

IN2P3 AD Forest Project



Michel Jouvin

LAL / IN2P3

jouvin@lal.in2p3.fr

- HEP and Nuclear Physics
 - 16 labs around France
 - 1 national computing center
 - Distinct from CEA/DAPNIA
- Each laboratory autonomous for computing
- Windows growing everywhere
 - NT4 domains existing in 8 labs
- LAL : only lab with 1 ActiveDirectory domain

Why an IN2P3 AD ?

- Management of a growing number of PCs is a challenge for all the labs
 - Lower the management cost for each lab
- Expertise available in a few labs
 - Don't reinvent the wheel everywhere
- Handle roaming between labs
- No lab (except LAL) has an AD domain
 - Easier to build an IN2P3 project
 - Pressure to have it available quickly

IN2P3 AD Design Principles...

- A national tree (forest)
 - One root domain : in2p3.fr (CC – Lyon)
 - One domain per lab : lab.in2p3.fr (recommended)
 - Including CC
- DNS namespace sharing with non-Windows usage
 - Same configuration as LAL
 - Lab.in2p3.fr served by standard (Unix) DNS : no dynamic update
 - Ad_zones.lal.in2p3.fr served by Windows : dynamic update enabled, integrated to AD

... IN2P3 AD Design Principles

- Accounts managed in each domain (lab)
- Distributed group of administrators
- Setup of an IN2P3 DFS
 - Mainly for sharing of administrative resources
 - No (significant) user file sharing expected
- Use of IntelliMirror at the forest level
 - One national repository of MSI : sharing of repackaging effort
 - Group policies per lab

Current Status and Plans...

- Bottom-top approach
 - Request from the labs and not from the management
- Pilot being started
 - 10 labs (including CC) participating
 - Not a production infrastructure : will be destroyed
 - Every lab has to provide needed computers for DC
 - Emphasis : DNS integration, network config/problems impact, group policy deployment, NT4 migration

... Current Status and Plans

- Production AD ready in September
 - Built on validated design principles from pilot
 - Keep a pilot domain in labs for some time
 - Integrated into production forest
 - Ask for some funding to buy main DCs hardware
 - Give an official status to this AD forest
 - Migrate existing NT4 domains as tree subdomains
 - Based on Windows.NET implementation ?
- Unresolved issue
 - LAL AD migration to forest (wait for W.NET ?)

Future Directions

- SMS deployment
 - LAL already used it and will continue to use it
 - SMS is a needed companion to IntelliMirror
 - Push update to stable machines
 - Update system
- Kerberos integration with Unix
- 1 lab wants to look at Exchange