Data Policy: Implementation

WP18 – Data access security and authz

Setting the scene

Organization

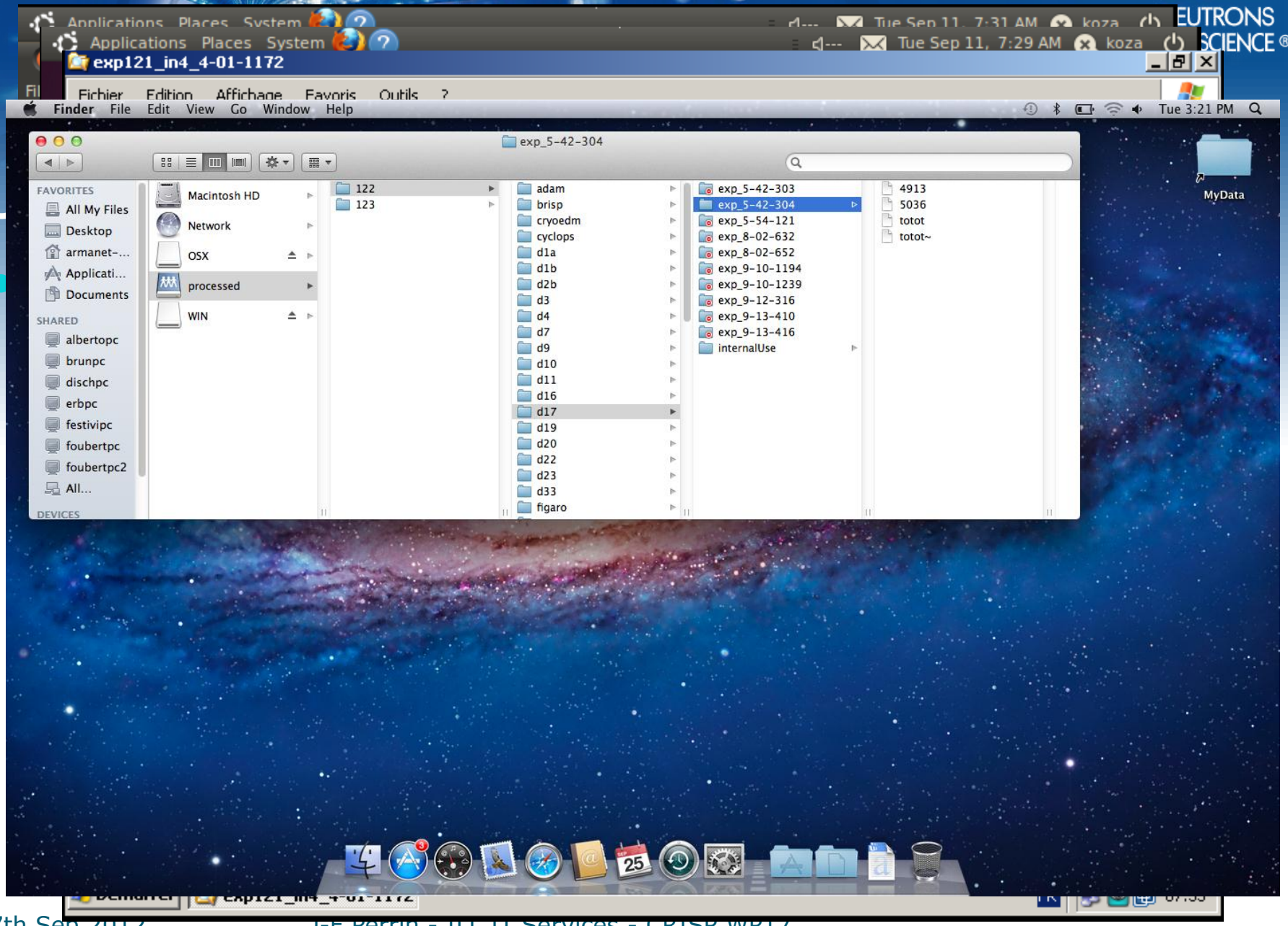
- Since the publication of the DP (Dec 2011). http://www.ill.eu/users/ill-data-policy/
- Creation of the DPP WG (Feb 2012)
  - Objective : « Prepare the implementation of the DP »
  - Representatives : Instrument responsible + Support services (IT, Computing, Instrument control)
  - Deadline 24th of October 2012

What is going to change quickly for the users

- Authentication of the users (removal of generic account)
- Identification of the raw data (Proposal #)
- Protection of the data (raw and processed)
- Change in the storage path
  - /illdata/cycle/instr/exp_9-10-1195/raw_data
  - /illdata/cycle/instr/exp_9-10-1195/processed_data

User experience improvements

- Metadata catalogue
- Security
- A single username/passord, Single Sign On in the future ?
- Better data management opens the possibility of new exiting projects.


Applications Places System
Tue Sep 11, 7:31 AM koza
Applications Places System
Tue Sep 11, 7:29 AM koza
exp121_in4_4-01-1172
Fichier Edition Affichage Favoris Outils ?
Finder File Edit View Go Window Help
Tue 3:21 PM
exp_5-42-304
FAVORITES
All My Files
Desktop
armanet-...
Applicati...
Documents
SHARED
albertopc
brunpc
dischpc
erbpc
festivipc
foubertpc
foubertpc2
All...
DEVICES
Macintosh HD
Network
OSX
processed
WIN
122
123
adam
brisp
cryoedm
cyclops
d1a
d1b
d2b
d3
d4
d7
d9
d10
d11
d16
d17
d19
d20
d22
d23
d33
figaro
exp_5-42-303
exp_5-42-304
exp_5-54-121
exp_8-02-632
exp_8-02-652
exp_9-10-1194
exp_9-10-1239
exp_9-12-316
exp_9-13-410
exp_9-13-416
internalUse
4913
5036
totot
totot~
MyData

Behind the scene

Technically

- Central Archive: move from NetApp to home made storage (100 TB replicated, $, performance improvement but loss of functionalities).
- Authentication: Kerberos (Windows, Linux, Mac)
- Access protocol:
  - Rsync (IC),
  - CIFS, NFSv3/4 (access for workstation)

Technical difficulties encountered so far …

- XFS (used as the archive fs): only 23 Acls per inode.
- MacOS X: NFSv4 not mature (sec=krb)

- MS AD as Kerberos server (only 1 realm)
  - Client are mostly Linux (MS often considered evil, insecure, …)

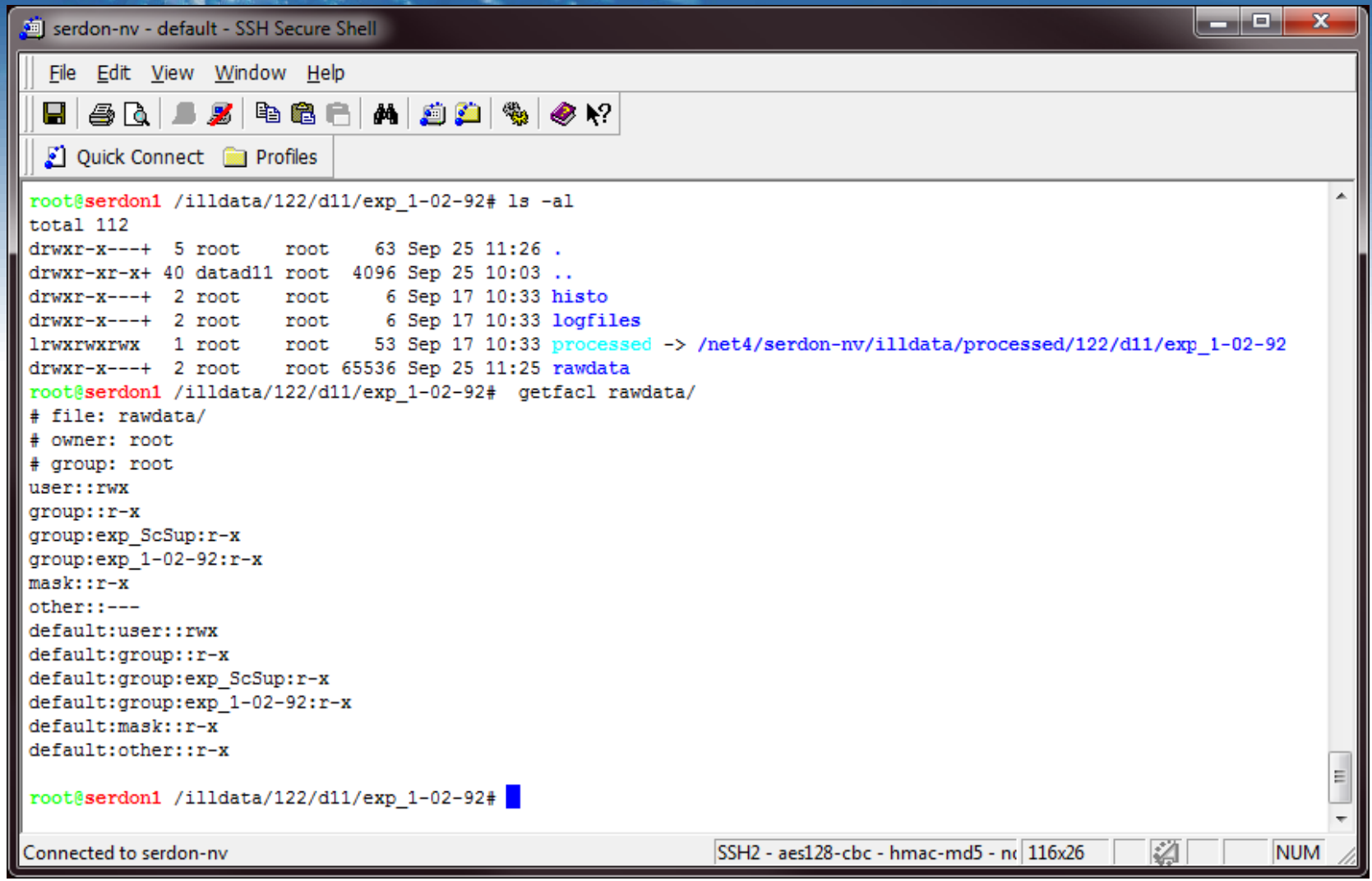
Technical difficulties encountered so far …

- Linux mount/export operation accepting only DES encryption (disabled on MS 2008R2 – 2102)
- Pincipal, which one ?
  - MIT Kerberos Linux: Principal
  - AD: UPN and SPN
- How to generate keytabs ?
- Heterogeneous environment
- Lack of up-to-date documentation
  - Example: Technet Kerberos interoperability (2000)
- …

Technical difficulties encountered so far …

- Commercial licenses (single user to 10,000)
- Software data path adaptation (roughly 60)
- …

ACLs


serdon-nv - default - SSH Secure Shell
File Edit View Window Help
Quick Connect Profiles
root@serdon1 /illdata/122/d11/exp_1-02-92# ls -al
total 112
drwxr-x---+ 5 root   root   63 Sep 25 11:26 .
drwxr-xr-x+ 40 datad11 root 4096 Sep 25 10:03 ..
drwxr-x---+ 2 root   root   6 Sep 17 10:33 histo
drwxr-x---+ 2 root   root   6 Sep 17 10:33 logfiles
lrwxrwxrwx   1 root   root   53 Sep 17 10:33 processed -> /net4/serdon-nv/illdata/processed/122/d11/exp_1-02-92
drwxr-x---+ 2 root   root 65536 Sep 25 11:25 rawdata
root@serdon1 /illdata/122/d11/exp_1-02-92# getfacl rawdata/
file: rawdata/
owner: root
group: root
user::rwx
group::r-x
group:exp_ScSup:r-x
group:exp_1-02-92:r-x
mask::r-x
other::---
default:user::rwx
default:group::r-x
default:group:exp_ScSup:r-x
default:group:exp_1-02-92:r-x
default:mask::r-x
default:other::r-x
root@serdon1 /illdata/122/d11/exp_1-02-92#
Connected to serdon-nv
SSH2 - aes128-cbc - hmac-md5 - n
116x26
NUM

Time consuming

- Tests and configuration of the different clients
- Python scripts for generating, config files and ACLs from the proposal database
- Solving Problems
- Communication with the scientists

Is NFSv4 safe ?

- Yes for LAN access, Kerberos ensure that the user is the one who authenticate.
- But could be improved on Linux/MacOS:
  - General adoption of AES instead of DES
  - TGT/TGS stored in memory instead of file (as done in windows env)

Planning

- August 2012: Central storage (serdon) ready
- Mid 2nd Cycle, evaluation period:
  - SendData
  - Transfer of some data to the new architecture

Today

  - 3 test instruments – fully ready
  - Further implementation on different instruments depending on the results of the first test

- General introduction 3rd Cycle 2012 (24th Oct)

Next task

- Define the authorization in Icat (instead of the proposal system)
- Increase the storage capacity and set of functionality