

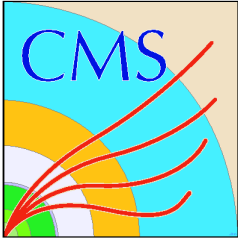
# Frontier Evolution

WLCG Database Technical Evolution Group Workshop

Dave Dykstra, Fermilab

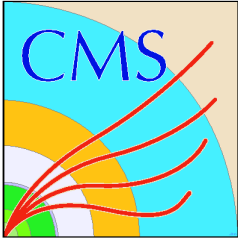
[dwd@fnal.gov](mailto:dwd@fnal.gov)

Work supported by the U.S. Department of Energy under contract No. DE-AC02-07CH11359



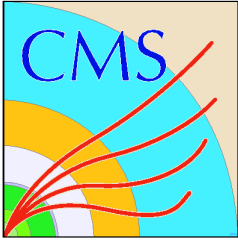
# Brief Intro

- Frontier is a distributed DB caching system
- Ideal for when many clients need basically the same data at close to the same time
- Commonalities success story: used by CMS (Online & Offline), ATLAS, and planned for LHCb
  - Uses standard HTTP caches, shared with other RESTful applications



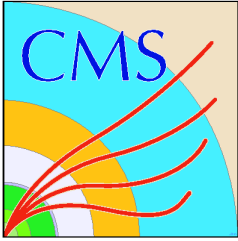
# Expected evolution (1)

- Replicate CMS database & Frontier servers
  - Use Oracle 11g's Active Data Guard after winter shutdown because far less DBA work than streams
  - Either at SafeHost or Fermilab
  - Will allow remote Frontier operations to continue when CERN's Oracle or WAN connection down
  - ATLAS currently streaming conditions to ~5 Tier 1s
    - Some have shut down, still too many in my opinion
    - ATLAS could switch to Active Data Guard and only one backup too



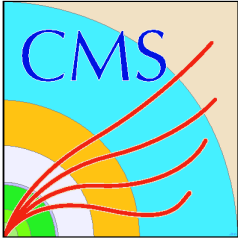
## Expected evolution (2)

- Deploy additional backup proxy squid servers for CMS
  - Co-located with Frontier “launchpad” servers
  - Coupled with disabling fail-overs to server, they keep the launchpad servers free from fail-overs
    - Better for serving the squids of normally functioning sites
    - Only failing sites will be harmed if too many site's fail-over at the same time
  - The fail-over monitoring that's now on the launchpad squids will be moved to these
  - ATLAS could do the same



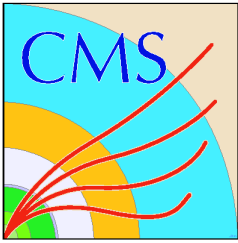
# Expected evolution (3)

- Automate the configuration of MRTG monitoring of worldwide squids
  - From AGIS configuration database for ATLAS
  - From CVS copies of site-local-config for CMS
  - Monitoring of squid proxies should be moved to WLCG responsibility because they're for multiple experiments and multiple applications
    - Also discovery of proxies by jobs (more later)



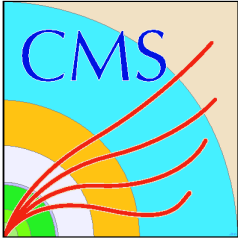
# Expected evolution (4)

- Authentication of sources
  - Currently vulnerable to man-in-the-middle + buffer-overflow attack
    - Obscure, but potentially highly valuable
  - Overcome the threat by adding to the response a digital signature of the request+most of response
- Use squid3 when it is ready
  - Total rewrite of squid2 in C++, multithreaded
  - Some important functionality still missing



# Increased usage expected

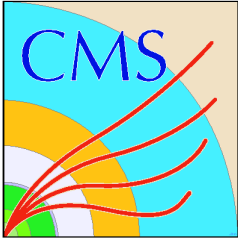
- CVMFS using HTTP squids
- LHCb planning to use Frontier
- Increased applications of both Frontier & HTTP caches by LHC experiments likely
  - Also other experiments sharing the same grids
- Natural growth of bandwidth demands for existing applications
  - On the other hand, whole-node multicore jobs will reduce load



# Results of increased usage (1)

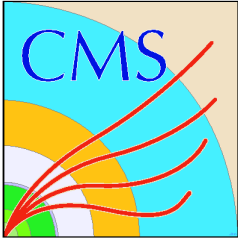
- Increased bandwidth will be needed
  - At a minimum add to bandwidth or replicate existing site squids
  - May eventually need to have heirarchy of squids at sites, such as a squid per rack fed from site squid





# Results of increased usage (2)

- Need a standard method for automated discovery of HTTP proxies
  - WLCG should provide this
  - Proxies should be shared for all production, approved applications
  - Also should be separate, opportunistic proxy caches to avoid interference with production



# Summary

- Increased usage of both Frontier & HTTP proxy caches expected
- Need a standard method for discovering & monitoring proxies