T10/00-101r0

Minutes of Access Controls teleconference - 11/18/99

by Rob Elliott (Robert.Elliott@compaq.com)
and Jim Hafner (hafner@almaden.ibm.com)

A conference call was held on 18 November 19999 from 10:00am-12:30pm Central Time to review T10/99-245r2 by Jim Hafner (IBM). The call was hosted by Compaq Computer Corporation.

### 1.1 Attendees

| Company | Name |
|---|---|
| Adaptec | Larry Lamers |
| Compaq | Rob Elliott |
| Compaq | Carl Zeitler |
| Compaq | Thomas Grieff |
| Compaq | Tod Rushton |
| Compaq | Jim Pherson |
| Crossroads | Dexter Anderson |
| IBM | Jim Hafner |
| IBM | David Chambliss |
| IBM | George Penokie |
| LSI Logic | Ralph Weber |
| LSI Logic | Rod Dekoning |
| LSI Logic | Charles Binford |
| Quantum | Mark Evans |
| Seagate | Gene Milligan |
| Sun | Bob Snively |
| Western Digital | April Zacker |
| Western Digital | Ken W…? |

### 1.2 Initiator identifier: access ID vs. transport ID

Revision 2 includes both access IDs and transport IDs. Transport IDs are needed for booting, since boot firmware may not have a place to store a previously assigned access ID. Ralph Weber questioned why access IDs are needed, since transport IDs must be used to boot. Jim pointed out that transport IDs need only be used for boot devices, while Access IDs can be used for all other devices. In an environment where systems boot from local storage, transport IDs would not be needed at all.

Charles Binford had a question about Note 2 on Page 9. He will follow up in email.

This proposal is focused on Fibre Channel FCP devices. There is no mention of how transport IDs would be defined for SCSI parallel devices (e.g. SPI-4). For SPI devices, the transport ID would likely equal the SCSI device ID. Other protocol standards like SVP and SST should be similar to FCP. Jim will add SPI considerations to the proposal.

### 1.3 Access controls for extents and elements

The proposal does not deal with extents. Ralph Weber agreed with this, noting they have been dropped from persistent reservations and SCSI.

Revision 2 includes support for elements. No representatives from media changer companies were present on the call; it's unclear whether tape vendors or users are interested. If tape support is not important, Ralph suggested removing details about element support (leaving probable needed fields reserved) until someone plans to use it. Jim Hafner agreed to check with Paul Suhler and Erich Oetting (StorageTek; SMC editor) about the level of interest from the tape community and to ask them to review the current proposal.

### 1.4 Preserve through power loss

If indicated, there is at least one bit per LUN that remembers if access controls were in place before power loss. Devices may optionally remember their entire access control list. The group agreed with the proposal.

### 1.5 Access Controls vs. Persistent Reservations

The group discussed Bob Snively's suggestion that persistent reservations could be extended to provide access-control capabilities. Bob felt the main different is the password/generation/access control key that devices must have to change the access controls. In PR, any device can easily register.

Ralph noted that persistent reservations are designed for cooperating initiators; access controls are designed for non-cooperating initiators.

Making the PR Register operation harder to do (with a more secure key) would allow exclusive-access-registrants-only persistent reservations to serve a similar purpose. Additional service actions would be needed to mimic the access control proxy feature with third-party reservations.

Ralph Weber noted that access controls are intended to be static, while persistent reservations are more likely to change dynamically. Access control management software is not intended to live in the clustering operating systems; it is run on a separate management device.

Jim noted that access controls works with non-quorum devices that don't know about reservations and clustering operating system which don't use persistent reservations. Ralph felt that existing persistent reservation algorithms might break any PR extension (from key overlap to the mechanisms to break through PR already present). Access controls do not depend on the clustering software to cooperate.

Access controls provide similar features to switch-based zoning (if implemented at the logical unit level). Bob Snively noted that Access Controls will keep the error messages at the SCSI level, where they belong. Bob reserved the right to oppose the proposal.

### 1.6 Overriding keys

The first revision asked devices to provide a serial number that could only be learned via physical access to the device to use to override access controls in case the management software fails or the device is returned to the factory. Some target vendors felt this was too expensive.

The second revision removed all mention of overriding keys, assuming that the management software must be reliable enough not to worry about losing keys. Factory overrides would be handled in a vendor-specific manner – perhaps a jumper on the device, or a vendor-specific command/mode page.

Bob Snively felt that a more generic means to override keys should be added. One possibility is to allow WRITE_BUFFER with the Download microcode option. This is currently a way to break through persistent reservations. This requires the management device to have copies of all necessary firmware, and to be able to identify the devices well enough to send the correct firmware. Bob suggested an Access Control service action. Some participants felt that would be too easy to accidentally or malevolently access. George Penokie suggested a new WRITE_BUFFER service action to override access controls. Since WRITE_BUFFER is not used by general-purpose software, so would be safer to use than an Access Control service action.

No resolution was reached on this issue. Total management software failure with loss of keys seems unlikely. If PAM fails, the devices might still maintain their access control lists (depending on their own preserve-through-power-loss capabilities).

### 1.7 Status from enrolling with no rights

There is no indication from the target whether any access rights were granted when an initiator enrolls. If the initiator has no rights, it still gets a GOOD status. Should there be a different status returned based on whether rights were granted? The group agreed to leave the status as GOOD and require software that cares about the result to run an Report Initiator ACL service action.

### 1.8 Unit Attention condition

If an initiator has access rights and PAM comes along and removes access, should it receive a Unit Attention? Bob Snively said the most important thing is that the transition from successful commands to

denied commands occur at exactly one time – after a command is denied, no subsequent commands should be allowed. All prior commands, on the other hand, must be allowed. Gene Milligan noted that commands could be queued with access control checks done when the commands are dequeued, so the text may need to reflect that. Jim will not add a special Unit Attention, and will clarify the wording regarding queuing and ordering.

### 1.9 Service actions

Bob Snively suggested a "reset all" service action rather than forcing software to reset everything individually. This action might require use of the manage ACL key.

### 1.10 Proxy

Discussion of this topic was deferred until the January meeting.

### 1.11 Access Controls vs. hiding devices by changing Inquiry data

Nobody felt that an alternative approach was needed.

### 1.12 Action Items

- Charles Binford will send Jim Hafner his question about Note 2 on page 9.
- Jim Hafner will document a transport ID definition for SPI devices.
- Jim Hafner will check with Paul Suhler and Erich Oetting about element support.
- Jim Hafner will clarify how the transition from allowed to denied must occur.
- Jim Hafner will consider a "reset all" service action.
- Jim Hafner will prepare Revision 3 in December, ready for the January SCSI Working Group meeting. Most of the interested parties plan to attend that meeting.