

OpenAFS Status 2013

Roller Coaster of Thrills

- D Brashear
- The OpenAFS Project
- 31 October 2013

History

- OpenAFS 1.6.0 was released on 1 September 2011.
- “rx ping” issue at CERN, DESY, others.
- Data corruption issues as well.
- 1.6.1 on 3 April 2012

OpenAFS 1.6.1

- rx ping avalanche
 - leak of AFS connections (with one Rx connection each) during server probes
 - issues with which Rx connection would exist
 - tracked per server so exactly one exists
- corruption due to CopyOnWrite speedup
 - reverted

OpenAFS 1.6.2

- Buffer overflow fixes
 - Presaged what would follow
- Improvements when a server went off into I/O wait forever
- Linux updates

Windows

- No more 1.6 releases
- XP being desupported when Microsoft does!
- Windows 8, 8.1, Server 2012
 - but no ARM support yet (Surface, Phone)
- Redirector released, over 50k deployments
- Cygwin AFS support for redirector
- NTFS symlink compatibility (drag between)

And then ...

Security vulnerability

- MIT 6.858 paper “Kerberos with 2 Heads Napping”
 - Recovery via brute force of a DES service ticket if used for encryption (like Kerberos session keys)
 - ... and AFS only supported DES
- Also allows derived subkeys to be compromised if the service key is
- Impetus for MIT rxgk work

OpenAFS 1.6.5

- 2 mitigations to rxkad since rxgk has not been completed yet.
 - rxkad-k5
 - backward compatible to clients
 - rxkad-kdf
 - more secure but harder to deploy

rxkad-k5

- Allows non-DES service keys
 - but KDC must still support DES for session keys
 - principal's service key not vulnerable

rxkad-kdf

- Uses non-DES session keys
 - KDC doesn't need DES.
 - But every client needs updated software
 - typically, "aklog"

Are we safe yet?

- rxkad-k5 allows the session key to be compromised
 - But it gets you history only
- rxkad-kdf protects that also
- but in the end, rxkad still uses a 56 bit key

rxgk

- Core rxgk spec is done
 - Waiting on GSS negotiation loop description
- rxgk-afs integration spec needs more work
 - How to represent cache manager identity so callbacks can be protected
- rxgk will support bos/bosserver after core spec is done
 - Actual fileserver and database support will take longer

What are you running?

- Folks here running previous-to-1.6.5
 - and before 1.6.5, you are vulnerable
- Oldest observed:
 - hephy.at with OpenAFS 1.4.11 and afs3.6 2.58

OpenAFS 1.6.5.1

- AIX client fix
 - Rx listener was broken
- Linux
 - kernels through 3.12rc4

OpenAFS 1.6.6

- Additional intelligence for disk cache error handling

Upcoming work

- MacOS 10.9 “Mavericks”
 - kpi did not change, 10.8 client will load
 - issue with symlink creation
 - with both 10.8 client and a 10.9 build
 - packaging out of date

Foundation

- Swore for years we'd get here
 - and now we do
- Agreement with IBM for use of the name
 - Concessions required for protocol and namespace backward compatibility
- Paperwork not yet available

Foundation

- Costs (for lawyers) so far: \$7000
- Left in the bank: \$12500
 - But more expenses pending
- Business plan still to be determined
 - Taking volunteers to help us craft it.

Talk back to us

- Mailing lists:
 - Openafs-info <http://lists.openafs.org/mailman/listinfo/openafs-info>
 - Openafs-devel <http://lists.openafs.org/mailman/listinfo/openafs-devel>
 - Foundation-discuss <http://lists.openafs.org/mailman/listinfo/foundation-discuss>
- IRC chat room: #openafs on freenode
- Jabber developer MUC:
openafs@conference.openafs.org