CentOS: Large LDAP deployments

Didi Hoffmann <didi@ribalba.de>

What

- What is the problem ?
- How can it be solved ?
- Why LDAP ?
- How to implement ?
  - Server
  - Client
- Questions

Who am I

- Student @ Bournemouth University

www.hacktags.org

Who is funding me

Bournemouth University computing degree

Bournemouth University

http://www.bournemouth.ac.uk

What is the problem

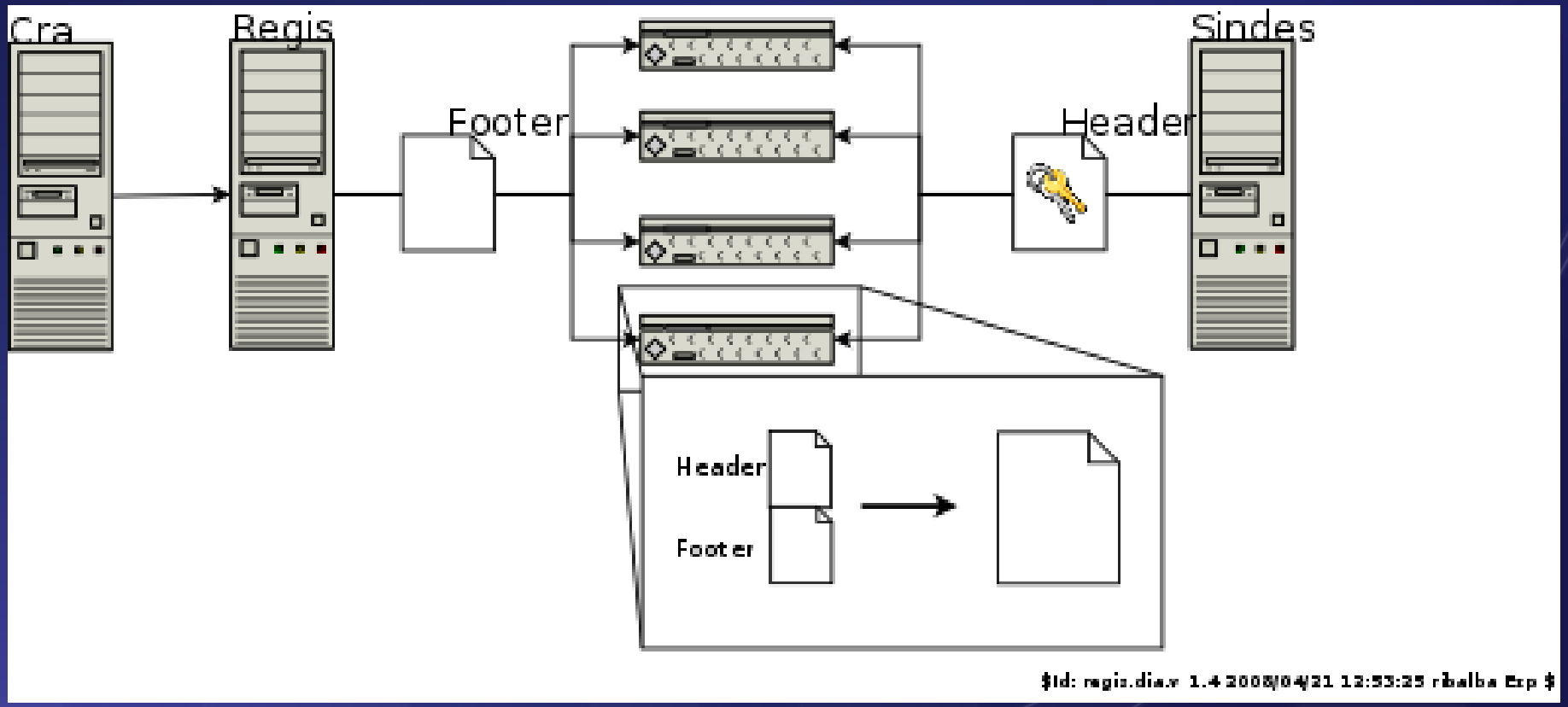
- One case:
- 263 million user accounts
  - 30000+ users 8000+ machines
- Every machine / user different
  - Apache, AFS
  - Different users allowed access
- Keep everything in sync

Solution ...

- NIS
- NIS+
- Distributed file p2p
- MySQL
- Something Microsoft Windows based?

Solutions

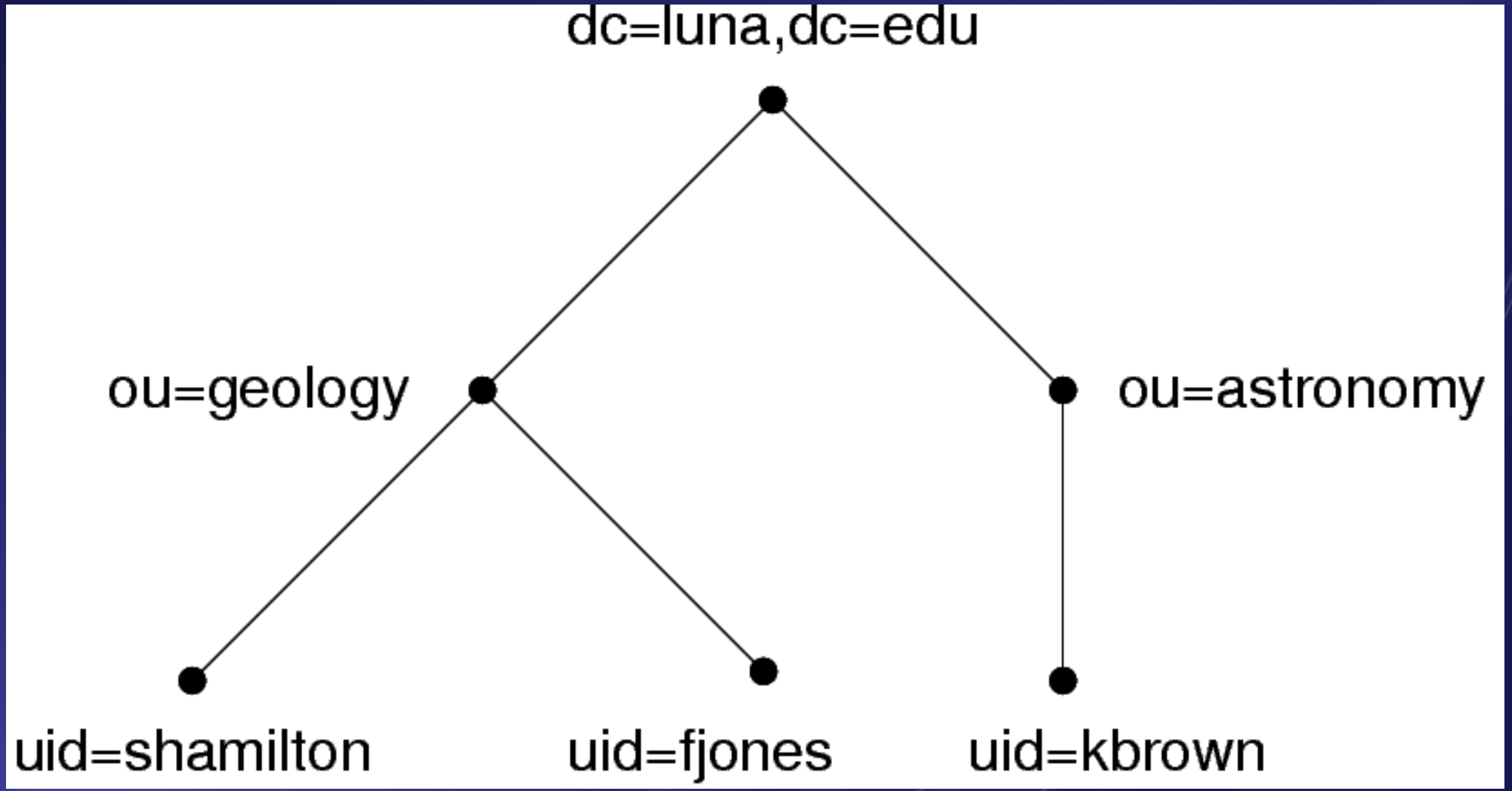
- File based



What is LDAP

- Lightweight Directory Access ***Protocol***
- Light X.500
- TCP/IP
- Currently LDAPv3

What is LDAP ...

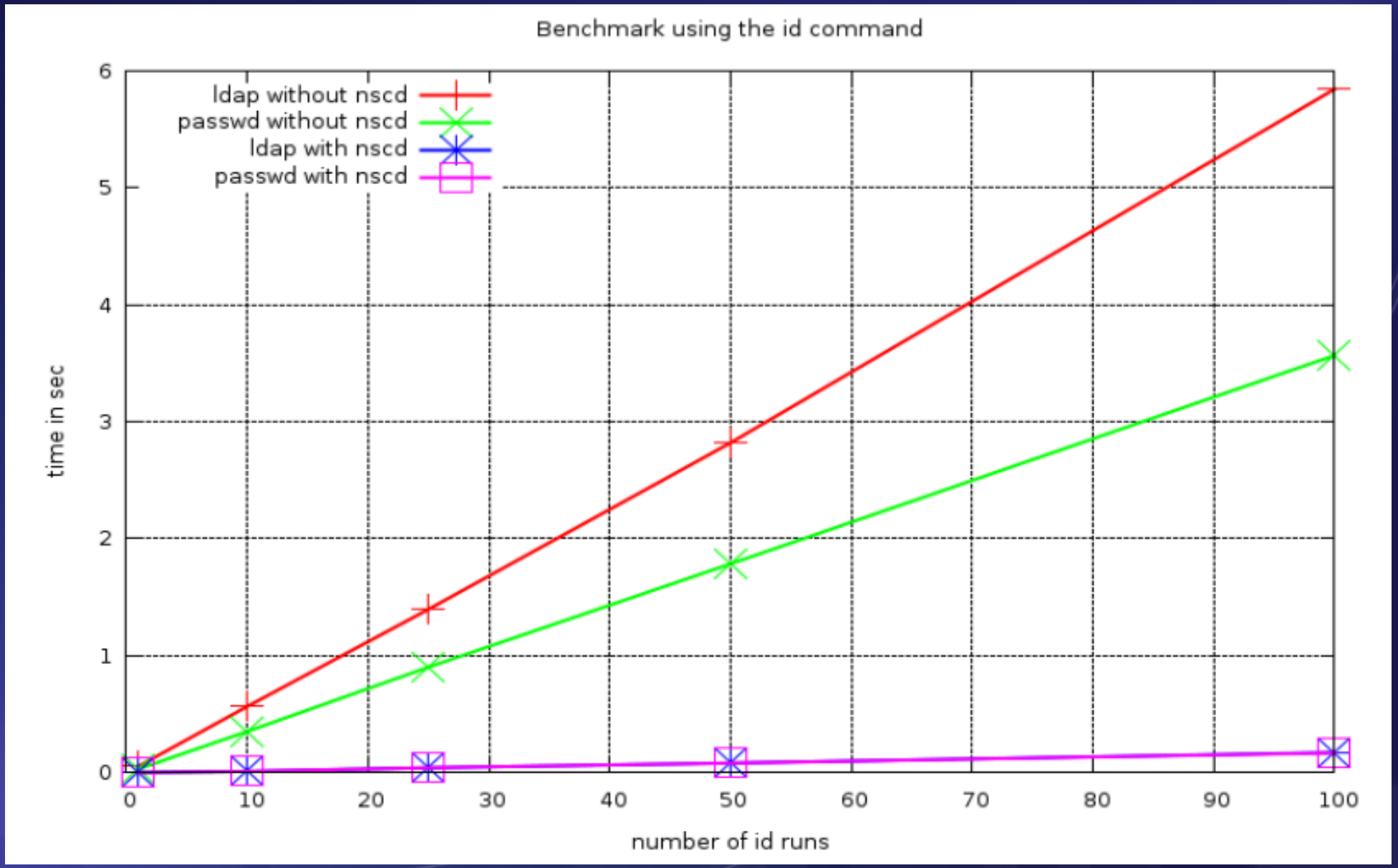


Buzzwords: Distinguished Name, LDAP Data Interchange Format (LDIF)

Why

- Reduce data redundancy
- Industry standard
- Pretty much all tools written and supported
- OS independent
- Scalable

Some info


Benchmark using the id command
ldap without nscd
passwd without nscd
ldap with nscd
passwd with nscd
time in sec
number of id runs
0
1
2
3
4
5
6
0
10
20
30
40
50
60
70
80
90
100

How

- OpenLDAP / Directory Server
- nss_ldap
- pam_ldap
- Nscd

- Everything well documented

How setup server

- Install the openldap, openldap-servers, and openldap-clients RPMs.
- Edit the /etc/openldap/slapd.conf
- /sbin/service ldap start
- ldapadd
- (ldapsearch)

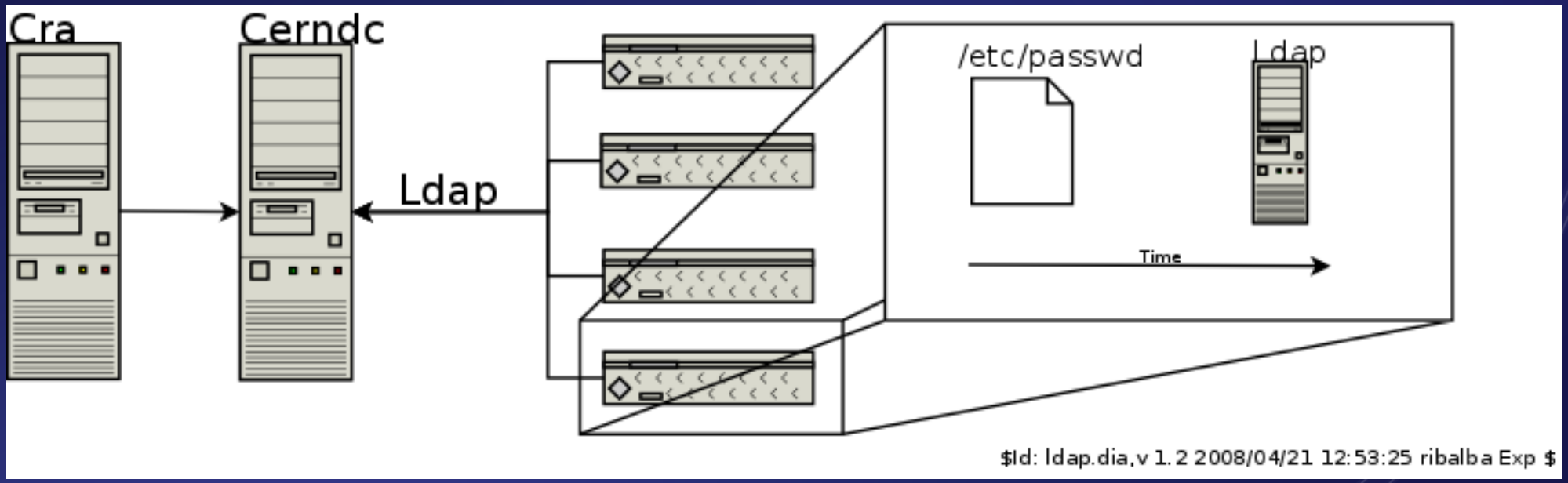
How setup client

- System-config-authentication

The good old way

- /etc/ldap.conf and /etc/openldap/ldap.conf
- /etc/nsswitch.conf

And now


Cra
Cerndc
Ldap
/etc/passwd
Ldap
Time
$Id: ldap.dia,v 1.2 2008/04/21 12:53:25 ribalba Exp $

Some packages

- openldap
- openldap-servers
- Openldap-devel
- Openldap-clients
- Python-ldap
- nss_ldap

Security

- TLS
- SASL
- Kerberos
- Unencrypted

Conclusion

- Good if you have many users that change often
- NFS uid sync
- Companies should always use it ;)
- Protocol / Program
- New protocol to learn
  - =>Not always straight forward

Finally