Table of Contents

CMS WebDAV protocol: Installation and Testing....1
Installation (for admins)....1
Testing (for admins)....1
1. Testing that the endpoint supports https access....1
1.1 Write....1
1.2 Read....1
1.3 Third Party Copy (TPC)....1
2. Testing that the endpoint supports tokens....1
2.1 Request and decode a Token....1
2.2 Write with a token....2
2.3 Read with a token....2
2.4 Third Party Transfer with a token....2
References....2

CMS WebDAV protocol: Installation and Testing

Installation (for admins)

WebDAV is ssuported by different storage systems. Please follow links to get instructions for WebDAV installation according to your storage system:

- **XRootD** [>= v4.10.0] CMS WebDAV/TPC setup instructions
- **dCache** [>= v5.2] WLCG DOMA WebDAV/TPC config instructions
- **DPM** [>= v1.14] WLCG DOMA WebDAV/TPC config information, WLCG DPM upgrade task force
- **EOS** [>= v4.6.8] WebDAV/TPC config instructions
- **StoRM** [>= v1.3.1] WebDAV/TPC installation and configuration instructions
- **ECHO** (and probably other CEPH based storage) [xrootd >= v5.1]

Once installed and configured, you can test by yourself the new endpoint with the following instructions.

Testing (for admins)

In the following we list 7 commands that should be used to progressively test the capabilities of a WebDAV endpoint.

N.B. in all cases --cacert and -E should point to a file with an X509 proxy with cms attribute. Also, please make sure you have read/write permissions on the endpoint and path you are attempting to use

1. Testing that the endpoint supports https access

1.1 Write

```
curl -v -L --capath /etc/grid-security/certificates/  -H 'X-No-Delegate:true' -H 'Credential: non
```

1.2 Read

```
curl -v -L --capath /etc/grid-security/certificates/  -H 'X-No-Delegate:true' -H 'Credential: non
```

1.3 Third Party Copy (TPC)

```
curl -v -L --capath /etc/grid-security/certificates/ -H  X-No-Delegate:true  -H  Credential: none
```

2. Testing that the endpoint supports tokens

2.1 Request and decode a Token

```
curl -L --capath /etc/grid-security/certificates/  -H  X-No-Delegate:true  -H  Credential: none'
```

Depending on the token format returned you can use one of the following tools to decode the token:

Scitokens are composed of 3 strings separated by dots. To decode paste the token in the encoded box in the following link: https://demo.scitokens.org/

Example of a scitoken:

```
eyJhbGciOiJIzI1NiJ9.eyJhdWQiOiJodHRwczpcL1wvMC4wLjAuMDo4NDQzIiwic3ViIjoiREM9Y2gsREM9Y2VybixPVT1Pc
```

Macaroons are a single string to decode paste the macaroon in the Verify - Input macaroon section of the following link: http://macaroons.io/

```
MDAxOGxvY2F0aW9uIFQyX1VTX1VDU0QKMDAzNGlkZW50aWZpZXIgNzUyOGE3OGUtZWM1MC00NGU4LThjYjQtNmM3YTZlNzEzZ
```

2.2 Write with a token

```
curl -v -L --capath /etc/grid-security/certificates/ -H X-No-Delegate:true -H Credential: none
```

2.3 Read with a token

```
curl -L --capath /etc/grid-security/certificates/ -H X-No-Delegate:true -H Credential: none
```

2.4 Third Party Transfer with a token

```
curl -v -L --capath /etc/grid-security/certificates/ -H X-No-Delegate:true -H Credential: none
```

References

1. Set Rucio from Gitlab
https://github.com/dmwm/CMSRucio/blob/master/docker/CMSRucioClient/scripts/setRucioFromGitlab

1. Diego Davila s fork: https://github.com/ddavila0/CMSRucio/tree/add_webDAV

-- Main.FelipeLeonardoGomezCortes - 2021-09-29

This topic: Sandbox > CMSWebDAVProtocolInstallationAndTesting
Topic revision: r5 - 2021-11-02 - FelipeLeonardoGomezCortes