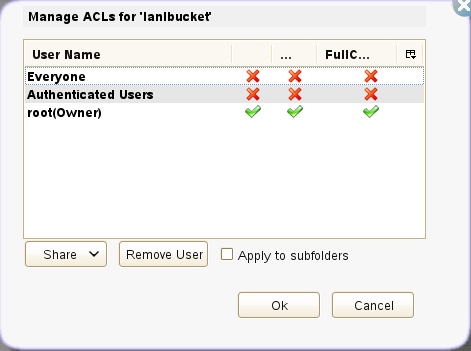
# Object Security

Object security needs to be enforced. However, the objects in the object store may belong to a single Object Store user with actual ownership defined by the GPFS metadata file system. In the ECS ViPR object store, here are the allowed permissions:

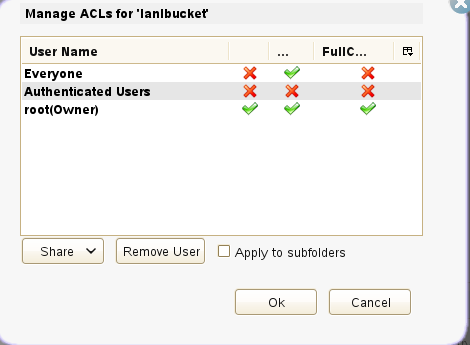


The ACL columns are “read”, “write”, and “Full Control”. If you can read the bucket, you can see what is in there.

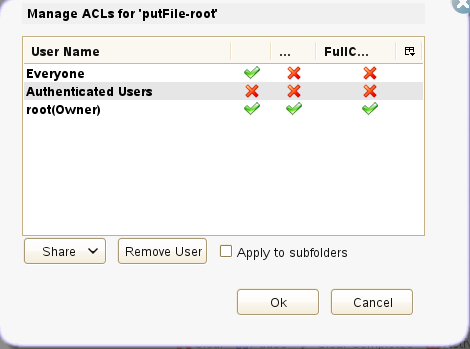
If there is just one user that owns everything it will need “read”, “write”, and “Full Control” to manage the objects’ lifecycle. Once someone knows that user and its object access key, it can just start at the root of the Object Store and walk the tree accessing all objects it owns.

**Try an experiment where I give “write”, but not “read” to Everyone on the bucket and see if we can create objects in there, but not list the contents of the bucket. Give “read”, but not “write” on the object and see if I can list it or cat it, but not change it.**

I changed the ACLs on lanlbucket (owned by root) to allow Everyone to write.



I uploaded a file, putFile-root with the content, “I am root putting this in root's area.”, and made it readable by Everyone.



I tried to list the contents of lanlbucket by root and it succeeds. I tried to list the contents of lanlbucket by [brettk@ccstar.lanl.gov](mailto:brettk@ccstar.lanl.gov) and got this result:

[brettk@rrz-fe1 s3-curl]$ ./s3curl.pl --id=personal -- http://10.140.0.15:9020/lanlbucket

<Error><Code>AccessDenied</Code><Message>Access Denied</Message><Resource>lanlbucket/null</Resource><RequestId>0a8c000f:14bfef55fec:e0d:0</RequestId></Error>

I tried to list the contents of lanlbucket/putFile-root by [brettk@ccstar.lanl.gov](mailto:brettk@ccstar.lanl.gov) and got this result:

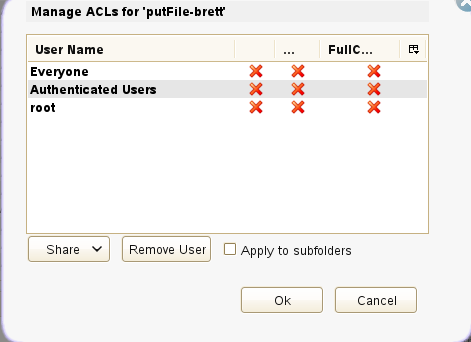
[brettk@rrz-fe1 s3-curl]$ ./s3curl.pl --id=personal -- http://10.140.0.15:9020/lanlbucket/putFile-root

I am root putting this in root's area.

I tried to put a file, putFile-brett, to lanlbucket and got this result:

[brettk@rrz-fe1 s3-curl]$ ./s3curl.pl --id=personal --put=putFile-brett -- http://10.140.0.15:9020/lanlbucket/putFile-brett

Here are the resulting ACLs on that object.



Even though it shows that no one has permissions for anything on this object, I can still list it, so as the one who wrote it, I have access to it even though my username does not show in the ACL list.

[brettk@rrz-fe1 s3-curl]$ ./s3curl.pl --id=personal -- http://10.140.0.15:9020/lanlbucket/putFile-brett

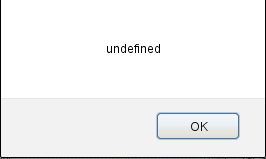
I am brett putting this in root's area.

However, root cannot access it. So, no one else, including root, can access the object even though I wrote it in root’s bucket.

[brettk@rrz-fe1 s3-curl]$ ./s3curl.pl --id=superuser -- http://10.140.0.15:9020/lanlbucket/putFi

<Error><Code>AccessDenied</Code><Message>Access Denied</Message><Resource>lanlbucket/putFile-brett</Resource><RequestId>0a8c000f:14bfef55fec:e1c:5</RequestId></Error>

And, I cannot, as root, change the permissions on the putFile-brett object.



Here’s what you get for metadata on an object to which you have access.

[brettk@rrz-fe1 s3-curl]$ ./s3curl.pl --id=personal --head -- http://10.140.0.15:9020/lanlbucket/putFile-root

HTTP/1.1 200 OK

ETag: "de564ef2f3143c0809d840d284ade65e"

Last-Modified: Fri, 20 Mar 2015 17:25:07 GMT

x-emc-mtime: 1426872307141

Date: Fri, 20 Mar 2015 20:40:26 GMT

Server: ViPR/1.0

x-amz-request-id: 0a8c000f:14bfef55fec:e1f:0

x-amz-id-2: d281f1700bae542f8a34d71be30d12ce79fdc334c96c697d15c28d32e391f241

Content-Length: 39

Content-Type: application/octet-stream

Here’s what you get for metadata on an object to which you do not have access.

[brettk@rrz-fe1 s3-curl]$ ./s3curl.pl --id=personal --head -- http://10.140.0.15:9020/lanlbucket/testfile9

HTTP/1.1 403 Forbidden

Date: Fri, 20 Mar 2015 20:42:01 GMT

x-amz-id-2:

x-amz-request-id: 0a8c000f:14bfef55fec:e20:0

Server: ViPR/1.0

Cache-Control: must-revalidate,no-cache,no-store

Content-Type: text/html;charset=ISO-8859-1

Content-Length: 1287

As root, I tried to delete the object to which only my personal account had access. It succeeded and should not have succeeded.

[brettk@rrz-fe1 s3-curl]$ ./s3curl.pl --id=superuser --delete -- http://10.140.0.15:9020/lanlbucket/putFile-brett

I tried to delete an object to which I only had read access. It succeeded and should not have succeeded.

[brettk@rrz-fe1 s3-curl]$ ./s3curl.pl --id=personal --delete -- http://10.140.0.15:9020/lanlbucket/putFile-root

Can we store a per object password on the metadata of each object in the object store? The object store server would need to know to only accept the password from certain sources.