Deploying Secure NFS in a Large Enterprise

Moritz Willers
mo@wit.ch

Overview

- Why are we doing it?
- NFS v4
- Secure NFS

Why are we doing it?

Because of the Auditors

Up to now ...

... it mostly works!

NFS v4

NFS v4

- Commonly quoted NFS v4 advantages
  - single port
  - strings instead of uid/gid to represent user
  - pseudo file system
  - caching / delegation
  - UTF-8
  - pNFS - with NFS v4.1
  - security

Access Control Lists!

FreeBSD

```
% setfacl -m group:writers:rwxpD:d:allow,\
    group:writers:rw:fi:allow,\
    group:readers:rx:d:allow,\
    group:readers:r:fi:allow dir
```

Solaris

```
% chmod A=group:writers:rwxpD:d:allow dir
% chmod A+group:writers:rw:fi:allow dir
% chmod A+group:readers:rx:d:allow dir
% chmod A+group:readers:r:fi:allow dir
```

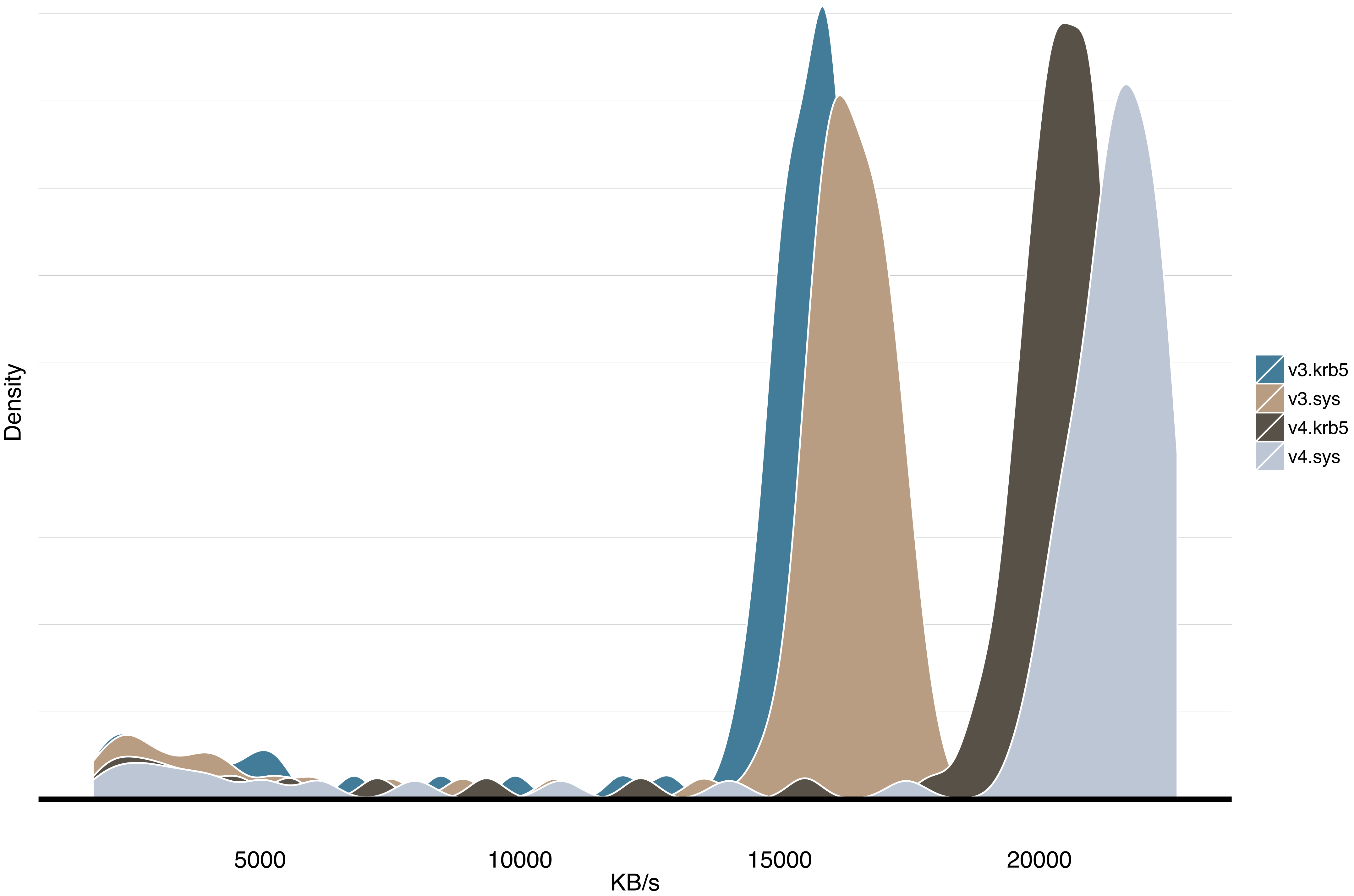
Linux

```
% nfs4_setfacl -s A:dg:writers@nfsdomain.com:rwxaD dir
% nfs4_setfacl -a A:fig:writers@nfsdomain.com:rw dir
% nfs4_setfacl -a A:dg:readers@nfsdomain.com:rx dir
% nfs4_setfacl -a A:fig:readers@nfsdomain.com:r dir
```

NFS v4
Deployment Obstacles

- id mapping
- NFS domain
- “0751”
- -actual
- keeping state
- performance
- bugs (chown)

NFS Performance – RHEL 6.4



Secure NFS

Secure NFS Deployment Obstacles

- Requires a sound Kerberos installation
- Security Negotiation
- NetApp Encryption support - DES only!
- rpc.gssd trouble
- access as root
- bugs (RHEL 5 kernel)

User Home Directories

Applications

Application Credentials

- keytab
  - cron
  - kstart
  - autosys
  - app code (kinit)
  - pam
  - gss-proxy

- Kharon
- S4U
  - every app?
  - pam?
  - gss-proxy?

Recap

- It mostly works
- Unified Name Space is the biggest initial hurdle
- Must have Kerberos well established and understood
- We need a better way to provide non-interactive users with credentials

?