

TO: T10 Membership, ADC-3 Working Group
FROM: Rod Wideman, Quantum; rod.wideman@quantum.com
DATE: April 21, 2009
SUBJECT: ADC-3 Remove Configure Encryption Policy mounted volume restriction
(document T10/08-247r2)

Rev0 – Initial draft.

Rev1 – Updated to accommodate feedback received on initial draft; now includes provision for use of offline and appropriate unit attention.

Rev2 – Updated per feedback received during April 1st 2009 working group meeting.

Related Documents

ADC-3r00b

Introduction

This document proposes a change to 6.3.5.3, Configure Encryption Policy page, to modify a restriction when a volume is mounted, as well as a change to 6.2.2.3.2, RMC logical unit descriptor format, to clarify what happens on a transition from offline.

Discussion

Subclause 6.3.5.3 currently states that if the DT device has a saved set of data encryption parameters or has a volume mounted the ADC device server shall terminate the command. This restriction creates a problem for automation devices, particularly in power-on scenarios. If one or more volumes are mounted in DT devices (i.e., drives), and a power cycle occurs, then this restriction would require the automation device to unmount each mounted volume prior to configuring each drive again, which can be impractical in certain automation products.

Following a power cycle, there would not be a saved set of data encryption parameters anyway, so this additional restriction for this scenario appears unnecessary (i.e., RMC application clients need to retrieve policy status again regardless). However, removing this restriction entirely may create a problem for applications that retrieved encryption control information when a volume was mounted, and expect it to remain unchanged for the duration of the volume mount.

Most recent working group discussion found that SSC-3 currently has statements that also restrict changing the encryption parameters while a volume is mounted, so this most recent revision now focuses on allowing the combination of the port being disabled and a volume mounted, in such a way that the DT device unmounts the medium to satisfy the requirement.

As a result, automation products should be able to re-establish encryption control following a power cycle without having to unmount each volume.

Proposed Changes to ADC-3

Proposed new text is shown in blue. Proposed deletions are shown in ~~red-strikeout~~.

Changes to 6.3.5.3

(Third paragraph following table 72)

The CONTROL POLICY CODE field specifies the data encryption parameters control policy for the DT device (see 4.10.1). If the DT device has a saved set of data encryption parameters, then the ADC device server shall terminate the command with CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to INVALID FIELD IN PARAMETER LIST.

[alternate A]

If the DT device has a medium mounted (i.e., is in load state (i), see 4.4.1) and the ENABLE bit set to zero in the RMC logical unit descriptor (see 6.2.2.3.2), then the DT device shall perform actions to cause the MTHRD bit (see 6.1.2.2) to be set to zero (i.e., unthread the medium). If the DT device has a medium mounted and the ENABLE bit set to one in the RMC logical unit descriptor, then the ADC device server shall terminate the command with CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to INVALID FIELD IN PARAMETER LIST.

[alternate B]

If the DT device has a medium mounted (i.e., is in load state (i), see 4.4.1) and would report the PE bit set to zero in all primary port descriptors returned in response to a MODE SENSE command requesting the DT Device Primary Port subpage (i.e., no primary ports are enabled, see 6.2.2.2), then the DT device shall perform actions to cause the MTHRD bit (see 6.1.2.2) to be set to zero (i.e., unthread the medium). If the DT device has a medium mounted and would report the PE bit set to one in any primary port descriptor returned in response to a MODE SENSE command requesting the DT Device Primary Port subpage (i.e., a primary port is enabled), then the ADC device server shall terminate the command with CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to INVALID FIELD IN PARAMETER LIST.

[Note: either alternate text is intended to be part of the first paragraph. The difference between them is the indicator used for the primary ports being enabled or not. Consideration for incorporation into ADC-3 would be for only one of the alternate texts.]