxycert.pem /etc/grid-security/daemon/proxykey.pem
xrd.tlsca  certdir /etc/grid-security/certificates
http.secxtractor  libXrdVoms.so
http.gridmap  /etc/grid-security/grid-mapfile
http.header2cgi  Authorization authz
http.tlsclientauth  off
http.cors  libXrdHttpCors.so
cors.origin  https://lhcb-productions.web.cern.ch https://lhcbdiracx.app.cern.ch
https://lhcbdiracx-cert.app.cern.ch
```

Enable HTTP

Proxy library

SECTIGO®

Forward token credentials to the MGM

Avoid annoying web-browser popup for certificate authentication

How to do it

A new XRootD server

```
all.role  proxy server
all.export  /eos/ readonly
xrd.protocol  XrdHttp:8443 libXrdHttp.so
ofs.osslib  libXrdPss.so
pss.origin  eoslhcb.cern.ch:1094
pss.persona  client noverify
xrd.tls  /etc/grid-security/daemon/proxycert.pem /etc/grid-security/daemon/proxykey.pem
xrd.tlsca  certdir /etc/grid-security/certificates
http.secxtractor  libXrdVoms.so
http.gridmap  /etc/grid-security/grid-mapfile
http.header2cgi  Authorization authz
http.tlsclientauth  off
http.cors  libXrdHttpCors.so
cors.origin  https://lhcb-productions.web.cern.ch https://lhcbdiracx.app.cern.ch
https://lhcbdiracx-cert.app.cern.ch
```

Enable HTTP

Proxy library

SECTIGO®

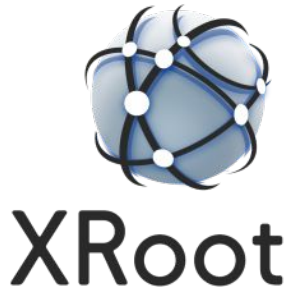
Forward token credentials to the MGM

Avoid annoying web-browser popup for certificate authentication

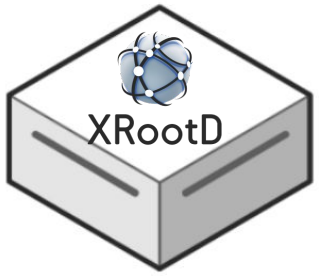
CORS

WLCG HTTP-TPC data integrity check

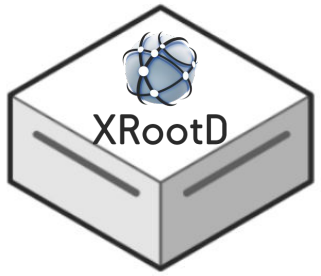
Reminder: HTTP - Third Party Copy



PULL



eoslhcb.cern.ch



eospublic.cern.ch

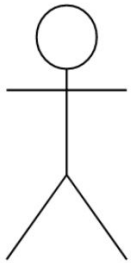
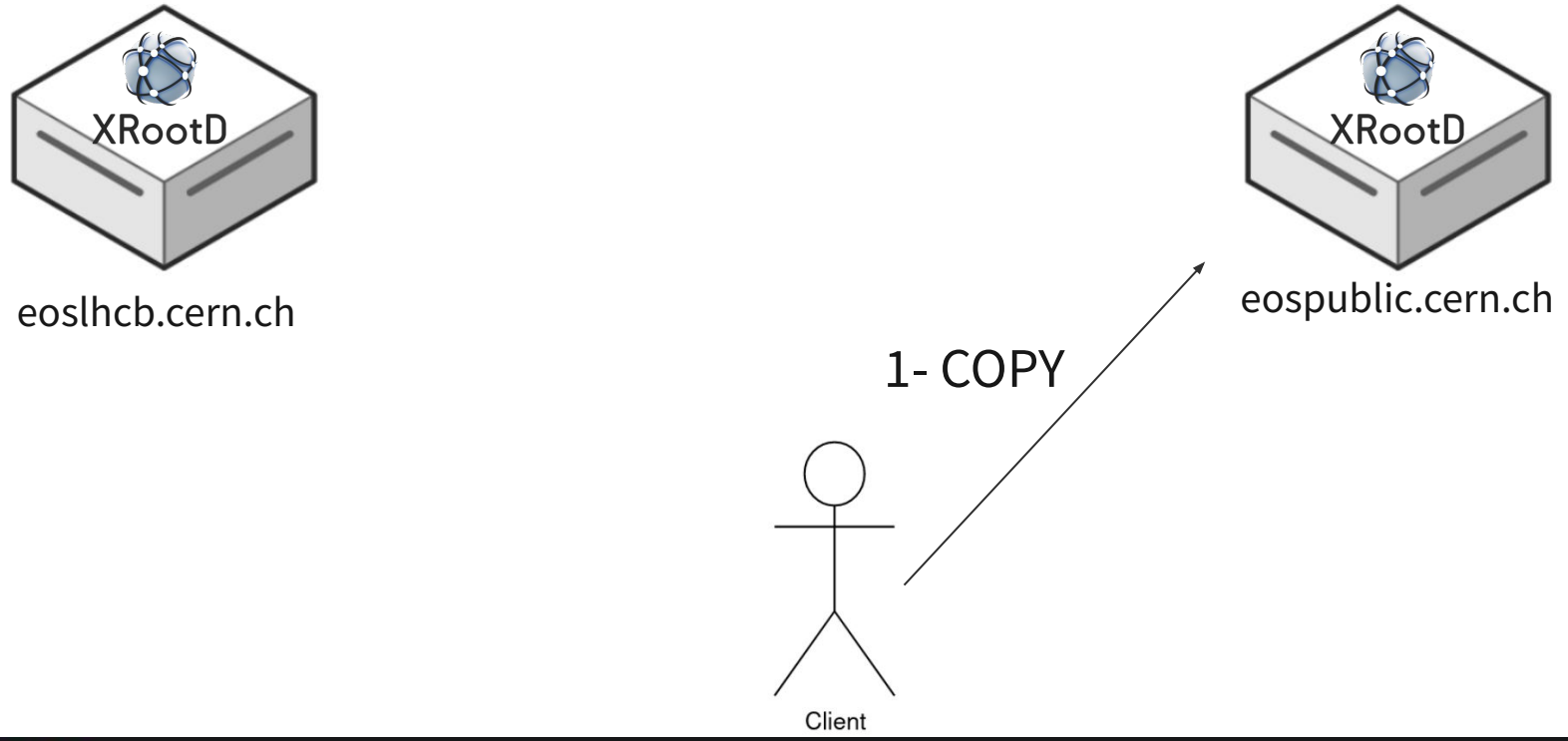


image: Flaticon.com

Reminder: HTTP - Third Party Copy

PULL

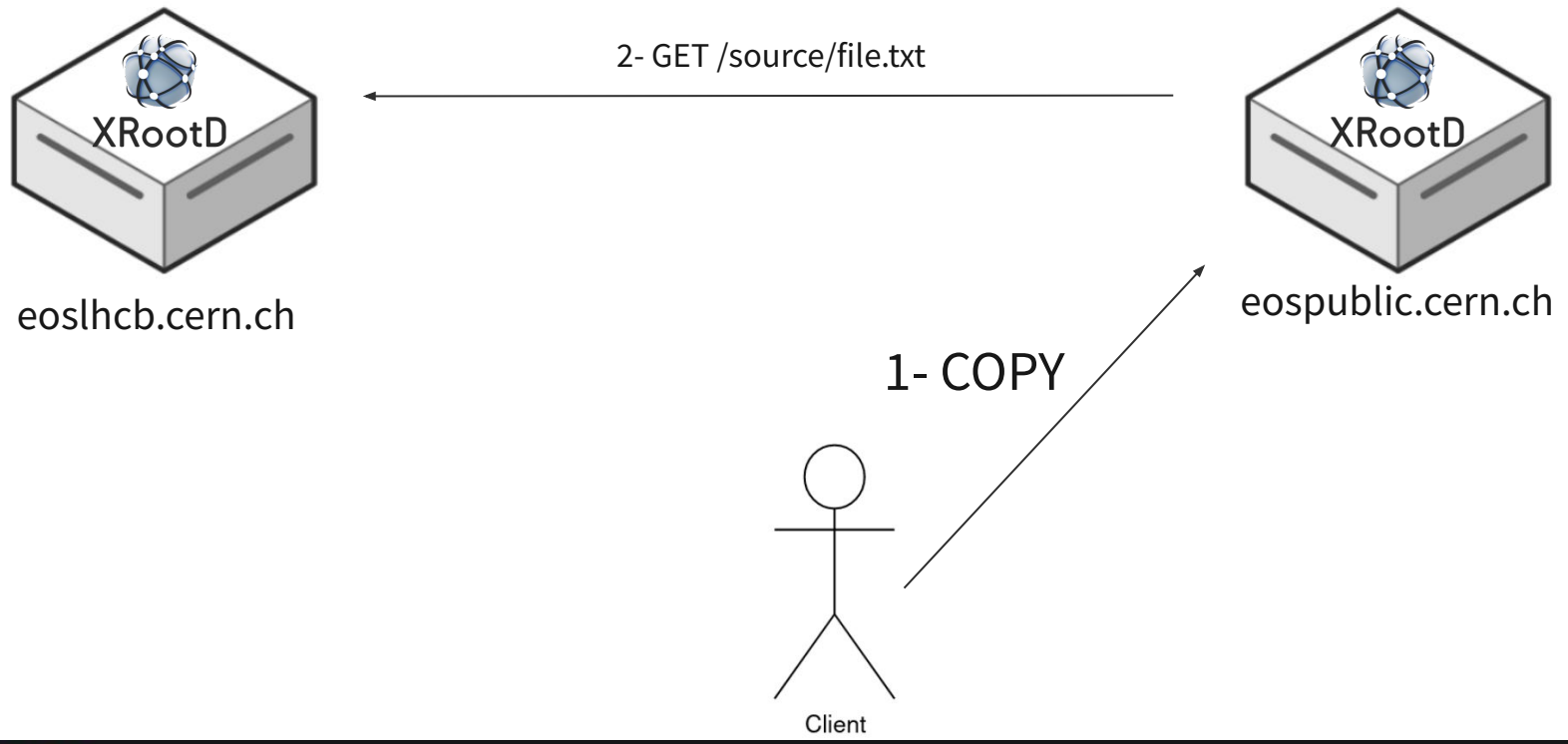



```
curl -X COPY -H 'Source: https://eoslhcb.cern.ch/source/file.txt' https://eospublic.cern.ch/dest/file.txt
```

image: Flaticon.com

Reminder: HTTP - Third Party Copy

PULL

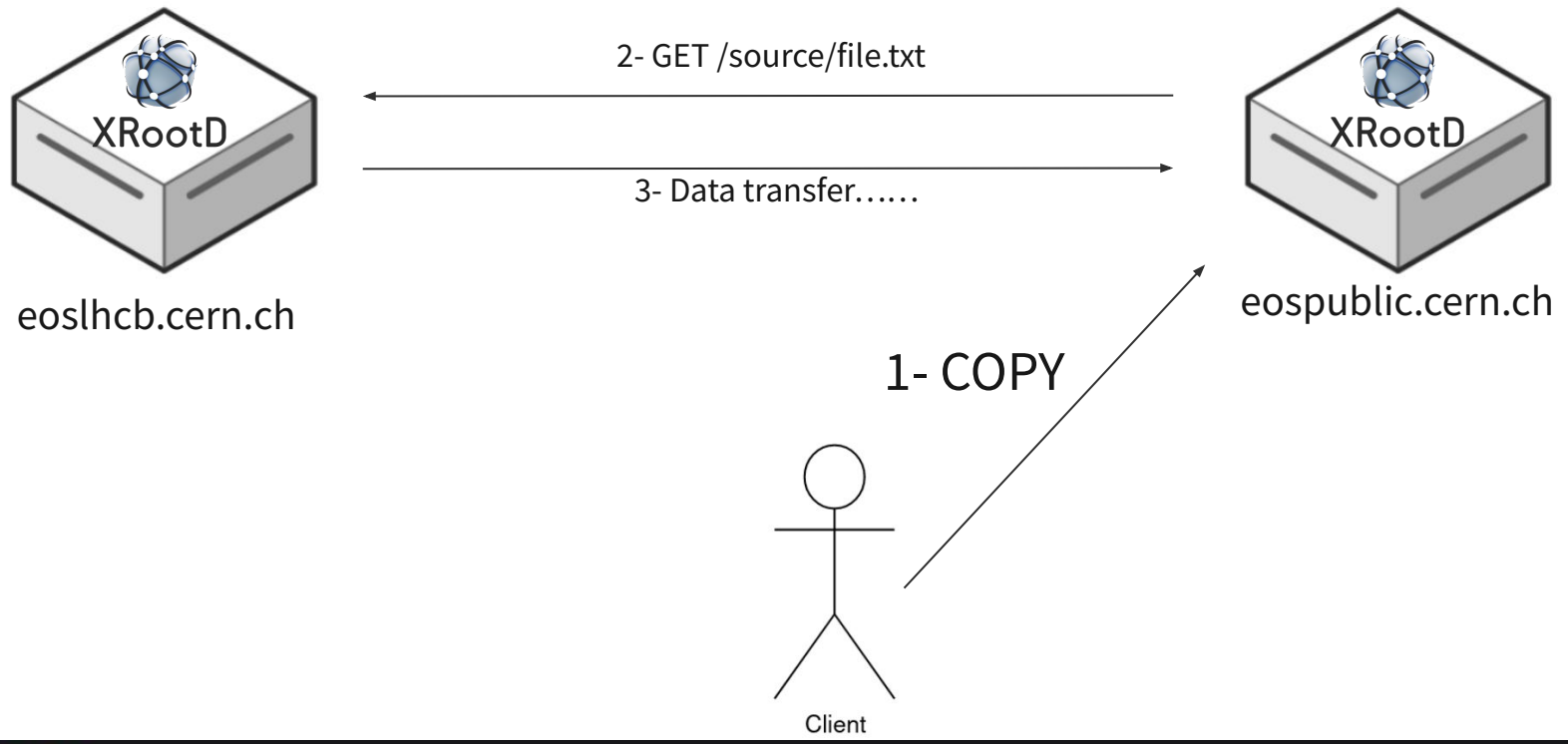



```
curl -X COPY -H 'Source: https://eoslhcb.cern.ch/source/file.txt' https://eospublic.cern.ch/dest/file.txt
```

image: Flaticon.com

Reminder: HTTP - Third Party Copy

PULL

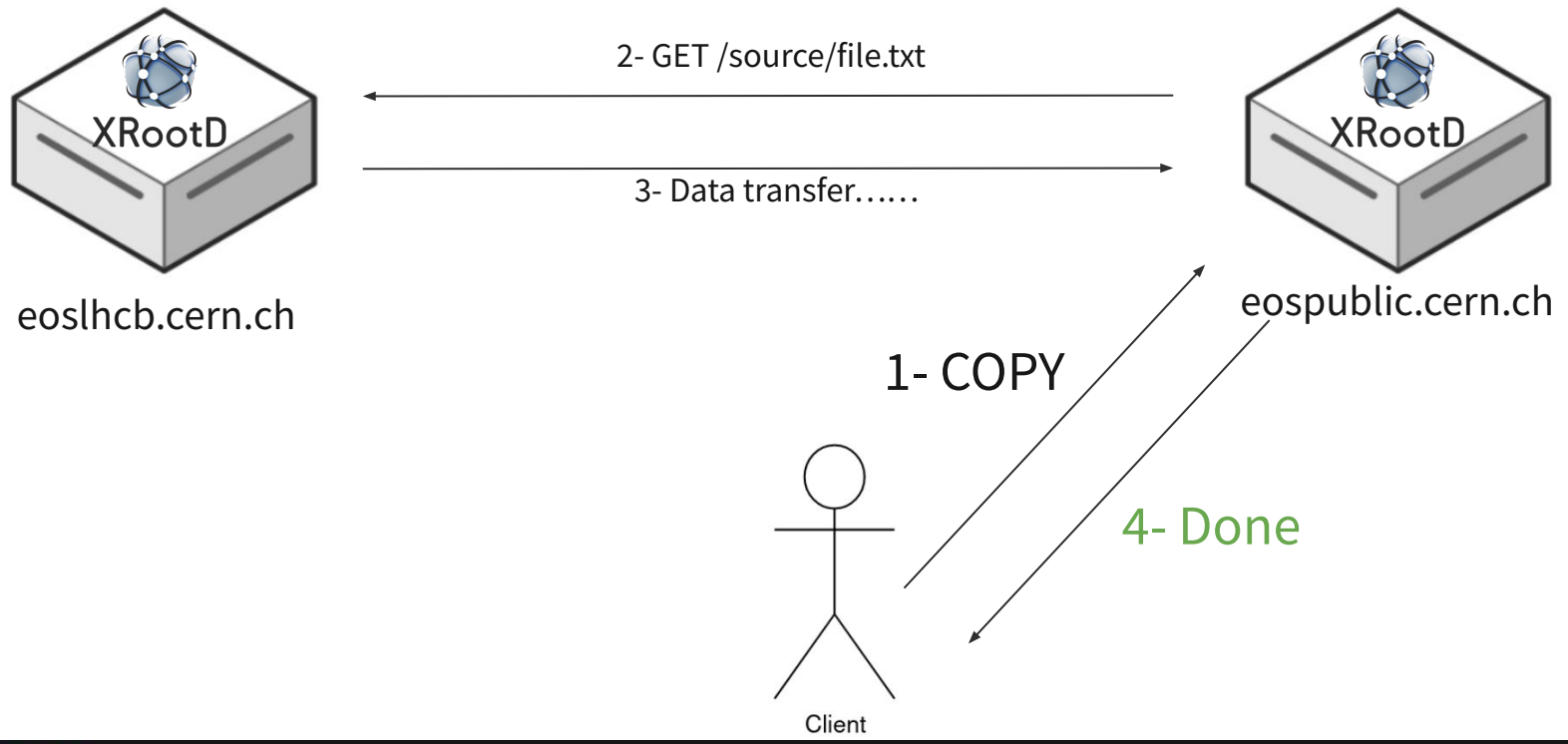



```
curl -X COPY -H 'Source: https://eoslhcb.cern.ch/source/file.txt' https://eospublic.cern.ch/dest/file.txt
```

image: Flaticon.com

Reminder: HTTP - Third Party Copy

PULL

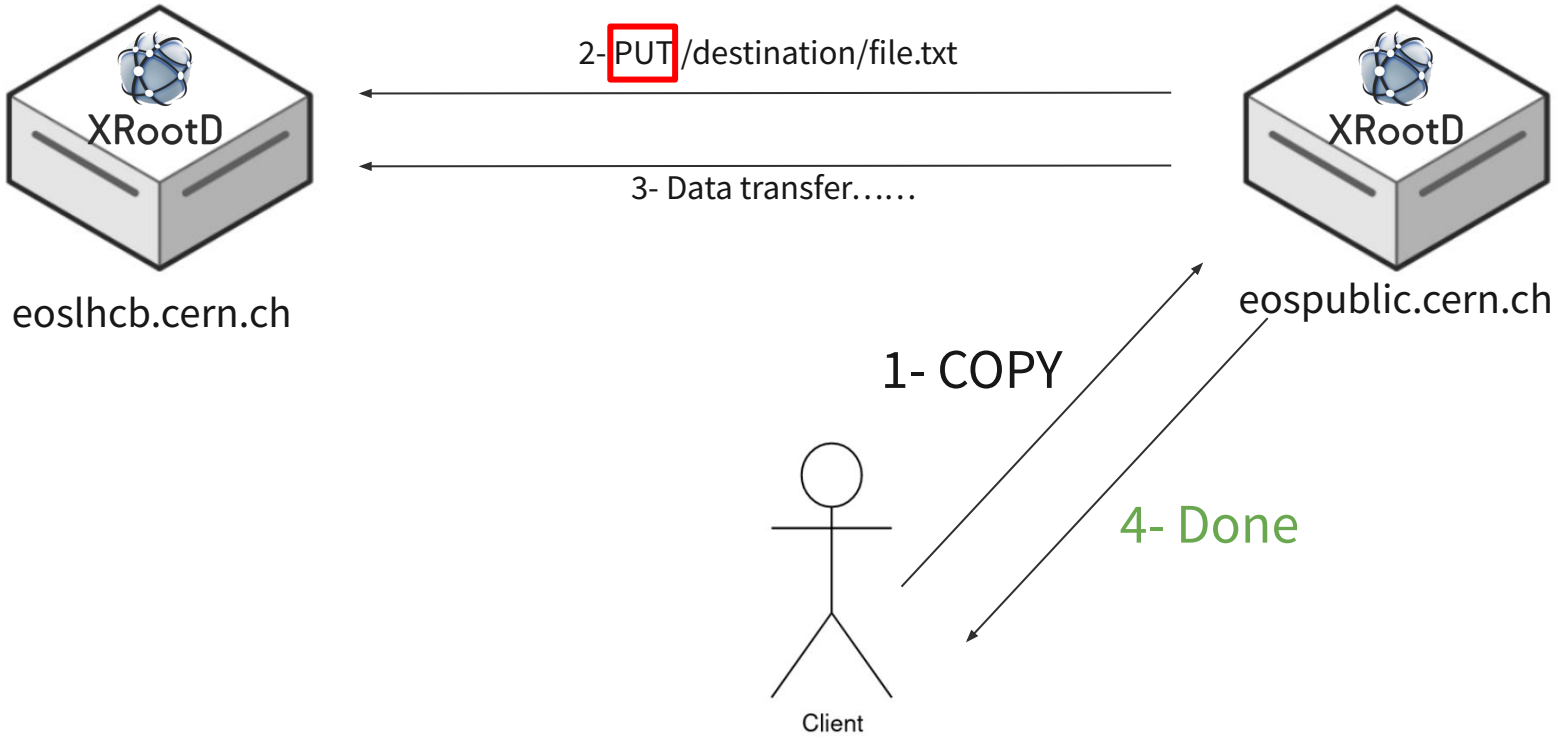



```
curl -X COPY -H 'Source: https://eoslhcb.cern.ch/source/file.txt' https://eospublic.cern.ch/dest/file.txt
```

image: Flaticon.com

Reminder: HTTP - Third Party Copy

PUSH




```
curl -X COPY -H 'Destination: https://eoslhcb.cern.ch/destination/file.txt' https://eospublic.cern.ch/source/file.txt
```

image: Flaticon.com

Context

WLCG HTTP-TPC

- Files copied directly between source storage and destination storage

Context

WLCG HTTP-TPC

- Files copied directly between source storage and destination storage
- FTS supervises copy

Context

WLCG HTTP-TPC

- Files copied directly between source storage and destination storage
- FTS supervises copy
  - Performs file verification at the end (file size + checksum)

Context

WLCG HTTP-TPC

- Files copied directly between source storage and destination storage
- FTS supervises copy
  - Performs file verification at the end (file size + checksum)

Problem

- Corrupted files may still end up on tape storages!

Context

WLCG HTTP-TPC

- Files copied directly between source storage and destination storage
- FTS supervises copy
  - Performs file verification at the end (file size + checksum)

Problem

- Corrupted files may still end up on tape storages!
  - File gets corrupted during transfer → deletion on tape RSE is usually forbidden
    - FTS cannot delete

Context

WLCG HTTP-TPC

- Files copied directly between source storage and destination storage
- FTS supervises copy
  - Performs file verification at the end (file size + checksum)

Problem

- Corrupted files may still end up on tape storages!
  - File gets corrupted during transfer → deletion on tape RSE is usually forbidden
    - FTS cannot delete → MANUAL CLEANING REQUIRED

Solution

XRootD

Let data storages deal with corrupted files

Solution

Let data storages deal with corrupted files

- Client passes the checksum alongside the COPY request

Solution

Let data storages deal with corrupted files

- Client passes the checksum alongside the COPY request
  - Using `Repr-Digest` header (RFC 9530)

Solution

Let data storages deal with corrupted files

- Client passes the checksum alongside the COPY request
  - Using `Repr-Digest` header (RFC 9530)
  - E.g: `Repr-Digest: adler32=:base64_encoded_binary_adler32:`

Solution

Let data storages deal with corrupted files

- Client passes the checksum alongside the COPY request
  - Using `Repr-Digest` header (RFC 9530)
  - E.g: `Repr-Digest: adler32=:base64_encoded_binary_adler32:`
    - `xrdadler32 /etc/passwd | cut -d' ' -f1 | xxd -r -p |  base64 -`

Solution

Let data storages deal with corrupted files

- Client passes the checksum alongside the COPY request
  - Using `Repr-Digest` header (RFC 9530)
  - E.g: `Repr-Digest: adler32=:base64_encoded_binary_adler32:`
    - `xrdadler32 /etc/passwd | cut -d' ' -f1 | xxd -r -p |  base64 -`
- Storage deletes the file received if checksum mismatch → No FTS File Transfer Service involved

Solution

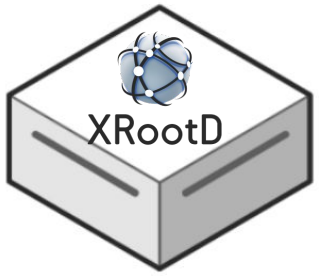
Let data storages deal with corrupted files

- Client passes the checksum alongside the COPY request
  - Using `Repr-Digest` header (RFC 9530)
  - E.g: `Repr-Digest: adler32=:base64_encoded_binary_adler32:`
    - `xrdadler32 /etc/passwd | cut -d' ' -f1 | xxd -r -p |  base64 -`
- Storage deletes the file received if checksum mismatch → No FTS involved

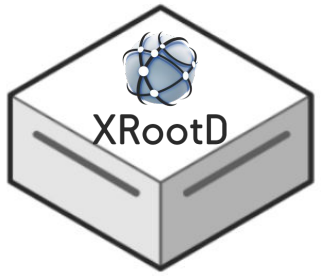
More infos: https://indico.cern.ch/event/1484669/contributions/6464759/attachments/3063730/5418458/WLCG_HSF_Workshop2025_DOMA_BDT_Plans.pdf and https://github.com/labkode/wlcg-tpc

WLCG data integrity check - HTTP TPC

PULL



eoslhcb.cern.ch



eospublic.cern.ch

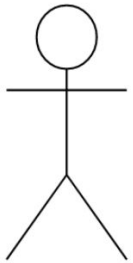
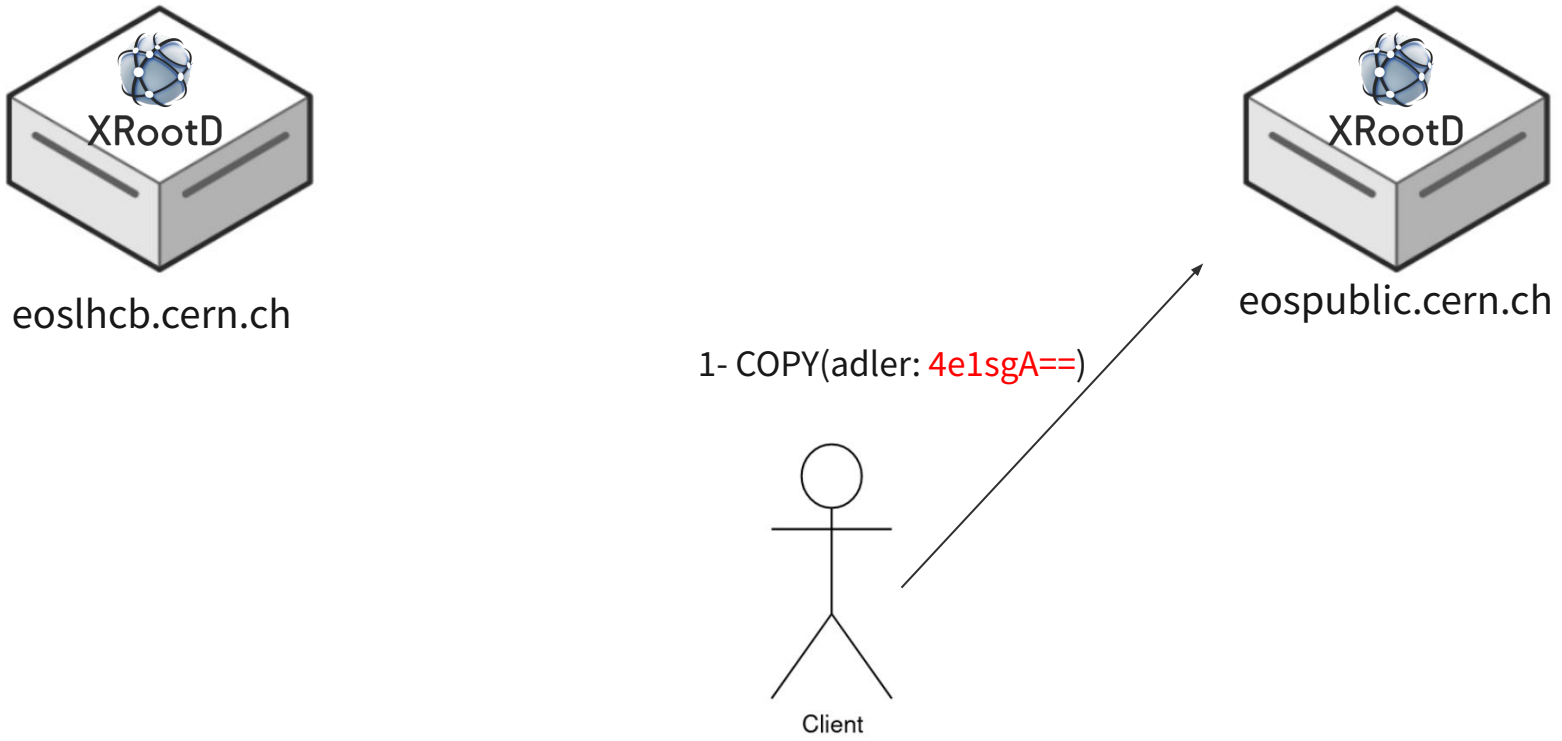


image: Flaticon.com

WLCG data integrity check - HTTP TPC

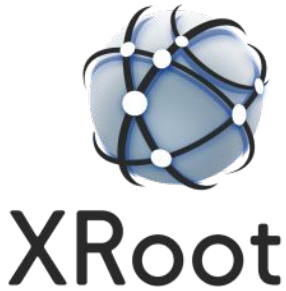
PULL



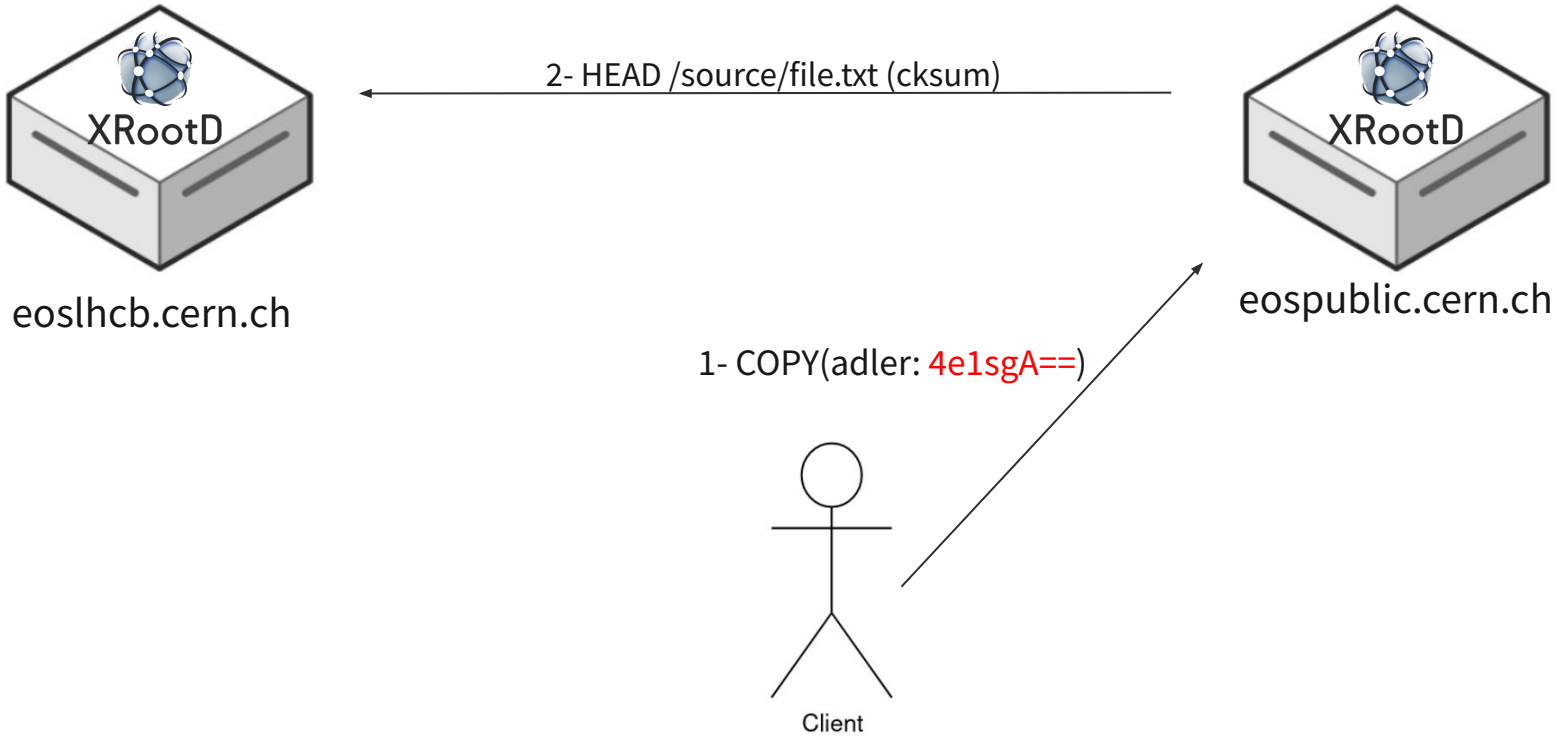

```
curl -X COPY -H 'Source: https://eoslhcb.cern.ch/source/file.txt' -H 'Repr-Digest: adler32=:4e1sgA==:' https://eospublic.cern.ch/
destination/file.txt
```

ge: Flaticon.com

WLCG data integrity check - HTTP TPC



PULL

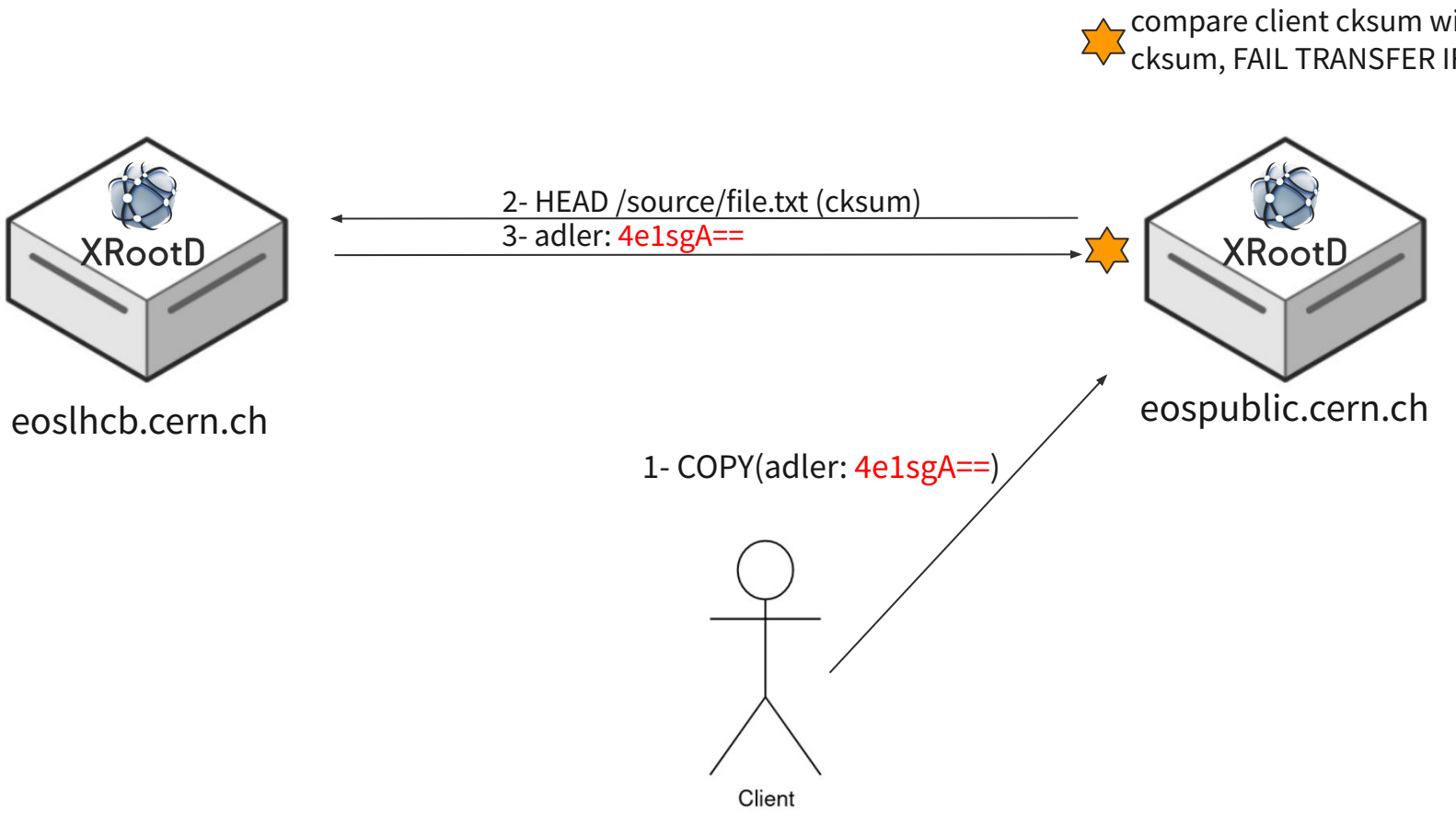



```
curl -X COPY -H 'Source: https://eoslhcb.cern.ch/source/file.txt' -H 'Repr-Digest: adler32=:4e1sgA==:' https://eospublic.cern.ch/
destination/file.txt
```

ge: Flaticon.com

WLCG data integrity check - HTTP TPC

PULL

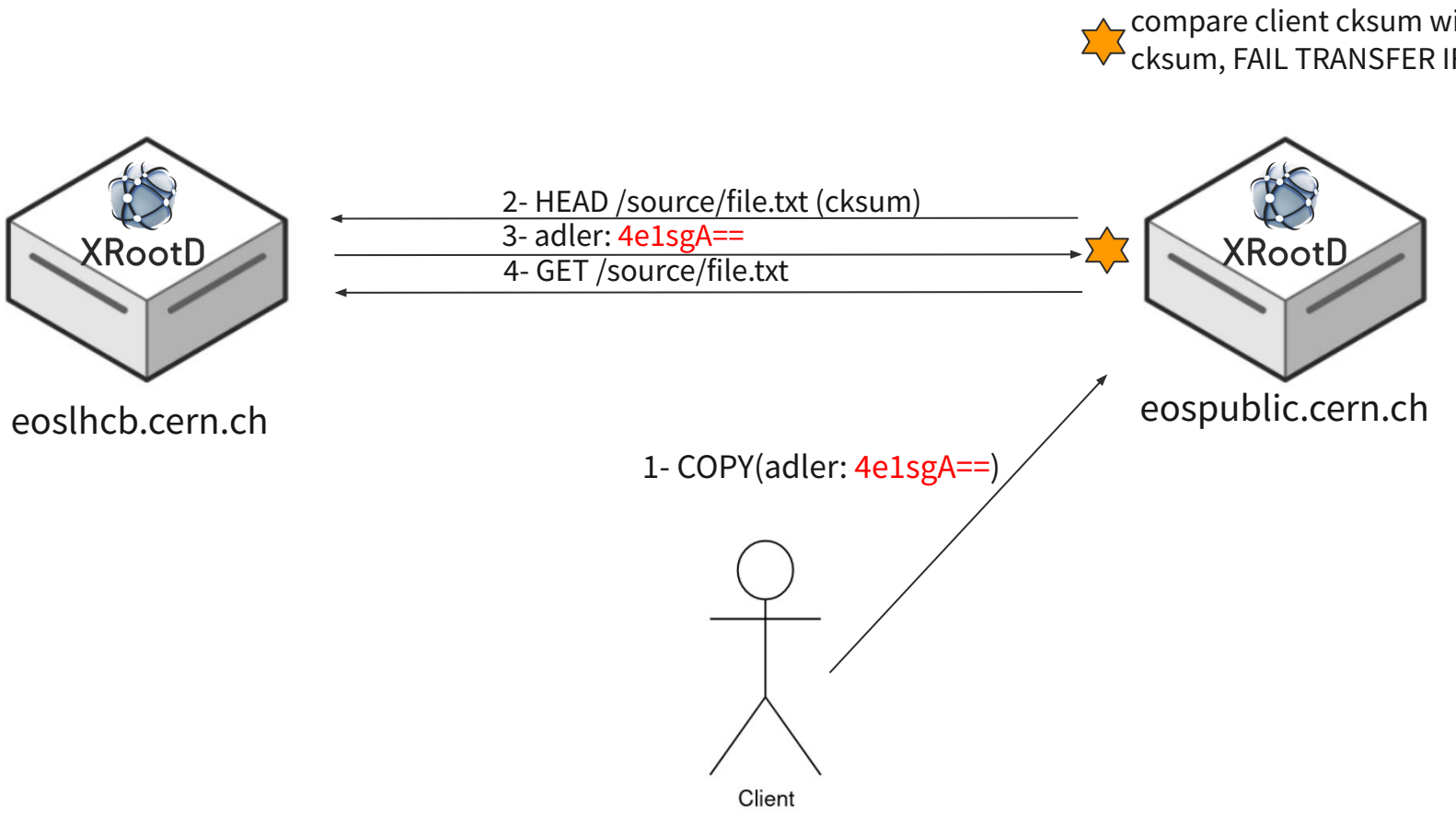



```
curl -X COPY -H 'Source: https://eoslhcb.cern.ch/source/file.txt' -H 'Repr-Digest: adler32=:4e1sgA==:' https://eospublic.cern.ch/
destination/file.txt
```

ge: Flaticon.com

WLCG data integrity check - HTTP TPC

PULL

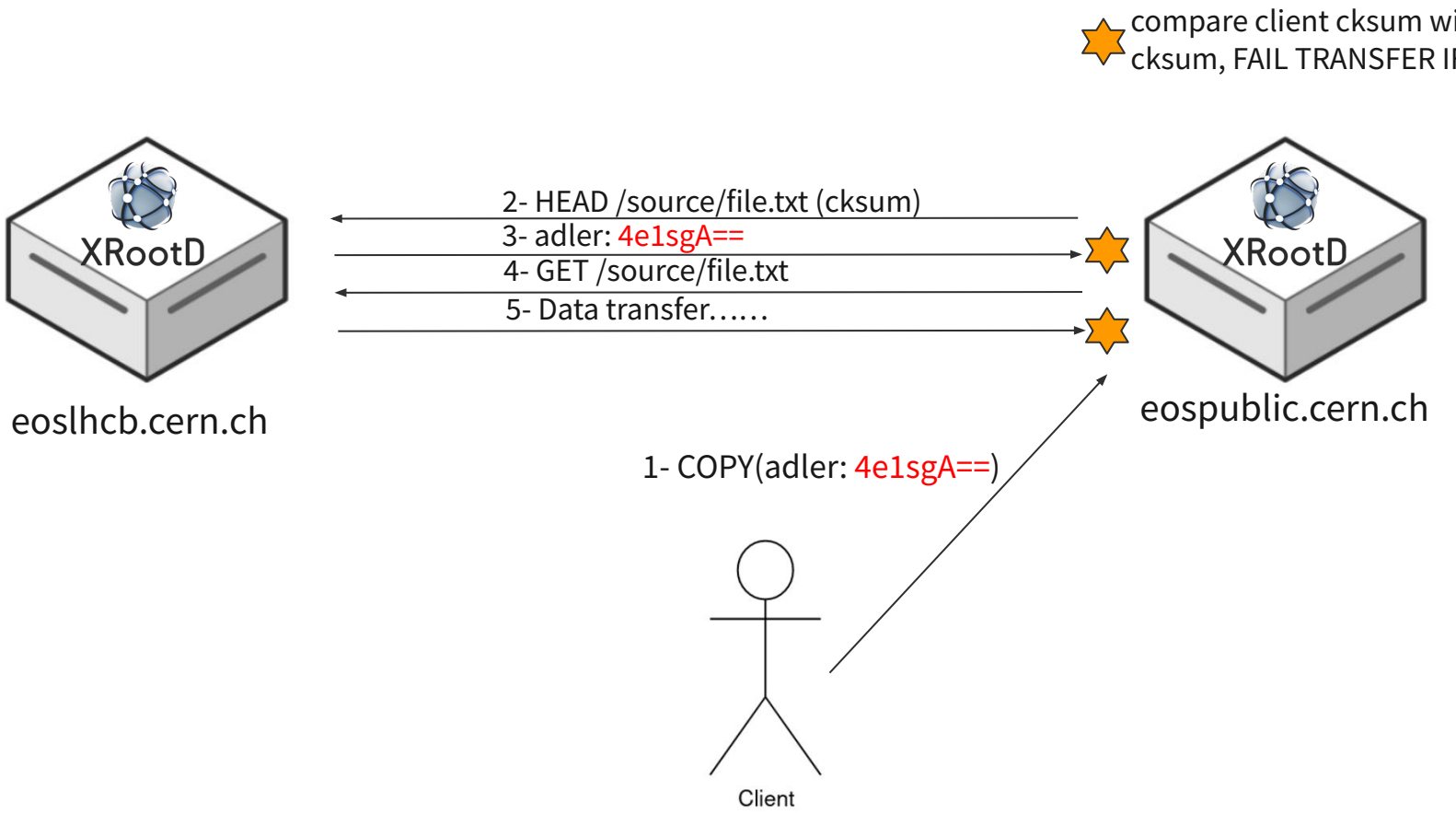



```
curl -X COPY -H 'Source: https://eoslhcb.cern.ch/source/file.txt' -H 'Repr-Digest: adler32=:4e1sgA==:' https://eospublic.cern.ch/destination/file.txt
```

ge: Flaticon.com

WLCG data integrity check - HTTP TPC

PULL

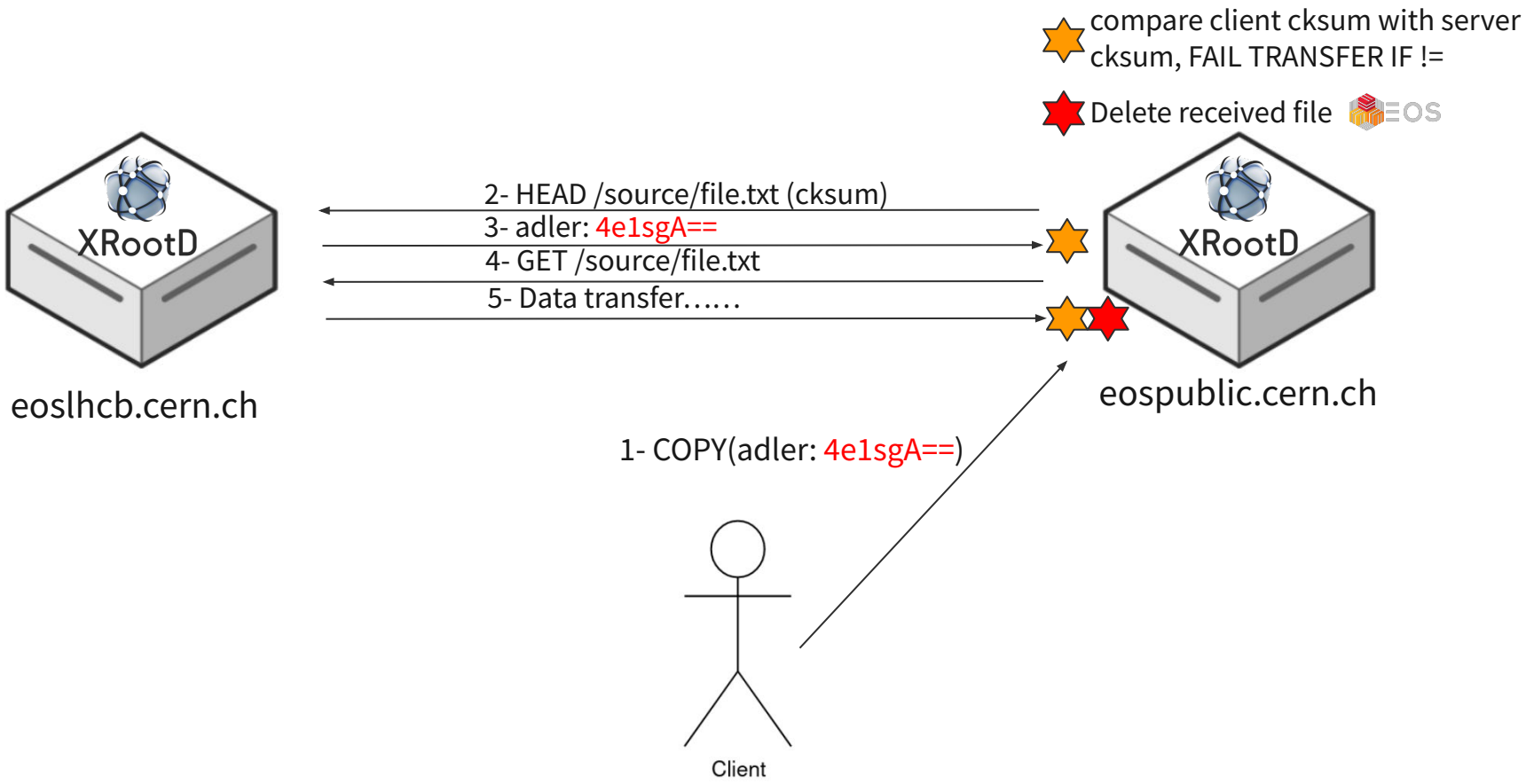



```
curl -X COPY -H 'Source: https://eoslhcb.cern.ch/source/file.txt' -H 'Repr-Digest: adler32=:4e1sgA==:' https://eospublic.cern.ch/
destination/file.txt
```

ge: Flaticon.com

WLCG data integrity check - HTTP TPC

PULL

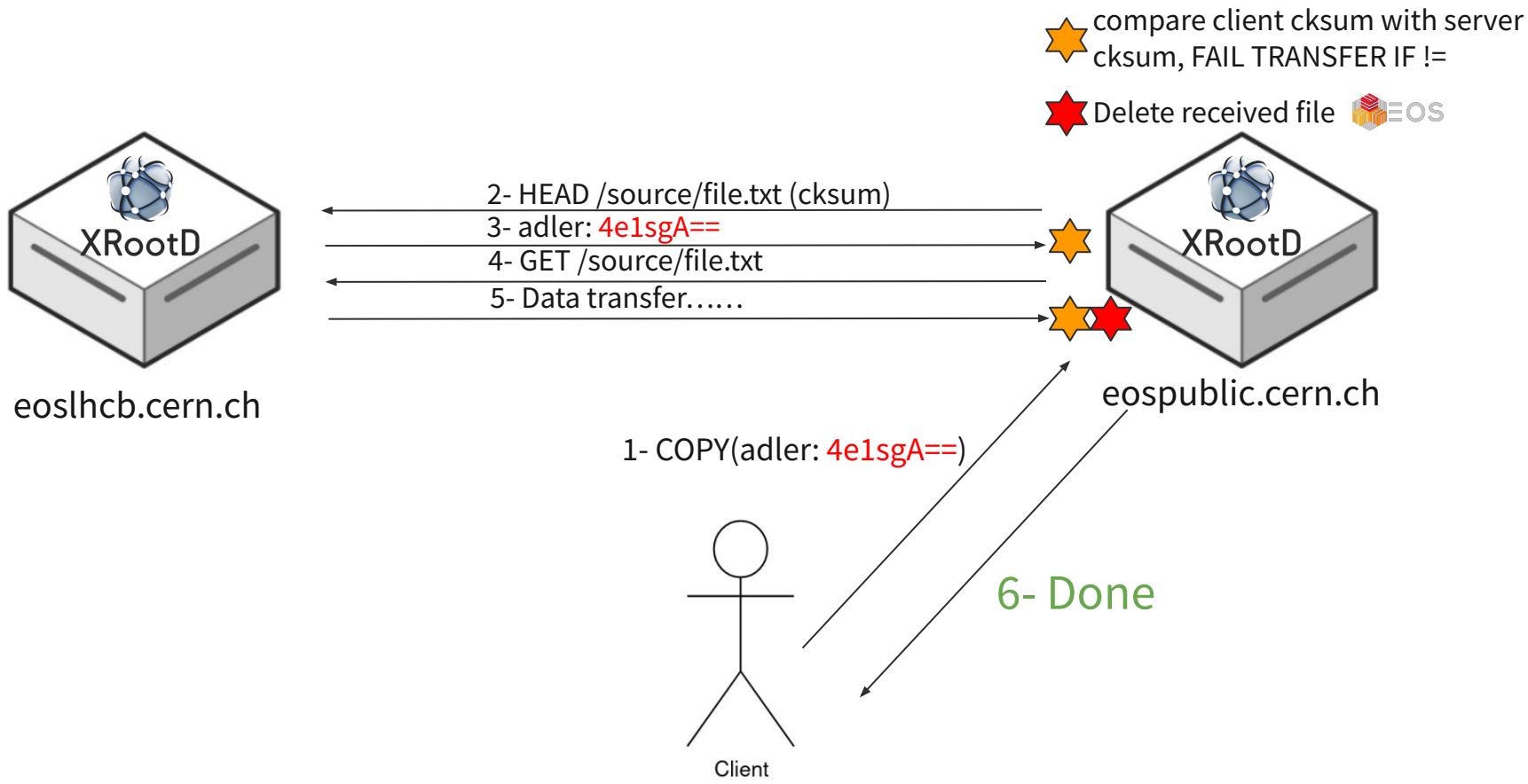



```
curl -X COPY -H 'Source: https://eoslhcb.cern.ch/source/file.txt' -H 'Repr-Digest: adler32=:4e1sgA==:' https://eospublic.cern.ch/destination/file.txt
```

ge: Flaticon.com

WLCG data integrity check - HTTP TPC

PULL

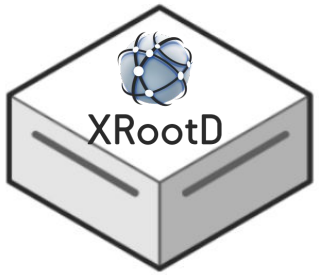



```
curl -X COPY -H 'Source: https://eoslhcb.cern.ch/source/file.txt' -H 'Repr-Digest: adler32=:4e1sgA==:' https://eospublic.cern.ch/destination/file.txt
```

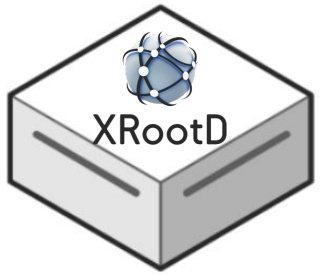
ge: Flaticon.com

WLCG data integrity check - HTTP TPC

PUSH



eoslhcb.cern.ch



eospublic.cern.ch

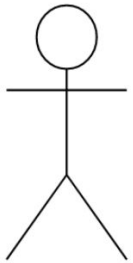
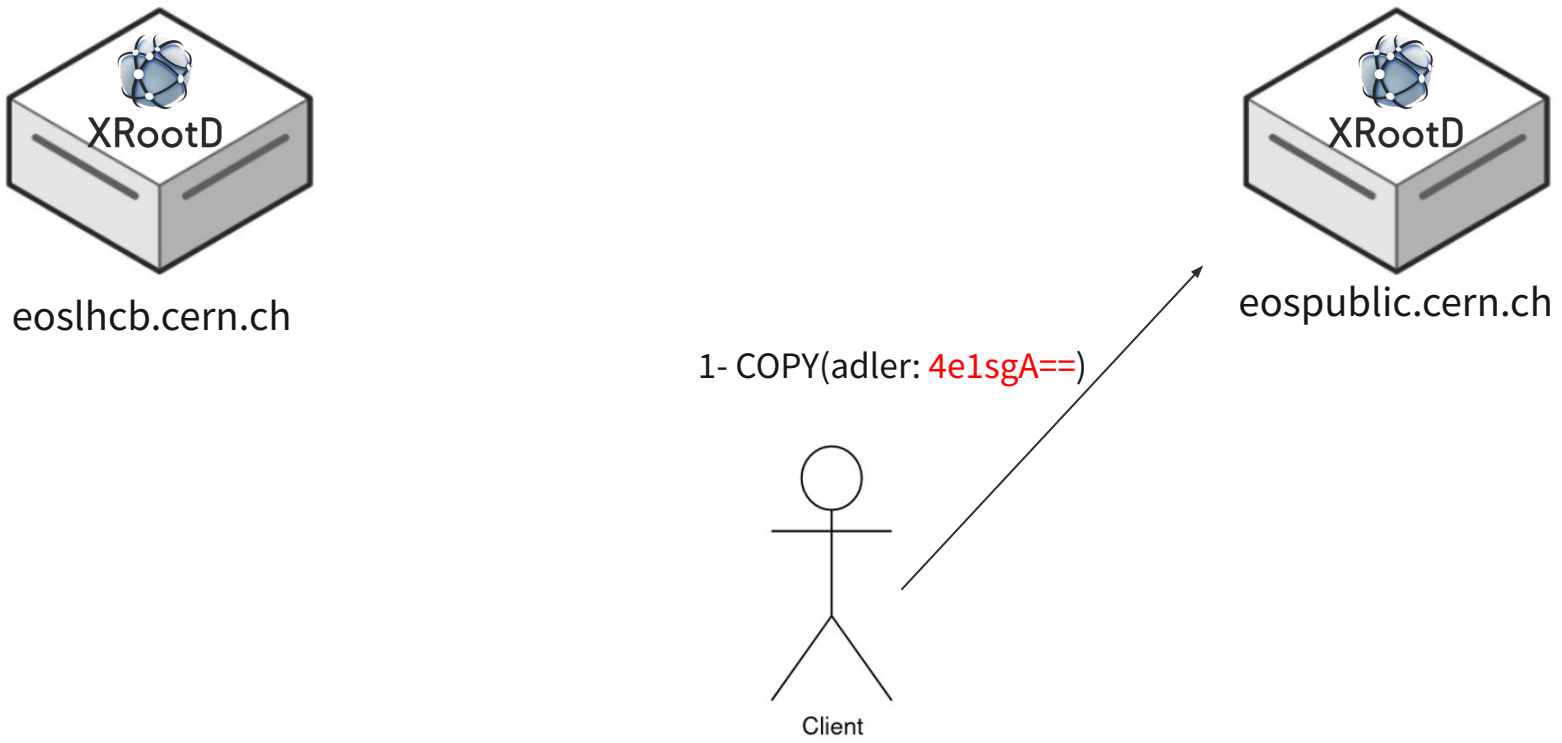


image: Flaticon.com

WLCG data integrity check - HTTP TPC

PUSH

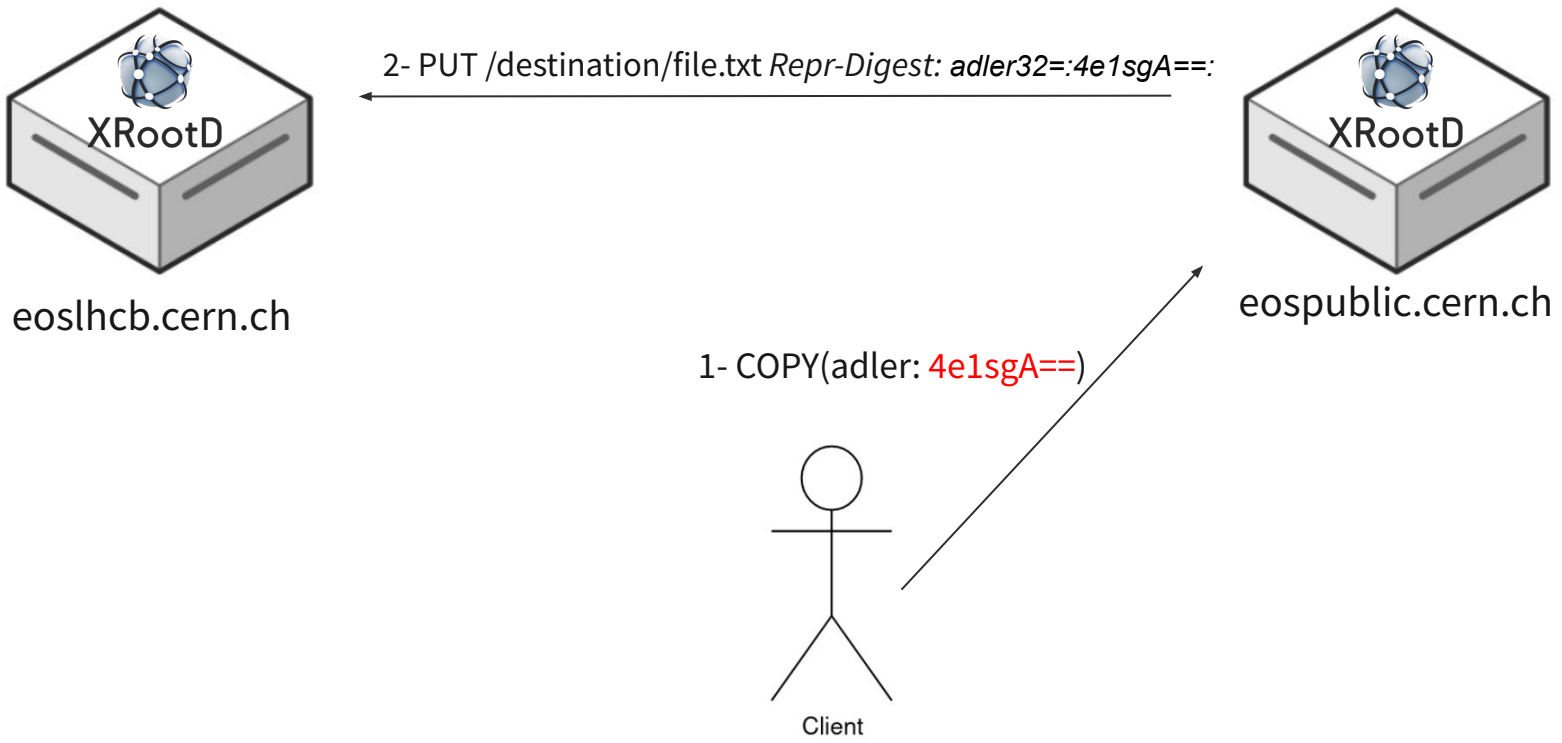



```
curl -X COPY -H 'Destination: https://eoslhcb.cern.ch/destination/file.txt' -H 'Repr-Digest: adler32=:4e1sgA==:'
https://eospublic.cern.ch/source/file.txt
```

image: Flaticon.com

WLCG data integrity check - HTTP TPC

PUSH

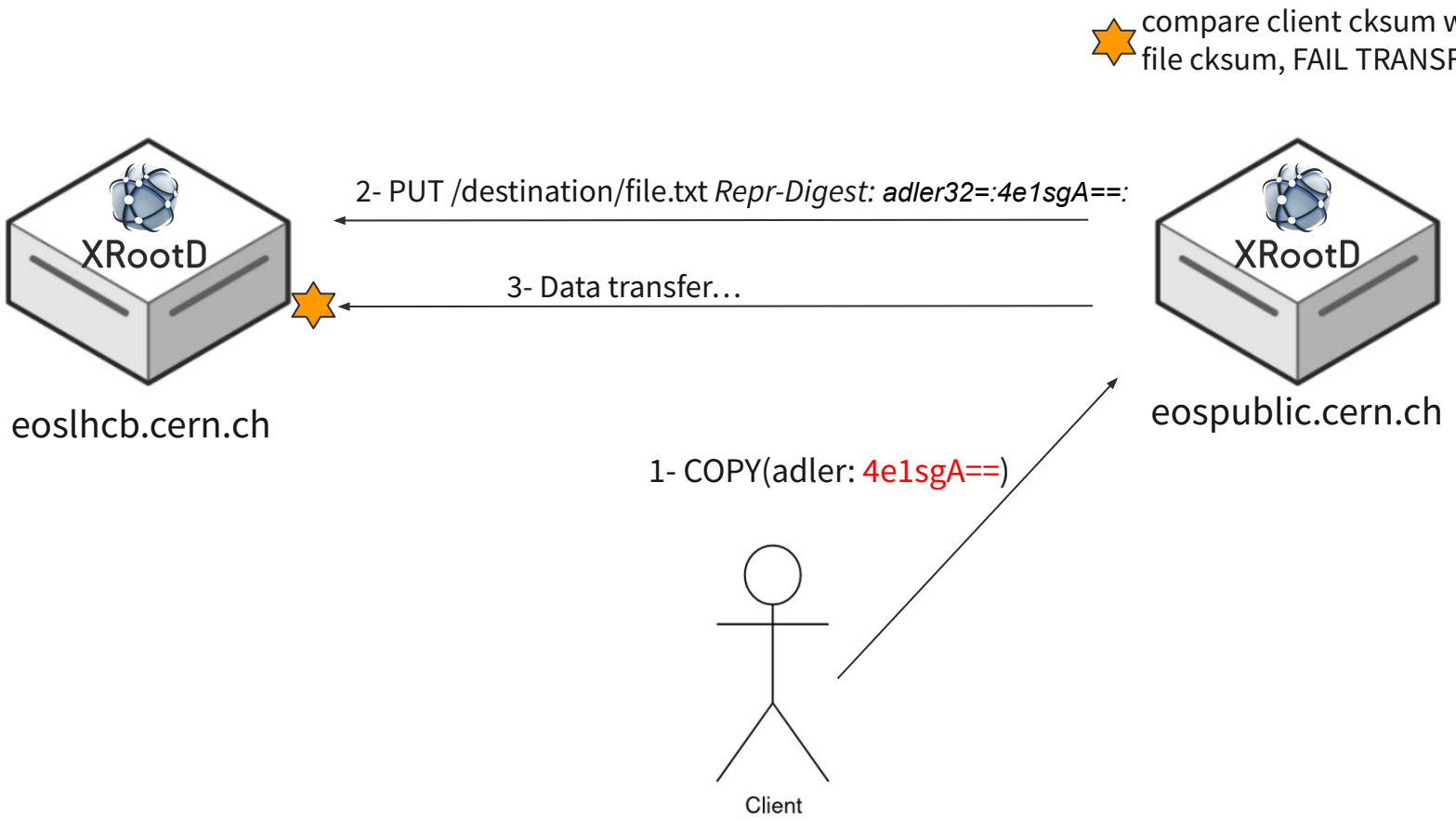



```
curl -X COPY -H 'Destination: https://eoslhcb.cern.ch/destination/file.txt' -H 'Repr-Digest: adler32=:4e1sgA==:'
https://eospublic.cern.ch/source/file.txt
```

image: Flaticon.com

WLCG data integrity check - HTTP TPC

PUSH

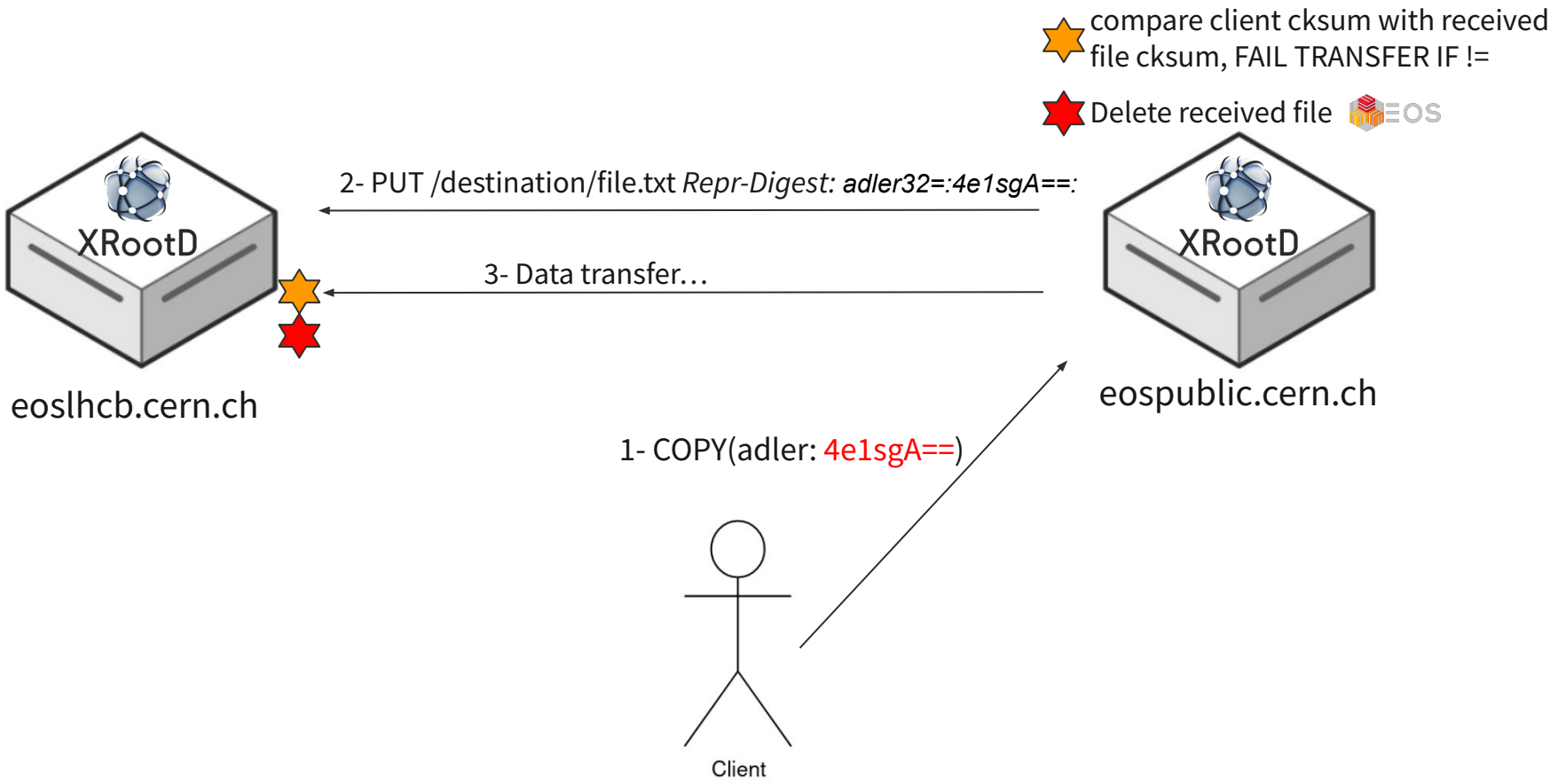



```
curl -X COPY -H 'Destination: https://eoslhcb.cern.ch/destination/file.txt' -H 'Repr-Digest: adler32=:4e1sgA==:'
https://eospublic.cern.ch/source/file.txt
```

image: Flaticon.com

WLCG data integrity check - HTTP TPC

PUSH

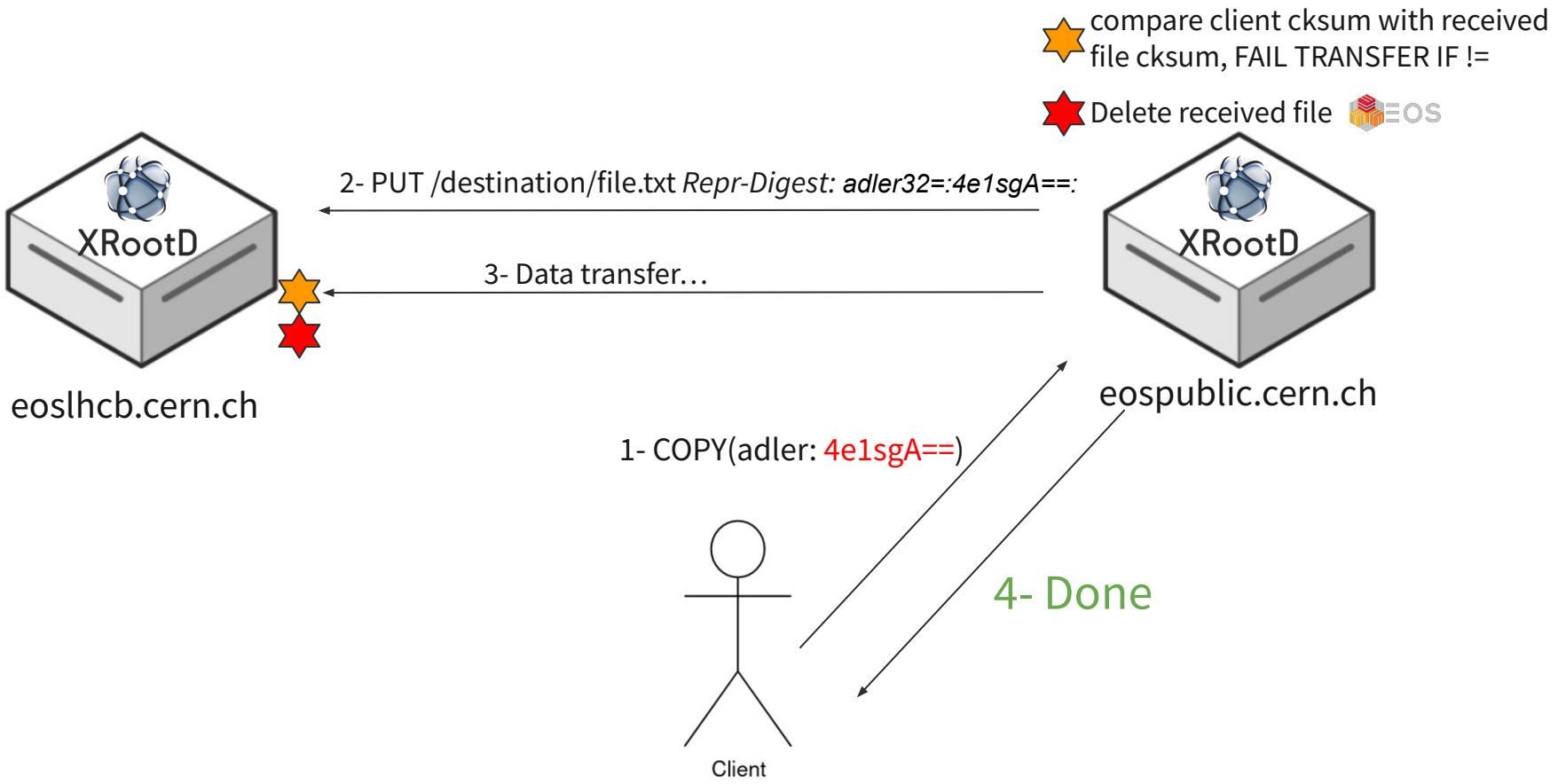



```
curl -X COPY -H 'Destination: https://eoslhcb.cern.ch/destination/file.txt' -H 'Repr-Digest: adler32=:4e1sgA==:'
https://eospublic.cern.ch/source/file.txt
```

image: Flaticon.com

WLCG data integrity check - HTTP TPC

PUSH

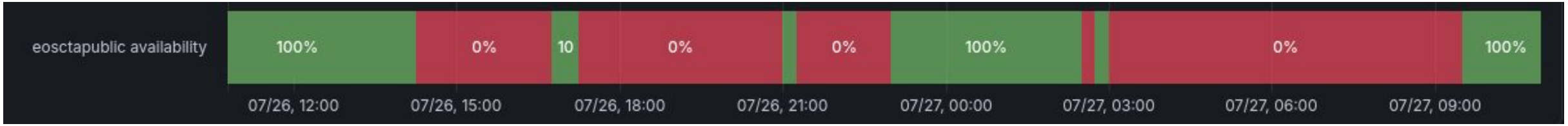


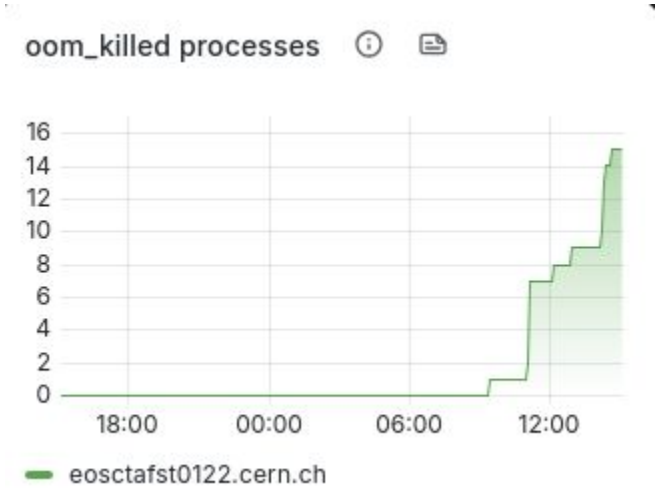

```
curl -X COPY -H 'Destination: https://eoslhcb.cern.ch/destination/file.txt' -H 'Repr-Digest: adler32=:4e1sgA==:'
https://eospublic.cern.ch/source/file.txt
```

image: Flaticon.com

After RUN 3 was over…

Production EOSCTA instance degradation





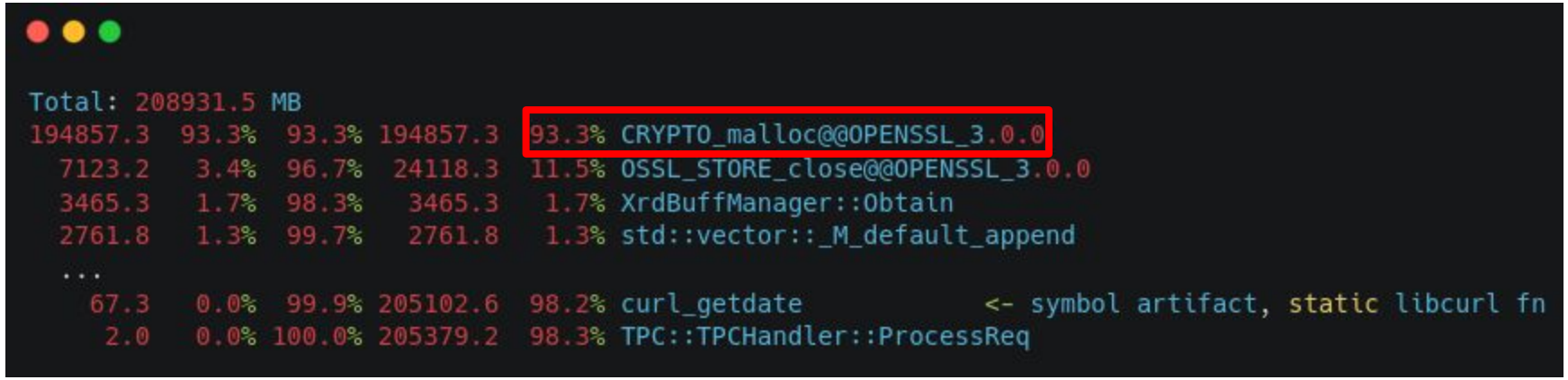
Production EOSCTA instance degradation

Jemalloc profiling from an affected server

```
Total: 208931.5 MB
194857.3  93.3%  93.3% 194857.3  93.3% CRYPTO_malloc@@OPENSSL_3.0.0
  7123.2   3.4%  96.7%  24118.3  11.5% OSSL_STORE_close@@OPENSSL_3.0.0
  3465.3   1.7%  98.3%   3465.3   1.7% XrdBuffManager::Obtain
  2761.8   1.3%  99.7%   2761.8   1.3% std::vector::_M_default_append
  ...
    67.3   0.0%  99.9% 205102.6  98.2% curl_getdate           <- symbol artifact, static libcurl fn
     2.0   0.0% 100.0% 205379.2  98.3% TPC::TPCHandler::ProcessReq
```

Production EOSCTA instance degradation

Jemalloc profiling from an affected server



```
Total: 208931.5 MB
194857.3  93.3%  93.3% 194857.3  93.3% CRYPTO_malloc@@OPENSSL_3.0.0
  7123.2   3.4%  96.7%  24118.3  11.5% OSSL_STORE_close@@OPENSSL_3.0.0
  3465.3   1.7%  98.3%   3465.3   1.7% XrdBuffManager::Obtain
  2761.8   1.3%  99.7%   2761.8   1.3% std::vector::_M_default_append
  ...
    67.3   0.0%  99.9% 205102.6  98.2% curl_getdate            <- symbol artifact, static libcurl fn
     2.0   0.0% 100.0% 205379.2  98.3% TPC::TPCHandler::ProcessReq
```

What is going on?

What is going on?

Especially, why now?

- No such issue during Run3…

What is going on?

Especially, why now?

- No such issue during Run3…

Claude to the rescue…

What is going on?

Especially, why now?

- No such issue during Run3…

Claude to the rescue…

- "Have a look at the XRootD HTTP TPC code and that jemalloc trace, tell me what makes this memory increase."

What is going on?

The cause identified by Claude

XRootD

What is going on?

The cause identified by Claude

- For each HTTP TPC transfer
  - OpenSSL parses and loads the CRLs into a new X509_Store

What is going on?

The cause identified by Claude

- For each HTTP TPC transfer
  - OpenSSL parses and loads the CRLs into a new X509_Store

BUT, why now?

What is going on?

The cause identified by Claude

- For each HTTP TPC transfer
  - OpenSSL parses and loads the CRLs into a new X509_Store

BUT, why now?

- Claude to the rescue
  - "Write a Python program using libcrypto and load the CA and CRL bundle used by XRootD to perform TLS. Measure the memory footprint of that X509_Store object and project the memory usage of 1000 parallel HTTP TPC transfer"

What is going on?

The cause

```
$ python measure_ca_store.py ./ca_file.pem ./crl_file.pem
input ./ca_file.pem: 0.14 MiB PEM, 82 certs, 0 CRLs
input ./crl_file.pem: 6.61 MiB PEM, 0 certs, 84 CRLs

  store   1: RSS +    38.7 MiB (  38.7 MiB/store)
  store   2: RSS +    77.5 MiB (  38.7 MiB/store)
  store   3: RSS +   116.2 MiB (  38.7 MiB/store)
  store   4: RSS +   154.9 MiB (  38.7 MiB/store)
  store   5: RSS +   193.7 MiB (  38.7 MiB/store)
  store   6: RSS +   232.4 MiB (  38.7 MiB/store)
  store   7: RSS +   271.1 MiB (  38.7 MiB/store)
  store   8: RSS +   309.9 MiB (  38.7 MiB/store)
  store   9: RSS +   348.6 MiB (  38.7 MiB/store)
  store  10: RSS +   387.4 MiB (  38.7 MiB/store)

38.7 MiB per parsed X509_STORE (387.4 MiB for 10)
parsed/PEM ratio: 5.7x

projection: 1000 concurrent single-stream TPC transfers => ~37.8 GiB
```

What is going on?

The cause

- Harica certificate revocation from March 2026 resulted in huge IGTF CRL size (~330k revoked certs)

What is going on?

The cause

- Harica certificate revocation from March 2026 resulted in huge IGTF CRL size (~330k revoked certs)
  - After RUN-3 was just a coincidence…

What is going on?

The cause

- Harica certificate revocation from March 2026 resulted in huge IGTF CRL size (~330k revoked certs)
  - After RUN-3 was just a coincidence…
- More information in
  - https://twiki.cern.ch/twiki/bin/view/LCG/WLCGOpsMeetingWeek260803#Monday

How to fix it?

Claude to the rescue…

- "Fix it, make no mistake"
  - Share one parsed CA/CRL store (X09_Store) across all HTTP-TPC transfers the XRootD server performs

How to fix it?

Confirmation the fix worked

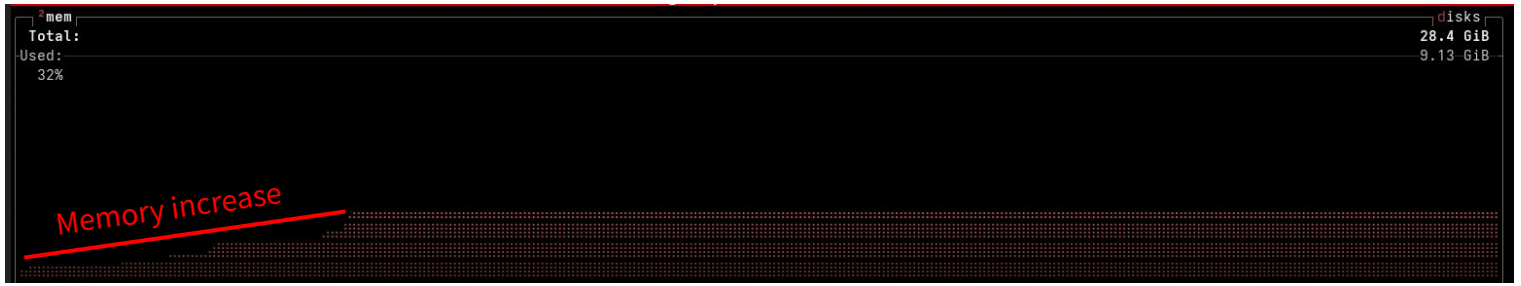
- 100 transfers in parallel on my development VM

How to fix it?

Confirmation the fix worked

- 100 transfers in parallel on my development VM

Before

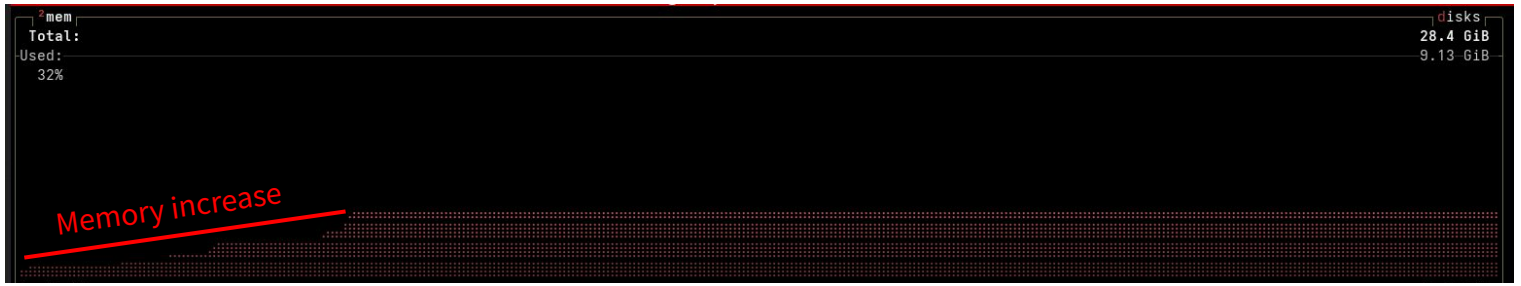


How to fix it?

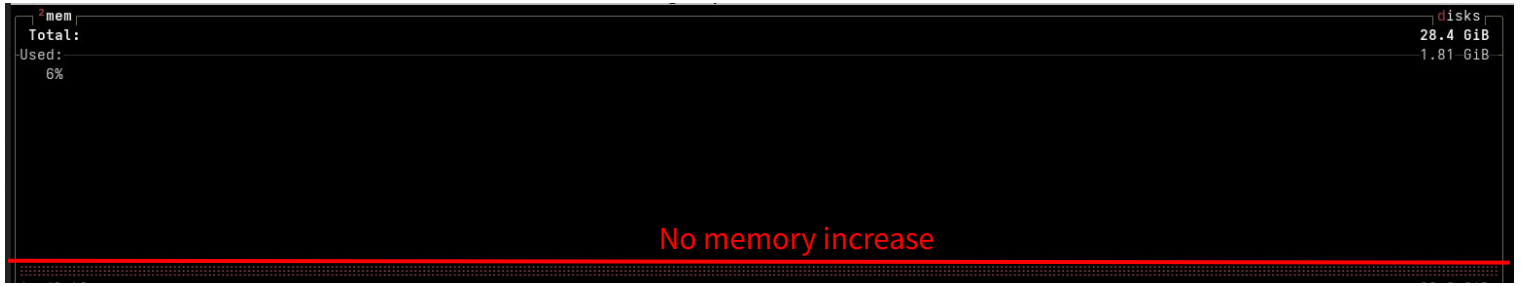
Confirmation the fix worked

- 100 transfers in parallel on my development VM

Before



After



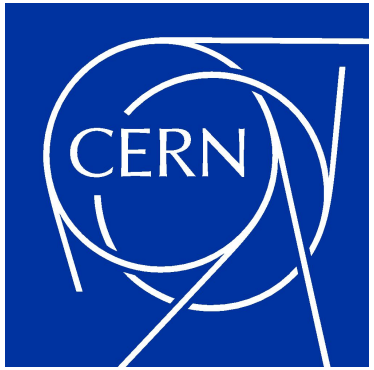
How to fix it?

XRootD version containing the fix

- XRootD >= 5.9.7, XRootD >= 6.1.1

Conclusion

- Publicly-trusted HTTPS gateway
  - New CORS plugin available for XRootD >= 5.9.1
- WLCG data integrity check
  - Repr-Digest and Want-Repr-Digest header support
  - File deletion only supported by EOS
- End-of-RUN 3 EOSCTA issue
  - Fixed in XRootD >= 5.9.7, XRootD >= 6.1.1
- **Any wish for future HTTP and HTTP-TPC improvements?**



home.cern

Backup slides