**MarFS**

**Rational, Design, and Configuration**

**What is it MarFS?**

MarFS provides a near POSIX look and feel file system but under the covers are multiple POSIX file systems to hold file system metadata. Also MarFS allows for data associated with files to be stored in either the POSIX file systems used for metadata or in external object repositories. It provides a global and scalable POSIX name space in that it allows you to map in many POSIX file systems under a single mountpoint. The point of MarFS is, if you are trying to provide a nearly complete POSIX look and feel for users but want to scale out metadata services and data service separately and leverage object stores for the file data including cloud oriented object stores via S3 like interfaces. Data and data movement can scale as N file systems or N object systems and it has features to be “friendly” to object systems by trying to form large multi-megabyte sized objects for efficient storage and tracking.

MarFS is a small amount of code including a very small Linux FUSE daemon, a relatively small parallel batch utility for mass movement into and out of MarFS as well as parallel tree walking of MarFS and other file systems, and a moderate sized library that both the FUSE daemon and the parallel batch tool call into.

The FUSE deamon provides nearly full POSIX access with a few exceptions like update in place discussed below. The parallel batch listing/movement utility is a load balanced, highly parallel utility on one node or across multiple nodes. It can walk the file system tree in parallel of any POSIX file system including MarFS. It can move data between any two POSIX file systems in parallel including MarFS. It can move many small files in parallel or break up big files and move them in parallel to/from any POSIX file system including MarFS.

If files in MarFS are configured to be placed into a POSIX file system, then data is put into the POSIX file system as any file system would work including parallel file systems like GPFS, Lustre, Panasas, etc. The file systems do not have to be parallel though. If files are configured to be stored into an object system, the metadata is stored in a POSIX file system but the data is stored into a configured object storage system. MarFS can put a file per object, pack many small files into one object, and spread a large file across many objects.

MarFS can support quotas for space and number of files in a lazy way using batch utilities to update space used infrequently.

If you are looking for a way to scale metadata service, but not stripe or hash metadata, MarFS might be the answer. If you are looking for a way to provide a very scalable POSIX file system look and feel over multiple POSIX file systems or over one or multiple Object Storage Systems, MarFS might be the answer.

Requirements include:

* Linux system(s) with C/C++ and FUSE support
* The batch utility uses MPI as its parallel communications library, so most any MPI library with a C interface can be used.
* Communications with the MPI library can utilize many communications methods like TCP/IP, Infiniband OFED, etc.
* If you plan to only use MarFS to glue together multiple POSIX file systems into one mount point, any POSIX file systems can be used.
* If you plan on using multi-node parallelism for either the FUSE daemon or the batch utilities, the file systems involved must be globally mounted on all nodes running MarFS FUSE or batch tools. This includes NFS and other global file systems.
* If you plan to store data on an object store, that object store needs to be accessible by all nodes running MarFS software and the POSIX file systems used to store the metadata for MarFS files stored in the object store must be capable of POSIX extended attributes (xattr) and must support sparse files (files that have a non zero size but that occupy no space). (Any file system that supports this can be used but GPFS has some ILM capabilities for managing massive amounts of metadata that helps immensely with batch processing for management of the system.)

**What MarFS is not**

MarFS does not allow users to update files in place for data repositories where update in place is not easy, like object stores. All programs will work unchanged except for programs that seek around in the file and write, append to the end of a file, or try to truncate a file in a place other than zero offset. This means that reading files works pretty much no matter what, but writing had to be done as a complete overwrite. The FUSE daemon enforces writing only serially from byte zero. It is possible to write data to MarFS in parallel by using the batch parallel copy program or by writing your own parallel data movement utility using the library.

MarFS does not fundamentally solve the scalabilty problem of very large single directories. It currently does not hash or split single directories up, it just glues together multiple name spaces into one name space spread across multiple file systems by tree. It would be possible to put a file system under MarFS that does hash single directories, and future MarFS features might include hashed single directories.

MarFS software does not check/lock to protect against multiple non coordinated writers into the same file. The batch utility does safely do muti-writers into a single file as wall as multi-readers in massively parallel but it doesn’t protect against a user using different commands/programs to update the same file concurrently.

MarFS currently is concentrating on providing a best in class scalable metadata service over a best in class scale out object storage system. It does not provide an object interface to the data, but this would be trivial to add as the MarFS metadata maps POSIX files onto Objects. There also is not currently an HDFS interface to MarFS except that MarFS is POSIX and HDFS does have the ability to use POSIX files. Optimization to provide layout information to an HDFS layer would also be trivial to provide and MarFS metadata does have object information for each POSIX file.

MarFS currently does not support file locking but that could be added. MarFS does not support hard links but symbolic links should work. In theory one should be able to mmap and execute off of MarFS, but mmap writing may not work if writing is not serially. MarFS is not really intended for mmap or execution, but what you want to do might work if it behaves relatively well.

MarFS is not intended to replace parallel file systems, as it does have important features missing/not supports on purpose, although it might suffice as a parallel file system in some settings.

MarFS is not intended to replace deep and/or parallel archives like HPSS, although in some settings it might work for that function.

MarFS, if you use an object store for storing data, does require some reconciliation of two systems, although all metadata except for object specific metadata is stored in the MarFS POSIX file sytems that store all the metadata. It is possible for garbage space could be used so infrequent reconciliation might be desired. Further, MarFS does try to minimize areas where truly transactional semantics are needed but does not make any real transactional guarantees. MarFS errs on the side of making it easy to run batch inode scans or tree walks due to the parallelism in the batch utilities and ability to use many POSIX file systems and metadata servers to make for easy management of the metadata/space/etc.

**Why MarFS**

Tools like Cleversafe, Scality, and EMC ViPR are moving towards the data lake concept where data can have multiple personalities including POSIX, Object, and HDFS. These solutions use erasure based disk systems to store the data. These tools are immature at least at this time. These tools may overtake what MarFS is suppose to provide, but for right now, MarFS allows you to use many POSIX metadata servers and one or multiple object stores to independently scale metadata and data service.

It is possible to put Object Storage Systems under scalable file systems like GPFS using a block interface over the Object Storage System, but the block write patterns of these parallel file systems are not well suited for getting the most from these Object Storage Systems. The ability to use any object storage system as a back end storage repo is also a plus for MarFS, as one could use any object store including cloud based services if you wanted to.

There doesnt appear to be other open source projects that provide the needed function exactly. Ceph provides a file system on objects but isn’t known for scaled out metadata service. GlusterFS is probably the closest thing to an alternative and indeed GlusterFS can be a global name space gluing multiple file systems together into one mount point. GlusterFS also hashes the file names across the file systems, which is something MarFS cant do at least right now. The main difference is the approach to what GlusterFS documentation refers to as unified file and object. GlusterFS has been integrated to be object storage for OpenStack Swift (for objects) and storage for OpenStack Cinder (for blocks). MarFS instead puts a POSIX interface over any Object Storage Service including OpenStack Swift. So you can see that MarFS is coming from a bit different angle for unifying file and object services.

Why not use an HSM like HPSS or DMF? These systems currently don’t utilize the enormous investments in industry on object storage. HPSS metadata performance is likely going to be 1/10th or less of a typical MarFS metadata performance. MarFS is open source and a tiny amount of coded compared to HSM’s. In fairness, MarFS is not an HSM, although batch utilities could be written easily to move data around under MarFS to various kinds of storage systems including HPSS, an HSM, LTFS, or other if someone wanted to write such code. Massive parallelism is also not typical of HSM systems like HPSS. MarFS is really designed for dozens to hundreds of metadata servers/name spaces and thousands or even tens of thousands of parallel data movement streams. HPSS is designed for about an order of magnitude less parallelism.

Why not use the General Atomics Nirvana Storage Resource Broker, IRODS, well these things are optimized for wan and hsm metadata rates. There are some capabilities for putting POSIX files over objects, but these methods are largely via NFS or other methods that try to mimic full file system semantics including update in place. These methods are not designed for massive parallelism in a single file, etc. What about other name space solutions? Well Maginatics from EMC is around but it is in its infancy and targeted at enterprise and there is an open source name space project called Camlistore but it appears to be targeted and personal storage.

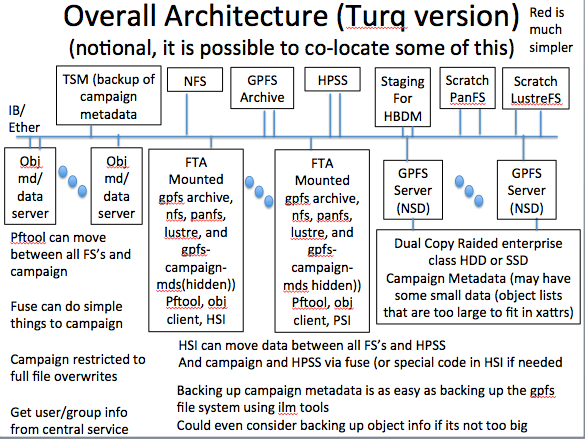
Do other name space solutions exist? Bridgestore is a posix name space over objects but they put their metadata in a flat space so rename of a directory is horribly painful. Avere NFS over objects is focused at NFS so N to 1 is a non starter.

Why not use just an object system without MarFS? MarFS assumes you want a first class POSIX metadata service over your files which a typical object store avoids. MarFS is trying to be the best of both worlds allowing data scaling like an object system, metadata scaling like N POSIX name spaces, with both kinds of access to the same data, the true data lake concept.

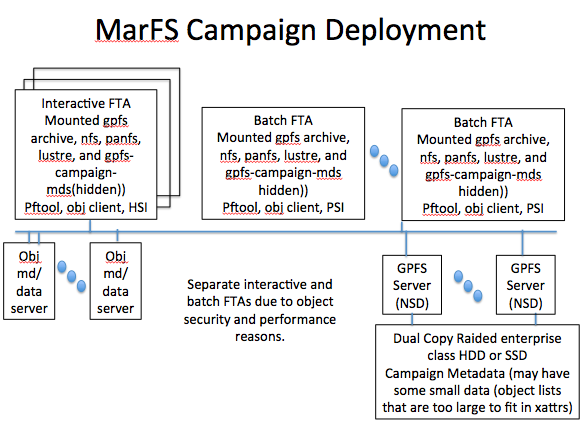
We need an open source piece of software that enables the described function to to deploy in production and to use to set the bar high for fully integrated solutions that provide the data lake multi-personality do data on erasure disk to beat.

**Architecture**

The architecture of MarFS is split into six parts. The FUSE file system that provides the near full POSIX interface to MarFS. The batch parallel listing/movement utility, the POSIX metadata file systems, and the back end storage systems which can be POSIX file systems or object systems. In the diagram below, you can see a very rough concept of how MarFS campaign storage would fit into our Turquoise environment. You can see all the normal services on the top and the MarFS campaign storage on the bottom. The File Transfer Agents (FTAs) are where the FUSE and Batch programs run and where the POSIX metadata file systems are mounted that make up the metadata service for MarFS as well as all the other non MarFS file system mounts to NFS, GPFS Archive, Scratch, etc. The MarFS metadata storage servers (in this case running GPFS NSD) provide very fast parallel metadata file systems for MarFS. The object servers provide a scalable data repository for MarFS files.



A closer look at how MarFS should be deployed is shown below. Notice separate interactive and batch FTA’s are recommended for security reasons and for performance reasons. Since the Object Security model does not match well wit the POSIX security model, it makes sense to not allow users to have access to keys needed to open/control the object stores, so those should be kept on the batch only FTA’s and provided only to the FUSE deamons on the interactive FTA’s using some secure method. The ability to control who can get access to the object servers directly without going through the FUSE daemon must be controlled. Interactive FTA’s would be used for LS, GREP, TAR, etc. These are all small/serial tools that can run by as users gaining access to files through the FUSE daemon which must run as a privileged user for a variety of reasons both management and security related.



How does MarFS work?

MarFS files are created into a POSIX metadata tree (where is determined by configuration) with no special metadata. If the file is to be a normal POSIX file (determined by configuration) then the file can be written and read as normal by the FUSE and batch utilities. Depending on the path, the MarFS file metadata/data will be placed into one of many possible POSIX file systems (determined by configuration). In this way, MarFS is a global name space. Again, files are not hashed across POSIX file systems, the total MarFS namespace is decomposed into separate POSIX file systems by tree (configuration). All normal POSIX ownerships/permission/attributes like dates/sizes/etc. are obeyed. One can even add user supplied xattrs to the files.

If however, you have configured the file data to go to an external object repository (via configuration files), then only the POSIX metadata is stored in the appropriate POSIX file system name space. The difference is, the data is written to objects in the external object data repo instead of into the POSIX file. All normal attributes are kept up to date in semantically reasonable ways like permissions, dates, and even file size. The file size is updated by truncating the POSIX file to the size of the desired file even though there may be no actual bytes/space in the file itself. For this reason the POSIX file systems used for holding file metadata for files that are stored in external object repos must support sparse files. Further, some reserved POSIX xattrs are used associated with the files to point at various config and back end object repo information so that where the data is and how to access it are preserved (in those xattrs). For this reason, the POSIX file system used for metadata for files stored in external object repos must support POSIX xattrs and furthermore, some xattr names are reserved and hidden from the user.

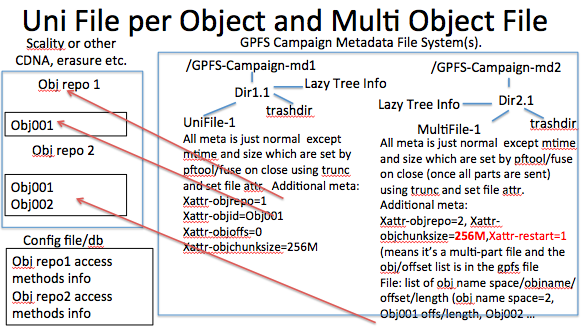
In this design all metadata operations like reading/creating directories, managing ownership, dates, permissions, user xattrs, etc. are all just performed on the POSIX file system being used for metadata (and data for normal non external object repo files). Only operations involving space management for files on external object repos need to be handled differently from just normal POSIX. In these operations, all the POSIX permissions are adhered to and additionally Object permissions are also obeyed based on the operation. Creating, writing, and reading these files with their data in external object repos uses/updates the POSIX attrs and xattrs appropriately to manage the access needed. For special space management operations like truncate and unlink, all references to the space being freed are renamed (in case of an unlink) or copied (in the case of a truncate) to a trash directory which can be used by a batch program for space reclamation from the object server. It does require a batch program to free the objects and clean out the trash. A trash recover utility could easily be written as well if desired.

The FUSE daemons on the interactive FTA nodes allows users to run interactive file system commands but the FUSE daemon has some drawbacks. It can not pack multiple small files into one object, this must be done by a batch program after the fact if written by FUSE. The FUSE daemon enforces no update in place for all files in data repos that do not make update in place easy (like object servers). This means if you want to update a file in place you need to copy it to a full service file system, modify it and put it back. Files can be read in any order of course and all metadata operations should work (chown,chmod,mkdir,etc.) You can only truncate to zero, meaning files have to be completely overwritten, not partially, and right now append is not supported either, but that could be added at some point.

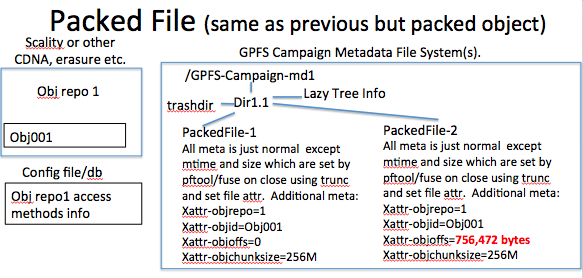
The parallel batch listing/movement utility is a load balanced, highly parallel utility on one node or across multiple nodes. It can walk the file system tree in parallel of any POSIX file system including MarFS. It can move data between any two POSIX file systems in parallel including MarFS. It can move many small files in parallel or break up big files and move them in parallel to/from any POSIX file system including MarFS. It only runs on the batch nodes and users cant not log into the batch nodes. This is for performance isolation and for security, as access to the object repo needs to be controlled to be either in a root owned FUSE daemon or on a non interactive batch only node to protect the object server from being compromised. From an interactive FTA, commands like pcp (parallel copy) and pls (parallel ls) and pcmp (parallel compare) can be used which will run a batch job interactively. Additionally scheduling long running data management tasks through a scheduler should be made possible via normal batch scheduling mechanisms.

There also needs to be a small suite of batch programs for managing the file system. These utilities are needed for counting up space used in a namespace or part of a name space for quota enforcement. Batch utilities for space management/reclaimation/packing/repacking of small files into objects etc. also need to be provided. If GPFS is used as the POSIX metadata file systems for MarFS, the GPFS ILM features that allow for very fast inode shadow table scanning and threaded name merges etc. can be utilized to look through millions of files in minutes to perform these management tasks. These utilities need to be specified at some point and would be easy to add to over time.

In the following diagram, you can see MarFS implemented in cartoon style showing a GPFS POSIX metadata tree that has xattrs pointing at external object repos for a Uni file (one object per file) and a large Multi file (multiple objects per file). In the case of the multi-object file, the list of objects that make up the file are stored in the metadata file (which implies that the chunksize of a large file has to be larger than an objectid), and the amount of real object id data in the metadata file is stored in an xattr so you know how much data is in the metadata file and the rest is just a hole so the size of the metadata file == the size of the file logically.



In the following diagram, you can see MarFS and a depiction of packed file which is where multiple files are packed into one object.



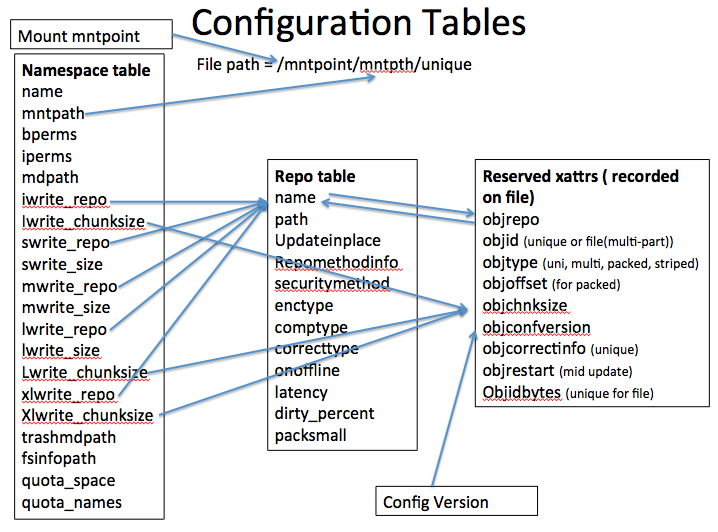
**Configuration File Information**

Much of understanding MarFS is understanding the configuration information.

**Reserved POSIX extended attributes (xattr)**

MarFS utilizes POSIX extended attributes (xattr) to place information about the data repository/objects that hold the data for files. Files are born without extended attributes and only acquire them when the file is written. Xattrs will only exist for files in which the data exists in external data repositories. Therefore, most any POSIX file system can be used for holding metadata and data, but the requirements for storing metadata for files in which data exists in external data repositories require xattr and sparse capabilities because xattrs are used to map to the external data repo and the POSIX size field is used to store the length of the file for files where the data lives in an external repo.

Below are the reserved attributes that are used and their descriptions:



|  |  |
| --- | --- |
| MAR\_objrepo | Records the name of the data repo that the file was written with. This points at an entry in the repo table int the configuration and all attributes about how to retrieve a file except for (objid, objtype, objoffset, objchnksz) are in the data repo entry for this name. This value is initially populated by the repo derived from the namespace configuration table via the path |
| MAR\_objid | Records either the object id in an external data repo where the file data is stored or a special value “file” which indicates that the object id’s that make up the file stored in the metadata file itself at the beginning of the file. The file is truncated to the size of the file, which implies that the object id’s must be smaller than the chunk size for multi-part files (files that are spread across more than one object). |
| MAR\_objtype | Records how the file data is stored in an external object repo, there are currently 4 types:  Uni – one object stores the entire file, object id is in MAR\_objid  Multi – a file is spread across multiple objects using chunk sized objects, object id’s are recorded in the metadata file  Packed – multiple files in each object which requires using the MAR\_objoffset xattr, object id is recorded in MAR\_objid. The chunk size is picked based on if this is interactive or batch and for batch, it is based on the size of the file being moved (large and xlarge) derived from the configuration file.  Striped – a file is striped across multiple objects using chunksize and round robin, object id’s are recorded in metadata file |
| MAR\_objoffset | Records offset into object where file data lives, this is only used in Packed MAR\_objtype (multiple files in one object) |
| MAR\_objchnksz | Records chunk size for multi or striped file, this value is initially populated from the repo configuration table for the file based on namespace/path, chunk size is picked based on if this is interactive or batch and for batch, it is based on the size of the file being moved, (large, xlarge) derived from the configuration file. |
| MAR\_objconfversion | Records the version number of the configuration file, this is used for debugging issues. The expectation is that every change to the configuration file changes the version number and all versions of the configuration files are kept forever, or until all references to name spaces and repos are gone in the metadata and all the referred to objects are reclaimed |
| MAR\_objcorrectinfo | Records a single value for correctness for the file, this is perhaps a CRC or checksum. If this is a multi-part file, this information will be put into the metadata file on a per object id basis |
| MAR\_objrestart | Records that a file is being written, used for batch parallel writing to a file. If the utility wants to use this flag for restart purposes. |
| MAR\_objidbytes | For multi-object files, records the number of bytes in the metadata file that contain objid information (the rest of the file is just a hole to make the size of the metadata file == the size of the file |

mult

**Configuration Information Details**

Mountpoint (there is only one of these)

|  |  |
| --- | --- |
| MAR\_mnttop | This is the top level directory under which all namespaces are placed. Specified as a path with slashes. |

Fuse/pftool will append MAR\_mnttop on the front of all the name space segments below to construct a namespace tree

Example :

MAR\_mnttop = /redsea

MAR\_namespace.mnt.mntpath = /projecta

MAR\_namespace.mnt.mdpath = /md/projecta

MAR\_namespace.mnt.mntpath = /roject

MAR\_namespace.mnt.mdpath = /md/project

User refers to /redsea/projecta and that refers to files metadata file system/namespace in /md/projecta

MAR\_namespace (there is one of these per name space you want to have appear under the mount point above

|  |  |
| --- | --- |
| mntpath | Specifies the path for this namespace, which is appended to the MAR\_mnttop (described above) (specified as a path with slashes) |
| bperms | Specifies permissions for batch programs. These permissions are above and beyond the POSIX permissions (rwx/ugo). This is because external repositories may have special permissions that don’t map exactly to POSIX permissions. The values are rmwmrdwdudtd:  rm – read metadata  wm – write metadata  rd – read data  wd – write data  ud – unlink data  td – truncate data  An example of interesting use is to allow read and write in POSIX permissions, allow metadata changes but not allow writing of data. This value is not stored with the file, it is interpreted real time, so this is a fast way to shut of write of data or metadata etc. This item can change based on allowed activity against this namespace and the data/space it represents. |
| Iperms | Specifies permissions for interactive (FUSE) programs. Same as bperms above. |
| Mdpath | Specifies the path for the POSIX file system that is to hold the metadata and potentially data for this namespace. If a file is to be written to an external repo, then only metadata is stored in this file sytem, but if data is to be stored into this file system then both data and metadata are used. Controlling whether data is written into the metadata file system is done in the repo configuration table using the repomethodinfo field so the repo you are writing to or reading from will be DIRECT (use the metadata file system) or some other external method like CDMI, S3, etc. This is specified using path notation using slashes. This can change if you have moved the metadata file system path for some reason. It might be hard to change on the fly though. |
| Iwrite\_repo | Specifies what repo interactive (FUSE) applications will write new files to, points at a name in the repo table. This can be changed as it just controls where new files are written to. |
| Iwrite\_chunksize | Chunksize for interactive |
| Swrite\_repo | Specifies what repo batch applications will write new small files to, points at a name in the repo table. This can be changed as it just controls where new files are written to. |
| Swrite\_size | Size below which is considered a small file. This can be changed as it just controls where new files are written to. |
| Mwrite\_repo | Specifies what repo batch applications will write new medium files to, points at a name in the repo table. This can be changed as it just controls where new files are written to. |
| Mwrite\_size | Size below which is considered a medium file. This can be changed as it just controls where new files are written to. |
| Lwrite\_repo | Specifies what repo batch applications will write new large files to, points at a name in the repo table. This can be changed as it just controls where new files are written to. |
| Lwrite\_size | Size below which is considered a large file. This can be changed as it just controls where new files are written to. |
| Lwrite\_chunksize | Chunksize for large files |
| xlwrite\_repo | Specifies what repo batch applications will write new xlarge files to, points at a name in the repo table. This can be changed as it just controls where new files are written to. |
| Xlwrite\_chunksize | Chunk size for xlarge files |
| trashmdpath | Specifies where in the namespace, information is stored on unlink and trunc/ftrunc operations, which could provide a trashcan function but is used by batch process for reclaiming space, repacking, reconciliation of space which is needed for external repo’s. All permanent deletion of data (both unlink and trunc) are done in batch for external repos. For “DIRECT” repos where the data is stored directly in the metadata file, unlink operations go to this path, but trunc’d space is not preserved. This is specified as a path with slashes. It is assumed that this is in the same metadata file system as the metadata file system for this name space, as rename is used for unlink operations. This value could change but much care would have to be taken because entries into this path can be occurring all the time and information about reclaimable space lives in this path. |
| fsinfopath | This is a path name specified with slashes to a file that contains the values one would get in a statfs/statvfs call like how much space is in the file system, how much space is used, etc. This file must be updated in a lazy way via periodic batch scans of inode space etc. Since the space for the files in a namespace may not be in the metadata file system associated with a name space, it is required that this info be provided in some way to be chosen by the site. It could involve walking the metadata tree or inode space and adding up spaced used or it could involve querying an external repository for space etc. This value could be change but care needs to be taken as statfs/statvfs calls will look in this file for providing information. |
| quota\_space | Specifies the space quota for this name space. This value is compared to information in the fsinfopath file above about how much space has been used which is populated via lazy batch runs to determine and record space used. This can be changed at any time, but will not take effect immediately as quota’s are done in a lazy way based on batch runs to update the fsinfopath file |
| quota\_name | Specifies the inode quota for this name space. This value is compared to information in the fsinfopath file above about how many inodes have been used which is populated via lazy batch runs to determine and record inodes used. This can be changed at any time, but will not take effect immediately as quota’s are done in a lazy way based on batch runs to update the fsinfopath file |

MAR\_datarepo (there is one of these for every repo that is referenced in the above namespace table and for every repo that any file stored anywhere in this MarFS instance (including older files that have older repos that you no longer write to so they may no longer be referred to in the namespace table) . The only way to know if you can get rid of a data repo in this list is to ensure no references exist in both the config namespaces and in the metadata for all the name spaces. It is really recommended that you don’t delete anything, just add another row with a new repo. A repo is just a logical name that connects the data of files in any name space to a particular use of place to store the file data. It is possible for multiple repos to point at a single external object storage server with different characteristics like compress and don’t compress etc. Repo’s represents a method for talking to some back end store.

|  |  |
| --- | --- |
| name | Name for this repo, this name is used in the namespace table above in the config file and it is also used stored with the file in xattr, so this can not be changed easily. It follows the same rules as deleting a repo in this list. |
| path | This is a path/url string associated with the repo used to access the repo |
| updateinplace | Updates in place for files in this repo are allowed. This lets you decide if a file is in a repo that can do update in place then the FUSE and batch programs can allow update in place. If a repo doesn’t allow this easily then you can forbid it. It is probably good practice to not allow this for all repo’s used in a namespace but you don’t have to do that. Update in place means that if you open for write, you have to overwrite the entire file from the beginning. It also means that you cannot truncate the file to any other value than zero. It also means that you cannot open with append and append to the file , (although this capability might be changed at a later date). The software can use update in place for DIRECT as the repomethodinfo (which tells the software to put the file data in the metadata file). (yes/no). This can be changed but it is not recommended. |
| repomethodinfo |  |
| securitymethod | Specifies a method for how security works on this repo (authentication/authorization), this can change as it is not recorded anywhere other than in this file but any backend storage system must be kept in sync with this method |
| enctype | Specifies a method for encryption for data for the repo. This can NOT change as all files that have data in this repo are encrypted with this type. |
| comptype | Specifies a method for compression for data for the repo. This can NOT change as all files that have data in this repo are compressed with this type. |
| correcttype | Specifies a method for correctness for data for the repo. This can NOT change as all files that have data in this repo have this correction information calculated and stored with this type. |
| onoffline | Specifies a method for bringing online a repo if the repo is of the type that allows it to be offline. This value can change as it is dynamic. |
| latency | Specifies a time it might take to bring a repo online. This value can change as it is dynamic. |
| dirty\_percent | Specifies a percent dirty that an object (not a file) could get before reclaim of space happens for all objects in this repo. This value can change as it is dynamic. |
| packfiles | Specifies that small files being written to this repo are to be packed if the program can do packing (FUSE cant pack multiple files but in batch it is possible) (Yes/NO) |

**Security section**

All POSIX security is obeyed by MarFS and in addition special security can be added by configuration to manage what parts of the name space allow metadata and data update/read, and you can control those special permissions for interactive and batch separately

These permissions are above and beyond the POSIX permissions (rwx/ugo). This is because external repositories may have special permissions that don’t map exactly to POSIX permissions. The values are rmwmrdwd:

rm – read metadata

wm – write metadata

rd – read data

wd – write data

ud – unlink data

td – truncate data

An example of interesting use is to allow read and write in POSIX permissions, allow metadata changes but not allow writing of data. This value is not stored with the file, it is interpreted real time, so this is a fast way to shut of write of data or metadata etc. This item can change based on allowed activity against this namespace and the data/space it represents.

Object Security is provided by the following methods

1. Vault method:  stash a password or a key to open a password in a file owned by linux user stgadm and the owner of the buckets/objects are stgadm over on the object server with a password for that user
   1. Fuse runs as root or similar so it can become stgadmin, read in the secret, then it is in the fuse daemons memory.  Since it is in a different process space run by root users can’t see that info.
   2. Pftool and other batch utilities would need to either run as stgadmin/root or use setuid sticky bits to gain access to the secret to open up the object repo.  This is somewhat dangerous so the most secure thing to do would be to run batch processes on other nodes or at least different containers or something.  This might not be a hardship because running batch on interactive nodes would just make interactive users doing ls and grep mad anyway.  We would need to make all batch run remote of the users process, a bit like  google, you type something and 100 machines go off and get you an answer or do a deed and you don’t have access to the batch machines except through a controlled interface.
   3. This method is easy to implement and uses a strong security method, it allows you to change the password on object server and in the little secret files owned by stg admin whenever you feel you need to, periodically or when an admin changes.  Its just like a group of people that have the combo to a shared vault.
   4. You could have more than one password, one per repo, one per namespace, one per …  but not too many, dozens might be manageable.
2. Per object:  this is where we get Scality/ViPR/etc. to add the ability to require a secret on each object request.   We would have to stuff the secret into the POSIX metadata for each file.  This would work as well and is pretty elegant too, but it doesn’t allow you to change something simple to re-secure compromised info.
3. Combo of 1 and 2  but its unclear that this is any better than 1 by itself, it might slow down the smart hacker but not much
4. Encryption used in our case, one could sniff the wire and get the data, we could encrypt the data path with tsl or something, but that would be more than we are doing now with mass data movement.  Encryption at rest doesn’t buy you much because the data is erasured on the server and that is a per object erasure, so you would have to steal a lot of disks to make any thing out of the data.  Encryption would need to be by name space or by repo or by object.  In all cases we have to stash the encryption keys somewhere and it essentially becomes number 1 or number 2 or a combo.
5. Number 1 looks like its pretty elegant as you can change the secret often etc.  It requires basically no coding, just some administration for the most part.

I think we should go with number 1 but leave room in our planning for a per file password just in case we decide to go down that path.

If at some point we find a better way that doesn’t require setuid/sticky then we could make the batch processes not protected, but frankly, it seems like this is essentially the Google model and it lets us get very creative on the batch side.  You could still run pcp or pls interactively, it would just run a batch program on the batch servers and connect the console to your interactive session, just like a Google search sort of.

Protecting the trash

Unlink and truncate operations leaves pointers to files and data in the trash directory for that namespace. It is important to protect the trash directory because it will contain trash names and space from various users/groups. It does not have a directory structure so maintaining control over access has to be managed since being able to find files requires the execute permission on the directory structure above a file. Through the library that the batch utilities and FUSE daemon uses, we deny all access to the trash directory. A trash utility will be created that allows users to interrogate the trash based on file ownership/groups/POSIX permissions, which is preserved when files are moved to the trash directory and when space is moved to the trash directory when files are truncated.

**Batch utilities/backup/space management**

* Periodically using the GPFS inode scan, scanning each GPFS file system in parallel to create information needed for statvfs/statfs and quota mgmt. as well as other useful histogram info from a simple and fast inode scan, files/space in histograms, histograms on file sizes, maybe also on dates (created in the last X days) modified in the last X days, maybe type histogram multi, uni, striped, packed, normal posix file, directory, maybe combos – why do all this, well its just so cheap, you reading the data in, keeping counters and adding stuff as you go is just amazingly cheap and it helps the sysadmins.
* Periodic walking of the trash tree for space reclaim, repack, etc.
* Backing up the metadata, this can be done by just backing up the metadata file systems assuming you are not storing a lot of real data in the metadata file systems, which will be typical for us. You need to preserver all metadata attrs and xattrs and file data (which might contain object id’s) \*\***You need to ensure the backup of the file system honors space holes, so backups are not huge, the MAR\_objidbytes xattr tells you if there are object id’s in the metadata file**
* A way to list objects used in the object repos might be nice for very infrequent reconciles
* Other utilities that use inode scanning or name merging, which can be run in parallel as each namespace can be a different gpfs metadata file system.

**Futures**

* Offline, latency optimizations/sorting
* Maybe append or sparse support, need to consider carefully
* Other access methods than cdni/object, hpss, remote, etc.
* HDFS alternate access of same data
* Would be nice to have restart for big files but that could be deferred
* Packed file support could be later but would be nice to have sooner to make it easy on object system
* Compression, encryption, remote copies, semantic copies, etc.
* Back up of object level metadata
* Fancier lazy fsinfo like indexing
* User supplied xattr with search (indexing)
* Would like to have V2 of erasure lib sooner than later, bw suffers
* Offline deep reconcile/repack – if trash is lost
* Investigate gpfs keeping track of changes for further optimizations of batch processes (only process changed parts of the tree)
* Fuse packing on write, fuse multipart write (maybe)
* May need a special way to load data from hpss to campaign that is very large, as we will need multi-part thru fuse or some other special way, in short term we could force this to go to scratch first for a while. Moving it from hpss is the hard part, once on scratch it would go fast to campaign, but need to figure a good way to do this at some point
* May want to do other optimizations to HPSS, like htar leveraging our