NAS: Regulatory compliance data store
A case study

Milan Shetti
Chief Technologist – NAS and File Services
Network Storage – Sun Microsystems Inc

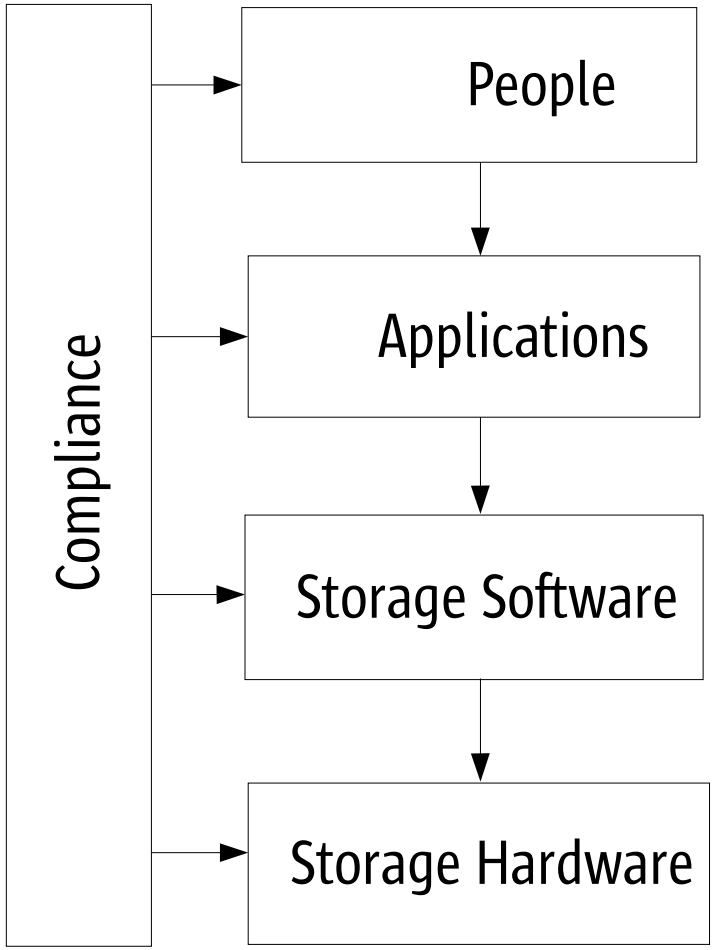
Keith Smith
Staff Engineer - Chief Architecture Office
Network Storage – Sun Microsystems Inc

Compliance Archiving Software
Big Picture

- Compliance offering for NAS family
- Software licensed module for SE 5310 NAS
- Provides:
  - WORM files
  - Retention periods
  - Administrative lock-down

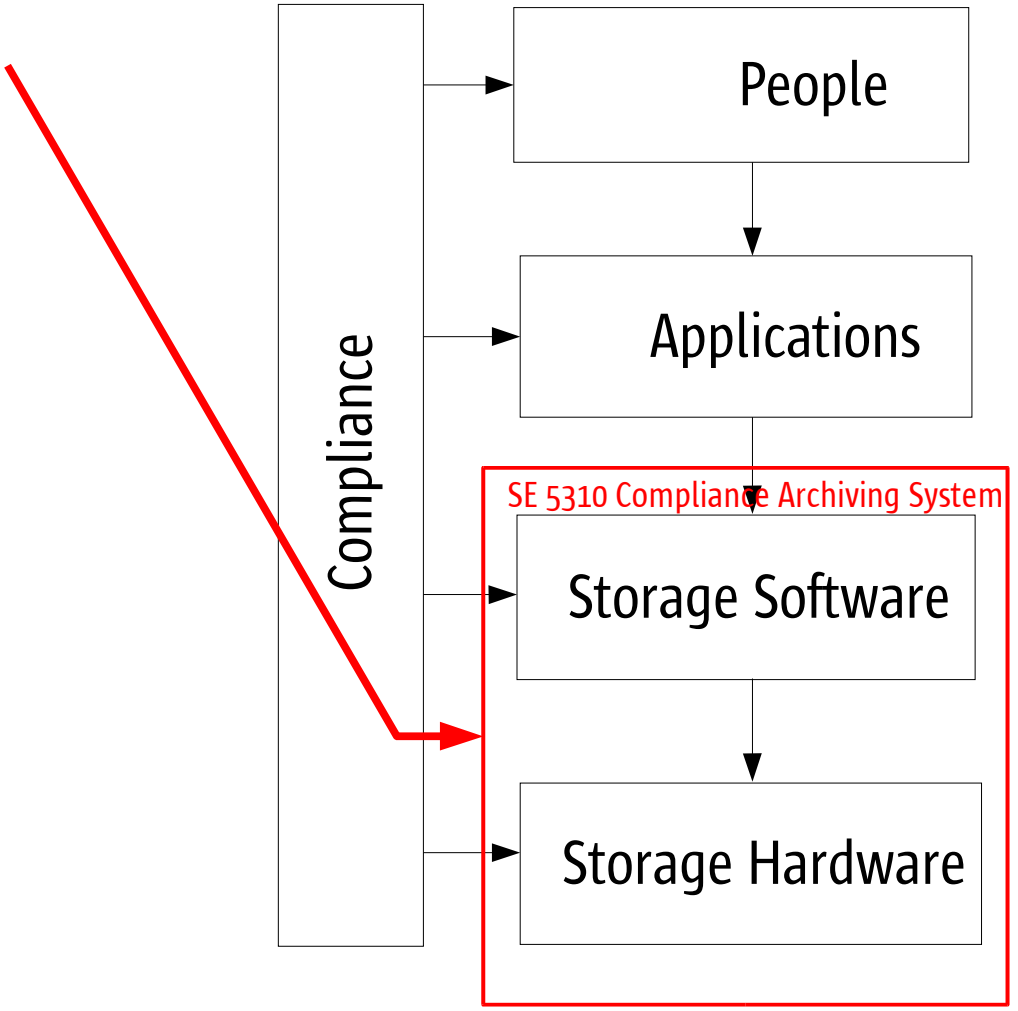
What is Compliance?

- Business process for birth-to-death management of records
- Ensure that records are preserved, protected, and accessible when needed
- Storage is only part of the solution



Role of SE 5310 Compliance

- SE 5310 goes here
- Expected use with "Compliance aware" applications
  - From ISVs
  - Home-grown customer applications



SE 5310 Compliance Features

- WORM files
- Retention Periods
- Administrative Lock-down

WORM Files

- Goal: Guarantee record immutability
- Solution: WORM Files
  - Permanently read-only files
  - Software enforced (by NAS file system)
  - Client application converts regular file to WORM
  - Can mix WORM and regular files on same system

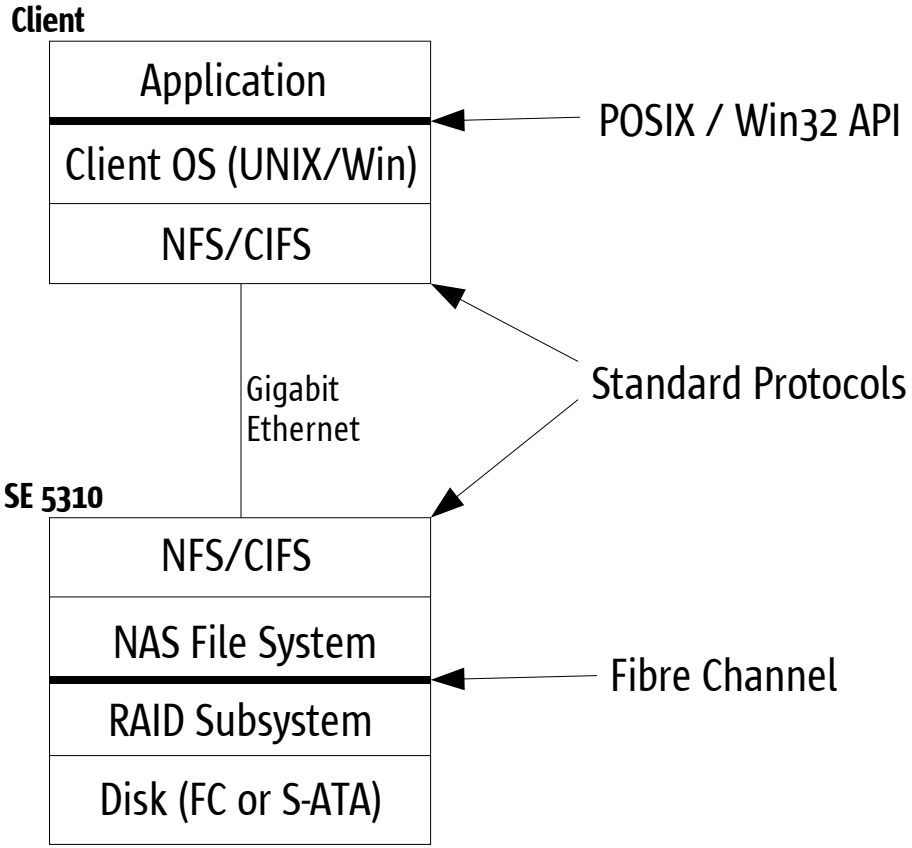
Retention Management

- Goal: Guarantee record lifetime
- Solution: Per-file *retention period*
  - File cannot be deleted during retention period
  - Only WORM files have retention periods
  - Retention period assigned when file becomes WORM
  - Retention can be extended, not decreased

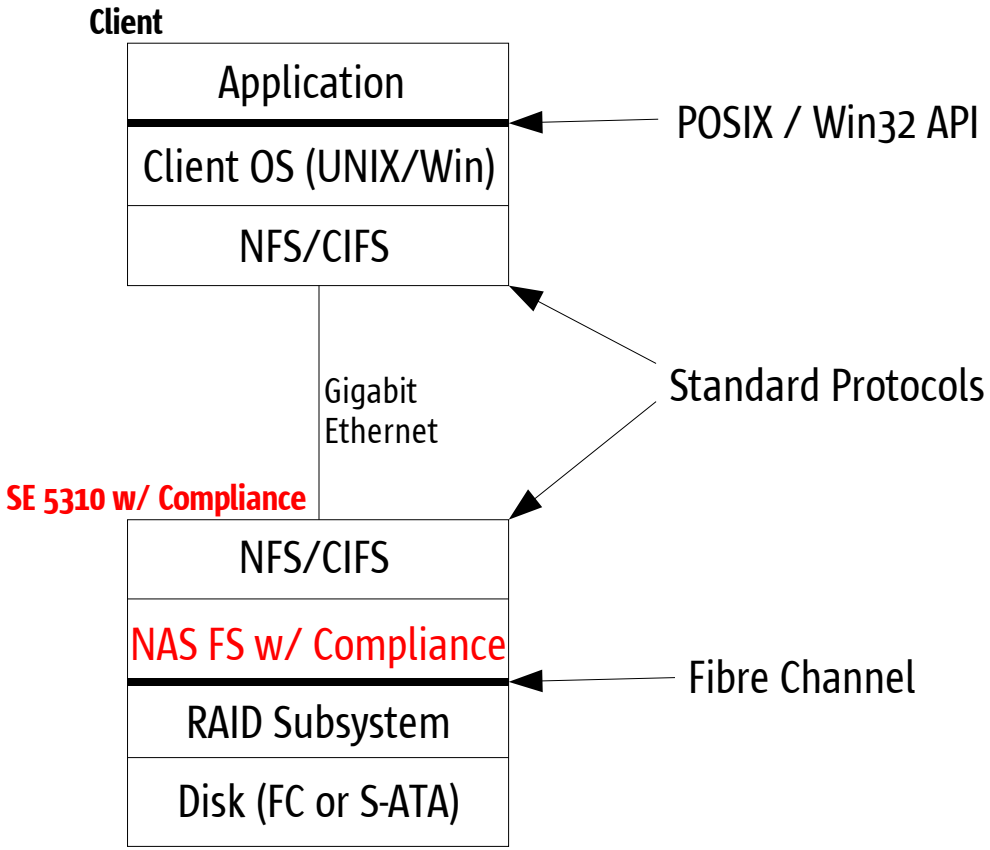
Administrative Lock-Down

- Goal: Prevent administrative subversion of WORM and retention
- Solution: Limit administrator capabilities
  - Cannot delete LUN or file system with WORM files
  - Cannot overwrite WORM files via snapshot restore
  - Secure Clock – cannot subvert retention by resetting system clock

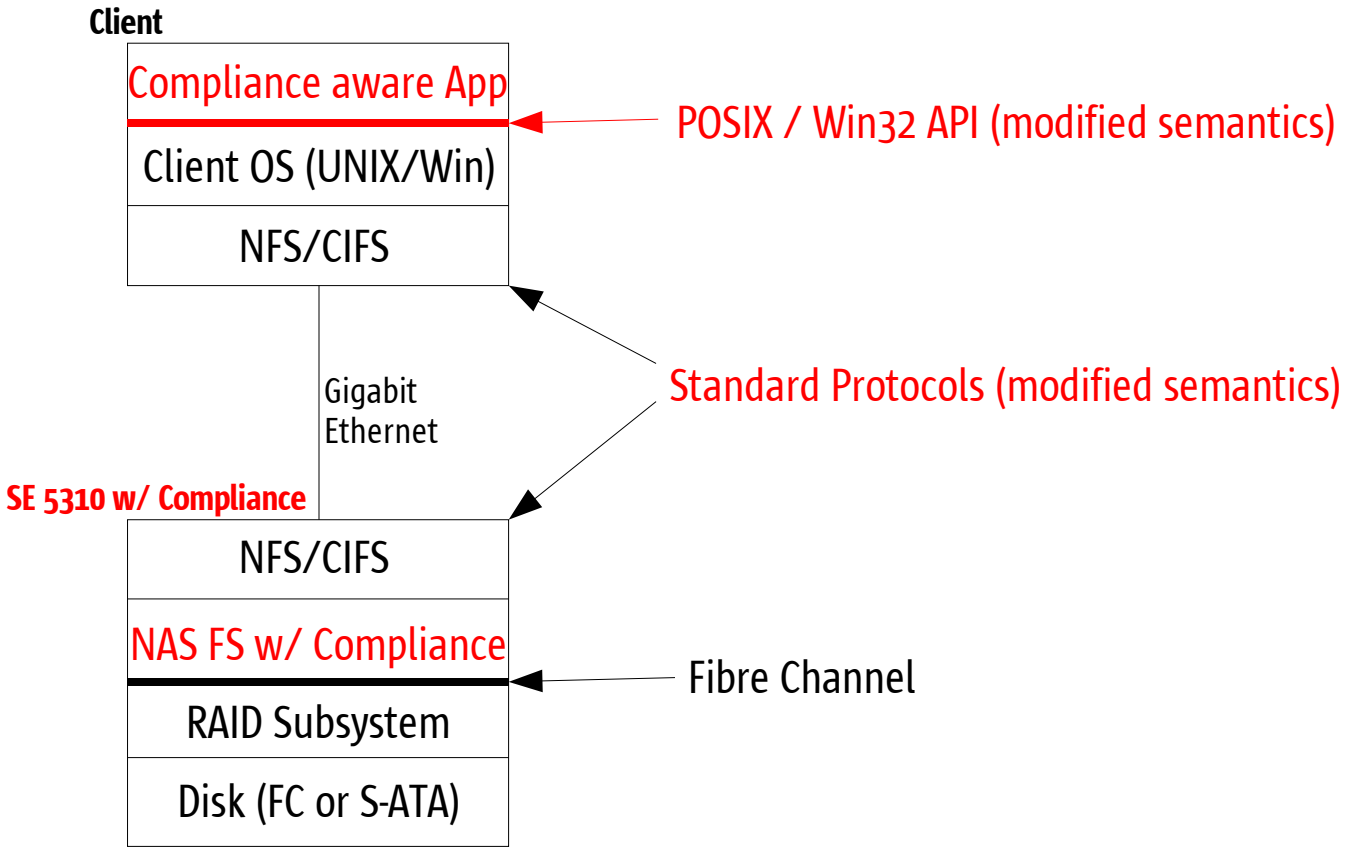
SE 5310 Compliance Implementation



SE 5310 Compliance Implementation



SE 5310 Compliance Implementation



SE5310 Compliance Interface

- Piggy-back on existing NFS and CFS protocols
- Store WORM status and retention period in standard file meta-data
- Overload existing commands to invoke compliance functionality
- Engage ISVs to support 5310 with content creation/mgmt. applications

SE5310 WORM Interface

- Changing permissions makes file WORM
  - chmod 4000 from UNIX clients
  - Set read-only and system bits from Windows clients
  - Executable files cannot be WORMed
- WORM files cannot be:
  - Modified, extended, overwritten
  - Renamed
  - Changed to non-WORM

SE5310 Retention Interface

- Clients store retention-end time in file's access time (atime) attribute
  - Via *utimes(2)* or *touch(1)* on UNIX clients
  - This is only way to modify atime
- Cannot delete WORM file unless current time is later than retention-end
- Default retention
  - If client does not provide retention-end time, default value is used

SE5310 Retention Interface

- Extending Retention
  - > Reset atime on WORM file
  - > Can extend retention or assign new retention to file with expired retention
  - > Cannot decrease retention
- Permanent Retention
  - > Preserve a file forever
  - > Never allow it to be deleted
  - > Indicated by special atime value (INT_MAX)

SE5310 Compliance
Typical Usage

- Create and write file
- Set atime to indicate retention period
- Issue worm trigger (e.g., chmod 4000)
  - File cannot be modified – ever
  - File cannot be deleted until end of retention

Call for enhancements in protocols

- Ability to assign new attribute
  - atime used by some backup applications
- Ability to assign extended attribute (search/query)
  - need query mechanism to search compliance data
- File close operations on NFS
  - thanks to NFSv4

NAS: Regulatory compliance data store
A case study

Milan Shetti
Chief Technologist – NAS and File Services
Network Storage – Sun Microsystems Inc

Keith Smith
Staff Engineer - Chief Architecture Office
Network Storage – Sun Microsystems Inc