Journal of Physics: Conference Series **513** (2014) 042044 doi:10.1088/1742-6596/513/4/042044

XRootd, disk-based, caching proxy for optimization of data access, data placement and data replication

L A T Bauerdick[1], K Bloom[3], B Bockelman[3], D C Bradley[4], S Dasu[4], J M Dost[2], I Sfiligoi[2], A Tadel[2], M Tadel[2,5], F Wuerthwein[2] and A Yagil[2] for the CMS collaboration

[1] Fermilab, Batavia, IL 60510-5011, USA
[2] UC San Diego, La Jolla, CA 92093, USA
[3] University of Nebraska – Lincoln, Lincoln, NE 68588, USA
[4] University of Wisconsin – Madison, Madison, WI 53706, USA
[5] To whom any correspondence should be addressed.

E-mail: mtadel@ucsd.edu

Abstract. Following the success of the XRootd-based US CMS data federation, the AAA project investigated extensions of the federation architecture by developing two sample implementations of an XRootd, disk-based, caching proxy. The first one simply starts fetching a whole file as soon as a file open request is received and is suitable when completely random file access is expected or it is already known that a whole file be read. The second implementation supports on-demand downloading of partial files. Extensions to the Hadoop Distributed File System have been developed to allow for an immediate fallback to network access when local HDFS storage fails to provide the requested block. Both cache implementations are in pre-production testing at UCSD.

1. Introduction

In February 2013 the CMS experiment [1] at the CERN LHC finished its first data taking period, called "Run 1," and entered into the "Long Shutdown 1" period expected to last until spring 2015. However, the physics analyses of the harvested data are still ongoing, as are the detector simulations and related computing activities required for an efficient commencement of the upcoming "Run 2." The 20 PB of data from the experiment in various formats is distributed among participating Tier 0, Tier 1 and Tier 2 computing sites with the goal of optimizing the usage of available computing resources as well as to provide sufficient processing power to all physicists that require access to the data. The "Anydata, Anytime, Anywhere project" (AAA) [2] was started with the goal of opening up the computing model of CMS to various degrees of remote data access among all the involved sites. The first stage happened in the US in 2011 by exposing all Tier 1 and Tier 2 storage to the collaboration via the XRootd system [3] and by implementing a comprehensive monitoring framework [4]. The main initial use case was interactive access for data analysis. Soon after, standard computing jobs were allowed to utilize remote access, both as a fallback in case of a local access error, as well as intentionally to better utilize the available CPU resources. Within the US, during the first half of 2013, the average data rate among all sites was 250 MB/s, corresponding to about 1,000 concurrent running jobs,

or about 4% of total US CMS capacity. There is an ongoing campaign to export data in this way from all remaining non US CMS computing centers before summer 2014.

The success of the AAA project, the expected increase in data rates for "Run 2," and the promise of 100 Gbps networks becoming available in 2014 are all arguing in favor of loosening up of the CMS computing model. In particular, the usage of Tier 2 CPU and disk resources should become more flexible: with all data available at Tier 1 sites there is little incentive for pre-placement of most data on Tier 2 sites — it can always be downloaded when it is actually needed and then kept for as long as it seems reasonable. A significant part of Tier 2 storage, potentially even more than 50%, could thus be operated as a fluid cache space. Furthermore, as it is known that the data exists elsewhere there is no need to store the files in a redundant manner as long as the fallback to remote access can be provided at any point of file access. Efficient reuse of data cached at Tier 2 centers requires further attention as job scheduling programs need to be both aware of, and interact with the file caching infrastructure.

This paper presents two implementations of an XRootd, disk-based caching proxy developed in the context of the AAA project. We believe that these two services can be used to demonstrate operation of a Tier 2 center on non-subscribed data sets. Section 2 describes the two caching proxy implementations in detail and section 3 shows results of a scaling test of a proxy running on standard server hardware.

2. Two implementations of a disk-based caching proxy

Since CMS data federation already relies completely on XRootd to provide remote file access, the decision to base caching proxies on XRootd was an obvious one. The XRootd system provides a basic proxy service [5] with a limited in-memory cache. Its main purpose is to provide access into and out of private networks. However, the implementation allows for a user-provided implementation to be loaded at startup as a plugin — our two implementations are such plugins, specializations of the *XrdOucCache* interface. Both of them are currently undergoing pre-production testing at UCSD.

2.1. Complete file auto-prefetching proxy

The first implementation simply prefetches complete files and stores them on local disk. This implementation is suitable for optimization of access latency, especially when reading is not strictly sequential or when it is known in advance that a significant fraction of a file will be read, potentially several times. Of course, once parts of a file are downloaded, access speed is the same as it would be for local XRootd access.

The prefetching is initiated by the file open request, unless the file is already available in full. Prefetching proceeds sequentially, using a configurable block size (1 MB is the default). Client requests are served as soon as the data becomes available. If a client requests data from parts of the file that have not been prefetched yet, the proxy puts this request to the beginning of its download queue so as to serve the client with minimal latency. Vector reads are also fully supported. If a file is closed before prefetching is complete, further downloading is also stopped. When downloading of the file is complete it could in principle be moved to local storage. Currently, however, there are no provisions in the proxy itself to coordinate this procedure. Scheme of proxy operation is shown in figure 1.

A state information file is maintained in parallel with each cached file to store the block size used for the file and a bit field of blocks that have been committed to disk; this allows for complete cache recovery in case of a forced restart. Information about all file accesses through the proxy (open & close time, # of bytes read and # of requests) is also put into the state file to provide cache reclamation algorithms with ample details about file usage.

It would be straightforward to modify the proxy code to only fetch blocks requested by

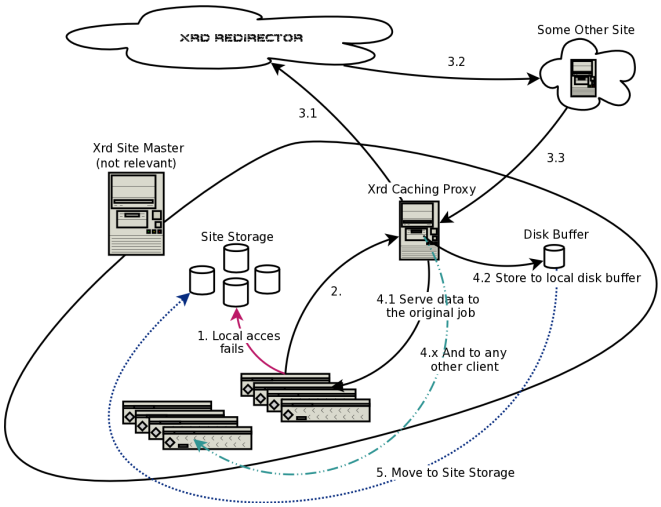

Figure 1. High-level diagram of caching-proxy operation. The same steps happen for both proxy implementations.

1. Reading from local storage fails.
2. Client contacts local proxy.
3. Proxy contacts a redirector to find a replica of the file on some other site.
4. Proxy downloads data, serves it to local clients and stores a copy to disk.
5. File or file fragments can be injected into local storage.

clients.[1] There are, however, several reasons to keep the caching-proxy operating on whole files. First, automatically establishing a full replica of a file provides a means for populating the on-demand caches at T2 sites. This is also interesting for non-HEP VOs in the context of OSG – the lack of storage space on OSG resources is in fact a common complaint from smaller VOs whose I/O stacks are also not suitable for remote data-access. Second, the analysis of client request lengths and offsets from detailed XRootd monitoring information of user analysis jobs, especially those reading private user and group files, shows there is significant unpredicatbility in data access from those types of jobs.

2.2. Partial file block-based on-demand proxy

The distinguishing feature of the second implementation is that it only downloads the requested fixed-size blocks of a file. The main motivation was to provide prefetching of HDFS blocks (typical size 64 or 128 MB) when they become unavailable at the local site, either permanently or temporarily due to server overload or other transient failures. When additional file replicas exist in a data federation, the remote data can be used to supplement local storage, to improve its robustness, and to provide a means for healing of local files. In particular, our intention is to avoid any local file replication of rarely used, non-custodial data at Tier 2 sites. As the HDFS block size is a per-file property, it has to be passed to the proxy on a per-file basis as an opaque URL parameter.

Unlike the full file prefetching version, the partial file proxy does not begin prefetching any data until a read request is actually received. At that point a check is made if data required to fulfill the request exists on disk, and, if it doesn't, the required blocks get queued for download. Chunks requested by the client are downloaded first to minimize the client delay. Each block is stored as a separate file, post-fixed by block size and its offset in the full file; this facilitates potential reinjection back into HDFS to heal or increase replication of a file block.

2.2.1. Extension of HDFS client for using XRootd fallback. After detailed inspection of HDFS client code [6] it was decided to develop *XFBFSInputStream* (standing for XRootd fall back file system input stream), a new specialization of *DFSInputStream* class, and to bind it to a custom protocol, *xfbfs*, in HDFS site configuration. This allows users to specify if they want XRootd fallback or not by simple selection of access protocol name. However, in typical HDFS

[1] This is, in spirit, how CMSSW currently accesses files over WAN: it starts an XRootd client and asks for data as they are needed.

deployment at US Tier 2 centers, HDFS is mounted via FUSE centrally for all users, thus breaking the flexibility of the scheme. To compensate for that, a special configuration entry allows system administrators to enumerate HDFS namespaces for which *XFBFSInputStream* should be instantiated. Note that one instance of input stream gets instantiated for every file that gets opened.

Internally, the work of maintaining an XRootd client instance and communicating to a block-based proxy gets delegated to a Java class *XrdBlockFetcher*, that has the majority of its functions implemented in C++ using JNI. This class only gets instantiated when lower-level classes of HDFS client cannot locate a data source and throw an exception that gets intercepted in *read()* functions of *XFBFSInputStream*. A list of bad blocks is kept so that any further attempts at accessing the same block get redirected to XRootd without retrying to locate it in HDFS. Both classes, *XFBFSInputStream* and *XrdBlockFetcher*, report their operations via UDP to allow monitoring of failures in real time, to estimate performance and load on the proxy, and to, eventually, provide information for storage healing algorithms. This is important because the XRootd fallback can get invoked on any node, for any HDFS client, and the common reporting scheme provides a way of aggregating reports from all computing nodes into a single log file.

3. Scaling test of a complete file prefetching caching-proxy

It is interesting to observe the limits of caching proxy in action as this affects its deployment setup at Tier 2 centers under various workload conditions. A standard, current server machine was chosen for the test: 2×6-core Xeon E5-2620 processors, 64 GB RAM, with ZFS file system over a RAID–5 disk array. One 1 Gbps NIC was used in the test, and kernel network parameters were tuned so as to saturate incoming traffic with a single multi-request stream, e.g., by running *xrdcp* on a file from FNAL.

The test itself was, of course, designed to cause trouble on the machine so that the weakest link in the setup could be determined. The test ran at the UCSD Tier 2. In the beginning the disk cache was empty and all data files used in the test were known to be available at other US Tier 1 and Tier 2 sites. After that, a dummy CMSSW job was started every 5 seconds on a set of worker machines, each opening a new, unique file. Each job was asking for 2.4 MB every 10 s (240 kB/s). The size of each file was about 1 GB. These numbers are based on average values observed over a large sample of CMS computing jobs, obtained from the AAA XRootd detailed monitoring.

Network traffic on the proxy node as a function of time is shown in figure 2. The prefetching traffic rose steeply from the start and began to saturate towards 800 Mbps when 25 connections were open (about 5 min into the test). Outgoing traffic rose linearly, fully satisfying the requested data rate up to 400 Mbps for 200 client connections (16 min). After that, a lower output rate increase continued for up to 240 connections. At that point, the disk of the machine become overloaded. The read rates and outgoing traffic become chaotic, soon dropping about 50%. Incoming traffic also dropped about 6% – apparently disk writes get higher priority than reads in ZFS. When prefetching of files began to ramp down, leading also to a reduced rate of write operations, the output rate soon climbed up to reach the total request rate of all 250 jobs. As another example, a 5-year old server machine with four disks joined into a single partition (non-RAID) using *ext4* file system got overloaded at input traffic of 600 Mbps and output rate of about 280 Mbps or 140 standard jobs.

Preliminary tests with *fio* [7] showed that by reducing the frequency of disk write requests (by reducing the prefetching data rate and increasing the write buffer size), one standard machine could serve up to 500 standard CMS jobs. Further work on the proxy code is required to achieve this level of performance – the current implementation is able to provision about 200 average CMS jobs. The ability to run a set of caching-proxy nodes behind a redirector is under development.

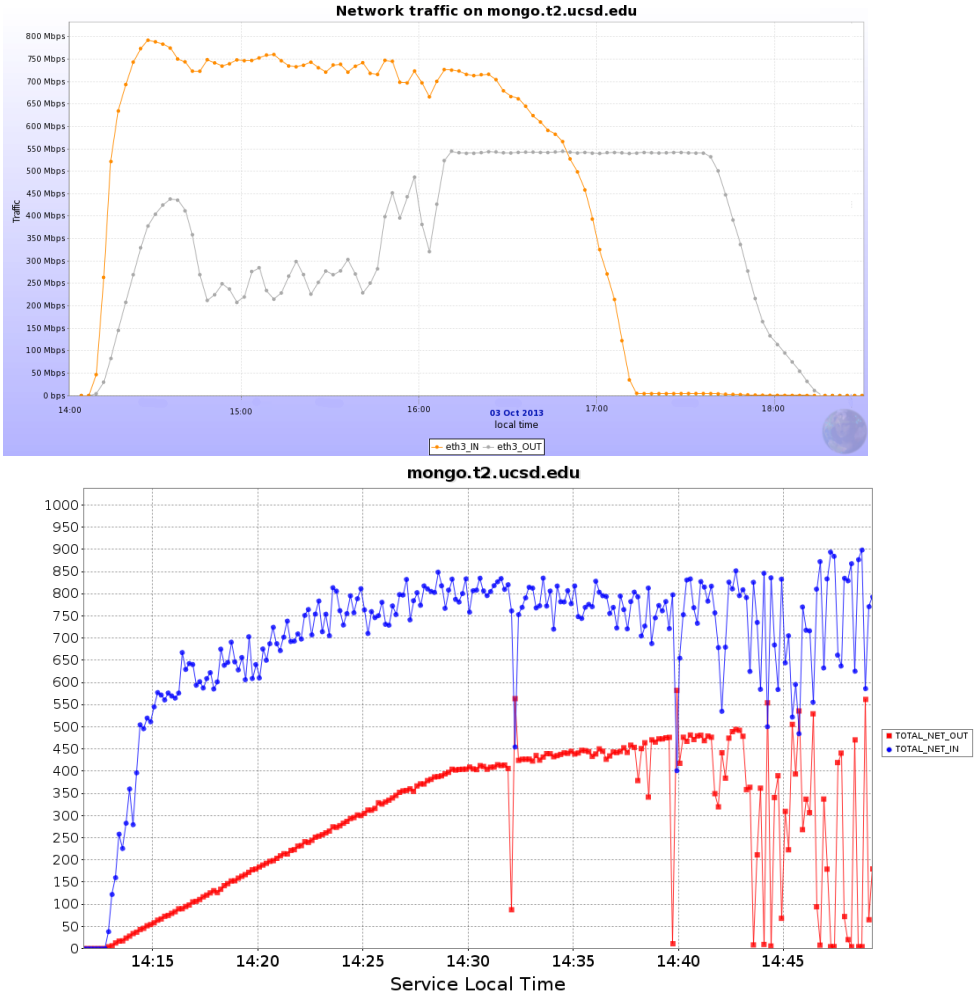

Figure 2. Network traffic on the caching proxy node during the scaling test. The top picture shows the complete test, data points are averages over 2 minute periods. The bottom figure shows detail of the ramp-up period, sampled every 15 s.

4. Conclusion

Two disk-based prototype implementations of an XRootd caching proxy have been presented. The main motivation for this development was to provide optimized access to remote data, both in terms of latency and data reuse, as well as to facilitate more flexible data placement strategies among Tier 2 and Tier 3 centers. The prefetching caching proxy implementation is also suitable for just-in-time data placement. The partial block caching proxy implementation, on the other hand, allows computing center operators to reduce replication factor of non-custodial files residing on HDFS-based storage, freeing up disk space for other uses.

Further work will focus first on final optimizations of the proxy implementations and on full-scale, production grade testing at UCSD. After that, in anticipation of proxy deployment across the whole data federation, integration with job scheduling will be investigated to provide early preloading of data and a better reuse of existing cached replicas. Interaction of caching with local storage will be studied, and the tools needed to manage block replication factors and block movement from cache into a running HDFS will be developed.

Acknowledgments
This work is partially sponsored by the US National Science Foundation under Grants No. PHY-0612805 (CMS Maintenance & Operations), PHY-1104549, PHY-1104447, and PHY-1104664 (AAA), and the US Department of Energy under Grant No. DE-FC02-06ER41436 subcontract No. 647F290 and NSF grant PHY-1148698 (OSG).

References
[1] CMS Collaboration 2008 *JINST* **3** S08004.
[2] Bauerdick L, *et al* 2012 "Using XRootd to Federate Regional Storage", *J.Phys.Conf.Ser.* **396** 042009.
[3] XRootd project page: http://www.xrootd.org/.
[4] Bauerdick L, *et al* 2012 "XRootd monitoring for the CMS experiment", *J.Phys.Conf.Ser.* **396** 042058.
[5] XRootd proxy service documentation, in http://xrootd.slac.stanford.edu/doc/prod/ofs_config.htm.
[6] White T 2012 *Hadoop: The Definitive Guide, 3rd Edition* (O'Reilly Media, Inc.) pp 67–70.
[7] Axboe J 2005–2013 *fio – Flexible IO Tester* http://git.kernel.dk/?p=fio.git.