A Proposal for Access Controls (aka SAN Boxes)

T10/99-278 revision 1

Jim Hafner
IBM
November 3, 1999

SAN Promise and Problem

- **Promise**: pool storage devices on SAN for ease of management
- **Problem**: SCSI not suited for "big shared bus"
  - data integrity and privacy at risk
  - Reservations inadequate
- **Conclusion**: We need something new!

[PAM = Partition Access Manager = "owner of AC config space"]

Design Points

- Access rights enforced at target
- Granularity
  - at initiator side: host/OS-image (not initiator HBA)
  - at target side: LU or Element within LU scope
- Access control config cmds initiator-independent (not like Reservations)
- Support all device types
- Minimum performance impact
- All parties (targets/hosts/PAM) have shared/balanced responsibilities

Host Identification for Access

- **AccessID**: transport independent (16bytes)
  - **ACCESS ID REGISTER:** registered over each port to target
  - target maps rights of AccessID to port(s)
  - mapping stable until "logout" of port
- **TransportID**: transport dependent
  - defined in appropriate protocol spec
  - for FCP: 24 bytes containing N_PortID, ProcessAssociator, WWPortName, WWNodeName (each with validity flag)
- **VS?**

Granting/Revoking Access - ACCESS CONTROL OUT

- **MANAGE ACL**: from PAM, used to manage
  - AC enable/disable, ID grant/revoke, persistence (PTPL), clear, flush, revoke proxies, etc.
  - ACCESS CONTROLS GENERATION value (optional)
    - used to scope use of MANAGE ACL service action
- **PROXY ACCESS**: from host *with* access to third party
- rights of port are logical "or" of all grant actions to IDs mapped to port
- Revocation:
  - revocation of all grants
  - abort of all commands (and other cleanup)

Preserving Access Controls

- target required to maintain minimal nonvolatile state flag per LU
  - any access restrictions on LU? none?
- target can/should support full nonvolatile preservation of entire access control info (PTPL)
  - list of PAM-granted access rights
  - ACCESS CONTROLS GENERATION value
  - proxies are not preserved

Reporting Access Controls - ACCESS CONTROLS IN

- **REPORT ACL**: report entire access control list (to PAM)
  - scopes for which AC are enabled
  - all AC entries for all scopes/Initiator Identifiers
  - all proxies
- **REPORT INITIATOR ACL**: report summary relevant to initiator (to host)

Verifying Access Rights

- all commands handled in usual way, when initiator has access rights:
  - AC disabled
  - port has proxy (and cmd is *not* PROXY ACCESS)
  - port has rights either by registered AccessID, TransportID, other
- if initiator has no access rights:
  - some commands allowed (same as if active reservation)
  - some commands blocked with new ASC/ASCQ
    - ACCESS DENIED - INITIATOR NOT AUTHORIZED
    - ACCESS DENIED - INITIATOR NOT REGISTERED

Proposed Command Set Summary

- **IN** service actions (Opcode 85h)
  - **REPORT ACL** (mandatory)
  - **REPORT INITIATOR ACL** (optional)
- **OUT** service actions (Opcode 86h)
  - **ACCESS ID REGISTER** (mandatory)
  - **MANAGE ACL** (mandatory)
  - **PROXY ACCESS** (optional)

(Formal request for opcode values is forthcoming.)

ASC/ASCQ Summary

ASC	ASCQ	Name	Function
XXh (2Eh)	00h	ACCESS DENIED	Initiator is not sufficiently authorized to make request
XXh (2Eh)	XXh (01h)	ACCESS DENIED - INITIATOR NOT REGISTERED	Initiator has not sent an ACCESS ID REGISTER service action
XXh (2Eh)	XXh (02h)	ACCESS DENIED - INITIATOR NOT AUTHORIZED	A registered initiator has access permissions insufficient for the requested command
XXh (2Eh)	XXh (03h)	ACCESS DENIED - INVALID GENERATION KEY	The GENERATION KEY value is not valid
XXh (55h)	XXh (05h)	INSUFFICIENT ACCESS CONTROL RESOURCES	The device server has exhausted its resources for access controls

(Formal request for values in parentheses is forthcoming.)

Accept/Reject Action Items

- Requirement for Access Controls (in some form)
- Requirement for new opcodes
- Requirement for new ACCESS DENIED ASC/ASCQs (or STATUS?)
- Principle of AccessID and/or TransportID and/or VS
- Principle of LU and/or element within LU granularity
- Set of service actions
  - REPORT ACL, REPORT INITIATOR ACL
  - ACCESS ID REGISTER, MANAGE ACL, PROXY ACCESS
- Principle of PTPL feature
- Principle of "access restricted cmds" analogous to reservations
- Principle of ACCESS CONTROLS GENERATION value and KEY in REPORT ACL and MANAGE ACL

Contacts

- **Details**: `ftp://ftp.t10.org/t10/document.99/99-245r1.pdf`
- **e-mail**: `hafner@almaden.ibm.com`
- **phone**: 408-927-1892
- **fax**: 408-927-4182