

Legacy filesystems

Förlegade filsystem

Per-Erik Persson

Technical IT-security
Infrastructure
Development
Identity management
DevSecOps
Platform engineering?
~40 years of hacking

index

FTP

NFS

AFS

SMB

ACL

More NFS

GlusterFS

Kubernetes

Questions?

FTP(File Transfer Protocol)

Cleartext

Sftp

Ftps

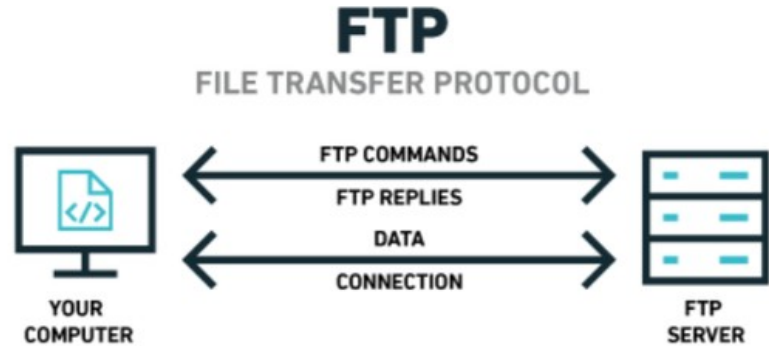
disabled in Google Chrome 88 in January 2021

1980 TCP/IP support

active/passive mode

NAT/FW :-(

TFTP(netboot, today replaced with https)



More forgotten protocols to ignore

Apple Filing Protocol (AFP)

NetWare Core Protocol (NCP)

Bittorent

NetBIOS/NetBEUI

WebDAV

Any commercial UNIX doing NFSv4

NFS(Network File System)

Version 1,2,3,4

Appears as a local filesystem. UGO, RWX 1984

V2 1989

V3 1995 TCP support, performance

webnfs(portmap, mount)

V4 2000 (AFS, SMB attributes)

V4.2 2016(pNFS, multipath, one port!)

All problem solved!



AFS Andrew File System

- + Secure
- + Distributed
- + Caching
- + Opensource
- Big shared files
- Really picky on DNS, NAT and firewalls
- ACL:s only on directories.
- Applications needs to be AFS-aware.
- Does not work in truly distributed environments.(laptops)
- Recompile your kernel.

`/afs/pdc.kth.se/home/<1st letter username>/<username>`



SMB Server Message Bloc

1982 for OS/2

1987 MS+3com

1996 SMB 1.0

Kerberos or NTLM.

SMB 3.1.1 not everywhere yet.

Have you disabled support for older versions?(bring out wireshark!)

Timing and locking problems in linux.(sqlite or pipelines)

SMB 2.0 has Unix extensions



ACL(which one do you mean?)

Filesystem ACL(getfacl)

POSIX.1e ACL(withdrawn drafts)

NFSv4 ACL(nfs4_getfacl)

Active Directory ACL(more complex than I understand, get-acl)

Linux has filesystem support for NFSv4_ACL but not kernel support.

Top problems with NFS3(sloppy admins)

Norootsquash

No IPACL/FW/conf

sara:x:1000:1000:Sara Z:/home/sara:/bin/bash

Multiple groups needed

More metadata needed.

Kerberos

Working DNS

More NFS problems

Nfs4 actually uses the permission model of nfs3 if kerberos is not enabled.

Kerberos requires `addprinc -randkey nfs/hostname@REALM` (on server)

`ktadd nfs/clientname@REALM`

Gssproxy (gssproxy.conf)

`sec=krb5/krb5i/krb5p`

Nfs4_acl applies on nfs3 exports, sometimes..

NFS4 is now working, now lets enable SMB

SMB supports POSIX ACL, which is almost NFS4 ACL, but how about your underlying filesystem?

Buy a netapp, money solves problems.

Enable NFS on windows server :-)

Export filesystem as NFS3 :-)

Acces the same file mounted over both NFS3 and NFS4

Copy and move the file and look what happens to the file.

Try and run sqlite on your nfs/smbmounted disk.

Race conditions on smbmounted disks.

NFS4+Kerberos

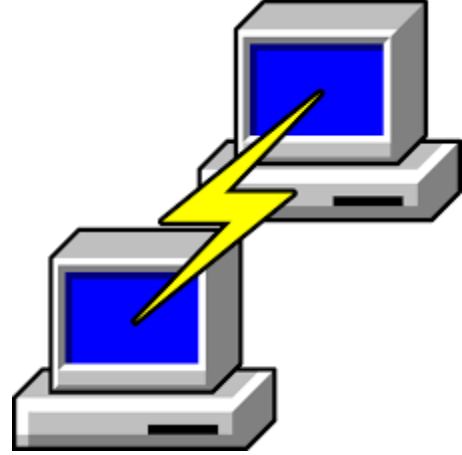
Usermounts requires a personal kerberos token.

How do you convert your ssh-key to a kerberos ticket?

Putty?

Ssh-agent

Can openssh combine different authentication mechanisms?



How to use kerberos with a ssh-key!

```
$ echo 'AuthenticationMethods gssapi-with-mic,publickey' >> /etc/ssh/sshd_config
```

Smartcard via ssh-agent+Kerberos<>sshkeys->Kerberos

Or just use some other MFA solution...

GlusterFS

Client/Server model, can export NFS/SMB

- + A real clustered filesystem.
- + Inotify is working!
- A real clustered filesystem.
- Linux only.
- Picky with versions.
- EOL 2024



Performance?

Jumboframes matters!

Encryption eats up to 50% on NFS4

Appliances claim >100GB/s

How fast can your VM write to the underlying storage system?

Many files on any networked filesystem kills performance, go for S3!

Enable ACL and SELinux to maximize the number of attributes on a file.

Server side copies are sometimes supported.

Kubernetes

All storage vendors wants to hang around with the new cool guy on the block.

Everyone has a csi-driver today.

Most csi-drivers are based on NFS

How do we secure NFS?



File System Changes

File System Protocols

NFSv4.1 with Kerberos

S3 API

Monitoring and Metrics

Supported Features

The Qumulo CSI Driver supports:

- Static and dynamic (expansion) provisioning over NFSv3
- The following Persistent Volume Claim access modes:
 - `ReadOnlyMany`
 - `ReadWriteMany`
 - `ReadWriteOnce`
 - `ReadWriteOncePod`
- NFSv4.1

Important

Even when you enable NFSv4.1 for your Qumulo cluster, you must explicitly [configure NFSv4.1 to work with Kerberos](#).

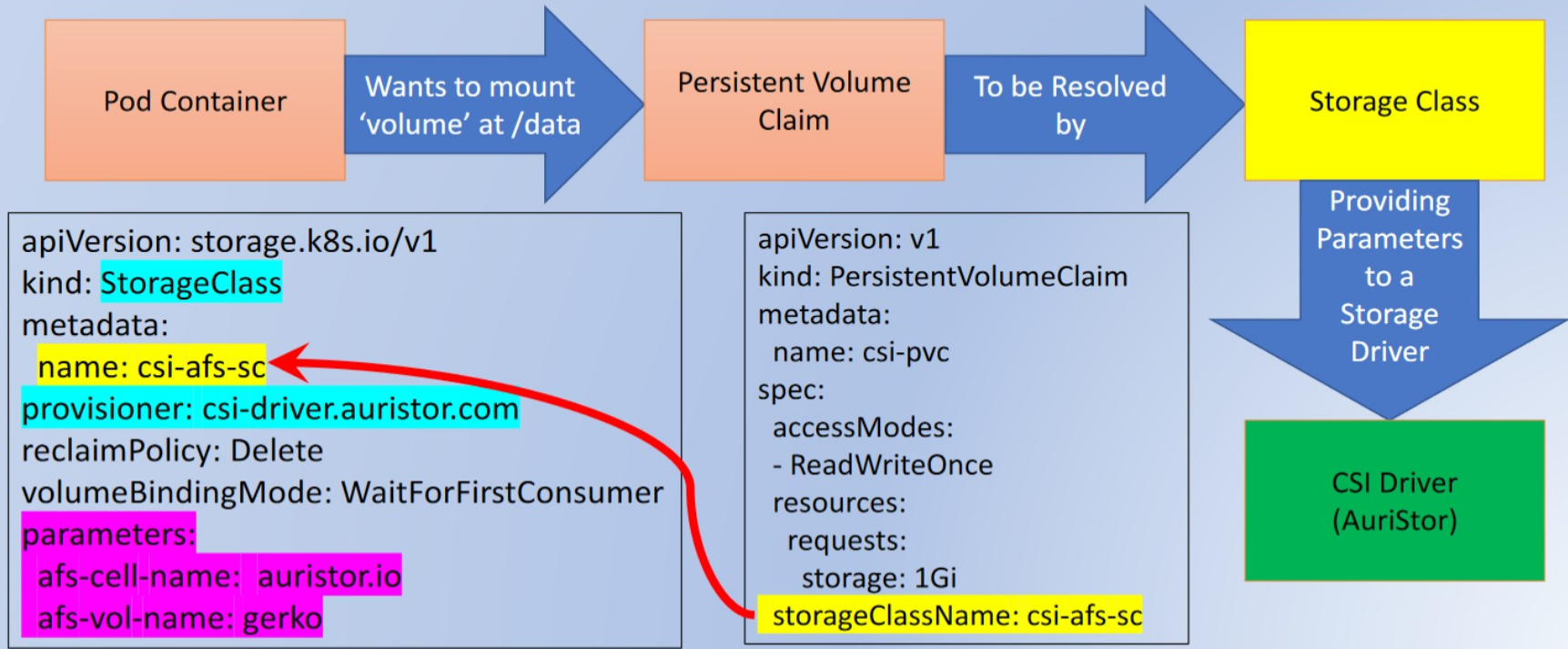
Unsupported Features

- Volume cloning 
- Volume snapshot and restore 

Could it be any worse?

What could be worse than NFS+AD as a dependency for your kubernetes cluster??

What the Cluster (Storage) admin Specifies



Summary

Don't be afraid of SMB as long as it is not served by a windows computer.

Avoid NFS or SMB in k8s, rewrite you applications to use modern patterns.

Can your k8s cluster survive without AD and vice versa?

Can one be compromised by the other one?

How many NFS3 servers and SMB1 shares do you have around?

And Glusters?

Storageevendors seems to like NFS, why should they use ceph or longhorn?

Questions?

peptekmail@gmail.com



gssproxy.conf

```
[service/my_app]
```

```
mechs = krb5
```

```
cred_store = keytab:/etc/path/to.keytab
```

```
euid = appuser
```

```
program = /usr/local/bin/my_app
```

