Data Sharing Suggestions

We recommend users share data with others on /scratch and /g/data through project memberships.

/scratch/$PROJECT and /g/data/$PROJECT

The scratch and gdata project folders are designed for collaborations within the project. By default the permission is set to 770 with the setgid bit enabled, allowing all project members to read, write and execute, and forcing all future files created inside the folder by default owned by the group $PROJECT. For example, the folder /scratch/xy11 has its permission set to rws for all the project members of xy11.

```
$ ls -ld /scratch/$PROJECT/
drwxrws--- 13 root xy11 16384 Nov 14  2019 /scratch/xy11/
```

Any folder created inside /scratch/$PROJECT by default has its permission set to 755 with the setgid bit enabled. For example, user abc111 has the default project folder on /scratch set to rs.

```
$ ls -ld /scratch/$PROJECT/$USER
drwxr-sr-x 5 abc111 xy11 16384 Jul 14 13:52 /scratch/xy11/abc111
```

By default, it is ready for all members in project xy11 to read and execute and forcing all future files and folders created inside it be owned by project xy11.

If you want to remove the group rx permission of all the files inside your own folder in your default scratch project folder, please run

```
chmod -R g-rx /scratch/$PROJECT/$USER
```

It is also possible to share data with someone outside the project by adding the rule into the access control list (ACL) but it has to be set by NCI admin to allow the access at the project folder level. Please launch a ticket on help.nci.org.au or send us (help@nci.org.au) an email with a short description of why the data has to be shared across projects.

/scratch/public

This folder can be used to share data across projects on /scratch temporarily and data created in /scratch/public is deleted in a week.

Data created in /scratch/public by default is owned by the owner's default project and is debited from that project's storage allocation on /scratch.

```
$ nci-files-report -f scratch -g xy11
------------------------------------------------------------------------------
project     user        space used      file size            count
------------------------------------------------------------------------------
public      abc111            147MB        147MB                    3
...
------------------------------------------------------------------------------
```

The permission is set to world readable by default so that all Gadi users can see the data.

```
$ mkdir /scratch/public/abc111_to_jjj777
$ touch /scratch/public/abc111_to_jjj777/log.log
$ ls -la /scratch/public/abc111_to_jjj777/
total 32
drwxr-xr-x   2 abc111 xy11 16384 Sep  1 14:43 .
drwxrwxrwt. 17 root   root 16384 Sep  1 14:42 ..
-rw-r--r--   1 abc111 xy11     0 Sep  1 14:43 log.log
```

To restrict the access, you can set ACLs to the files. For example, to allow only the user jjj777 to copy the file log.log, remove the access of others first, and then add rX access for jjj777 to the folder abc111_to_jjj777 recursively.

```
$ chmod 700 /scratch/public/abc111_to_jjj777
$ setfacl -Rm u:jjj777:rX /scratch/public/abc111_to_jjj777
$ getfacl /scratch/public/abc111_to_jjj777
getfacl: Removing leading '/' from absolute path names
# file: scratch/public/abc111_to_jjj777
# owner: abc111
# group: xy11
user::rwx
user:jjj777:r-x
group::---
mask::r-x
other::---
```

$HOME

On Gadi, by default, the access permission of home folder $HOME is set to 700, only accessible by the user owns it. For example,

```
$ ls -ld $HOME
drwx------ 44 abc123 xy11 24576 Jul 17 16:46 /home/111/abc111
```

The default 700 permission can be modified, however, we remove group- and/or world-writeable permissions on any home folders once they are detected.

We insist on no writable permissions on any home folders for anyone other than the owner because it contains configuration files for user account and once writable to others, user account can be compromised.