Open ID Connect for dCache

Configuration to Support OIDC Authentication in dCache

Christian Voss
Hamburg, 13th January 2020

HELMHOLTZ RESEARCH FOR GRAND CHALLENGES

DESY.

Requirements to Support for OIDC

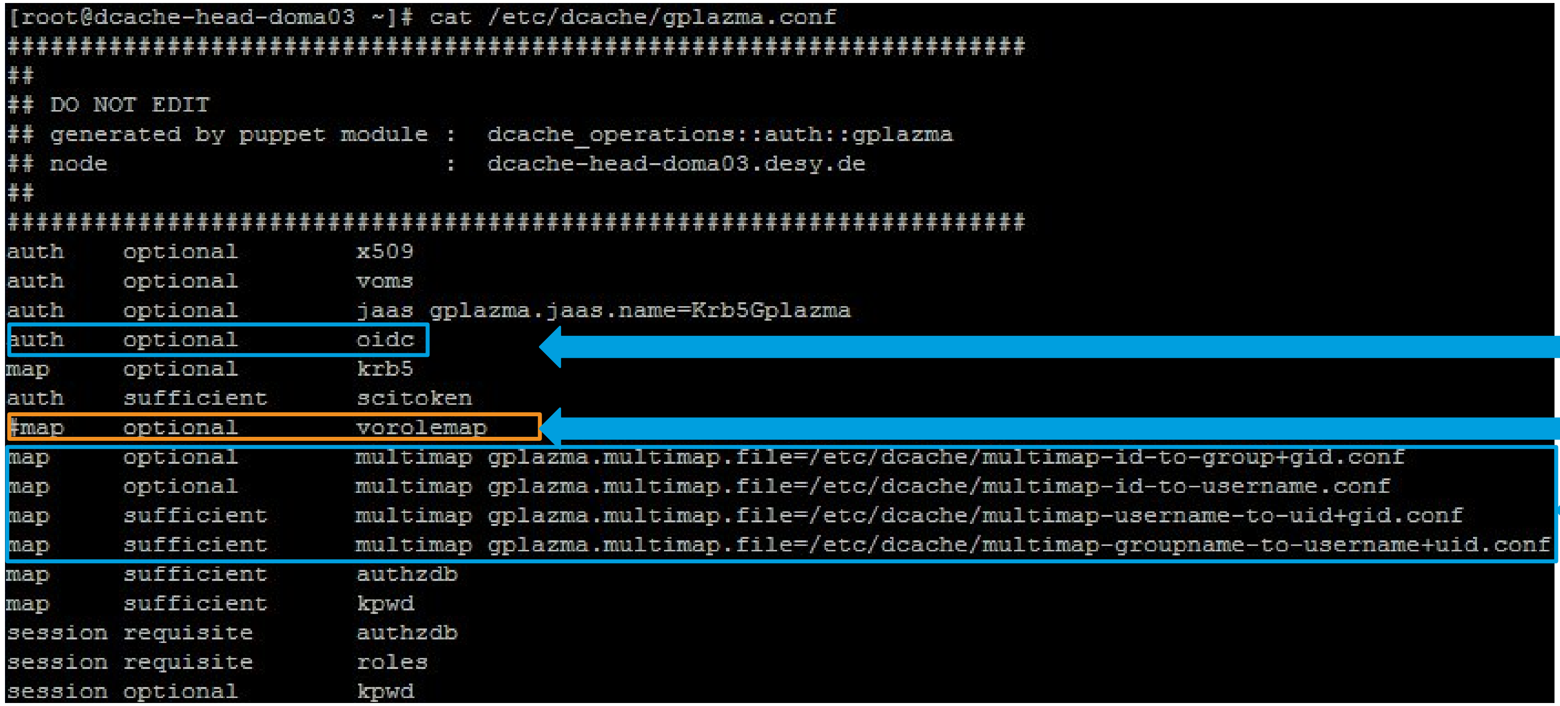
Release and Services of dCache

- Running dCache installation
- Suggest: latest feature release 6.0 (continued fixes to OIDC plug-in and user mapping)
- Required services:
  - gPlazma with specific configuration
  - Dedicated WebDav door
  - Frontend optional
  - Pools to store data
- Browser-friendly host certificates recommended ➡ avoid security exceptions handling in browser
  - Installed on WebDav Doors
  - Installed on dCache Pools

Enable OIDC Support in gPlazma

Introduction to multimap and OIDC Plug-ins in dCache

- Dedicated OIDC plugin for authenticating
- For Mapping use `multimap` plug-in: map many different credentials to dCache `uid` and `gid`
- Changes to `gPlazma.conf` file



```
[root@dcache-head-doma03 ~]# cat /etc/dcache/gplazma.conf
######################################################################
##
## DO NOT EDIT
## generated by puppet module :  dcache_operations::auth::gplazma
## node                      :  dcache-head-doma03.desy.de
##
######################################################################
auth    optional        x509
auth    optional        voms
auth    optional        jaas gplazma.jaas.name=Krb5Gplazma
auth    optional        oidc
map     optional        krb5
auth    sufficient      scitoken
#map    optional        vorolemap
map     optional        multimap gplazma.multimap.file=/etc/dcache/multimap-id-to-group+gid.conf
map     optional        multimap gplazma.multimap.file=/etc/dcache/multimap-id-to-username.conf
map     sufficient      multimap gplazma.multimap.file=/etc/dcache/multimap-username-to-uid+gid.conf
map     sufficient      multimap gplazma.multimap.file=/etc/dcache/multimap-groupname-to-username+uid.conf
map     sufficient      authzdb
map     sufficient      kpwd
session requisite       authzdb
session requisite       roles
session optional        kpwd
```

Enable `oidc` authentication plugin

Replacing usual `vorolemap` plug-in

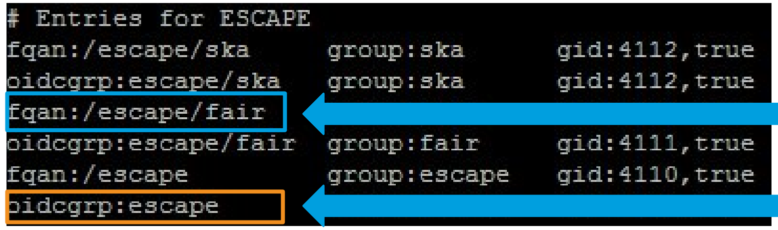
Configuring `multimap` plug-in

Setting up the Different Mutlimap Files

Mapping incoming OIDC Credentials of Well Known to Internal Users

- Some users well known to the local admin

1. Map incoming credentials to groups: `multimap-id-to-group+gid.conf`



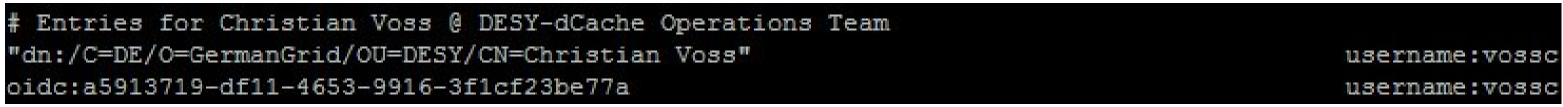
```
# Entries for ESCAPE
fqan:/escape/ska       group:ska        gid:4112,true
oidcgrp:escape/ska     group:ska        gid:4112,true
fqan:/escape/fair
oidcgrp:escape/fair    group:fair       gid:4111,true
fqan:/escape           group:escape     gid:4110,true
oidcgrp:escape
```

Mapping normal proxy *fqan*

Mapping OIDC group contained in token

- Map to group called escape with group-id 4110
- *true* indicates primary group

2. Map well known individual user credentials: `multimap-id-to-username.conf`

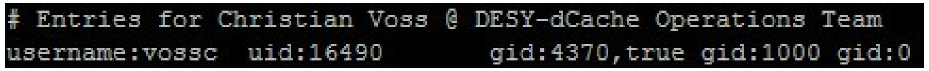


```
# Entries for Christian Voss @ DESY-dCache Operations Team
"dn:/C=DE/O=GermanGrid/OU=DESY/CN=Christian Voss"                       username:vossc
oidc:a5913719-df11-4653-9916-3f1cf23be77a                               username:vossc
```

Mapping proxy *dn*

Mapping *oidc* token

3. Map dCache internal user to user-id: `multimap-username-to-uid+gid.conf`



```
# Entries for Christian Voss @ DESY-dCache Operations Team
username:vossc  uid:16490       gid:4370,true gid:1000 gid:0
```

My DESY user-id

DESY grid group-id

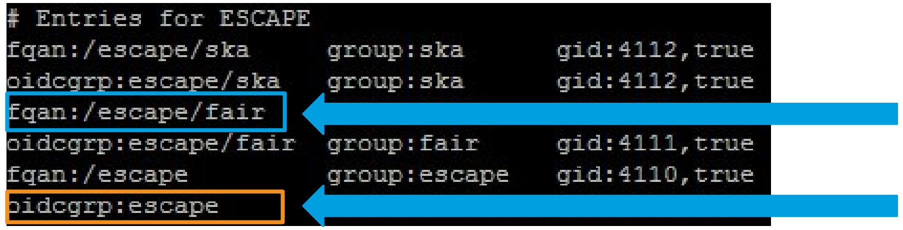
DESY additional group-ids

Setting up the Different Mutlimap Files

Mapping incoming OIDC Credentials of Unknown Users to Internal Users

- Not all incoming users known to local admin ➡configure default fallback users

1. Map incoming credentials to groups: `multimap-id-to-group+gid.conf`



```
# Entries for ESCAPE
fqan:/escape/ska      group:ska       gid:4112,true
oidcgrp:escape/ska    group:ska       gid:4112,true
fqan:/escape/fair
oidcgrp:escape/fair   group:fair      gid:4111,true
fqan:/escape          group:escape    gid:4110,true
oidcgrp:escape
```

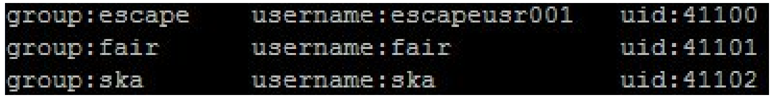
Mapping normal proxy *fqan*

Mapping OIDC group contained in token

   - Map to group called escape with group-id 4110
   - `true` indicates primary group

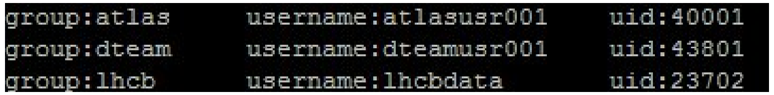
2. None of the specific users will match

3. Map to dCache internal default user-id: `multimap-groupname-to-username+uid.conf`



```
group:escape      username:escapeusr001    uid:41100
group:fair        username:fair            uid:41101
group:ska         username:ska             uid:41102
```

   - Anyone mapped to group `escape` handled as user `escapeusr001`
   - Similar approach to mapping VO users

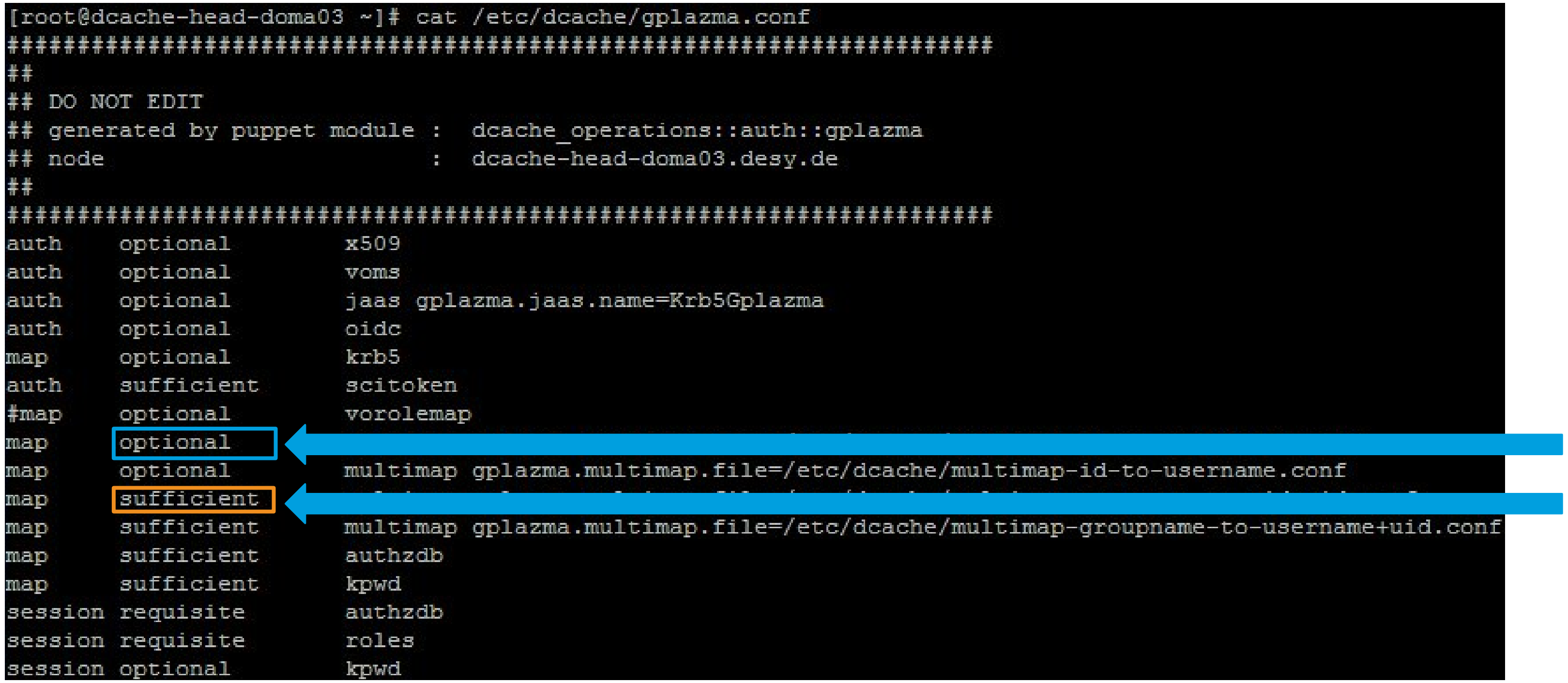


```
group:atlas      username:atlasusr001    uid:40001
group:dteam      username:dteamusr001    uid:43801
group:lhcb       username:lhcbdata       uid:23702
```

Assure User Mapping and Granting Access

Step Back to `gPlazma` Configuration and `/etc/grid-security/storage-authzdb`

- Assure well known mapping is not overwritten by default users

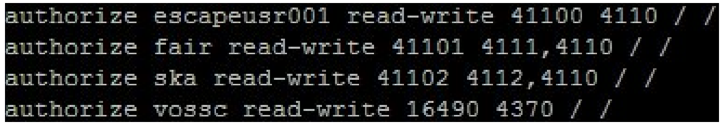


```
[root@dcache-head-doma03 ~]# cat /etc/dcache/gplazma.conf
######################################################################
##
## DO NOT EDIT
## generated by puppet module :  dcache_operations::auth::gplazma
## node                       :  dcache-head-doma03.desy.de
##
######################################################################
auth     optional        x509
auth     optional        voms
auth     optional        jaas gplazma.jaas.name=Krb5Gplazma
auth     optional        oidc
map      optional        krb5
auth     sufficient      scitoken
#map     optional        vorolemap
map      optional
map      optional        multimap gplazma.multimap.file=/etc/dcache/multimap-id-to-username.conf
map      sufficient
map      sufficient      multimap gplazma.multimap.file=/etc/dcache/multimap-groupname-to-username+uid.conf
map      sufficient      authzdb
map      sufficient      kpwd
session requisite        authzdb
session requisite        roles
session optional         kpwd
```

`optional` continues mapping

`sufficient` finishes mapping

- Configure write access: necessary entries in `/etc/grid-security/storage-authzdb`



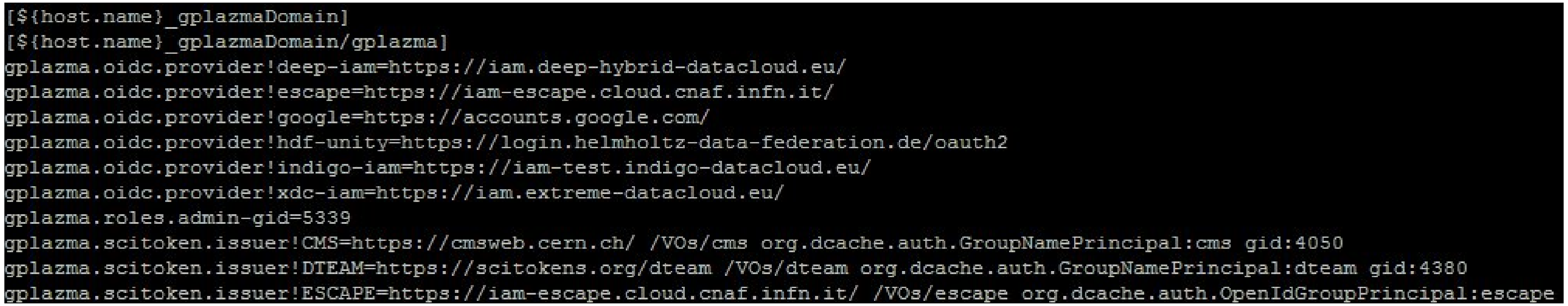
```
authorize escapeusr001 read-write 41100 4110 / /
authorize fair read-write 41101 4111,4110 / /
authorize ska read-write 41102 4112,4110 / /
authorize vossc read-write 16490 4370 / /
```

  - Similar to mapping VO users before

Configuring Layout Files

Setup `gPlazma` Configuration in `/etc/dcache/layouts/`

- Need to configure OIDC plug-in



```
[${host.name}_gplazmaDomain]
[${host.name}_gplazmaDomain/gplazma]
gplazma.oidc.provider!deep-iam=https://iam.deep-hybrid-datacloud.eu/
gplazma.oidc.provider!escape=https://iam-escape.cloud.cnaf.infn.it/
gplazma.oidc.provider!google=https://accounts.google.com/
gplazma.oidc.provider!hdf-unity=https://login.helmholtz-data-federation.de/oauth2
gplazma.oidc.provider!indigo-iam=https://iam-test.indigo-datacloud.eu/
gplazma.oidc.provider!xdc-iam=https://iam.extreme-datacloud.eu/
gplazma.roles.admin-gid=5339
gplazma.scitoken.issuer!CMS=https://cmsweb.cern.ch/ /VOs/cms org.dcache.auth.GroupNamePrincipal:cms gid:4050
gplazma.scitoken.issuer!DTEAM=https://scitokens.org/dteam /VOs/dteam org.dcache.auth.GroupNamePrincipal:dteam gid:4380
gplazma.scitoken.issuer!ESCAPE=https://iam-escape.cloud.cnaf.infn.it/ /VOs/escape org.dcache.auth.OpenIdGroupPrincipal:escape
```

- Configure OIDC provider: pick the `iam-escape` option

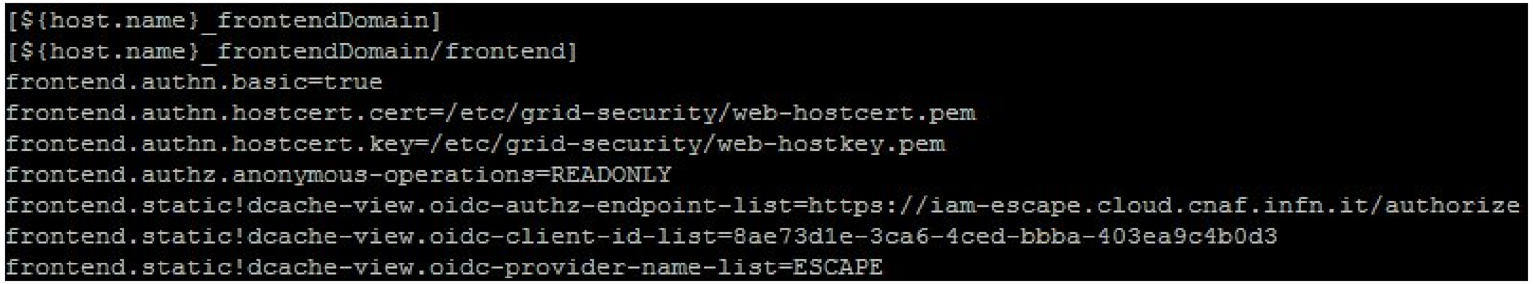
- Completeness: `scitoken` issuer also shown

- Changes require restart of Domain containing the `gPlazma` service

Configuring Layout Files

Setup `Frontend/WebDav` Configuration in `/etc/dcache/layouts/`

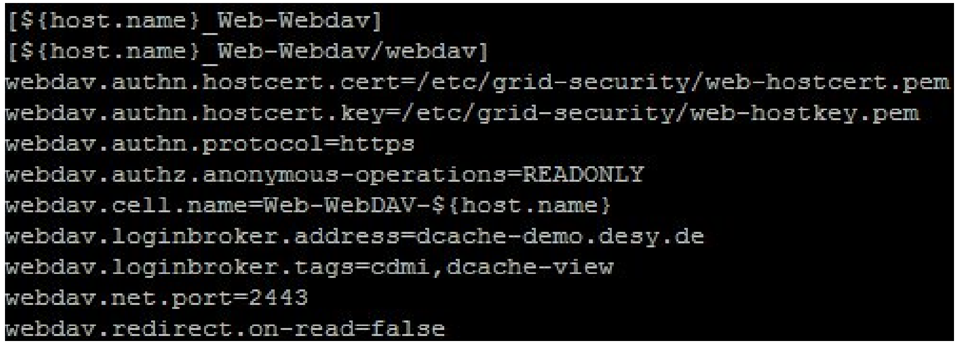
- Need to configure **`Frontend`** to use OIDC endpoint



```
[${host.name}_frontendDomain]
[${host.name}_frontendDomain/frontend]
frontend.authn.basic=true
frontend.authn.hostcert.cert=/etc/grid-security/web-hostcert.pem
frontend.authn.hostcert.key=/etc/grid-security/web-hostkey.pem
frontend.authz.anonymous-operations=READONLY
frontend.static!dcache-view.oidc-authz-endpoint-list=https://iam-escape.cloud.cnaf.infn.it/authorize
frontend.static!dcache-view.oidc-client-id-list=8ae73d1e-3ca6-4ced-bbba-403ea9c4b0d3
frontend.static!dcache-view.oidc-provider-name-list=ESCAPE
```

- Need to register **`Frontend`** service as a client with ESCAPE `IAM`

- Provide path to browser-friendly host certificates similar for the associated **`WebDav`** door



```
[${host.name}_Web-Webdav]
[${host.name}_Web-Webdav/webdav]
webdav.authn.hostcert.cert=/etc/grid-security/web-hostcert.pem
webdav.authn.hostcert.key=/etc/grid-security/web-hostkey.pem
webdav.authn.protocol=https
webdav.authz.anonymous-operations=READONLY
webdav.cell.name=Web-WebDAV-${host.name}
webdav.loginbroker.address=dcache-demo.desy.de
webdav.loginbroker.tags=cdmi,dcache-view
webdav.net.port=2443
webdav.redirect.on-read=false
```

- Changes require restart of Domain containing the **`Frontend`** and **`WebDav`** services

Thank you