Security Recommendations: SE

Ákos Frohner

EGEE'08, Istanbul, September 2008

www.eu-egee.org

Information Society and Media

The Disk Pool Manager (DPM)

- lightweight solution for disk storage
- SRM v1.1, v2.2
- rfio, gridftp, http(s), xrootd
- more than 100 instances

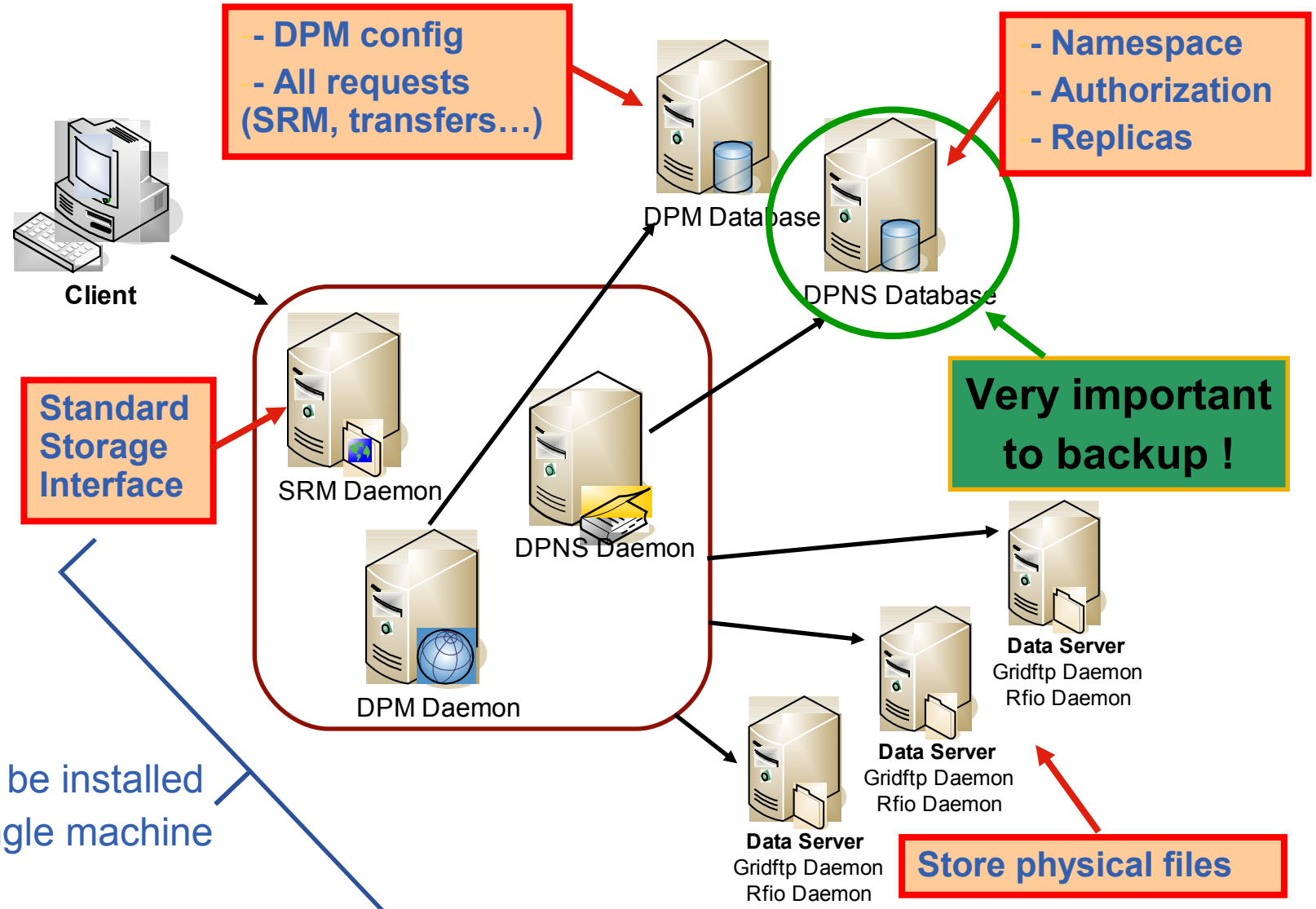
Documentation

https://twiki.cern.ch/twiki/bin/view/LCG/DpmGeneralDescription

DPM tutorial for Tier-2 administrators

http://indico.cern.ch/materialDisplay.py?
contribId=3&sessionId=s0&materialId=slides&confId=a058483

Architecture



Services/ports

- dpns (5010) - DPM name service for the hierarchical namespace and metadata
- dpm(5015) - storage management, proprietary protocol
- srmv1(8443), srmv2(8444), srmv2.2(8446) – storage management, web service protocols over httpg
- secure rfio(5001,20000-25000) - file access protocol
- gridftp(2811,20000-25000) - grid file transfer protocol
- http(s)(80,443) - HTTP(S) file access protocol (optional)
- xroot(1094,1095)- xroot file access protocol (optional)
- ldap (2170) - standard BDII GIP

IPv6 support since v1.6.9

Important log files

The services are logging to local log files directly

- DPM server: /var/log/dpm/log
- DPM Name Server: /var/log/dpns/log
- SRM servers: /var/log/srmv1/log, /var/log/srmv2/log, /var/log/srmv2.2/log
- RFIO server: /var/log/rfiod/log
- DPM-enabled GridFTP: /var/log/dpm-gsiftp/gsiftp.log, /var/log/dpm-gsiftp/dpm-gsiftp.log
- Optional web server (Apache); errors also in syslog: /var/log/dpm-httpd/access, /var/log/dpm-httpd/errors
- Optional xrootd: /var/log/xrootd/log, /var/log/olbd/log

Log files are rotated daily, keeping the last 90 days.

gsiftp.log might grow quickly!

Starting/Stopping Services

General pattern:

service <name> start|stop|restart

Head node:

- **dpm**
- **dpnsdaemon**
- **srmv1, srmv2, srmv2.2**
- **dpm-manager-xrd, dpm-manager-olb (optional xrootd)**

Disk nodes:

- **dpm-gsiftp**
- **rfiod**
- **dpm-xrd, dpm-olb (optional xrootd)**
- **Dpm-httpd (optional http(s))**

Optional Services

Disable HTTP(s) and xrootd, if not needed:

- **DPM_HTTPS="no"**
- **DPM_XROOTD="no"**

in the site configuration and re-run yaim!

Virtual users and groups

- **Users (X509 DN) and groups (VOMS FQANs) are virtual, added to DPM's DB on-the-fly, when first seen**
  - Experts only: can be disabled, but needs manual user management!
- **Downside: not possible to disable an individual user planning to use LCAS for this**
  - Can disable CA in /etc/grid-security/certificates
  - Can disable VO in /etc/grid-security/vomsdir
    Also remove user from /opt/lcg/etc/lcgdm-mapfile!
- **All files are owned by 'dpmmgr'**
  - No other interference with other system users
  - Experts only: DPM disk node could be even on the WN

Trusted hosts

DPM services interact with each other on the users behalf

- srmv2.2 -> dpm: storage operations
- rfio -> dpns: file access checks

- **'forwarding' client attributes, no delegation**
- **By default: host name based trust: /etc/shift.conf:**

  DPNS TRUST <headnode> <disk-node-1> ...

  DPM TRUST <headnode> <disk-node-1> ...
- **Any program on the trusted nodes is trusted, so do not deploy any user activity on DPM nodes!**
  - Experts only: trust can be X509 or Kerberos5 based