WebDAV access on Public dCache

Dmitry Litvintsev *(DMS/DMD)*

March 22, 2013

Abstract

Public dCache (FNDCA) serves data to Fermilab and world-wide user community. It provides several I/O protocols, such as `gridftp`, `ftp` (GSS authenticated and password authenticated), `dcap` ("plain", GSS and GSI authenticated). Currently WAN access it predominantly via `griftp`. As one of its strategic goals dCache collaboration pursues adoption of standard and widely used I/O protocols such as HTTP and NFS. This brief node describes functionality of WebDAV door that implements certificate authenticated access to the data via HTTP(s) protocol.

1 WebDAV

Web Distributed Authoring and Versioning (WebDAV) is an extension of the Hypertext Transfer Protocol (HTTP) that allows users to create and modify web content. Many operating systems provide built-in client support for WebDAV.

dCache [1] implements WebDAV [2] server as dCache door running on port 2880. dCache door is an I/O protocol translator that provides access to the data stored in dCache. dCache WebDAV door can be accessed by users having DOE or KCA certificates loaded in their browsers or using standard Linux clients like `wget`, `curl`. WebDAV content can be mounted via using the `davfs2` and the `fuse` system modules, KDE has native WebDAV support. This enables Dolphin, Konqueror. and every other KDE application to interact directly with WebDAV servers. All applications using GIO, including Nautilus, have access to WebDAV through GVFS.

2 Security

To limit access to data, dCache comes with an authentication and authorization interface called gPlazma. gPlazma is an acronym for Grid-aware PLuggable AuthorZation Manage-

ment.

A user connects to a WebDAV door and logins with credentials that prove user identity. These credentials are X.509 certificates. The door collects the credential information from the user and sends a login request to gPlazma service. Within gPlazma the configured plug-ins try to verify the user identity and determine access rights. From this a response is created that is then sent back to the door and added to the entity representing the user in dCache. This entity is called subject. GPlazma service running on Public dCache at Fermilab is configured to perform authorization via callouts to GUMS server with a fallback to `decache.kpwd` file. GUMS server performs user DN to username mapping. Mapping of username to local UID/GID plus user root and home directory is captured in `storage-authzdb` file.

The authentication/authorization procedure is uniform across all I/O protocols supported by dCache (with the exception of anonymous dcap and ftp access).

The WebDAV door is configured to use authenticated HTTP (HTTPS) protocol with jglobus authentication module that requires users to provide X.509 certificate during login procedure. Similarly to FTP, the WebDAV door uses user root directory extracted from `storage-authzdb` file to effectively `chroot` to it, thus exposing only files/directories belonging to this user only.

3 Data Access

3.1 Access using browser

To access data read only user needs to direct a web browser to `https://fndca4a.fnal.gov:2880`. DOE grid or KCA certificate need to be loaded in the browser. It is possible to browse namespace and download data. It is not possible to upload the data.

3.2 Using `curl` to access the data

User needs to generate grid certificate proxy like so:

```
$ grid-proxy-init
Your identity: /DC=org/DC=doegrids/OU=People/CN=Dmitry Litvintsev 257737
Enter GRID pass phrase for this identity:
Creating proxy ..................................... Done
Your proxy is valid until: Tue Feb 12 04:37:20 2013
```

Use the following `curl` command to put/get data using WebDAV door:

```
# example of put:

$ curl  -L --capath /etc/grid-security/certificates \
  --cert /tmp/x509up_u8637  -T /etc/fstab
  https://fndca4a.fnal.gov:2880/fermigrid/volatile/fermilab/litvinse/curl.txt
# example of get

$ curl  -L --capath /etc/grid-security/certificates
  --cert /tmp/x509up_u8637 \
  https://fndca4a.fnal.gov:2880/fermigrid/volatile/fermilab/litvinse/curl.txt\
   -o curl1.txt
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1266  100  1266    0     0   4487      0 --:--:-- --:--:-- --:--:--  4487
```

In this example GUMS mapped my DN to username `fgtest` which is mapped to local user with the following login record (as extracted from `storage-authzdb`):

```
authorize fgtest read-write 13160 9767 / /pnfs/fnal.gov/usr/fermigrid/volatile/fermilab \
/pnfs/fnal.gov/usr/fermigrid/volatile/fermilab
```

WebDAV service is setup to build paths relative to system root directory (`/pnfs/fnal.gov/usr`).

4 Request for WebDAV Service

Existing public dCache users can just start using WebDAV service. Any new users added to the system can use the WebDAV service without any additional administrative steps.

5 Administrative Support

The configuration of WebDAV door has been setup by DMD and is captured in so called dCache configuration RPM.

6 Operational Support

Operating WebDAV door is similar to operating GSI dcap or FTP doors. It requires presence of grid host certificate and standard CRL infrastructure usually available in `/etc/grid-security` directory.

7 Conclusion

Public dCache at Fermilab provides certificate based web access to the experiments' data via WebDAV door running on `https://fndca4a.fnal.gov:2880`.

References

[1] `http://www.dcache.org`

[2] `http://en.wikipedia.org/wiki/WebDAV`

[3] `http://www.dcache.org/manuals/index.shtml`

[4] `http://savannah.nongnu.org/projects/davfs2`