



# User Management in LHCb

Gary Moine, CERN  
31/01/2007

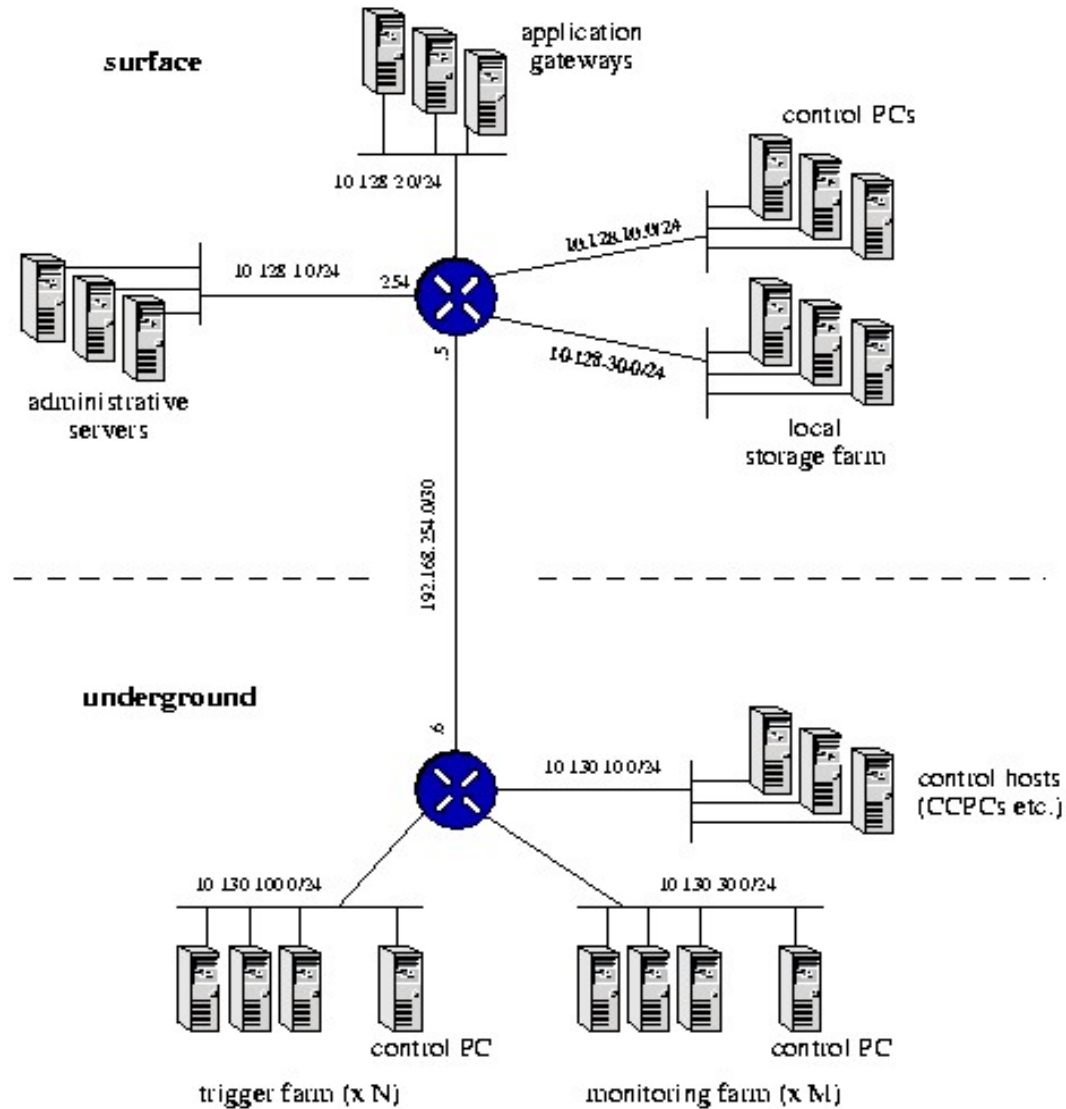
# Introduction

- Overview of internal network
- Description of system administration
- First problem: a classic: Unix and Windows
- A requirement : Single Sign On solution for experiment users
- Adopted solution: pGina and pam module
- Home directories common to both world:  
NFS and SAMBA
- Summary

# Experiment Internal Network

- 2 main Networks completely separate: DAQ & Control. System administration services on Control.
- Additional private Network for switch/router management
- All are disconnected from CERN. Access only via Application Gateways.
- Dedicated link to CERN for storage of Physics data.
- Central services used: Castor - DNS

# Experiment Internal Network





## Network services used

- NIS for User information
- Authentication with Kerberos
- NFS + Automount
- Active Directory - RIS
- Quattor
- DNS, DHCP, NTP, TFTP, PXE ...

# One problem: User management

- Obvious to say: 2 different system = 2 very different ways of doing management
- **We have:** all farms node PCs + most of control PCs on Linux [1000/1500], remaining control PCs and most of Desktop for control room on Windows [50/100].
- **We do not want :** Necessity to manage users accounts on both systems: Need to find a Single Sign On solution:  
→ An Open Source project meet our needs:  
**pGina**

# What is Gina

- What is GINA ? it stands for: **G**raphical **I**dentification a**Nd** **A**uthentication.
- It's a "kind of" PAM for Windows.
- GINA is a dynamically linked library that is loaded in the context of the Winlogon process when the machine is started... In other words, it's something behind this:



## What is pGina

- pGina is an Open source replacement for MS Gina dynamic library
- pGina is a Pluggable GINA: It provides various modules to allow different other authentication methods on Windows.
- PAM Plugin is the one used in our setup
- It consist of 2 parts: pGina with PAM plugin on each Windows client . And 1 Linux PC running a PAM-aware daemon which use the PAM authentication stack: Kerberos in our case.
- More on pGina: <http://www.pgina.org>



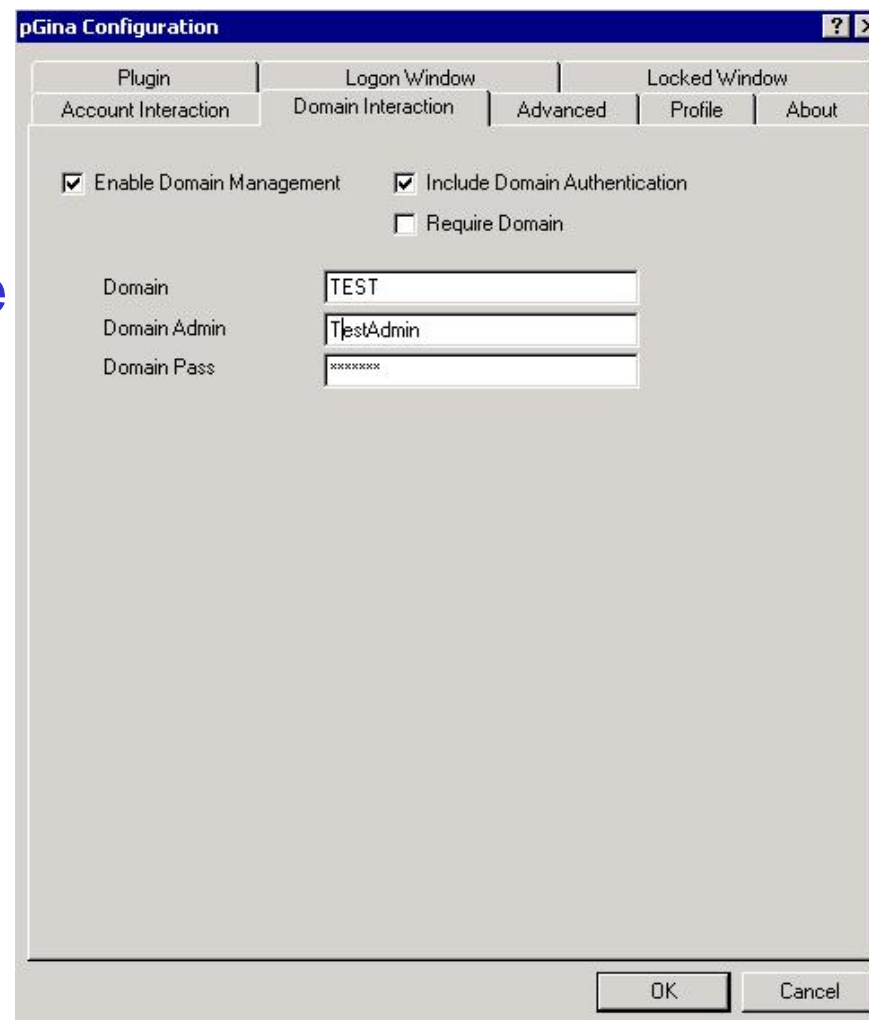
## What the User sees

- LHCb pGina login prompt:



# Overview of pGina

- pGina provides a Domain Interaction. A user can be added to AD when he/she successfully authenticates.
- It also include others usefull Windows options like Drive mapping on login or Groups membership, etc..



# Home Directories

- Home directories stored centrally on a Disk server
- NFS exported and Samba shared
- Automount'ed on Linux client
- Mapped drive on Windows PC

# Summary

- User management done on Linux side
- Kerberos for authentication
- pGina with PAM plugin' for integrating Windows user mgmt to this Unix schema.
- Home stored on Linux side, NFS exported and SAMBA shared.