AFS 3	NFS 3
Architecture	
File servers and clients form a logical administrative unit called a *cell*.	File servers and clients. Each file server is managed independently.
Administration by collections of files called *volumes*.	Administration by individual files.
Common, global name space viewed by all machines.	Name space not always viewed consistently across machines.
Automatic file location tracking by system processes and Volume Location Database.	Mountpoints for tracking file's physical location set by administrators and users.
Stateful servers.	Nearly stateless servers.
Performance	
Robust disk caching reduces file server and network load.	Memory caching with small buffers.
Server callbacks guarantee cache consistency. Open-to-close semantics. Attributes cached several hours.	Time-based cache consistency may cause inconsistencies to occur. Attributes cached 3-30 seconds.
Network traffic reduced by callbacks, large buffers.	Network traffic increased by limited caching.
Replicas spread the load among preferred servers.	No replication to reduce load.
Excellent performance in wide-area configurations.	Inefficient in wide-area configurations.
Scaleable; maintains performance in any size installation.	Best in small- to medium-size installations.

AFS 3	NFS 3
Availabilty	
Read-only replication by volume. Automatic switchover to available replica.	No staelcation to reduce load.dard data replication.
Files remain available to users during reconfiguration. File names remain the same.	Users lose access to files during reconfiguration. File moves require mountpoint changes to adjust file names.
Management	
Management tasks executed from any machine.	Management tasks frequently require telnet to designated machines.
Disk quotas based on volumes; easy for user to check status.	Disk quotas based on user ID; difficult for user to check status.
No system downtime with AFS Backup System.	Standard UNIX backup requires system downtime.
Backup clones often used for user-controlled restores.	All restores require administrator assistance.
Security	
Kerberos version 4 authentication.	Unencrypted user IDs, trusted users and hosts. Can be kerberized.
Access control lists for fine tuning directory access. UNIX mode bits for the owner.	Access control with standard UNIX mode bits on files and directories.
User-definable groups.	Groups defined by system administrator.
Mutual authentication by system processes and databases. Always uses secure RPC.	Can use secure RPC.