JobSub - Idea #22383

Change superuser behavior to not need VOMS authentication

04/16/2019 10:14 AM - Shreyas Bhat

Status:	New	**Start date:**	04/16/2019
Priority:	Normal	**Due date:**	
Assignee:	Shreyas Bhat	**% Done:**	0%
Category:	JobSub Server RPM	**Estimated time:**	0.00 hour
Target version:	v1.3.4	**Spent time:**	0.00 hour
Stakeholders:			

Description

This is an idea that Kevin Retzke came up with when realizing that, for example, for landscape certs to properly access sandboxes in jobsub, he needed to make sure that he was in every single VO that jobsub supports.

The idea is that a global superuser shouldn't need VOMS to do anything. If they present a cert that FERRY maps to a global superuser, then they should be authenticated to *at least* read files.

I filed this as an idea because it's a major change that needs discussion.

History

#1 - 04/23/2019 10:27 AM - Shreyas Bhat

Log output as an example

```
[22/Apr/2019:10:04:06]  [139982376310528]: jobsub_api.py starting: JOBSUB_INI_FILE:/opt/jobsub/server/conf/job
sub.ini cacheing:False cache_duration:120 seconds
[22/Apr/2019:10:04:06]  [139982376310528:scheddload.py:index] acctgroup=uboone, kwargs={}
[22/Apr/2019:10:04:06]  [139982376310528:condor_commands.py:ui_condor_status_totalrunningjobs] condor_status -
schedd -constraint 'stringListMember(name,"jobsub01.fnal.gov,jobsub02.fnal.gov")&&(supportedvolist=?=Null || s
tringlistimember("uboone",supportedvolist)=?=true)&&!isUndefined(InDownTime) && (InDownTime =!= True)&&(InDown
Time =!= "True") && stringListMember(name,"jobsub01.fnal.gov,jobsub02.fnal.gov")' -af name TotalRunningJobs
[22/Apr/2019:10:07:45]  [139982628067072]: jobsub_api.py starting: JOBSUB_INI_FILE:/opt/jobsub/server/conf/job
sub.ini cacheing:False cache_duration:120 seconds
[22/Apr/2019:10:07:45]  [139982376310528]: jobsub_api.py starting: JOBSUB_INI_FILE:/opt/jobsub/server/conf/job
sub.ini cacheing:False cache_duration:120 seconds
[22/Apr/2019:10:07:45]  [139982376310528:jobsub.py:default_voms_role] default voms role for accel : Analysis
[22/Apr/2019:10:07:45]  [139982376310528:auth.py:wrapper]
[22/Apr/2019:10:07:45]  [139982376310528:auth.py:wrapper] args = (<sandboxes.SandboxesResource object at 0x7f5
02862c8d0>,) kwargs={'acctgroup': 'accel', 'user_id': 'tropin', 'job_id': '18652252.0@jobsub02.fnal.gov', 'fil
e_id': 'lbnf2019-apex.sh_20190421_040136_2385450_0_1_cluster.18652252.132.out'}
[22/Apr/2019:10:07:45]  [139982376310528:auth.py:wrapper] request method=GET
[22/Apr/2019:10:07:45]  [139982376310528:auth.py:wrapper] DN: /DC=org/DC=incommon/C=US/ST=IL/L=Batavia/O=Fermi
 Research Alliance/OU=Fermilab/CN=jobview-graphitesrv01.fnal.gov, acctgroup: accel
[22/Apr/2019:10:07:45]  [139982376310528:auth.py:create_voms_proxy] create_voms_proxy: Authenticating DN: /DC=
org/DC=incommon/C=US/ST=IL/L=Batavia/O=Fermi Research Alliance/OU=Fermilab/CN=jobview-graphitesrv01.fnal.gov
[22/Apr/2019:10:07:45]  [139982376310528:auth.py:authenticate] Authentication method precedence: ['ferry']
[22/Apr/2019:10:07:45]  [139982376310528:auth.py:authenticate] Authenticating using method: ferry
[22/Apr/2019:10:07:45]  [139982376310528:auth_ferry.py:authenticate] acctgroup=accel, acctrole=Analysis
[22/Apr/2019:10:07:45]  [139982376310528:authutils.py:json_from_file] checking for /var/lib/jobsub/ferry/vo_ro
le_fqan_map.json
[22/Apr/2019:10:07:45]  [139982376310528:authutils.py:json_from_file] age of /var/lib/jobsub/ferry/vo_role_fqa
n_map.json is 397.629441023
[22/Apr/2019:10:07:45]  [139982376310528:auth_ferry.py:authenticate] fqan=None
[22/Apr/2019:10:07:45]  [139982376310528:authutils.py:json_from_file] checking for /var/lib/jobsub/ferry/fqan_
user_map.json
[22/Apr/2019:10:07:45]  [139982376310528:authutils.py:json_from_file] age of /var/lib/jobsub/ferry/fqan_user_m
ap.json is 397.6242342
[22/Apr/2019:10:07:45]  [139982376310528:authutils.py:json_from_file] checking for /var/lib/jobsub/ferry/dn_us
er_roles_map.json
[22/Apr/2019:10:07:45]  [139982376310528:authutils.py:json_from_file] age of /var/lib/jobsub/ferry/dn_user_rol
es_map.json is 388.222054958
[22/Apr/2019:10:07:45]  [139982376310528:auth_ferry.py:authenticate] ferry mapped dn '/DC=org/DC=incommon/C=US
/ST=IL/L=Batavia/O=Fermi Research Alliance/OU=Fermilab/CN=jobview-graphitesrv01.fnal.gov' fqan 'None' to 'kret
zke'
[22/Apr/2019:10:07:45]  [139982376310528:auth.py:create_voms_proxy] create_voms_proxy: Authorizing user: kretz
ke acctgroup: accel role: Analysis
```

```
[22/Apr/2019:10:07:45]  [139982376310528:auth.py:authorize] Authorizing method precedence: ['ferry']
[22/Apr/2019:10:07:45]  [139982376310528:auth.py:authorize] Authorizing using method: ferry
[22/Apr/2019:10:07:45]  [139982376310528:jobsub.py:default_voms_role] default voms role for accel : Analysis
[22/Apr/2019:10:07:45]  [139982376310528:authutils.py:x509_proxy_fname] Using x509_proxy_name=/var/lib/jobsub/
creds/proxies/accel/x509cc_kretzke_Analysis
[22/Apr/2019:10:07:45]  [139982376310528:authutils.py:needs_refresh] /var/lib/jobsub/creds/proxies/accel/x509c
c_kretzke_Analysis 3600
[22/Apr/2019:10:07:45]  [139982376310528:authutils.py:needs_refresh] /var/lib/jobsub/creds/proxies/accel/x509c
c_kretzke_Analysis does not exist, need to refresh
[22/Apr/2019:10:07:45]  [139982376310528:jobsub.py:should_transfer_krb5cc] group accel is NOT authorized to tr
ansfer krb5 cache
[22/Apr/2019:10:07:45]  [139982376310528:auth_myproxy.py:authorize] /usr/bin/myproxy-logon -n -l "/DC=org/DC=i
ncommon/C=US/ST=IL/L=Batavia/O=Fermi Research Alliance/OU=Fermilab/CN=jobview-graphitesrv01.fnal.gov" -s mypro
xy.fnal.gov -t 24 -o /var/lib/jobsub/tmp/x509cc_kretzke_Analysis_11s10t
[22/Apr/2019:10:07:45]  [139982376310528:auth_myproxy.py:authorize] out= A credential has been received for us
er /DC=org/DC=incommon/C=US/ST=IL/L=Batavia/O=Fermi Research Alliance/OU=Fermilab/CN=jobview-graphitesrv01.fna
l.gov in /var/lib/jobsub/tmp/x509cc_kretzke_Analysis_11s10t.

[22/Apr/2019:10:07:45]  [139982376310528:authutils.py:x509pair_to_vomsproxy] tmp_proxy_fname=/var/lib/jobsub/t
mp/x509cc_kretzke_Analysis_11s10t_mzB1N_
[22/Apr/2019:10:07:45]  [139982376310528:authutils.py:x509pair_to_vomsproxy] /usr/bin/voms-proxy-init -noregen
 -rfc -ignorewarn -valid 24:00 -bits 1024 -voms fermilab:/fermilab/accel/Role=Analysis -out            /var/li
b/jobsub/tmp/x509cc_kretzke_Analysis_11s10t_mzB1N_ -cert /var/lib/jobsub/tmp/x509cc_kretzke_Analysis_11s10t -k
ey /var/lib/jobsub/tmp/x509cc_kretzke_Analysis_11s10t
[22/Apr/2019:10:07:45]  [139982376310528:authutils.py:make_proxy_from_cmd] cmd=/usr/bin/voms-proxy-init -noreg
en -rfc -ignorewarn -valid 24:00 -bits 1024 -voms fermilab:/fermilab/accel/Role=Analysis -out            /var/
lib/jobsub/tmp/x509cc_kretzke_Analysis_11s10t_mzB1N_ -cert /var/lib/jobsub/tmp/x509cc_kretzke_Analysis_11s10t
-key /var/lib/jobsub/tmp/x509cc_kretzke_Analysis_11s10t proxy_fname=/var/lib/jobsub/tmp/x509cc_kretzke_Analysi
s_11s10t tmp_proxy_fname=/var/lib/jobsub/tmp/x509cc_kretzke_Analysis_11s10t_mzB1N_ role=Analysis
[22/Apr/2019:10:07:46]  [139982376310528:authutils.py:make_proxy_from_cmd] failed tb=Traceback (most recent ca
ll last):
  File "/opt/jobsub/server/webapp/authutils.py", line 533, in make_proxy_from_cmd
    cmd_out, cmd_err = subprocessSupport.iexe_cmd(cmd, child_env=env_dict)
  File "/opt/jobsub/server/webapp/subprocessSupport.py", line 87, in iexe_cmd
    exitStatus, stdoutdata, stderrdata))
CalledProcessError: Command '/usr/bin/voms-proxy-init -noregen -rfc -ignorewarn -valid 24:00 -bits 1024 -voms
fermilab:/fermilab/accel/Role=Analysis -out            /var/lib/jobsub/tmp/x509cc_kretzke_Analysis_11s10t_mzB1
N_ -cert /var/lib/jobsub/tmp/x509cc_kretzke_Analysis_11s10t -key /var/lib/jobsub/tmp/x509cc_kretzke_Analysis_1
1s10t' returned non-zero exit status 1:
EXITCODE:1
STDOUT:Your identity: /DC=org/DC=incommon/C=US/ST=IL/L=Batavia/O=Fermi Research Alliance/OU=Fermilab/CN=jobvie
w-graphitesrv01.fnal.gov/CN=1938932606/CN=1849485194
Contacting  voms2.fnal.gov:15001 [/DC=org/DC=incommon/C=US/ST=IL/L=Batavia/O=Fermi Research Alliance/OU=Fermil
ab/CN=voms2.fnal.gov] "fermilab" Failed

Trying next server for fermilab.
Contacting  voms1.fnal.gov:15001 [/DC=org/DC=incommon/C=US/ST=IL/L=Batavia/O=Fermi Research Alliance/OU=Fermil
ab/CN=voms1.fnal.gov] "fermilab" Failed

STDERR:
Error: fermilab: Unable to satisfy B/fermilab/accel:Analysis request!

Error: fermilab: Unable to satisfy B/fermilab/accel:Analysis request!

None of the contacted servers for fermilab were capable
of returning a valid AC for the user.
[22/Apr/2019:10:07:46]  [139982376310528:auth_myproxy.py:authorize] Traceback (most recent call last):
  File "/opt/jobsub/server/webapp/auth_myproxy.py", line 76, in authorize
    x509_tmp_fname, x509_tmp_fname, x509_tmp_fname, acctgroup, acctrole)
  File "/opt/jobsub/server/webapp/authutils.py", line 475, in x509pair_to_vomsproxy
    make_proxy_from_cmd(cmd, proxy_fname, tmp_proxy_fname, role=acctrole)
  File "/opt/jobsub/server/webapp/authutils.py", line 533, in make_proxy_from_cmd
    cmd_out, cmd_err = subprocessSupport.iexe_cmd(cmd, child_env=env_dict)
  File "/opt/jobsub/server/webapp/subprocessSupport.py", line 87, in iexe_cmd
    exitStatus, stdoutdata, stderrdata))
CalledProcessError: Command '/usr/bin/voms-proxy-init -noregen -rfc -ignorewarn -valid 24:00 -bits 1024 -voms
fermilab:/fermilab/accel/Role=Analysis -out            /var/lib/jobsub/tmp/x509cc_kretzke_Analysis_11s10t_mzB1
N_ -cert /var/lib/jobsub/tmp/x509cc_kretzke_Analysis_11s10t -key /var/lib/jobsub/tmp/x509cc_kretzke_Analysis_1
1s10t' returned non-zero exit status 1:
EXITCODE:1
STDOUT:Your identity: /DC=org/DC=incommon/C=US/ST=IL/L=Batavia/O=Fermi Research Alliance/OU=Fermilab/CN=jobvie
w-graphitesrv01.fnal.gov/CN=1938932606/CN=1849485194
Contacting  voms2.fnal.gov:15001 [/DC=org/DC=incommon/C=US/ST=IL/L=Batavia/O=Fermi Research Alliance/OU=Fermil
ab/CN=voms2.fnal.gov] "fermilab" Failed
```

```
Trying next server for fermilab.
Contacting  voms1.fnal.gov:15001 [/DC=org/DC=incommon/C=US/ST=IL/L=Batavia/O=Fermi Research Alliance/OU=Fermil
ab/CN=voms1.fnal.gov] "fermilab" Failed

STDERR:
Error: fermilab: Unable to satisfy B/fermilab/accel:Analysis request!

Error: fermilab: Unable to satisfy B/fermilab/accel:Analysis request!

None of the contacted servers for fermilab were capable
of returning a valid AC for the user.

[22/Apr/2019:10:07:46]  [139982376310528:auth.py:authorize] myproxy authoriziation failed, Error authorizing D
N='/DC=org/DC=incommon/C=US/ST=IL/L=Batavia/O=Fermi Research Alliance/OU=Fermilab/CN=jobview-graphitesrv01.fna
l.gov' for AcctGroup='accel'
[22/Apr/2019:10:07:46]  [139982376310528:auth.py:authorize] Failed to authorize dn '/DC=org/DC=incommon/C=US/S
T=IL/L=Batavia/O=Fermi Research Alliance/OU=Fermilab/CN=jobview-graphitesrv01.fnal.gov' for group 'accel' with
 role 'Analysis' using known authentication methods
[22/Apr/2019:10:07:46]  [139982376310528:auth.py:wrapper] User authorization has failed: Error authenticating
DN='/DC=org/DC=incommon/C=US/ST=IL/L=Batavia/O=Fermi Research Alliance/OU=Fermilab/CN=jobview-graphitesrv01.fn
al.gov' for AcctGroup='accel'
```

#2 - 05/17/2019 01:21 PM - Dennis Box

- Target version set to v1.3.4

- Assignee set to Shreyas Bhat

#3 - 10/03/2019 11:45 AM - Shreyas Bhat

Yesterday, Bruno (coimbra) presented a very interesting problem that has everything to do with this ticket. He was able to look at an egp job's logs when he wasn't a member of the egp group. In this ticket, we note that jobview wasn't authorized to do so, because Kevin Retzke (kretzke) wasn't a member of all the applicable VOs. Why?

Two important pieces of info:

1) Bruno used his own personal CILogon Basic CA cert in his own instance of jobview to authenticate.
2) Above, jobview (Kevin) was using the jobview service cert, which is an Incommon CA cert

The decorator that handles authenticaton/authorization is here:
https://cdcvs.fnal.gov/redmine/projects/jobsub/repository/revisions/v1.2.9.1/entry/server/webapp/auth.py#L273. In line 332, if we're not trying to submit jobs, we try to get the username using the request data or uid_from_client_dn().

This function tries to parse the DN and figure out the username from it. For a service cert (2), that won't work, but it will for a CILogon Basic CA personal cert (1). If it gets a username and the user is a superuser (of any kind), the user is authorized and jobsub doesn't try to get any VOMS credential if it doesn't need to. This was the case for (1).

If the function cannot give a username, then jobsub tries to get a VOMS proxy, and gets the username from there (via whatever the configured auth method is). This brings up another issue, which presented in (2) above. The user kretzke was registered in VOMS to many accounting groups (groups in VOMS). In VOMS, DNs are registered to users, and users are members of groups. There is no connection between a user, DN, and group. However, in FERRY, new DNs are registered to a user *and* group (affiliation unit in FERRY). In the migration to FERRY, any existing DNs registered to kretzke in VOMS were also assigned in FERRY to all groups that kretzke was a part of in VOMS. However, any new DN (like the jobview service cert DN) would only be registered to the group specified at registration time (via the SNOW form), not ALL of kretzke's groups. This is why authorization failed for the jobview DN (the reason this ticket exists).

The proposed fix is as follows: change uid_from_client_dn() (
https://cdcvs.fnal.gov/redmine/projects/jobsub/repository/revisions/v1.2.9.1/entry/server/webapp/request_headers.py#L43) to first check FERRY to get the username.
Pseudo code would be something like this:

```
from auth import authenticate (at the top)

# New signature for func
def uid_from_client_dn(acctgroup=None, acctrole=None):
    uid = None
    cdn = get_client_dn()
    # New code
    uid = authenticate(cdn, acctgroup, acctrole)
    if uid is not None:
        return uid
    # rest of current code in func
```

There's another point that makes this more complicated to troubleshoot due to differences in how FERRY and VOMS register DNs. When FERRY pushes data to VOMS, it uses the affiliation units registered to figure out which VOMS servers to contact. Thus, this is what the FERRY registration (via a pivoted gridmapfile) looks like for the jobview DN:

```
    "/DC=org/DC=incommon/C=US/ST=IL/L=Batavia/O=Fermi Research Alliance/OU=Fermilab/CN=jobview-graphitesrv01.f
nal.gov": {
        "volist": [
            "cdf",
            "dune",
            "des",
            "uboone"
        ],
        "mapped_uname": {
            "default": "kretzke"
        }
    },
```

What is confusing is that, strictly, by FERRY standards, the jobview DN should not be authorized to do anything outside of the four groups in volist. However, because these four groups represent the four VOMS servers, we are guaranteed by this volist that FERRY has registered the jobview DN on each voms server. And since VOMS doesn't care what group a DN is affiliated with, just the user, voms-proxy-init will work for any group that shares a VOMS server with any of the four groups listed. That's why jobview has worked thus far. We're okay with keeping it that way.