LEGAL NOTICE:

© Copyright 2008 to 2024 NVM Express®, Inc. ALL RIGHTS RESERVED.

This Technical Proposal is proprietary to the NVM Express, Inc. (also referred to as "Company") and/or its successors and assigns.

NOTICE TO USERS WHO ARE NVM EXPRESS, INC. MEMBERS: Members of NVM Express, Inc. have the right to use and implement this Technical Proposal subject, however, to the Member's continued compliance with the Company's Intellectual Property Policy and Bylaws and the Member's Participation Agreement.

NOTICE TO NON-MEMBERS OF NVM EXPRESS, INC.: If you are not a Member of NVM Express, Inc. and you have obtained a copy of this document, you only have a right to review this document or make reference to or cite this document. Any such references or citations to this document must acknowledge NVM Express, Inc. copyright ownership of this document. The proper copyright citation or reference is as follows: **"© 2008 to 2024 NVM Express, Inc. ALL RIGHTS RESERVED."** When making any such citations or references to this document you are not permitted to revise, alter, modify, make any derivatives of, or otherwise amend the referenced portion of this document in any way without the prior express written permission of NVM Express, Inc. Nothing contained in this document shall be deemed as granting you any kind of license to implement or use this document or the specification described therein, or any of its contents, either expressly or impliedly, or to any intellectual property owned or controlled by NVM Express, Inc., including, without limitation, any trademarks of NVM Express, Inc.

LEGAL DISCLAIMER:

THIS DOCUMENT AND THE INFORMATION CONTAINED HEREIN IS PROVIDED ON AN "**AS IS**" BASIS. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, NVM EXPRESS, INC. (ALONG WITH THE CONTRIBUTORS TO THIS DOCUMENT) HEREBY DISCLAIM ALL REPRESENTATIONS, WARRANTIES AND/OR COVENANTS, EITHER EXPRESS OR IMPLIED, STATUTORY OR AT COMMON LAW, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, VALIDITY, AND/OR NONINFRINGEMENT.

All product names, trademarks, registered trademarks, and/or servicemarks may be claimed as the property of their respective owners.

The NVM Express® design mark is a registered trademark of NVM Express, Inc.

NVM Express Workgroup
c/o VTM, Inc.
3855 SW 153rd Drive
Beaverton, OR 97003
USA
info@nvmexpress.org

NVM Express® Technical Proposal (TP)

Technical Proposal ID	TP4152 Post Sanitize Media Verification
Revision Date	2024-04-01
Builds on Specification(s)	NVM Express Base Specification 2.0c NVM Express NVM Command Set Specification 1.0c NVM Express Zoned Namespace Command Set Specification 1.1c NVM Express Key Value Command Set Specification 1.0c
References	

Technical Proposal Author(s)

Name	**Company**
David Black	Dell EMC
Austin Bolen	Dell EMC
Chandra Nelogal	Dell EMC
Curtis Ballard	HPE
Matt Goepfert	HPE
John Geldman	KIOXIA
Paul Suhler	KIOXIA
Dan Hubbard	Micron
Mike Allison	Samsung
Judy Brock	Samsung
Bill Martin	Samsung
Andrés Baez	Solidigm
Jonathan Hughes	Solidigm
Christoph Hellwig	Western Digital
Yoni Shternhell	Western Digital

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

Technical Proposal Overview

This proposal defines extensions to the Sanitize command, sanitize operations and the Read command that enable verifying correct sanitization by reading sanitized user data from media. A state machine encompasses existing sanitization behavior as well as the new behaviors defined in this proposal. This state machine defines existing behavior and adds the Media Verification state and the Post-Verification Deallocation state, which support verification of sanitized media.

If a Read command is processed while the NVM subsystem is in the Media Verification state, then the command returns data from media, even if the sanitize operation invalidated internal checksums. Multiple reads of the same logical block are allowed to return differing data; this serves to obscure media characteristics that might be inferred from analysis of repeated reads of the media.

A new sanitize action in the Sanitize command changes the NVM subsystem from the Media Verification state to normal operation. During that change to normal operation, the NVM subsystem is in the Post-Verification Deallocation state and all user data is deallocated.

Revision History

Revision Date	Change Description
2023-02-08	Initial draft
2023-02-18	Fixes to review comments and additional contents
2023-02-24	Merged content from multiple changes
2023-03-01	Changed the generic “reports sanitize completion by Asynchronous Event” to the specific AENs. Removed hyphens from all seven instances of “post-sanitize”. (29 instances did not have the hyphen.) Removed descriptions of media verification mode occurring *after* a sanitize operation. Tentatively use “completion of sanitize processing” to refer to the point at which crypto erase, block erase, or overwrite is done, and the Media Verification state is entered. Added comments on areas that will be affected by TP4153 (Sanitize Per Namespace). Added Annex A.
2023-03-03	Added Persistent Event Log event for entry to post-sanitize media verification mode. Additional editorial clean up
2023-03-07	Added co-authors. Removed acronyms for states. Removed “Sanitize” from state names in text and in the state machine figure. Removed “post sanitize” from “media verification”. Changed some legacy instances of “contains” to “indicates”. Aligned the wording of all instances of “Enter Media Verification Mode bit”. Expanded the Media Verification Support into three bits, one for each sanitize action. Closed accepted comments; to be removed in next revision.

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant’s agreement. Copyright © 2008 to 2024 NVM Express, Inc.

2023-03-14	Added a definition for sanitization target. Prohibited a Sanitize command from specifying Media Verification and the Overwrite sanitize action. Removed the OWVS (support) bit. Prohibited a Sanitize command from specifying Media Verification and the No-Deallocate After Sanitize bit set to '1. Added the Deallocation state to the state machine. Moved additional media modification from state transitions into the In Processing states. Added a field to the Sanitize Status log page to indicate the state machine state. Added a section for possible changes to the NVM Command Set Spec.
2023-03-16	Added missing sponsors. Added requirement that CLR shall not change the state. This removed the transition from Media Verification state to Idle state. Swapped transition labels C/D, so that A-B and A-C are successful sanitization. Swapped transition labels E/F, so that E is in the pre-TP4152 implied state machine. G and H are the new transitions for TP4152. Addressed comments by Dan Hubbard. Added Verify Media bit to the Read command.
2023-03-20	Addressed new comments by Dan Hubbard. Added Controller Level Reset to each state transition figure (table). Modified state transition figures to have a separate column for labels. Added NVM Express header page.
2023-03-29	Added first draft of Technical Proposal Overview. Filled in details of the descriptions of changes for changes documents. Incorporated comments from Matt Goepfert. Accepted comments were closed *without* replying "Accepted". Added new wording for not aborting a Read because of bad checksums, while in the Media Verification state. Specified transitions for changing the composition of the NVM subsystem. Restructured requirements for Read commands in Media Verification state. Added effects of changes in composition of the NVM subsystem preventing completion of sanitize processing. Corrected actions of the Media Verification:Deallocating transition.
2023-04-05	Incorporated Mike Allison's comments from 2023-04-04, and resolved some. Moved details of Read command with VM bit = 1 into the NVM Cmd Set Spec. Deleted previously-closed comments. Closed resolved comments from Matt Goepfert.
2023-05-17	Removed changes to Read command SQE, i.e., removed the VM bit. Added new Successful Media Verification Read status code to Base and NVM Cmd Set specs. Updated Read command media verification state requirements to return it.

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

	Merged BEVS and CEVS bits into a single Verification Support (VERS) bit. Modified transitions from In Process Restricted/Unrestricted states to consider CLRs that were caused by NVM Subsystem Reset, PCIe Conventional Reset, or PCIe Function Level Reset. (This excludes CLRs due to host clearing the CC.EN property to '0'.) Added Media Verification Cancelled (MVCAND) bit to the Sanitize Status log page. MVCAND is used to determine some state transitions. Added change to Figure 140 (Sanitize Operations and Format NVM Command – Admin Commands Allowed). Replaced references to restricted/unrestricted completion mode with references to the appropriate states. Added self-loop transitions to the In Process states to define the effects of the different resets.
2023-05-19	Changes from 2023-05-18 Technical WG meeting and comments from Mike Allison: Fig. 140: Simplified additional restriction description for the Sanitize command and moved detailed requirements to the description of each state. Added verification cancelled bit to the PEL Sanitize Completion Event. Added explanation of clearing the Sanitize Media Verification AEN. Rewrote the descriptions of the self-loop transitions for the In Process states for clarity. Accepted all changes.
2023-05-24	Addressed most new comments from Dan Hubbard, especially those pertaining to resets.
2023-05-25	Changes from the 2023-05-25 meeting of the Technical WG: • Revised descriptions of PCIe events that cause CLRs. • Clarified usage of BES and CES bits. • Clarified SPROG field in Figure 267. • Corrected text describing when the MVCAND bit shall be '0' in Figure 267. Deleted comments that were closed prior to the meeting. Added Austin Bolen's comments and resolved some. New questions in comments: • Should the Sanitize Progress (SPROG) field be extended to report on the Deallocating state? • If Sanitize specifies Exit Media Verification State when not in Media Verification state, should the status code be Invalid Field in Command or Command Sequence Error?
2023-06-05	Addressed most new 2023-05-25 comments from Dan Hubbard. Resolved more comments from Austin Bolen: • Moved additional media modification from the legacy description (being an operation that follows a sanitize operation) into sanitize processing. This should be backwards compatible. Changes from the 2023-06-01 Technical WG meeting: • Reorganized requirements in the Read command description (NVM Cmd Set spec. • Enumerated more error conditions for the Read command. • In each Transition Conditions table, merged all transition conditions for the same transition into a single cell with an "or" bullet list.

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

	• Changed state descriptions to not use “shall”. This change may not always be appropriate. Other: • Made it implementation specific whether SPROG is cleared to 0h if a reset occurs during sanitize processing. • Clarified that Estimated Time fields in the Sanitize Status log page apply to the time in the In Processing state. • Added an Estimated Time For Deallocating State field. • Updated the Sanitize Progress (SPROG) field in the Sanitize Status log page to include the Deallocating state. Added description of setting SPROG to descriptions of the relevant states and transitions. Added an informative description of how SPROG is used to 8.24. • All state descriptions (i.e., “In this state …” use descriptive terminology (i.e., the verb “to be”) and do not contain “shall” or ”may” requirements. • Clarifications in Annex A. • Changed purple strikethrough in move destinations to red strikethrough.
2023-06-07	Deleted comments that were marked as resolved in the previous revision. Included comments from Austin Bolen and resolved some. In the ZNS section, changed Sanitize Status for two rows.
2023-06-09	Changes from the 2023-06-08 meeting of the Technical WG: • Incompatible Changes lists: Updated explanations. • Identify Controller data structure: defined Estimated Time fields to cover sanitize processing, as time difference between entry/exit of the In Processing states. • Closed comments that had been addressed prior to the meeting. • Deleted comments that had been closed before the meeting.
2023-06-22	Changes from the 2023-06-22 ad hoc meeting, from Austin Bolen’s comments, and from an e-mail discussion: • Defined the entire sanitize operation to be in background. • Removed text allowing SPROG to be reset if there’s a reset during processing. The current spec does not address this. • Removed transition list items stating that deallocation occurred during the transition. • Removed statement from the Media Verification state that media is read only. This is enforced by current restrictions and doesn’t conflict with allowing Read commands. • Removed requirement that no unexpected deallocation occurred for entry to MV state. • Added transitions from Deallocating state. Deallocation failure causes transition to a Failure state. • Removed change in composition of NVM subsystem as a cause of transition from Deallocating state to Idle state. Such a change would be a failure, and that now transitions to a Failure state.
2023-06-27	Changes from the 2023-06-27 ad hoc meeting and from an e-mail discussion: • Added Failure State field to Sanitize Status log page. • ZNS Command Set Spec: Moved logical block content requirement from Fig. 51 into a separate paragraph.
2023-06-29	• Editorial fixes. • Added requirement to KV Cmd Set Spec that AMM and MV state are not supported for KV namespaces. Changes from the 2023-06-29 meeting of the Technical WG: • Replaced values of the AUSE bit with “[un]restricted completion mode”.
2023-07-13	• Changed In Process Restricted and In Process Unrestricted state names to Restricted Processing and Unrestricted Processing. • Changed Failure Restricted and Failure Unrestricted state names to Restricted Failure and Unrestricted Failure • Added comments from Mike Allison. • Added comments from Austin Bolen. Changes from 2023-07-13 meeting of Technical WG:

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant’s agreement. Copyright © 2008 to 2024 NVM Express, Inc.

	• Clarified setting of MVCAND for the MV:Deallocating transition. • (no change) Confirmed that SPROG field must be cleared upon every entry to a Processing state or the Deallocating state. • In the state and transition sections, changed all descriptive (“is”) verbs to imperative (“shall be”) statements. • Resolved some comments marked for resolution in Phase 3. • Deleted all resolved comments. • Accepted all changes.
Phase 3 Changes	
2023-08-04	Changes from offline discussions among authors. • Aligned both transitions causing the Sanitize Operation Entered Media Verification State AEN to be reported on the controller that processed the Sanitize command. • Clarified fetched vs. processed wording in specifying which commands are allowed during a sanitize operation or a sanitize failure. Deleted redundant items from two bullet lists. • Implemented various suggestions. • Converted all cross references to static text. • Changed state transition labels to be unique.
2023-08-21	Changes from offline discussions among authors. • Clarified support for the FAILS field. • Specified setting the FAILS field on each transition into a Failed state. • Added paragraph to Restricted Processing state, Unrestricted Processing state, and Deallocating state to clarify that deallocation in a processing state is different from that performed in the Deallocating state, and vice-versa. • ZNS Cmd Set Spec: Moved the new paragraph from the 4.1.7 Sanitize command section into a new 5.TBD Sanitize Operations section, as is done in the NVM and KV command set specs. Now section 4.1.7 is completely unchanged. • Added clarifications for deallocation being performed as part of sanitize processing.
2023-08-29	Changes from 2023-08-24 meeting of Technical WG: • Change MVCAND to MVCNCLD. • Change VCAND to VCNCLD. • Accepted changes to NVM, ZNS, and KV command set specs. Changes from e-mail discussion among authors.
2023-09-06	Changes from e-mail discussions with authors and the 2023-08-31 meeting of the Technical WG. • Reorganized the start of 8.21 to better explain sanitize processing, additional media modification, media verification, and deallocation after media verification. • Deleted transitions from state transition conditions tables self-loop transitions for which no actions were described. • Renamed Deallocating state to Post Verification Deallocation state. • Sanitize command with SANACT set to EMVb will be aborted in any state other than Media Verification state. • Reorganized some transition condition descriptions to place the value of EMVS bit at the start of the sentence. • Additional changes from Austin’s comments of 2023-09-05 and -06.
2023-09-07	Changes from the 2023-09-07 meeting of the Technical WG. • AENs are only reported by the controller that received the Sanitize command on its Admin Queue, i.e., not if received by a Management Endpoint. This is added to general requirements for reporting AENs in 8.21.TBD+1. • Use “if required” for deallocation in the two Processing states. • Use “if required” for additional media modification. • Transition condition references to fields in the Sanitize command are in the past tense, and reference to other events are in the present tense.

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant’s agreement. Copyright © 2008 to 2024 NVM Express, Inc.

2023-09-12	Resolution of (new) comments by Mike Allison with input from authors: • Removed VCNCNCLD bit from Sanitize Completion Event Data Format. It is redundant because it is also in the Sanitize Status field. This leaves no new information in Figure 240, so deleted all changes to that figure. • Changed description (and the newly-invented name) of Sanitize Operation Status value 000b from “never sanitized” to “sanitize never initiated”. This is compatible with legacy behavior. • In descriptions of the Sanitize command, replaced “specifying [un]restricted completion mode” with the value of the AUSE bit and “(i.e., [un]restricted completion mode”). • Event data for the Sanitize Media Verification Event was one reserved byte. Deleted that (new) figure, required Event Length field = 0h, and added “if any” to the description of the Event Data field in Figure 225.
2023-09-14	Changes from the 2023-09-14 meeting of the Technical WG: • Edits to Annex A. • Accepted all changes and stopped tracking. Note: Comments related to TP4153 remain in this revision.
Member Review Changes	
2023-09-14	Revision for entry to Member Review. • Removed all comments other than those noting coloration that might be missed. • Renamed value in Figure 267 to “Sanitize Never Initiated” to “Sanitize Never Started”, per discussion in Technical WG meeting today.
2023-10-06	Added comments from Pure Storage (Randy Jennings).
2023-10-19	Added comments from Samsung (Judy Brock and Mike Allison). Added initial resolution of comments. Added comments from Dell (Austin Bolen). Added further resolution of comments. (More comments remain to be resolved.) Comments that are accepted and resolved are marked as done. Comments that are rejected are open. Comments that are not resolved are open. Changes are tracked with respect to the revision that entered Member Review (i.e., 2023-09-14).
2023-11-22	Changes based on authors’ discussions on 2023-11-17. In the state machine description, changed purple text to blue and deleted red strikethrough text, because there was insufficient context to make those markups useful.
2023-11-28	Changes from 2023-11-28 authors’ meeting. All comments, resolved and unresolved, are included in this revision.
2023-11-30	Deleted all comments. Accepted all changes.
2023-12-01	Diff of 2023-11-30 revision from 2023-09-14 revision (Member Review entry).
Second Member Review Changes	
2023-12-13	Revision for entry to Second Member Review. • Scrubbed for duplication of prescriptive requirements (shoulds & shalls). • Added to descriptions of Restricted and Unrestricted Failure states that failure occurred in Post-Verification Deallocation state. • Added Figure 352 and changed bits 2:0 of the Sanitize Status log page to “SOS field”. • Removed setting of the SOS field from state transitions. • Changed the description of the MVCNCLD bit to be informative (“is set/cleared”) and added reference to the state machine for details. • Removed setting/clearing of the GDE bit from the state machine. Normative statements are in the bit description, in the Sanitize Status log page. • Accepted all changed and stopped tracking.

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant’s agreement. Copyright © 2008 to 2024 NVM Express, Inc.

2023-12-14	Final revision for entry to Second Member Review: • Modified description of Media Verification Canceled (MVCNCLD) bit to include that a change in the composition of the NVM subsystem in a processing state also causes setting MVCNCLD to'1'.
2024-01-22	Revision containing all comments from second Member Review.
2024-02-12	Comment resolution • Reworded all Estimated Time fields. • Clarified that verification refers to *allocated" user data", to avoid the incorrect inference that deallocated user data was accessible. • In the state machine, qualified deallocation as "if permitted", a change from "if required". • Aligned descriptions of additional media modification in the state machine and the annex. • Added editorial change to ZNS Cmd Set Spec Figure 51. • Globally changed "deallocation of user data" to "deallocation of media used for user data". • NVM Cmd Set: Defined effects of reading a deallocated LBA, including effects of DULBE.
2024-02-21	• Added comments by Austin Bolen. Resolved those. • NVM Cmd Set Spec changes: Added reference to Base Spec. • Changes from 2024-02-15 meeting of the Technical WG: • Aligned wording of Estimated Time For Post-Verification Deallocation State field with existing estimated time fields. • Revised additional media modification and Read command to clarify that integrity errors caused by sanitize processing do not cause a command to be aborted.
2024-02-22	Changes from Tech WG meeting of 2024-02-22: • Clarifying editorial changes.
2024-02-22a	• Accepted all changes and stopped tracking. • Deleted all closed comments. • Converted all cross-references to text.
2024-02-23	• Additional editorial cleanups from Austin Bolen and David Black.
2024-03-20	• Integrated
2024-03-27	• Additional editorial cleanups from Chandra Nelogal

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

Description for Changes Document for NVM Express Base Specification 2.0c

New Features/Feature Enhancements/Required Changes:

- Sanitize Media Verification (Optional)
    - Description of change:
        - Added Sanitize Operation Entered Media Verification State to the Asynchronous Event Information – I/O Command Specific Status.
        - Added Sanitize Media Verification Event to the Persistent Event log page.
        - Added Sanitize State (SANS) field to the Sanitize Status log page.
        - Added Verification Support (VERS) bit to the Identify Controller data structure.
        - Added Enter Media Verification State (EMVS) bit to the Sanitize command.
        - Modified the Sanitize command description to refer to the Sanitize Operation State Machine.
        - Added Sanitize Operation State Machine, including requirements for states and for transitions.
    - **New requirement / incompatible change**
        - The Sanitize Progress (SPROG) field indicates progress separately for the Processing states and for the Post-Verification Deallocation state. Previously, this field indicated progress for the entire sanitize operation.
        - Hosts that are not aware of Media Verification will not recognize the new Sanitize Operation Entered Media Verification State AEN.
    - References
        - Technical Proposal 4152.

Description for Changes Document for NVM Express® NVM Command Set Specification 1.0c

New Features/Feature Enhancements/Required Changes:

- Sanitize Media Verification (Optional)
    - Description of change:
        - Defined new behavior of the Read command while in the Media Verification state.
    - **New requirement / incompatible change:**
        - During Media Verification state, Read commands will complete with status codes other than Sanitize In Progress. Hosts that are not aware of Media Verification will not expect these status codes.
    - References
        - Technical Proposal 4152.

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

Description for Changes Document for NVM Express® Zoned Namespace Command Set Specification 1.1c

New Features/Feature Enhancements/Required Changes:

- Sanitize Media Verification (Optional)
    - Description of change:
        - During Media Verification state, logical block content is as defined in the NVM Command Set Specification.
    - **New requirement / incompatible change:**
        - During Media Verification state, logical block content is as defined in the NVM Command Set Specification.
    - References
        - Technical Proposal 4152.

Description for Changes Document for NVM Express® Key Value Command Set Specification 1.0c

New Features/Feature Enhancements/Required Changes:

- Sanitize Media Verification (Optional)
    - Description of change:
        - Namespaces associated with the Key Value Command Set do not support additional media modification.
    - **New requirement / incompatible change:**
        - During Media Verification state and Post-Verification Deallocation state, namespaces associated with the Key Value Command Set are not accessible.
    - References
        - Technical Proposal 4152.

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

Markup Conventions:

Black:	Unchanged (however, hot links are removed)
~~Red Strikethrough~~:	Deleted
Blue:	New
Blue Highlighted:	TBD values, anchors, and links to be inserted in new text.
~~Purple Strikethrough~~:	Moved text – source
Purple:	Moved text – destination
<Green Bracketed>:	Notes to editor

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

Description of Specification Changes for the NVM Express Base Specification 2.0c

1 Introduction

…

1.5 Definitions

1.5.6 audit

The process of accessing media to determine correct operation of a sanitize operation. Refer to section 8.21 and to ISO/IEC 27040.

…

1.5.DEF1 sanitization target

The target of a sanitize operation (i.e., an NVM subsystem).

…

1.8 References

…

IEEE Std 2883™-2022, IEEE Standard for Sanitizing Storage. Available from https://standards.ieee.org.

…

3 NVM Express Architecture

…

3.3 NVM Queue Models

…

3.3.3 Queueing Data Structures

…

3.3.3.2 Common Completion Queue Entry

…

3.3.3.2.1 Status Field Definition

…

3.3.3.2.1.2 Command Specific Status Definition

…

Figure 96: Status Code – Command Specific Status Values, I/O Commands

Value	Description
…	
9Ch	Successful Media Verification Read
9Dh ~~84h~~ to B7h	Reserved
B8h	Zoned Boundary Error
…	

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

Figure 96: Status Code – Command Specific Status Values, I/O Commands

Value	Description
Notes: 1. A = All I/O Command Sets, C = Command Set Specific.	

5 Admin Command Set

…

Figure 140 lists the Admin commands that are allowed while a ~~during the processing of a~~ sanitize operation is in progress and the Admin commands that should be allowed during the processing of a Format NVM command.

If a Format NVM command is in progress, then an Admin command not listed in Figure 140 that is submitted for any namespace affected by that Format NVM command may be aborted. If aborted for that reason, then a status code of Format in Progress should be returned.

If there are Admin commands not listed in Figure 140 being processed for a namespace, then a Format NVM command which is submitted that affects that namespace may be aborted. If aborted for that reason, then a status code of Command Sequence Error should be returned.

Figure 140: Sanitize Operations and Format NVM Command – Admin Commands Allowed

Admin Command	Additional Restrictions for Format NVM command	Additional Restrictions for sanitize operations
…		
Sanitize		Prohibited during sanitize operations if the SANACT field is set to a value other than 101b (i.e., Exit Media Verification State). Sanitize operations are described in section 8.21.
…		

…

5.2 Asynchronous Event request command

…

5.2.1 Command Completion

…

Figure 148: Asynchronous Event Information – I/O Command Specific Status

Value	Description
00h	**Reservation Log Page Available:** Indicates that one or more Reservation Notification log pages (refer to section 5.16.1.24) have been added to the Reservation Notification log.
01h	**Sanitize Operation Completed:** Indicates that a sanitize operation has completed (including any associated additional media modification, refer to the No-Deallocate Modifies Media After Sanitize field in Figure 275) without unexpected deallocation of all media allocated for user data (refer to section 5.27.1.19) and status is available in the Sanitize Status log page (refer to section 5.16.1.25).

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

Figure 148: Asynchronous Event Information – I/O Command Specific Status

Value	Description
02h	**Sanitize Operation Completed With Unexpected Deallocation:** Indicates that a sanitize operation for which No-Deallocate After Sanitize (refer to Figure 303) was requested has completed with the unexpected deallocation of all media allocated for user data (refer to section 5.27.1.19) and status is available in the Sanitize Status log page (refer to section 5.16.1.25).
03h	**Sanitize Operation Entered Media Verification State:** Indicates that sanitize processing was successful, the sanitize operation entered the Media Verification state (refer to section 8.21), and status is available in the Sanitize Status log page (refer to section 5.16.1.25).
04h ~~03h~~ to FFh	Reserved

5.14 Format NVM command

…

Figure 189: Format NVM – Command Dword 10

Bits	Description
…	
11:09	**Secure Erase Settings (SES):** This field specifies whether a secure erase should be performed as part of the format and the type of the secure erase operation. The erase applies to all user data, regardless of location (e.g., within an exposed LBA (refer to the NVM Express NVM Command Set Specification), within a cache, within deallocated logical blocks, etc.). **Value** / **Definition** 000b: No secure erase operation requested 001b: **User Data Erase:** All user data shall be erased, contents of the media allocated for user data after the erase is indeterminate (e.g., the user data may be zero filled, one filled, etc.). If a User Data Erase is requested and all affected user data is encrypted, then the controller is allowed to use a cryptographic erase to perform the requested User Data Erase. 010b: **Cryptographic Erase:** All user data shall be erased cryptographically. This is accomplished by deleting the encryption key. 011b to 111b: Reserved
…	

…

5.16 Get Log Page command

…

5.16.1 Log Specific Information

…

5.16.1.14 Persistent Event (Log Identifier 0Dh)

…

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

Figure 224: Persistent Event Log Page

<table>
<tr><th>Bytes</th><th>Description</th></tr>
<tr><td colspan="2">Persistent Event Log Header</td></tr>
<tr><td>…</td><td></td></tr>
<tr><td>511:480</td><td>Supported Events Bitmap: This field contains a bitmap indicating support for the persistent event log events. Each bit in the bitmap corresponds to the value for the event type (refer to Figure 226) (e.g., bit 222 decimal, DEh, corresponds to event type value DEh, Vendor Specific Event). A bit set to ‘1’ indicates that the corresponding event is supported. A bit cleared to ‘0’ indicates that the corresponding event is not supported.
<table>
<tr><th>Bits</th><th>Definition</th><th>Reference</th></tr>
<tr><td>255:224</td><td>Reserved</td><td></td></tr>
<tr><td>223</td><td>TCG Defined</td><td>TCG Storage Interface Interactions Specification</td></tr>
<tr><td>222</td><td>Vendor Specific Event Supported</td><td>5.16.1.14.1.14</td></tr>
<tr><td>221:~~14~~ 15</td><td>Reserved</td><td></td></tr>
<tr><td>14</td><td>Sanitize Media Verification Event Support</td><td>5.16.1.14.1.TBD</td></tr>
<tr><td>13</td><td>Thermal Excursion Event Support</td><td>5.16.1.14.1.13</td></tr>
<tr><td>…</td><td></td><td></td></tr>
</table></td></tr>
<tr><td>…</td><td>…</td></tr>
</table>

…

The format of the Persistent Events in the Persistent Event log is shown in Figure 225.

Figure 225: Persistent Event Format

Bytes	Description
…	
Persistent Event Log Event Data	
EHL+EL+2: EHL+3+VSIL	**Event Data:** This field contains persistent event log ~~events~~ event data, if any (refer to section 5.16.1.14.1).

…

5.16.1.14.1Persistent Event Log Events

…

Figure 226: Persistent Event Log Event Types

Type	O/M[1]	Event	Reference Section
…			
0Dh	O	Thermal Excursion	5.16.1.14.1.13
0Eh	O	Sanitize Media Verification Event	5.16.1.14.1.TBD
0Fh ~~0Eh~~ to DDh		Reserved	
DEh	O	Vendor Specific Event	5.16.1.14.1.14
DFh	O	TCG Defined	5.16.1.14.1.15
E0h to FFh		Reserved	

Notes:
1. O/M definition: O = Optional, M = Mandatory.
2. Mandatory for NVMe over PCIe implementations, Optional for NVMe over Fabrics implementations.
3. Mandatory if the command used to initiate the activity reported by the event is supported.

…

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant’s agreement. Copyright © 2008 to 2024 NVM Express, Inc.

5.16.1.14.1.9 Sanitize Start Event (Event Type 09h)

A Sanitize Start event shall be recorded in the Persistent Event Log at the start of a sanitize operation (i.e., the sanitization target transitions to the Restricted Processing state or the Unrestricted Processing state, as described in section 8.21.TBD+2).

The Sanitize Start event shall set the Persistent Event Log Event Format Header:

- Event Type field to 09h; and
- Event Type Revision field to 01h.

Figure 239: Sanitize Start Event Data Format (Event Type 09h)

Bytes	Description
03:00	**SANICAP:** Contains the contents of the SANICAP field from the Identify Controller data structure.
07:04	**Sanitize CDW10:** Contains the value from command Dword 10 of the Sanitize command (refer to Figure 303).
11:08	**Sanitize CDW11:** Contains the value from command Dword 11 of the Sanitize command (refer to Figure 304).

5.16.1.14.1.10 Sanitize Completion Event (Event Type 0Ah)

A Sanitize Completion event shall be recorded in the Persistent Event Log at the completion of a sanitize operation (i.e., the sanitization target transitions to the Idle state, the Restricted Failure state, or the Unrestricted Failure state, as described in section 8.21.TBD+2).

The Sanitize Completion event shall set the Persistent Event Log Event Format Header:

- Event Type field to 0Ah; and
- Event Type Revision field to 01h.

Figure 240: Sanitize Completion Event Data Format (Event Type 0Ah)

Bytes	Description
1:0	**Sanitize Progress:** Contains the sanitize progress at the time of this event using the format specified for the SPROG field in the Sanitize Status log page (refer to section 5.16.1.25).
3:2	**Sanitize Status:** Contains the sanitize status for the time of this event using the format specified for the SSTAT field in the Sanitize Status log page. (e.g., the Global Data Erase bit indicates the status at the time of this event).
5:4	**Completion Information:** Contains a vendor specific value that may provide more information about the completion of the sanitize operation (e.g., if the sanitize operation did not complete successfully, then this field may contain a vendor specific code that indicates a vendor specific reason).
7:6	Reserved

…

5.16.1.14.1.TBD Sanitize Media Verification Event (Event Type 0Eh)

A Sanitize Media Verification event shall be recorded in the Persistent Event log page upon transition to the Media Verification state (refer to section 8.21.TBD+2.6).

No Event Data (refer to Figure 225) is defined for this event.

The Sanitize Media Verification event shall set the Persistent Event Log Event Format Header:

- Event Type field to 0Eh;
- Event Type Revision field to 01h; and
- Event Length field to 0h.

…

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

5.16.1.25 Sanitize Status (Log Identifier 81h)

< Note to Editor: The description of bytes 3:2 is moved into a sub-table, and additional text is added. >

Figure 267: Sanitize Status Log Page

Bytes	Description
01:00	**Sanitize Progress (SPROG):** This field indicates the fraction complete of the: • sanitize ~~operation~~ processing state (i.e., the Restricted Processing state or the Unrestricted Processing state); or • Post-Verification Deallocation state, if the Post-Verification Deallocation state is entered as part of the sanitize operation. The value is the ~~a~~ numerator of the fraction complete that has 65,536 (10000h) as its denominator. This value shall be set to FFFFh if ~~bits 2:0 of the SSTAT~~ the Sanitize Operation Status (SOS) field ~~are~~ is ~~not~~ set to a value other than 010b (i.e., Sanitizing) or if the sanitization target is in the Media Verification state. Refer to section 8.21.TBD+2 for the effects of state changes that change the value of this field. ~~If a sanitize operation has been started by a Sanitize command with the No Deallocate After Sanitize bit set to '1' (refer to section 5.24) and if NODMMAS field in the Identify Controller data structure is set to 10b (refer to Figure 275), then the fraction reported shall include the time related to the additional media modification.~~

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

<table>
<tr><td>03:02</td><td>
Sanitize Status (SSTAT): This field contains the status associated with the most recent sanitize operation.
<table>
<tr><th>Bits</th><th>Description</th></tr>
<tr><td>15:~~09~~ 10</td><td>Reserved</td></tr>
<tr><td>09</td><td>Media Verification Canceled (MVCNCLD): This bit indicates whether the Media Verification state is canceled.
If the most recent sanitize operation was started by a Sanitize command with the EMVS bit set to ‘1’ and during the Restricted Processing state, the Unrestricted Processing state, or the Media Verification state:
a) a change in the composition of the NVM subsystem prevents media verification ; or
b) a Controller Level Reset of any controller in the NVM subsystem occurs that is caused by:
• a transport-specific reset type (refer to the applicable NVMe Transport specification); or
• an NVM Subsystem Reset,
then this bit is set to ‘1’. Otherwise, this bit is cleared to ‘0’.
Refer to the Sanitize Operation State Machine defined in section 8.21.TBD+2 for conditions that affect the setting of this bit.</td></tr>
<tr><td>08</td><td>Global Data Erased (GDE): If ~~set to ‘1’, then~~ no ~~namespace~~ user data ~~in the NVM subsystem~~ has been written to the NVM subsystem and no Persistent Memory Region in the NVM subsystem has been enabled:
a) since being manufactured and the NVM subsystem has never been sanitized; or
b) since the most recent successful sanitize operation~~.~~,
then this bit shall be set to ‘1’. Otherwise, this bit shall be cleared to ‘0’.
~~If cleared to ‘0’, then a namespace user data in the NVM subsystem has been written to or a Persistent Memory Region in the NVM subsystem has been enabled:~~
~~a) since being manufactured and the NVM subsystem has never been sanitized; or~~
~~b) since the most recent successful sanitize operation of the NVM subsystem.~~</td></tr>
<tr><td>07:03</td><td>Overwrite Passes Completed (OPC): This field shall indicate ~~contains~~ the number of completed passes if the most recent sanitize operation was an Overwrite. This field shall be cleared to 0h if the most recent sanitize operation was not an Overwrite.</td></tr>
<tr><td>02:00</td><td>Sanitize Operation Status (SOS): This field indicates ~~contains~~ the status of the most recent sanitize operation as shown below. Sanitize states are described in section 8.21.TBD+2.
<table>
<tr><th>Value</th><th>Definition</th></tr>
<tr><td>000b</td><td>Sanitize Never Started: ~~The NVM subsystem has never been sanitized.~~ If a sanitize operation has never been started in the NVM subsystem, then this value shall be reported. Otherwise, this value shall not be reported.</td></tr>
<tr><td>001b</td><td>Sanitized: If:
a) ~~T~~the most recent sanitize operation completed successfully ~~including any additional media modification (refer to the No Deallocate Modifies Media After Sanitize field in Figure 275)~~; and</td></tr>
</table>
</td></tr>
</table>
</td></tr>
</table>

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant’s agreement. Copyright © 2008 to 2024 NVM Express, Inc.

	b) the Sanitize Operation State Machine is in the Idle state, then this value shall be reported. Otherwise, this value shall not be reported.
010b	**Sanitizing:** If ~~A~~ a sanitize operation is currently in progress (i.e., in the Restricted Processing state, the Unrestricted Processing state, the Media Verification state, or the Post-Verification Deallocation state), then this value shall be reported. Otherwise, this value shall not be reported.
011b	**Sanitize Failed:** If ~~T~~the most recent sanitize operation failed, then this value shall be reported. Otherwise, this value shall not be reported. This value shall be reported when the Sanitize Operation State Machine is in the Restricted Failure state or the Unrestricted Failure state. This value is able to be reported when the Sanitize Operation State Machine is in the Idle state.
100b	**Sanitized Unexpected Deallocate:** If: a) ~~T~~the most recent sanitize operation for which No-Deallocate After Sanitize (refer to section 5.24) was requested has completed successfully with deallocation of all media allocated for user data (refer to section 5.27.1.19); and b) the Sanitize Operation State Machine is in the Idle state, then this value shall be reported. Otherwise, this value shall not be reported.
101b to 111b	Reserved

~~Bits 15:9 are reserved.~~

~~Bit 8 **(Global Data Erased):** If set to '1', then no namespace user data in the NVM subsystem has been written to and no Persistent Memory Region in the NVM subsystem has been enabled:~~

~~a) since being manufactured and the NVM subsystem has never been sanitized; or~~
~~b) since the most recent successful sanitize operation.~~

~~If cleared to '0', then a namespace user data in the NVM subsystem has been written to or a Persistent Memory Region in the NVM subsystem has been enabled:~~

~~a) since being manufactured and the NVM subsystem has never been sanitized; or~~
~~b) since the most recent successful sanitize operation of the NVM subsystem.~~

~~Bits 7:3 contains the number of completed passes if the most recent sanitize operation was an Overwrite. This field shall be cleared to 0h if the most recent sanitize operation was not an Overwrite.~~

~~Bits 2:0 contains the status of the most recent sanitize operation as shown below.~~

~~Value~~	~~Definition~~
~~000b~~	~~The NVM subsystem has never been sanitized.~~

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

Bytes	Description
	~~001b~~ ~~The most recent sanitize operation completed successfully including any additional media modification (refer to the No-Deallocate Modifies Media After Sanitize field in Figure 275).~~ ~~010b~~ ~~A sanitize operation is currently in progress.~~ ~~011b~~ ~~The most recent sanitize operation failed.~~ ~~100b~~ ~~The most recent sanitize operation for which No-Deallocate After Sanitize (refer to section 5.24) was requested has completed successfully with deallocation of all user data (refer to section 5.27.1.19).~~ ~~101b to 111b~~ ~~Reserved~~
07:04	**Sanitize Command Dword 10 Information (SCDW10):** This field shall indicate ~~contains~~ the value of the Command Dword 10 field of the Sanitize command that started the sanitize operation whose status is reported in the SSTAT field. Refer to Figure 303.
11:08	**Estimated Time For Overwrite:** This field shall indicate~~s~~ the number of seconds required to complete sanitize processing (i.e., the time difference between entering and exiting the Restricted Processing state or the Unrestricted Processing state) of an Overwrite sanitize operation with 16 passes in the background (refer to section 5.24) when the No-Deallocate Modifies Media After Sanitize field (refer to Figure 275) is ~~not~~ set to a value other than 10b. A value of 0h indicates that the sanitize processing ~~operation~~ is expected to be completed in the background when the Sanitize command that started that operation is completed. A value of FFFFFFFFh indicates that no time period is reported.
15:12	**Estimated Time For Block Erase:** This field shall indicate~~s~~ the number of seconds required to complete sanitize processing (i.e., the time difference between entering and exiting the Restricted Processing state or the Unrestricted Processing state) of a Block Erase sanitize operation in the background (refer to section 5.24) when the No-Deallocate Modifies Media After Sanitize field (refer to Figure 275) is ~~not~~ set to a value other than 10b. A value of 0h indicates that the sanitize processing ~~operation~~ is expected to be completed in the background when the Sanitize command that started that operation is completed. A value of FFFFFFFFh indicates that no time period is reported.
19:16	**Estimated Time For Crypto Erase:** This field shall indicate~~s~~ the number of seconds required to complete sanitize processing (i.e., the time difference between entering and exiting the Restricted Processing state or the Unrestricted Processing state) of a Crypto Erase sanitize in the background (refer to section 5.24) when the No-Deallocate Modifies Media After Sanitize field (refer to Figure 275) is ~~not~~ set to a value other than 10b. A value of 0h indicates that the sanitize processing ~~operation~~ is expected to be completed in the background when the Sanitize command that started that operation is completed. A value of FFFFFFFFh indicates that no time period is reported.
23:20	**Estimated Time For Overwrite With No-Deallocate Media Modification:** This field shall indicate~~s~~ the number of seconds required to complete sanitize processing (i.e., the time difference between entering and exiting the Restricted Processing state or the Unrestricted Processing state) of an Overwrite sanitize operation, ~~and the~~ including associated additional media modification, ~~after the Overwrite sanitize operation~~ in the background (refer to section 5.24) when: a) the No-Deallocate After Sanitize bit was set to '1' in the Sanitize command that requested the Overwrite sanitize operation; and b) the No-Deallocate Modifies Media After Sanitize field (refer to Figure 275) is set to 10b. A value of 0h indicates that the sanitize processing ~~operation~~ is expected to be completed in the background when the Sanitize command that started that operation is completed. A value of FFFFFFFFh indicates that no time period is reported.

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

Bytes	Description
27:24	**Estimated Time For Block Erase With No-Deallocate Media Modification:** This field shall indicate~~s~~ the number of seconds required to complete sanitize processing (i.e., the time difference between entering and exiting the Restricted Processing state or the Unrestricted Processing state) of a Block Erase sanitize operation, ~~and the~~ including associated additional media modification, ~~after the Block Erase sanitize operation~~ in the background (refer to section 5.24) when: a) the No-Deallocate After Sanitize bit was set to '1' in the Sanitize command that requested the Block Erase sanitize operation; and b) the No-Deallocate Modifies Media After Sanitize field (refer to Figure 275) is set to 10b. A value of 0h indicates that the sanitize processing ~~operation~~ is expected to be completed in the background when the Sanitize command that started that operation is completed. A value of FFFFFFFFh indicates that no time period is reported.
31:28	**Estimated Time For Crypto Erase With No-Deallocate Media Modification:** This field shall indicate~~s~~ the number of seconds required to complete sanitize processing (i.e., the time difference between entering and exiting the Restricted Processing state or the Unrestricted Processing state) of a Crypto Erase sanitize operation, ~~and the~~ including associated additional media modification, ~~after the Crypto Erase sanitize operation~~ in the background (refer to section 5.24) when: a) the No-Deallocate After Sanitize bit was set to '1' in the Sanitize command that requested the Crypto Erase sanitize operation; and b) the No-Deallocate Modifies Media After Sanitize field (refer to Figure 275) is set to 10b. A value of 0h indicates that the sanitize processing ~~operation~~ is expected to be completed in the background when the Sanitize command that started that operation is completed. A value of FFFFFFFFh indicates that no time period is reported.
35:32	**Estimated Time For Post-Verification Deallocation State:** This field shall indicate the number of seconds required to deallocate all media allocated for user data after exiting the Media Verification state (i.e., the time difference between entering and exiting the Post-Verification Deallocation state), if that state is entered as part of the sanitize operation. A value of FFFFFFFFh indicates that no time period is reported.

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

<table>
<tr><th>Bytes</th><th>Description</th></tr>
<tr><td>36</td><td>Sanitize State Information (SSI): This field indicates additional information about the state of sanitization.
<table>
<tr><th>Bits</th><th>Description</th></tr>
<tr><td>7:4</td><td>Failure State (FAILS): If the SOS field is set to 011b (i.e., Sanitize Failed), then this field shall indicate the state of the Sanitize Operation State Machine (refer to Figure FigSM) in which the failure occurred.

The values of this field are sanitize states, defined in the description of the SANS field.

If the VERS bit is cleared to ‘0’, then this field shall be cleared to 0h.

If the SOS field is set to a value other than 011b (i.e., Sanitize Failed), then this field shall be cleared to 0h.</td></tr>
<tr><td>3:0</td><td>Sanitize State (SANS): This field shall indicate the current state of the Sanitize Operation State Machine (refer to Figure FigSM).

If the VERS bit is cleared to ‘0’, then this field shall be cleared to 0h.
<table>
<tr><th>Value</th><th>State</th><th>Reference</th></tr>
<tr><td>0h</td><td>Idle</td><td>8.21.TBD+2.1</td></tr>
<tr><td>1h</td><td>Restricted Processing</td><td>8.21.TBD+2.2</td></tr>
<tr><td>2h</td><td>Restricted Failure</td><td>8.21.TBD+2.3</td></tr>
<tr><td>3h</td><td>Unrestricted Processing</td><td>8.21.TBD+2.4</td></tr>
<tr><td>4h</td><td>Unrestricted Failure</td><td>8.21.TBD+2.5</td></tr>
<tr><td>5h</td><td>Media Verification</td><td>8.21.TBD+2.6</td></tr>
<tr><td>6h</td><td>Post-Verification Deallocation</td><td>8.21.TBD+2.7</td></tr>
<tr><td>All other values</td><td>Reserved</td><td></td></tr>
</table></td></tr>
</table></td></tr>
<tr><td>511:~~32~~ 37</td><td>Reserved</td></tr>
</table>

…

5.17 Identify command

…

5.17.2 Identify Data Structures

5.17.2.1 Identify Controller Data Structure (CNS 01h)

The Identify Controller data structure (refer to Figure 275) is returned to the host for the controller processing the command.

Figure 275: Identify Controller Data Structure

Bytes	I/O[1]	Admin[1]	Disc[1]	Description
…				

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant’s agreement. Copyright © 2008 to 2024 NVM Express, Inc.

<table>
<tr>
<td>331:328</td>
<td>O</td>
<td>O</td>
<td>R</td>
<td>
Sanitize Capabilities (SANICAP): This field indicates attributes for sanitize operations. If the Sanitize command is supported, then this field shall be non-zero. If the Sanitize command is not supported, then this field shall be cleared to 0h. Refer to section 8.21.
<table>
<tr><th>Bits</th><th>Description</th></tr>
<tr><td>31:30</td><td>
No-Deallocate Modifies Media After Sanitize (NODMMAS): This field indicates if media is additionally modified by the controller as part of sanitize processing ~~after a sanitize operation successfully completes~~ that had been started by a Sanitize command with the No-Deallocate After Sanitize bit set to ‘1’.

~~The work required for the associated additional media modification is included both in the estimated time for each sanitize operation and in the Sanitize Progress field (refer to Figure 267).~~
<table>
<tr><th>Value</th><th>Definition</th></tr>
<tr><td>00b</td><td>~~Additional media modification after sanitize operation successfully completes is not defined. Only controllers compliant with NVM Express Base Specification, Revision 1.3 and earlier or that have bits 2:0 of the SANICAP field cleared to 000b are allowed to return this value.~~ Additional media modification as part of sanitize processing is not defined. Only controllers compliant with NVM Express Base Specification, Revision 1.3 and earlier, or controllers that do not support the Sanitize command are allowed to return this value.</td></tr>
<tr><td>01b</td><td>Media ~~is~~ shall not be additionally modified by the controller as part of sanitize processing ~~after sanitize operation completes successfully~~.</td></tr>
<tr><td>10b</td><td>Media ~~is~~ shall be additionally modified by the controller as part of sanitize processing that had been started by a Sanitize command with the No-Deallocate After Sanitize bit set to ‘1’ ~~after sanitize operation completes successfully~~. ~~The Sanitize Operation Completed event does not occur until the additional media modification associated with this field has completed~~.</td></tr>
<tr><td>11b</td><td>Reserved</td></tr>
</table>
~~If bits 2:0 of the SANICAP field are cleared to 000b, then the controller shall clear this field to 00b.~~
</td></tr>
<tr><td>29</td><td>
No-Deallocate Inhibited (NDI): If this bit is set to ‘1’ and the No-Deallocate Response Mode bit (refer to Figure 352) is set to ‘1’, then the controller deallocates ~~after the sanitize operation~~ all media allocated for user data before the Restricted Processing:Idle transition occurs or the Unrestricted Processing:Idle transition occurs (refer to section 8.21.TBD+2), even if the No-Deallocate After Sanitize bit is set to ‘1’ in a Sanitize command.

If:
a) this bit is set to ‘1’;
b) the No-Deallocate After Sanitize bit is set to ‘1’ in a Sanitize command, and:
1) the No-Deallocate Response Mode bit ~~(refer to Figure 352)~~ is cleared to ‘0’; or
</td></tr>
</table>
</td>
</tr>
</table>

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant’s agreement. Copyright © 2008 to 2024 NVM Express, Inc.

Bytes	I/O[1]	Admin[1]	Disc[1]	Description		
						2) the Sanitize Config Feature (refer to section 5.27.1.19) is not supported, then the controller aborts the Sanitize command with a status code of Invalid Field in Command. If the No-Deallocate After Sanitize bit is cleared to '0' in a Sanitize command, then the value of this bit has no effect on the processing of that Sanitize command or on the sanitize operation that is started by that Sanitize command. If this bit is cleared to '0', then the controller supports the No-Deallocate After Sanitize bit in a Sanitize command. ~~If bits 2:0 of the SANICAP field are cleared to 0h, then the controller shall clear this bit to '0'.~~
					28:~~03~~ 04	Reserved
					03	**Verification Support (VERS):** If this bit is set to '1', then the controller supports the Media Verification state and the Post-Verification Deallocation state. If this bit is cleared to '0', then the controller does not support the Media Verification state and does not support the Post-Verification Deallocation state. If the BES bit is cleared to '0' and the CES bit is cleared to '0', then this bit shall be cleared to '0'.
					02	**Overwrite Support (OWS):** If set to '1', then the controller supports the Overwrite sanitize operation. If cleared to '0', then the controller does not support the Overwrite sanitize operation.
					01	**Block Erase Support (BES):** If set to '1', then the controller supports the Block Erase sanitize operation. If cleared to '0', then the controller does not support the Block Erase sanitize operation.
					00	**Crypto Erase Support (CES):** If set to '1', then the controller supports the Crypto Erase sanitize operation. If cleared to '0', then the controller does not support the Crypto Erase sanitize operation.
…						

…

5.24 Sanitize command

The Sanitize command is used to start a sanitize operation that targets the NVM subsystem or to recover from a previously failed sanitize operation that targeted the NVM subsystem. The sanitize operation types that may be supported are Block Erase, Crypto Erase, and Overwrite.

A sanitize operation consists of:

- sanitize processing (refer to section 8.21), which may include:
  - deallocation of all media allocated for user data; and
  - additional media modification;
- optional verification of media allocated for user data; and
- post-verification deallocation of all media allocated for user data following media verification, if any, as described in section 8.21.

All sanitize operations are ~~processed~~ performed in the background (i.e., completion of the Sanitize command that starts a sanitize operation does not indicate completion of ~~the~~ that sanitize operation). Refer to section 8.21 for details on the sanitize operation.

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

If the NVM subsystem supports multiple domains and the Sanitize command is not able to start a sanitize operation as a result of the NVM subsystem being divided (refer to section 3.2.4), then the controller shall abort the Sanitize command ~~shall be aborted~~ with a status code of Asymmetric Access Inaccessible or Asymmetric Access Persistent Loss.

~~When a sanitize operation starts on any controller, all controllers in the NVM subsystem:~~

- ~~Shall clear any outstanding Sanitize Operation Completed asynchronous event or Sanitize Operation Completed With Unexpected Deallocation asynchronous event;~~
- ~~Shall update the Sanitize Status log (refer to section 5.16.1.25);~~
- ~~Shall abort any command (submitted or in progress) not allowed during a sanitize operation with a status code of Sanitize In Progress (refer to section 8.21.1);~~
- ~~Shall abort device self-test operations in progress;~~
- ~~Suspends autonomous power state management activities as described in section 8.15.2; and~~
- ~~Shall release stream identifiers for any open streams.~~

~~If a sanitize operation is not in progress and the most recent sanitize operation did not fail, then a Sanitize command with a Sanitize Action set to 001b (i.e., Exit Failure Mode) shall complete with a status code of Successful Completion and perform no other action.~~

~~While a sanitize operation is in progress, all controllers in the NVM subsystem shall abort any command not allowed during a sanitize operation with a status code of Sanitize In Progress (refer to section 8.21.1) and the Persistent Memory Region shall behave as described in section 8.30.1.~~

~~After a sanitize operation fails, all controllers in the NVM subsystem shall abort any command not allowed during a sanitize operation with a status code of Sanitize Failed (refer to section 8.21.1) and the Persistent Memory Region shall behave as described in section 8.21.1 until a subsequent sanitize operation is started or successful recovery from the failed sanitize operation occurs.~~

~~If the most recent failed sanitize operation was started in unrestricted completion mode (i.e., the AUSE bit was set to '1' in the Sanitize command), failure recovery requires the host to issue a subsequent Sanitize command in restricted or unrestricted completion mode or to issue a subsequent Sanitize command with the Exit Failure Mode action.~~

~~If the most recent failed sanitize operation was started in restricted completion mode (i.e., the AUSE bit was cleared to '0' in the Sanitize command), failure recovery requires the host to issue a subsequent Sanitize command in restricted completion mode. In the case of a sanitize operation failure in restricted completion mode, before starting another sanitize operation:~~

- ~~any subsequent Sanitize command issued with the Exit Failure Mode action shall be aborted with a status code of Sanitize Failed; and~~
- ~~any Sanitize command issued in unrestricted completion mode shall be aborted with a status code of Sanitize Failed.~~

The Sanitize Capabilities (SANICAP) field in the Identify Controller data structure (refer to Figure 275) indicates:

a) the sanitize operation types supported;
b) whether setting the No-Deallocate After Sanitize (NDAS) bit (~~i.e., Sanitize command Dword 10 bit 9~~ refer to Figure 303) causes media to be modified as part of sanitize processing ~~after a successful sanitize operation completes~~; ~~and~~
c) whether the controller inhibits the functionality of the No-Deallocation After Sanitize bit in the Sanitize command; and
d) whether the controller supports the Media Verification state and the Post-Verification Deallocation state (refer to the Verification Support (VERS) bit in the SANICAP field in Figure 275).

If ~~an unsupported sanitize operation type is selected by~~ a Sanitize command specifies an unsupported value in the SANACT field (refer to Figure 303), then the controller shall abort the command with a status code of Invalid Field in Command.

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

If the Verification Support (VERS) bit is cleared to '0' and a Sanitize command specifies the Enter Media Verification State (EMVS) bit set to '1' (refer to Figure 303), then the controller shall abort the command with a status code of Invalid Field in Command.

If the Verification Support (VERS) bit is set to '1' and a Sanitize command is processed that specifies:

a) the Enter Media Verification State (EMVS) bit set to '1', the SANACT field set to a value of 010b (i.e., Block Erase) or a value of 100b (i.e., Crypto Erase), and the No-Deallocate After Sanitize (NDAS) bit cleared to '0', then successful sanitize processing is followed by entry to the Media Verification state;

b) the Enter Media Verification State (EMVS) bit set to '1' and:

   a) the SANACT field set to 011b (i.e., Overwrite); or
   b) the No-Deallocate After Sanitize (NDAS) bit set to '1',

   then the controller shall abort the command with a status code of Invalid Field in Command;

c) the SANACT field set to 101b (i.e., Exit Media Verification State) and the sanitization target is in the Media Verification state, then:

   - the controller does not start a new sanitize operation; and
   - the sanitization target transitions from the Media Verification state to the Post-Verification Deallocation state, in which all media allocated for user data in the NVM subsystem is deallocated;

or

d) the SANACT field set to 101b (i.e., Exit Media Verification State) and the sanitization target is not in the Media Verification state, then the controller shall abort the command with a status code of Invalid Field in Command.

If any Persistent Memory Region is enabled in an NVM subsystem, then the controller shall abort any Sanitize command with a status code of Sanitize Prohibited While Persistent Memory Region is Enabled. ~~A sanitize operation is prohibited while any Persistent Memory Region is enabled.~~

If any namespace is write protected in an NVM subsystem (refer to section 8.12), then the controller aborts any Sanitize command with a status code of Namespace is Write Protected. ~~A sanitize operation is prohibited while any namespace is write protected.~~

If a firmware activation with reset is pending, then the controller shall abort any Sanitize command.

If the Firmware Commit command that established the pending firmware activation with reset condition returned a status code of:

a) Firmware Activation Requires Controller Level Reset;
b) Firmware Activation Requires Conventional Reset; or
c) Firmware Activation Requires NVM Subsystem Reset,

then the controller should abort the Sanitize command with that same status code.

If the Firmware Commit command that established the pending firmware activation with reset condition completed successfully or returned a status code other than:

a) Firmware Activation Requires Controller Level Reset;
b) Firmware Activation Requires Conventional Reset; or
c) Firmware Activation Requires NVM Subsystem Reset,

then the controller should abort the Sanitize command with a status code of Firmware Activation Requires Controller Level Reset.

Activation of new firmware is prohibited during a sanitize operation (refer to section 8.21.TBD+3).

Support for Sanitize commands in a Controller Memory Buffer (i.e., submitted to an Admin Submission Queue in a Controller Memory Buffer or specifying an Admin Completion Queue in a Controller Memory Buffer) is implementation specific. If an implementation does not support Sanitize commands in a Controller

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

Memory Buffer and a controller's Admin Submission Queue or Admin Completion Queue is in the Controller Memory Buffer, then the controller shall abort all Sanitize commands with a status code of Command Not Supported for Queue in CMB.

All sanitize operations (i.e., Block Erase, Crypto Erase, and Overwrite) are performed in the background (i.e., Sanitize command completion does not indicate sanitize operation completion). If a sanitize operation ~~is started~~ starts as a result of a Sanitize command, then the controller shall complete ~~the~~ that Sanitize command with a status code of Successful Completion. If the controller completes a Sanitize command with any status code other than Successful Completion, then the controller:

- shall not start the sanitize operation for that command;
- shall not modify the Sanitize Status log page; and
- shall not alter any user data.

The Sanitize command uses Command Dword 10 and Command Dword 11. All other command specific fields are reserved.

Figure 303: Sanitize – Command Dword 10

Bits	Description
31:~~10~~11	Reserved
10	**Enter Media Verification State (EMVS):** If this bit is set to '1', then the Media Verification state shall be entered if sanitize processing completes successfully (i.e., the Global Data Erased (GDE) bit is set to '1' (refer to Figure 267)). If this bit is cleared to '0', then this bit shall have no effect. If the SANACT field does not specify starting a sanitize operation (i.e., is set to any value other than 010b, 011b, or 100b), then this bit shall be ignored by the controller.
09	**No-Deallocate After Sanitize (NDAS):** If this bit is set to '1' and the No-Deallocate Inhibited bit (refer to Figure 275) is cleared to '0', then the controller shall not deallocate any media allocated for user data as a result of successfully completing the sanitize operation. If this bit is: a) cleared to '0'; or b) set to '1' and the No-Deallocate Inhibited bit is set to '1', then the controller should deallocate all media allocated for user data as a result of successfully completing the sanitize operation. ~~This bit shall be ignored if the Sanitize Action field is set to 001b (i.e., Exit Failure Mode).~~ If the SANACT field does not specify starting a sanitize operation (i.e., is set to any value other than 010b, 011b, or 100b), then this bit shall be ignored by the controller.
08	**Overwrite Invert Pattern Between Passes (OIPBP):** If this bit is set to '1', then the Overwrite Pattern shall be inverted between passes. If this bit is cleared to '0', then the overwrite pattern shall not be inverted between passes. ~~This bit shall be ignored unless~~ If the Sanitize Action field is ~~not~~ set to a value other than 011b (i.e., Overwrite), then this bit shall be ignored by the controller.
07:04	**Overwrite Pass Count (OWPASS):** This field specifies the number of overwrite passes (i.e., how many times the media is to be overwritten) using the data from the Overwrite Pattern field of this command. A value of 0h specifies 16 overwrite passes. ~~This field shall be ignored unless~~ If the Sanitize Action field is ~~not~~ set to a value other than 011b (i.e., Overwrite), then this field shall be ignored by the controller.
03	**Allow Unrestricted Sanitize Exit (AUSE):** If this bit is set to '1', then the sanitize processing ~~operation~~ is performed in unrestricted completion mode (i.e., in the Unrestricted Processing state; refer to section 8.21.TBD+2.4). If this bit is cleared to '0', then the sanitize processing ~~operation~~ is performed in restricted completion mode (i.e., in the Restricted Processing state; refer to section 8.21.TBD+2.2). ~~This bit shall be ignored if the Sanitize Action field is set to 001b (i.e., Exit Failure Mode).~~ If the SANACT field does not specify starting a sanitize operation (i.e., is set to any value other than 010b, 011b, or 100b), then this bit shall be ignored by the controller.

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

Figure 303: Sanitize – Command Dword 10

Bits	Description
02:00	**Sanitize Action (SANACT):** This field specifies the sanitize action to perform. **Value** / **Description** 000b – Reserved 001b – Exit Failure Mode 010b – Start a Block Erase sanitize operation 011b – Start an Overwrite sanitize operation 100b – Start a Crypto Erase sanitize operation 101b – Exit Media Verification State 110b ~~101b~~ to 111b – Reserved

Figure 304: Sanitize – Command Dword 11

Bits	Description
31:00	**Overwrite Pattern (OVRPAT):** ~~This field is ignored unless the Sanitize Action field in Command Dword 10 is set to 011b (i.e., Overwrite).~~ This field specifies a 32-bit pattern that is used for the Overwrite sanitize operation. Refer to section 8.21. If the Sanitize Action field is set to a value other than 011b (i.e., Overwrite), then this field shall be ignored by the controller.

5.24.1 Command Completion

When the command is complete, the controller shall post a completion queue entry to the Admin Completion Queue indicating the status for the command. All sanitize operations are performed in the background (i.e., completion of the Sanitize command that started that sanitize operation does not indicate completion of the sanitize operation). If a sanitize operation ~~is started~~ starts (refer to section 8.21.TBD+2), then the Sanitize Status log page shall be updated before posting the completion queue entry for the command that started that sanitize operation.

Sanitize command specific status values (i.e., SCT field set to 1h) are shown in Figure 305.

Figure 305: Sanitize – Command Specific Status Values

Value	Description
0Bh	**Firmware Activation Requires Conventional Reset:** The sanitize operation could not be started because a firmware activation is pending and a Conventional Reset is required.
10h	**Firmware Activation Requires NVM Subsystem Reset:** The sanitize operation could not be started because a firmware activation is pending and an NVM Subsystem Reset is required.
11h	**Firmware Activation Requires Controller Level Reset:** The sanitize operation could not be started because a firmware activation is pending and a Controller Level Reset is required.
23h	**Sanitize Prohibited While Persistent Memory Region is Enabled:** A sanitize operation is prohibited while the Persistent Memory Region is enabled.

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

5.27 Set Features command

…

5.27.1 Feature Specific Information

…

5.27.1.19 Sanitize Config (Feature Identifier 17h)

…

Figure 352: Sanitize Config – Command Dword 11

Bits	Description
31:01	Reserved
00	**No-Deallocate Response Mode (NODRM):** If the No-Deallocate Inhibited bit~~)~~ is set to '1' in the Sanitize Capabilities field of the Identify Controller data structure (refer to Figure 275), then this bit defines the response of the controller to a Sanitize command processed with the No-Deallocate After Sanitize (NDAS) bit set to '1' (refer to Figure 303) ~~set to '1'~~. If this bit is set to '1' (i.e., No-Deallocate Warning Response Mode), then the controller shall process such Sanitize commands, and if the resulting sanitize operation is completed successfully, then ~~bits 2:0 of the Sanitize Status field in the Sanitize Status log page shall be set to 100b~~ the SOS field shall be set to 100b (i.e., Sanitized Unexpected Deallocate) in the Sanitize Status log page (refer to Figure 267). If this bit is cleared to '0' (i.e., No-Deallocate Error Response Mode), then the controller shall abort such Sanitize commands with a status code of Invalid Field in Command. If the No-Deallocate Inhibited bit in the Sanitize Capabilities field of the Identify Controller data structure (refer to Figure 275) is cleared to '0', then this bit has no effect.

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

8 Extended Capabilities

…

8.21 Sanitize Operations

A sanitize operation alters all user data in the ~~NVM subsystem~~ sanitization target such that recovery of any previous user data from any cache, the non-volatile media, or any Controller Memory Buffer is not possible. It is implementation specific whether Submission Queues and Completion Queues within a Controller Memory Buffer are altered by a sanitize operation; all other data stored in all Controller Memory Buffers is altered by a sanitize operation. If a portion of the user data was not altered and the sanitize operation completed successfully, then the NVM subsystem shall ensure permanent inaccessibility of that portion of the media allocated for user data for any future use within the NVM subsystem (e.g., retrieval from NVM media, caches, or any Controller Memory Buffer) and permanent inaccessibility of that portion of the media allocated for user data via any interface to the NVM subsystem, including management interfaces as defined by the NVM Express Management Interface Specification.

8.21.TBD Elements of Sanitize Operations

A sanitize operation consists of:

- sanitize processing, which may include:
  - deallocation of all media allocated for user data; and
  - additional media modification;
- optional verification of media allocated for user data; and
- post-verification deallocation of all media allocated for user data following media verification, if any.

Sanitize processing is performed in either restricted completion mode (i.e., in the Restricted Processing state) or in unrestricted completion mode (i.e., in the Unrestricted Processing state), as specified by the Allow Unrestricted Sanitize Exit (AUSE) bit in the Sanitize command (refer to Figure 303).

Additional media modification may be performed as part of sanitize processing (i.e., in the Restricted Processing state or the Unrestricted Processing state) to prevent commands that access media after completion of sanitize processing from encountering data integrity errors caused by that sanitize processing.

Additional media modification shall be performed if the NODMMAS field is set to 10b (refer to Figure 275) and the Sanitize command that started the sanitize operation specifies:

- the Enter Media Verification State (EMVS) bit cleared to ‘0’; and
- the No-Deallocate After Sanitize (NDAS) bit set to ‘1’.

Verification of media allocated for user data is able to be performed by the host if the Sanitize Operation State Machine is in the Media Verification state. A Block Erase sanitize operation or Crypto Erase sanitize operation may invalidate error correction codes on the media, causing subsequent reads to fail because of media errors. In the Media Verification state, reads are successful regardless of such invalid error correction codes which enables the host to perform an audit (refer to section 1.5.6) to verify that the media was sanitized. Refer to the applicable I/O Command Set specification for details. Media verification is performed if the Sanitize command that starts a sanitize operation specifies the EMVS bit set to ‘1’ and sanitize processing completes successfully.

If a sanitize operation includes deallocation of all media allocated for user data, then that deallocation shall be performed in exactly one of the following states:

- Restricted Processing state;
- Unrestricted Processing state; or
- Post-Verification Deallocation state.

If the Sanitize command (refer to Figure 303) that starts a sanitize operation specifies:

- the Enter Media Verification State (EMVS) bit cleared to ‘0’;

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant’s agreement. Copyright © 2008 to 2024 NVM Express, Inc.

- the AUSE bit cleared to ‘0’; and
- the No-Deallocate After Sanitize (NDAS) bit is:
  - cleared to ‘0’; or
  - set to ‘1’ and the controller encounters a condition that results in unexpected deallocation of all media allocated for user data (refer to section 5.27.1.19),

then deallocation of all media allocated for user data shall be performed in the Restricted Processing state. If that deallocation fails, then sanitize processing fails.

If Media Verification state is canceled (i.e., the MVCNCLD bit is set to ‘1’) during the Restricted Processing state, then deallocation of all media allocated for user data shall be performed in the Restricted Processing state.

If the Sanitize command that starts a sanitize operation specifies:

- the Enter Media Verification State (EMVS) bit cleared to ‘0’;
- the AUSE bit set to ‘1’; and
- the No-Deallocate After Sanitize (NDAS) bit is:
  - cleared to ‘0’; or
  - set to ‘1’ and the controller encounters a condition that results in unexpected deallocation of all media allocated for user data (refer to section 5.27.1.19),

then deallocation of all media allocated for user data shall be performed in the Unrestricted Processing state. If that deallocation fails, then sanitize processing fails.

If the Media Verification state is canceled (i.e., the MVCNCLD bit is set to ‘1’) during the Unrestricted Processing state, then deallocation of all media allocated for user data shall be performed in the Unrestricted Processing state.

In the Post-Verification Deallocation state the controller deallocates all user data.

In the Post-Verification Deallocation state, if the controller:

- successfully completes deallocating all media allocated for user data, then the sanitization target enters the Idle state; or
- fails to deallocate all media allocated for user data, then the sanitization target enters the Restricted Failure state or the Unrestricted Failure state, as described in section 8.21.TBD+2.7.

A Controller Level Reset may cause the sanitize operation not to include the Media Verification state and the Post-Verification Deallocation state, as described in section 8.21.TBD+2.

8.21.TBD+1 Sanitize Operation Types and Support

The scope of a sanitize operation is all locations in the NVM subsystem that are able to contain user data, including caches, Persistent Memory Regions, and unallocated or deallocated areas of the media.

If the composition of the NVM subsystem (refer to section 3.2.4) changes (e.g., a new domain is added, or a division event occurs) and that change prevents the successful completion of a sanitize operation, then the sanitize operation shall fail.

If the composition of the NVM subsystem changes (e.g., a new domain is added, or a division event occurs) and that change prevents verification of media allocated for user data, then the Media Verification state is canceled and the MVCNCLD bit is set to ‘1’.

Sanitize operations do not affect the Replay Protected Memory Block, boot partitions, or other media and caches that do not contain user data. A sanitize operation also may alter log pages as necessary (e.g., to prevent derivation of user data from log page information). A sanitize operation is only able to be started if the NVM subsystem is not divided (refer to section 3.2.4). ~~Once started, a~~ A sanitize operation in the Restricted Processing state, the Unrestricted Processing state, the Media Verification state, or the Post-Verification Deallocation state is not able to be aborted and continues after a Controller Level Reset, including across power cycles. Refer to Annex A for further information about sanitize operations.

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant’s agreement. Copyright © 2008 to 2024 NVM Express, Inc.

The Sanitize command (refer to section 5.24) is used to start a sanitize operation, ~~or~~ to recover from a previously failed sanitize operation, or to exit the Media Verification state. All sanitize operations are performed in the background (i.e., completion of the Sanitize command that starts a sanitize operation does not indicate completion of ~~the~~ that sanitize operation). The completion of a sanitize operation ~~is~~ and the optional transition into the Media Verification state are indicated in the Sanitize Status log page, and with ~~(if an Asynchronous Event Request Command is outstanding) either~~:

- the Sanitize Operation Completed asynchronous event,
- the Sanitize Operation Completed With Unexpected Deallocation asynchronous event, or
- the Sanitize Operation Entered Media Verification State asynchronous event.

If the Sanitize command that started a sanitize operation was submitted to a controller's Admin Submission Queue, then the asynchronous event shall be reported only by that controller. If the Sanitize command that started a sanitize operation was submitted to a Management Endpoint (refer to the NVM Express Management Interface Specification), then the asynchronous event shall not be reported by any controller in the NVM subsystem.

The Sanitize Capabilities (SANICAP) field of the Identify Controller data structure (refer to Figure 275) indicates the sanitize operation types supported and controller attributes specific to sanitize operations.

The sanitize operation types are:

- ~~T~~the Block Erase sanitize operation, which alters user data with a low-level block erase method that is specific to the media for all locations on the media within the ~~NVM subsystem~~ sanitization target in which user data may be stored;
- ~~T~~the Crypto Erase sanitize operation, which alters user data by changing the media encryption keys for all locations on the media within the ~~NVM subsystem~~ sanitization target in which user data may be stored; and
- ~~T~~the Overwrite sanitize operation, which alters user data by writing a fixed data pattern or related patterns one or more times to all locations on the media within the ~~NVM subsystem~~ sanitization target in which user data may be stored ~~one or more times~~. Figure 474 defines the data pattern or patterns that are written.

Controller attributes specific to sanitize operations include:

- ~~The~~ the No-Deallocate Modifies Media After Sanitize (NODMMAS) field, which indicates ~~if~~ whether media is modified by the controller ~~after a sanitize operation successfully completes~~ as part of sanitize processing that had been requested with the No-Deallocate After Sanitize (NDAS) bit set to '1' in the Sanitize command that started the sanitize operation; ~~and~~
- the No-Deallocate Inhibited (NDI) bit, which indicates if the controller supports the No-Deallocate After Sanitize bit in the Sanitize Command; and
- the Verification Support (VERS) bit, which indicates if the controller supports the Media Verification state and the Post-Verification Deallocation state for sanitization operations that perform block erase or crypto erase.

~~The NODMMAS field in the Identify Controller data structure (refer to Figure 275), specifies that if a Sanitize command includes No-Deallocate After Sanitize set to '1' and NODMMAS is set to 10b, then a sanitize operation has an associated additional media modification operation.~~ If the NODMMAS field indicates a value of 10b in the Identify Controller data structure (refer to Figure 275) and a Sanitize command that starts a sanitize operation specifies the No-Deallocate After Sanitize (NDAS) bit set to '1', then sanitize processing includes additional media modification. ~~This additional media modification operation acts upon the results of the requested sanitize operation with the purpose of making all LBA contents readable.~~ Refer to Annex A.3 for further information about sanitize operations and interactions with integrity circuits.

~~This additional media modification shall complete before the NVM subsystem:~~

~~a) reports sanitize completion by Asynchronous Event (refer to section 5.2); and~~
~~b) reports sanitize completion in the Sanitize Status log (refer to section 5.16.1.25).~~

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

The Overwrite sanitize operation is media specific and may not be appropriate for all media types. For example, if the media is NAND, multiple pass overwrite operations may have an adverse effect on media endurance.

Figure 474: Sanitize Operations – Overwrite Mechanism

OIPBP[1]	Overwrite Pass Count[1]	Overwrite Pass Number	User Data except PI Metadata	Protection Information[2]
'0'	All	All	Overwrite Pattern[1]	Each byte set to FFh
'1'	Even	First	Inversion of Overwrite Pattern[1]	Each byte cleared to 00h
		Subsequent	Inversion of Overwrite Pattern[1] from previous pass (i.e., each bit XORed with '1')	
'1'	Odd	First	Overwrite Pattern[1]	Each byte set to FFh
		Subsequent	Inversion of Overwrite Pattern[1] from previous pass (i.e., each bit XORed with '1')	

Notes:
1. Parameters are specified in Command Dword 10 and Command Dword 11 of the corresponding Sanitize command that started the Overwrite operation. The Overwrite Invert Pattern Between Passes (OIPBP) field is defined in Command Dword 10. The Overwrite Pass Count field is defined in Command Dword 10. The Overwrite Pattern field is defined in Command Dword 11. Refer to section 5.24.
2. If Protection Information is present within the metadata.

To start a sanitize operation, the host submits a Sanitize command specifying ~~one of the sanitize operation types (i.e., Block Erase, Overwrite, or Crypto Erase).~~the SANACT field set to:

- 010b (i.e., start a Block Erase type sanitize operation);
- 011b (i.e., start a Overwrite type sanitize operation); or
- 100b (i.e., start a Crypto Erase type sanitize operation).

The ~~host sets~~ Sanitize command specifies other parameters, including: ~~the Allow Unrestricted Sanitize Exit bit, and the No-Deallocate After Sanitize bit.~~

- the Allow Unrestricted Sanitize Exit (AUSE) bit;
- the No-Deallocate After Sanitize (NDAS) bit; and
- the Enter Media Verification State (EMVS) bit.

After validating the Sanitize command parameters, the controller starts the sanitize operation in the background, updates the Sanitize Status log page, and then completes the Sanitize command with Successful Completion status. ~~If the sanitize operation is to be followed by an associated additional media modification operation (refer to NODMMAS in Figure 275), then the associated additional media modification operation shall be completed before the controller reports sanitize operation complete.~~

If a Sanitize command is completed with any status code other than Successful Completion, then the controller shall not start the sanitize operation and shall not update the Sanitize Status log page. The controller ~~ignores~~ shall ignore Critical Warning(s) in the SMART / Health Information log page (e.g., read only mode) and ~~attempts~~ shall attempt to complete the sanitize operation requested. Refer to section 5 for further information about restrictions on Admin Commands during the processing of a Sanitize ~~Format NVM~~ command.

Following a successful sanitize operation, the values of user data~~, protection information, and non-PI metadata~~ (including protection information (PI), if any, and non-PI metadata, if any) that result from an audit (refer to section 1.5.6) of the ~~NVM subsystem~~ sanitization target are defined in the I/O command set specifications.

The Sanitize Status log page (refer to section 5.16.1.25) indicates ~~contains~~ estimated times for sanitize operations and a consistent snapshot of information about the most recently started sanitize operation,

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

including whether a sanitize operation is in progress, the sanitize operation parameters, and the status of the most recent sanitize operation. The controller shall report that a sanitize operation is in progress if: ~~either a~~

- sanitize processing ~~operation~~ is in progress ~~or an~~ (including ~~associated~~ additional media modification, if required) ~~operation is in progress~~;
- the sanitization target is in the Media Verification state; or
- the sanitization target is in the Post-Verification Deallocation state.

If a sanitize operation is not in progress, then the Global Data Erased (GDE) bit in the log page indicates whether the ~~NVM subsystem~~ sanitization target may contain any user data (i.e., whether the sanitization target has ~~not~~ been written to since the most recent successful sanitize operation).

The Sanitize Status log page shall be ~~updated as described~~:

- ~~Initialize~~ initialized before any controller in the NVM subsystem is ready as described in sections 3.5.3 and 3.5.4; and
- updated when any state transition occurs (refer to section 8.21.TBD+2).
- ~~Update before a Sanitize command that starts a sanitize operation is completed (i.e., prior to the completion queue entry being posted for the Sanitize command); and~~
- ~~Update when a sanitize operation is complete (e.g., immediately prior to the completion queue entry being posted for the Sanitize Operation Completed asynchronous event, or for the Sanitize Operation Completed With Unexpected Deallocation asynchronous event).~~

The Sanitize Status log page ~~should be~~ is updated periodically during a sanitize operation to make progress information available to hosts.

During a sanitize operation, the host may periodically examine the Sanitize Status log page to check for progress, however, the host should limit this polling (e.g., to at most once every several minutes) to avoid interfering with the progress of the sanitize operation itself.

The Sanitize Progress (SPROG) field in the Sanitize Status log page indicates progress during states that may take long times to complete (i.e., the Restricted Processing state, the Unrestricted Processing state, and the Post-Verification Deallocation state). The SPROG field is cleared to 0h upon entry to any of those states, and while in any of those states is updated as described in Figure 267. The SPROG field shall not be modified under any conditions not explicitly permitted by this specification.

A sanitize operation completes when the sanitization target enters any of the following states (refer to section 8.21.TBD+2):

- the Idle state;
- the Restricted Failure state; or
- the Unrestricted Failure state.

~~On completion of a sanitize operation:~~

- ~~If the sanitize operation is successful, then the Global Data Erased bit shall be set to '1';~~
- ~~The Sanitize Status log page is updated;~~
- ~~The controller to which the Sanitize command was submitted completes an Asynchronous Event Request command (if one is outstanding) with the following information:~~
  - ~~The Log Page Identifier field is set to 81h (i.e., Sanitize Status);~~
  - ~~The Asynchronous Event Information field is set to Sanitize Operation Completed or to Sanitize Operation Completed With Unexpected Deallocation asynchronous event (refer to section 5.2); and~~
  - ~~The Asynchronous Event Type field is set to 110b (i.e., I/O Command specific status);~~

  ~~and~~
- ~~All controllers in the NVM subsystem may resume any power management that was suspended when the sanitize operation started.~~

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

Upon completion of a sanitize operation or upon entry to the Media Verification state, the host should read the Sanitize Status log page with the Retain Asynchronous Event bit cleared to '0' (which clears the asynchronous event, if one was generated).

If a sanitize operation fails (i.e., the sanitization target enters the Restricted Failure state or the Unrestricted Failure state), all controllers in the NVM subsystem shall abort any command not allowed during a sanitize operation with a status code of Sanitize Failed (refer to section ~~8.21.1~~ 8.21.TBD+3) until a subsequent sanitize operation is started or successful recovery from the failed sanitize operation occurs. A subsequent successful sanitize operation or the Exit Failure Mode action may be used to recover from a failed sanitize operation. Refer to section 5.24 for recovery details.

If the Sanitize command is supported, then all controllers in the NVM subsystem ~~and all controllers~~ shall:

- ~~S~~support the Sanitize Status log page;
- ~~S~~support the Sanitize Operation Completed asynchronous event;
- ~~S~~support the Sanitize Operation Completed With Unexpected Deallocation asynchronous event, if the Sanitize Config feature is supported;
- ~~S~~support the Exit Failure Mode action for a Sanitize command;
- ~~S~~support at least one of the following sanitize operation types: Block Erase, Overwrite, or Crypto Erase;
- Ssupport the same set of sanitize operation types; ~~and~~
- ~~I~~indicate the supported sanitize operation types in the Sanitize Capabilities field in the Identify Controller data structure; and
- if the Verification Support (VERS) bit is set to '1' in the Identify Controller data structure (refer to Figure 275), support:
  - the FAILS field in the Sanitize Status log page (refer to section 5.16.1.25);
  - the SANS field in the Sanitize Status log page;
  - the Media Verification state;
  - the Post-Verification Deallocation state; and
  - the Sanitize Operation Entered Media Verification State asynchronous event.

The Sanitize Config Feature Identifier (refer to section 5.27.1.19) contains the No-Deallocate Response Mode (NODRM) bit that specifies the response of the controller to a Sanitize command ~~processed with~~ specifying the No-Deallocate After Sanitize (NDAS) bit (refer to Figure 303) set to '1' if the No-Deallocate Inhibited bit is set to '1' in the Sanitize Capabilities field of the Identify Controller data structure (refer to Figure 275). In the No-Deallocate Error Response Mode, the controller aborts such Sanitize commands with a status code of Invalid Field in Command. In the No-Deallocate Warning Response Mode, the controller processes such Sanitize commands, and if a resulting sanitize operation is completed successfully, then ~~bits 2:0 of the Sanitize Status field are~~ the SOS field is set to 100b (i.e., Sanitized Unexpected Deallocate) in the Sanitize Status log page (refer to Figure 267).

~~8.21.1 Sanitize Operation Restrictions~~

~~While performing a sanitize operation and while a failed sanitize operation has occurred but successful recovery from that failure has not occurred, all enabled controllers and namespaces in the NVM subsystem are restricted to performing only a limited set of actions.~~

~~While a sanitize operation is in progress:~~

- ~~All controllers in the NVM subsystem shall only process the Admin commands listed in Figure 140 subject to the additional restrictions stated in that figure;~~
- ~~All I/O Commands other than a Flush command shall be aborted with a status code of Sanitize In Progress;~~
- ~~Processing of a Flush command is specified in section 7.1;~~
- ~~Any command or command option that is not explicitly permitted in Figure 140 shall be aborted with a status code of Sanitize In Progress if fetched by any controller in the NVM subsystem; and~~
- ~~The Persistent Memory Region shall be prevented from being enabled (i.e., setting PMRCTL.EN to '1' does not result in PMRSTS.NRDY being cleared to '0').~~

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

~~While a failed sanitize operation has occurred, a subsequent sanitize operation has not started and successful recovery from the failed sanitize operation has not occurred:~~

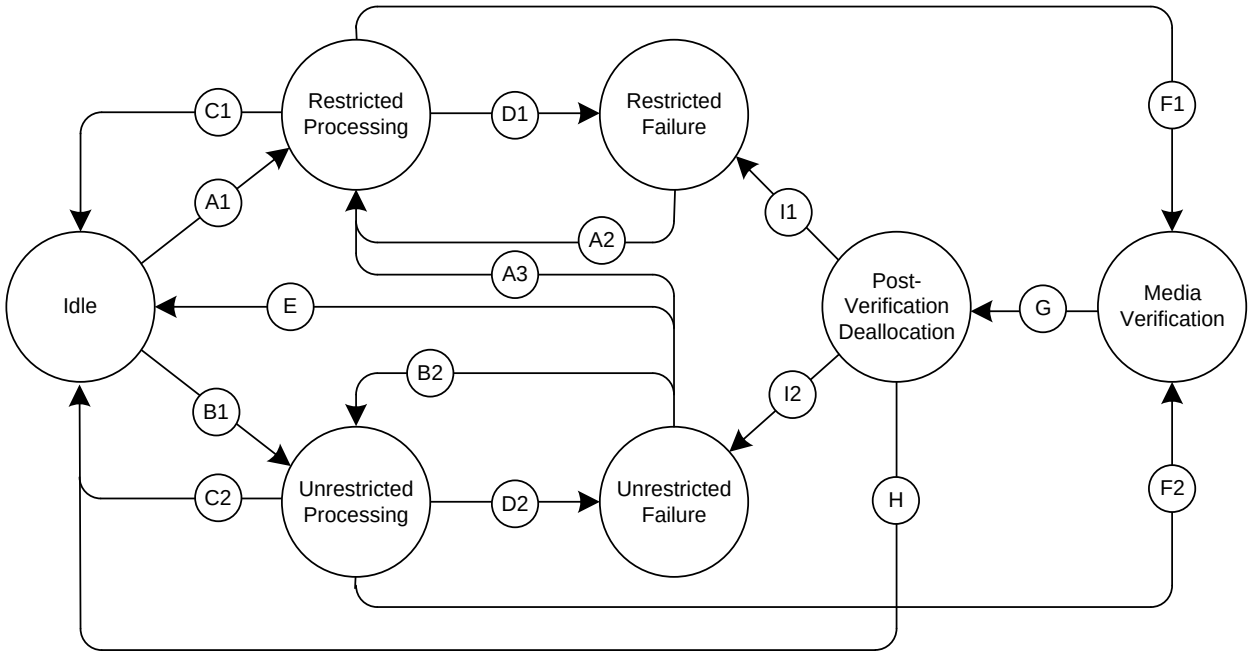
- ~~All controllers in the NVM subsystem shall only process the Sanitize command (refer to section) and the Admin commands listed in Figure 140 subject to the additional restrictions noted in that figure;~~
- ~~All I/O Commands other than a Flush command (refer to section 7.1) shall be aborted with a status code of Sanitize Failed;~~
- ~~The Sanitize command is permitted with action restrictions (refer to section 5.24);~~
- ~~Aside from the Sanitize command, any other command or command option that is not explicitly permitted in Figure 140 shall be aborted with a status code of Sanitize Failed if fetched by any controller in the NVM subsystem; and~~
- ~~The Persistent Memory Region shall be prevented from being enabled (i.e., setting PMRCTL.EN to '1' does not result in PMRSTS.NRDY being cleared to '0').~~

8.21.TBD+2 Sanitize Operation State Machine

< Editor: Text in this section which is in ~~red strikethrough~~ has been moved to here from another section and then deleted. >

The Sanitize Operation State Machine (refer to Figure FigSM) defines the state of sanitization of a sanitization target. The label on each transition begins with a letter and may include a number. The letter indicates the condition causing that transition, as described in the section for each state. The number differentiates between different transitions that have the same transition condition.

Figure FigSM: Sanitize Operation State Machine



In the state transitions described in this section, asynchronous events are reported as described in section 8.21.TBD+1. In Completion Queue Entry Dword 0 (refer to Figure 144) for the Asynchronous Event Request command:

a) the Log Page Identifier field shall be set to 81h (i.e., Sanitize Status log page);
b) the Asynchronous Event Information field (refer to section 5.2) shall be set to:

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

- 01h (i.e., Sanitize Operation Completed);
- 02h (i.e., Sanitize Operation Completed With Unexpected Deallocation); or
- 03h (i.e., Sanitize Operation Entered Media Verification State);

and

c) the Asynchronous Event Type field shall be set to 110b (i.e., I/O Command specific status).

In each state transition described in this section, the controller shall set the Sanitize State (SANS) field to the value corresponding to the state being entered.

8.21.TBD+2.1 Idle State

In this state, no sanitize operation is in process. This state applies in the following cases:

a) no sanitize operation has ever been performed on the NVM subsystem since the NVM subsystem was manufactured;
b) the most recent sanitize operation on the NVM subsystem was successful; and
c) the most recent sanitize operation failed in unrestricted completion mode (i.e., the Sanitize command specified the AUSE bit set to '1') and then the Sanitize Operation State Machine transitioned from the Unrestricted Failure state to the Idle state when any controller in the NVM subsystem performed an Exit Failure Mode action.

In this state, any controller in the NVM subsystem processing a Sanitize command specifying the Sanitize Action field set to 001b (i.e., Exit Failure Mode) shall not be considered an error.

In this state, all controllers in the NVM subsystem are permitted to resume any power management that was suspended by any prior sanitize operation.

Figure FigSTZI: Idle State Transition Conditions

State Transition			Transition Condition
Starting	**Ending**	**Label** [1]	
Idle	Restricted Processing	A1	The controller starts a sanitize operation in restricted completion mode (i.e., the Sanitize command specified the AUSE bit cleared to '0').
	Unrestricted Processing	B1	The controller starts a sanitize operation in unrestricted completion mode (i.e., the Sanitize command specified the AUSE bit set to '1').

Notes:
1. Refer to Figure FigSM.

Transition Idle:Restricted Processing:

The controller shall clear the:
a) Sanitize Progress (SPROG) field to 0h; and
b) Media Verification Canceled (MVCNCLD) bit to '0'.

Transition Idle:Unrestricted Processing:

The controller shall clear the:
a) Sanitize Progress (SPROG) field to 0h; and
b) Media Verification Canceled (MVCNCLD) bit to '0'.

8.21.TBD+2.2 Restricted Processing State

In this state, if the sanitize operation fails, then the sanitization target transitions to the Restricted Failure state.

In this state:

a) the controller shall set the Sanitize Progress (SPROG) field as described in Figure 267;
b) the controller shall perform additional media modification, if required, as described in section 8.21.TBD;

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

c) the controller should deallocate all media allocated for user data, if permitted, as described in section 8.21.TBD;
d) if a change in the composition of the NVM subsystem occurs then the MVCNCLD bit shall be set to '1';
e) if a Controller Level Reset of any controller in the NVM subsystem occurs that is caused by:
   - a transport-specific reset type (refer to the applicable NVMe Transport specification); or
   - an NVM Subsystem Reset,

   then the MVCNCLD bit shall be set to '1; and
f) all controllers and Management Endpoints in the NVM subsystem shall process commands as described in section 8.21.TBD+3.

Figure FigSTZIPR: Restricted Processing State Transition Conditions

State Transition			Transition Condition
Starting	**Ending**	**Label [1]**	
Restricted Processing	Idle	C1	Sanitize processing completes successfully and the EMVS bit was: a) cleared to '0' in the Sanitize command that started the sanitize operation; or b) set to '1' in the Sanitize command that started the sanitize operation, the MVCNCLD bit is set to '1', and deallocation of all media allocated for user data completes successfully.
	Restricted Failure	D1	Sanitize processing fails.
	Media Verification	F1	The EMVS bit was set to '1' in the Sanitize command that started the sanitize operation, the sanitize processing completes successfully, and the MVCNCLD bit is cleared to '0'.
Notes: 1. Refer to Figure FigSM.			

Transition Restricted Processing:Idle:

The controller shall:

a) report the Sanitize Operation Completed asynchronous event or the Sanitize Operation Completed With Unexpected Deallocation asynchronous event as described in section 8.21.TBD+1.

Transition Restricted Processing:Restricted Failure:

The controller shall:

a) set the FAILS field to 1h (i.e., Restricted Processing state); and
b) report the Sanitize Operation Completed asynchronous event or the Sanitize Operation Completed With Unexpected Deallocation asynchronous event as described in section 8.21.TBD+1.

Transition Restricted Processing:Media Verification:

The controller shall:

a) report the Sanitize Operation Entered Media Verification State asynchronous event as described in section 8.21.TBD+1.

8.21.TBD+2.3 Restricted Failure State

This state is entered if sanitize processing was performed in the Restricted Processing state and:

a) sanitize processing failed; or
b) a failure occurred during deallocation of media allocated for user data in the Post-Verification Deallocation state.

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

In this state:

a) all controllers and Management Endpoints in the NVM subsystem shall process commands as described in section 8.21.TBD+3;
b) failure recovery requires the host to issue a subsequent Sanitize command specifying the AUSE bit cleared to '0' (i.e., restricted completion mode);
c) all controllers in the NVM subsystem shall abort a Sanitize command specifying:
   - the SANACT field set to 001b (i.e., Exit Failure Mode), with a status code of Sanitize Failed;
   - the SANACT field set to 101b (i.e., Exit Media Verification State), with a status code of Invalid Field in Command; or
   - the AUSE bit set to '1' (i.e., unrestricted completion mode), with a status code of Sanitize Failed;

   and
d) the Persistent Memory Region shall behave as described in section 8.21.TBD+3.

Figure FigSTZFR: Restricted Failure State Transition Conditions

State Transition			Transition Condition
Starting	**Ending**	**Label [1]**	
Restricted Failure	Restricted Processing	A2	The controller starts a sanitize operation in restricted completion mode (i.e., the Sanitize command specified the AUSE bit cleared to '0').

Notes:
1. Refer to Figure FigSM.

Transition Restricted Failure:Restricted Processing:

The controller shall start a sanitize operation in the Restricted Processing state. The controller shall:
a) clear the Sanitize Progress (SPROG) field to 0h; and
b) clear the Media Verification Canceled (MVCNCLD) bit to '0'.

8.21.TBD+2.4 Unrestricted Processing State

In this state, if the sanitize operation fails, then the sanitization target transitions to the Unrestricted Failure state, from which it is able to transition to the Idle state without successful sanitization.

In this state:

a) the controller shall set the Sanitize Progress (SPROG) field as described in Figure 267;
b) the controller shall perform additional media modification, if required, as described in section 8.21.TBD;
c) the controller should deallocate all media allocated for user data, if permitted, as described in section 8.21.TBD;
d) if a change in the composition of the NVM subsystem occurs then the MVCNCLD bit shall be set to '1;
e) if a Controller Level Reset of any controller in the NVM subsystem occurs that is caused by:
   - a transport-specific reset type (refer to the applicable NVMe Transport specification); or
   - an NVM Subsystem Reset,

   then the MVCNCLD bit shall be set to '1; and
f) all controllers and Management Endpoints in the NVM subsystem shall process commands as described in section 8.21.TBD+3.

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

Figure FigSTZIPU: Unrestricted Processing State Transition Conditions

State Transition			Transition Condition
Starting	**Ending**	**Label** [1]	
Unrestricted Processing	Idle	C2	The sanitize processing completes successfully and the EMVS bit was: a) cleared to '0' in the Sanitize command that started the sanitize operation; or b) set to '1' in the Sanitize command that started the sanitize operation, the MVCNCLD bit is set to '1', and deallocation of all media allocated for user data completes successfully.
	Unrestricted Failure	D2	The sanitize processing fails.
	Media Verification	F2	The EMVS bit was set to '1' in the Sanitize command that started the sanitize operation, the sanitize processing completes successfully, and the MVCNCLD bit is cleared to '0'.
Notes: 1. Refer to Figure FigSM.			

Transition Unrestricted Processing:Idle:

The controller shall:

a) report the Sanitize Operation Completed asynchronous event or the Sanitize Operation Completed With Unexpected Deallocation asynchronous event as described in section 8.21.TBD+1.

Transition Unrestricted Processing:Unrestricted Failure:

The controller shall:

a) set the FAILS field to 3h (i.e., Unrestricted Processing state); and
b) report the Sanitize Operation Completed asynchronous event or the Sanitize Operation Completed With Unexpected Deallocation asynchronous event as described in section 8.21.TBD+1.

Transition Unrestricted Processing:Media Verification:

The controller shall:

a) report the Sanitize Operation Entered Media Verification State asynchronous event as described in section 8.21.TBD+1.

8.21.TBD+2.5 Unrestricted Failure State

This state is entered if sanitize processing was performed in the Unrestricted Processing state and:

a) sanitize processing failed; or
b) a failure occurred during deallocation of media allocated for user data in the Post-Verification Deallocation state.

In this state:

a) all controllers and Management Endpoints in the NVM subsystem shall process commands as described in section 8.21.TBD+3;
b) all controllers in the NVM subsystem shall abort a Sanitize command specifying the SANACT field set to 101b (i.e., Exit Media Verification State) with a status code of Invalid Field in Command;
c) all controllers in the NVM subsystem shall abort a Sanitize command specifying the SANACT field set to a value other than:

- 001b (i.e., Exit Failure Mode);
- 010b (i.e., Start a Block Erase sanitize operation);
- 011b (i.e., Start an Overwrite sanitize operation); or
- 100b (i.e., Start a Crypto Erase sanitize operation),

with a status code of Sanitize Failed; and

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

d) the Persistent Memory Region shall behave as described in section 8.21.TBD+3.

Figure FigSTZFU: Unrestricted Failure State Transition Conditions

State Transition			Transition Condition
Starting	**Ending**	**Label [1]**	
Unrestricted Failure	Restricted Processing	A3	The controller starts a sanitize operation in restricted completion mode (i.e., the Sanitize command specified the AUSE bit cleared to '0').
	Unrestricted Processing	B2	The controller starts a sanitize operation in unrestricted completion mode (i.e., the Sanitize command specified the AUSE bit set to '1').
	Idle	E	Any controller in the NVM subsystem performs an Exit Failure Mode action.
Notes: 1. Refer to Figure FigSM.			

Transition Unrestricted Failure:Restricted Processing:

The controller shall start a sanitize operation in the Restricted Processing state. The controller shall:
a) clear the Sanitize Progress (SPROG) field to 0h; and
b) clear the Media Verification Canceled (MVCNCLD) bit to '0'.

Transition Unrestricted Failure:Unrestricted Processing:

The controller shall start a sanitize operation in the Unrestricted Processing state. The controller shall:
a) clear the Sanitize Progress (SPROG) field to 0h; and
b) clear the Media Verification Canceled (MVCNCLD) bit to '0'.

Transition Unrestricted Failure:Idle:

If any controller in the NVM subsystem performs an Exit Failure Mode action, then the controller shall recover from the sanitization failure by transitioning the Sanitize Operation State Machine to the Idle state and shall complete the Sanitize command that specified the Exit Failure Mode action with a status code of Successful Completion.

8.21.TBD+2.6 Media Verification State

In this state, the sanitize processing completed successfully, and all media allocated for user data in the sanitization target is readable by the host for purposes of verifying sanitization.

In this state:
a) the Sanitize Operation State Machine shall transition to the Post-Verification Deallocation state if any controller in the NVM subsystem performs an Exit Media Verification State action;
b) all controllers in the NVM subsystem shall abort a Sanitize command specifying the SANACT field not set to 101b (i.e., Exit Media Verification State) with a status code of Invalid Field in Command; and
c) all controllers and Management Endpoints in the NVM subsystem shall process commands as described in section 8.21.TBD+3, with exceptions as described in the appropriate I/O command set specification (e.g., the Read command in the NVM Command Set is processed as described in the Media Verification section of the NVM Command Set Specification).

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

Figure FigSTZMV: Media Verification State Transition Conditions

State Transition			Transition Condition
Starting	**Ending**	**Label [1]**	
Media Verification	Post-Verification Deallocation	G	Either: a) any controller in the NVM subsystem performs an Exit Media Verification State action; b) an NVM Subsystem Reset occurs in any domain in the NVM subsystem; c) a Controller Level Reset caused by a transport-specific reset type (refer to the applicable NVMe Transport specification) of any controller in the NVM subsystem occurs; or d) a change in the composition of the NVM subsystem prevents media verification.
Notes: 1. Refer to Figure FigSM.			

Transition Media Verification:Post-Verification Deallocation:

The controller shall:

a) clear the Sanitize Progress (SPROG) field to 0h;
b) set the Media Verification Canceled (MVCNCLD) bit to '1', if any controller in the NVM subsystem processes a Controller Level Reset caused by:
   - an NVM Subsystem Reset; or
   - a transport-specific reset type (refer to the applicable NVMe Transport specification), if any;
c) set the Media Verification Canceled (MVCNCLD) bit to '1', if a change in the composition of the NVM subsystem prevents media verification; and
d) complete the Sanitize command with a status code of Successful Completion, if any controller in the NVM subsystem performs an Exit Media Verification State action.

8.21.TBD+2.7 Post-Verification Deallocation State

In this state:

a) the controller shall deallocate all media allocated for user data in the sanitization target;
b) the Sanitize Progress (SPROG) field shall be set as described in Figure 267; and
c) all controllers and Management Endpoints in the NVM subsystem shall process commands as described in section 8.21.TBD+3.

Figure FigSTZMV: Post-Verification Deallocation state Transition Conditions

State Transition			Transition Condition
Starting	**Ending**	**Label [1]**	
Post-Verification Deallocation	Idle	H	The controller completes deallocation of all media allocated for user data.
	Restricted Failure	I1	The sanitize operation was started by a Sanitize command specifying the AUSE bit cleared to '0' (i.e., restricted completion mode), and a failure occurs during deallocation of all media allocated for user data.
	Unrestricted Failure	I2	The sanitize operation was started by a Sanitize command specifying the AUSE bit set to '1' (i.e., unrestricted completion mode), and a failure occurs during deallocation of all media allocated for user data.
Notes: 1. Refer to Figure FigSM.			

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

Transition Post-Verification Deallocation:Idle:

The controller shall:

a) report the Sanitize Operation Completed asynchronous event as described in section 8.21.TBD+1.

Transition Post-Verification Deallocation:Restricted Failure:

The controller shall:

a) report the Sanitize Operation Completed asynchronous event as described in section 8.21.TBD+1; and
b) set the FAILS field to 6h (i.e., Post-Verification Deallocation state).

Transition Post-Verification Deallocation:Unrestricted Failure:

The controller shall:

a) report the Sanitize Operation Completed asynchronous event as described in section 8.21.TBD+1; and
b) set the FAILS field to 6h (i.e., Post-Verification Deallocation state).

~~8.21.1~~ 8.21.TBD+3 Sanitize Operation Restrictions

In the following states:

- Restricted Processing;
- Restricted Failure;
- Unrestricted Processing;
- Unrestricted Failure;
- Media Verification; and
- Post-Verification Deallocation,

~~While performing a sanitize operation and while a failed sanitize operation has occurred but successful recovery from that failure has not occurred,~~ all enabled controllers ~~and namespaces~~ in the NVM subsystem are restricted to performing only a limited set of actions.

When a sanitize operation starts on any controller (i.e., a transition into the Restricted Processing state occurs or a transition into the Unrestricted Processing state occurs), all controllers in the NVM subsystem shall:

- ~~Shall~~ clear ~~any~~ all of the following outstanding asynchronous events:
    - Sanitize Operation Completed asynchronous event, if any; ~~or~~
    - Sanitize Operation Completed With Unexpected Deallocation asynchronous event, if any; and
    - Sanitize Operation Entered Media Verification State asynchronous event, if any;
- ~~Shall~~ update the Sanitize Status log page (refer to section 5.16.1.25);
- ~~Shall~~ abort any command (submitted or in progress) not allowed during a sanitize operation (refer to Figure 140) with a status code of Sanitize In Progress ~~(refer to section 8.21.1)~~, unless otherwise specified;
- ~~Shall~~ abort device self-test operations in progress;
- ~~Suspends~~ suspend autonomous power state management activities as described in section 8.15.2; and
- ~~Shall~~ release stream identifiers for any open streams.

If ~~While~~ a sanitize operation is in ~~progress~~ any of the following states (i.e., is in progress):

- Restricted Processing;
- Unrestricted Processing;
- Media Verification; or
- Post-Verification Deallocation,

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

then for each controller in the NVM subsystem:

- ~~All controllers in the NVM subsystem shall only process the Admin commands listed in Figure 140 subject to the additional restrictions stated in that figure;~~
- ~~A~~all I/O Commands other than a Flush command shall be aborted with a status code of Sanitize In Progress, unless otherwise specified;
- ~~P~~processing of a Flush command is specified in section 7.1;
- ~~A~~any command or command option that is not explicitly permitted in Figure 140 shall be aborted with a status code of Sanitize In Progress if ~~fetched~~ processed by the controller ~~by any controller in the NVM subsystem; and~~;
- ~~T~~the Persistent Memory Region shall be prevented from being enabled (i.e., setting PMRCTL.EN to '1' does not result in PMRSTS.NRDY being cleared to '0'); and
- ~~A~~activation of new firmware is prohibited ~~during a sanitize operation (refer to section 8.21.1)~~.

~~While a failed sanitize operation has occurred, a subsequent sanitize operation has not started and successful recovery from the failed sanitize operation has not occurred:~~ While the sanitization target is in the Restricted Failure state or the Unrestricted Failure state, then for each controller in the NVM subsystem:

- ~~All controllers in the NVM subsystem shall only process the Sanitize command (refer to section 5.24) and the Admin commands listed in Figure 140 subject to the additional restrictions noted in that figure;~~
- any command or command option that is not explicitly permitted in Figure 140 shall be aborted with a status code of Sanitize In Progress if processed by the controller;
- ~~A~~all I/O Commands other than a Flush command (refer to section 7.1) shall be aborted with a status code of Sanitize Failed;
- ~~T~~the Sanitize command is permitted with action restrictions (refer to section 5.24); and
- ~~Aside from the Sanitize command, any other command or command option that is not explicitly permitted in Figure 140 shall be aborted with a status code of Sanitize Failed if fetched by any controller in the NVM subsystem; and~~
- ~~T~~the Persistent Memory Region shall be prevented from being enabled (i.e., setting PMRCTL.EN to '1' does not result in PMRSTS.NRDY being cleared to '0').

When a sanitize operation starts on any controller in an NVM subsystem (i.e., a transition into the Restricted Processing state occurs or a transition into the Unrestricted Processing state occurs), all Management Endpoints in the NVM subsystem shall perform the sanitize operation as described in the NVM Express Management Interface Specification.

…

Annex A. Sanitize Operation Considerations (Informative)

A.1 Overview

The Sanitize command ~~initiates~~ starts a sanitize operation that makes all user data previously written to the ~~device~~ sanitization target inaccessible (i.e., all user data has been purged, as defined in IEEE Std 2883-2022). ~~To do this a Sanitize command is provided over the device's physical interface that cause the controller to process the requested operation. The actual result of the operation is very difficult to prove as complete~~ It is very difficult to prove that the sanitize operation successfully purged all user data. This annex provides some context and considerations for understanding the result of the operation and the practical limitations for auditing the result of the sanitize operation.

A.2 Hidden Storage (Overprovisioning)

Sanitize operations ~~affect~~ purge all physical storage in the sanitization target that is able to hold user data. Many NVMe SSDs contain more physical storage than is addressable through the interface (e.g., overprovisioning). ~~, which~~ That physical storage is used for vendor specific purposes ~~that~~ which may include providing increasing endurance, improving performance, and providing extra capacity to allow retiring bad or worn-out storage without affecting capacity. This excess capacity as well as any retired storage are not accessible through the interface. Vendor specific innovative use of this extra capacity supports advantages

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

to the end user, but the lack of observability makes it difficult to ensure that all storage within the ~~device has been affected~~ sanitization target was correctly purged. Only the accessible storage is able to be audited for the results of a sanitization operation.

A.3 Integrity checks and No-Deallocate After Sanitize

Another issue is availability of the data returned through the interface. Some of the sanitize operations (e.g., Block Erase) affect the physical devices in such a way that directly reading the accessible storage may trigger internal integrity checks resulting in error responses instead of returning the contents of the storage. Other sanitize operations (e.g., Crypto Erase) may scramble the vendor specific internal format of the data, also resulting in error responses instead of returning the contents of the storage.

~~Some devices compensate for these issues by performing an additional internal write operation on all storage that is able to be allocated for user data.~~To compensate for these issues, a controller may perform additional internal write operations to media that is able to be allocated for user data (i.e., additional media modification, refer to section 8.21.TBD) so that all media that is allocated for user data is readable without error. However, this has the side effect of potentially significant additional wear on the ~~device~~ media as well as the side effect of obscuring the results of the initial sanitize operation (i.e., the writes ~~forensically~~ destroy the ability to forensically audit the result of the initial sanitize operation). Given this side effect, process audits of sanitize behavior only ~~prove~~ provide effective results when the No-Deallocate After Sanitize bit is set the same way (e.g., set to '1') for both process audits and the individual forensic device audits.

The Sanitize command introduced in NVM Express Base Specification revision 1.3 included a mechanism to specify that sanitized ~~addressable storage~~ media allocated for user data not be deallocated, thereby allowing observations of the results of the sanitization operation. However, some architectures and products (e.g., integrity checking circuitry) interact with this capability in such a way as to defeat the sanitize result observability purpose. New features were added to NVM Express Base Specification revision 1.4 that include extended information about the sanitization capabilities of devices, a new asynchronous event, and configuration of the response to No-Deallocate After Sanitize requests. These features are intended to both support new systems that understand the new capabilities, as well to help manage legacy systems that do not understand the new capabilities without losing the ability to sanitize as requested.

These issues in returning the contents of accessible storage do not apply if the sanitization target is in the Media Verification state (refer to section 8.21.TBD+2.6). In that state, failure of internal integrity checks do not cause error responses to Read commands (refer to the Media Verification section of the NVM Command Set Specification). Because the Sanitize command that caused entry to the Media Verification state specified the Enter Media Verification State (EMVS) bit set to '1', the controller does not perform the additional media modification described in this section.

A.4 Bad Media and Vendor Specific NAND Use

Another audit capability that is not supported by NVM Express is checking that any media that could not be sanitized (e.g., bad physical blocks) has been removed from the pool of storage that is able to be used as addressable storage.

An approach that is performed under some circumstances is removing the physical storage components from the NVM Express device after a sanitize operation and reading the contents in laboratory conditions. However, this approach also has multiple difficulties. When physical storage ~~devices~~ components are removed from a NVM Express device, much context is lost. This includes:

a) any encoding for zero's/one's balance;
b) identification of which components contain device firmware or other non-data information; and
c) which media has been retired and cannot be sanitized.

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

Description of Specification Changes for the NVM Express NVM Command Set Specification 1.0c

5 Extended Capabilities

…

5.6 Sanitize Operations

Sanitize operates as defined in the NVM Express Base Specification. NVM Command Set specific definitions and extensions are defined in this section.

Following a successful sanitize operation, the values of user data, protection information, and non-PI metadata that result from an audit (refer to the NVM Express Base Specification) of the ~~NVM subsystem~~ sanitization target are specified in Figure 138. If the controller deallocates ~~user data~~ logical blocks after successful completion of a sanitize operation, then values read from deallocated logical blocks are described in section 3.2.3.2.1. The host may specify that sanitized logical blocks not be deallocated by setting the No-Deallocate After Sanitize bit to '1' in the Sanitize command.

Figure 138: Sanitize Operation~~s~~ Types – User Data Values

Sanitize Operation Type	User Data
Block Erase	Vendor specific value
Crypto Erase	Indeterminate value
Overwrite	Refer to Sanitize Operations – Overwrite Mechanism in the NVM Express Base Specification

5.6.TBD Media Verification

While the sanitization target is in the Media Verification state (refer to the Sanitize Operation State Machine Section in the NVM Express Base Specification), the controller processes Read commands as described in this section and shall not abort those commands with a status code of Sanitize In Progress.

If:

- the controller processes a Read command that does not specify any Protection Information (PI) checking (i.e., the PRCHK field is cleared to 000b; refer to Figure 9); and
- for each LBA specified by that command for which media is allocated, the controller is able to read data from the media,

then:

- for each LBA specified by that command for which media is allocated, the controller:
  - shall ignore data integrity errors, if any (e.g., shall not abort that command with a status code of Unrecovered Read Error if the controller is able to read that media);
  - shall return data that is read from that media; and
  - may return different data for successive reads (i.e., without any writes between those reads) of the same LBA (e.g., to obscure media reliability);
- for each LBA specified by that command for which media is not allocated, the controller shall return data or abort that command with a status code of Deallocated or Unwritten Logical Block as described in section 3.2.3.2.1; and
- the controller shall complete that command with a status code of Successful Media Verification Read if the command has not been aborted with a different status code (e.g., Deallocated or Unwritten Logical Block).

If the controller processes a Read command that does not specify any PI checking and is unable to read the data from the media for any LBA specified by that command for which media is allocated, then the controller shall abort the command with a status code of Unrecovered Read Error.

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

If the controller processes a Read command specifying PI checking (i.e., the PRCHK field is set to a non-zero value), then the controller shall abort that command with a status code of Invalid Field in Command.

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

Description of Specification Changes for the NVM Express Zoned Namespace Command Set Specification 1.1c

4 Admin Commands for the Zoned Namespace Command Set

4.1 Admin Command behavior for the Zoned Namespace Command Set

…

4.1.7 Sanitize command

…

Figure 51: Sanitize Behavior for the Zoned Namespace Command Set

No Deallocate After Sanitize	No-Deallocate Modifies Media After Sanitize (NODMMAS)	No-Deallocate Inhibited (NDI)	No-Deallocate Response Mode (NODRM)	Results of a successful sanitize operation		
				Zone State [1]	Logical Block Content [2]	Sanitize Status [4]
0b	n/a [3]	n/a [3]	n/a [3]	ZSE:Empty	Refer to section 2.1.1.2.1.2	001b
…						

Notes:
1. ZSO:Offline state is a valid zone state as a result of a successful sanitize operation.
2. This field describes the read value from a deallocated logical block. Refer to the Deallocated or Unwritten Logical Blocks section in the NVM Command Set Specification.
3. This value is not relevant in the setup conditions defined in that row.
4. Value reported in the Sanitize Operation Status (SOS) field ~~bits 2:0~~ of the Sanitize Status (SSTAT) field in the Sanitize Status log page (Log Identifier 81h) (refer to the NVM Express Base Specification).
5. Sanitize command is aborted with a status code of Invalid Field in Command.

…

5 Extended Capabilities

…

5.TBD Sanitize Operations

If the NVM subsystem is in the Media Verification state (refer to the Sanitize Operations section of the NVM Express Base Specification), then the logical block content is described in the Media Verification section of the NVM Express NVM Command Set Specification.

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

Description of Specification Changes for the NVM Express Key Value Command Set Specification 1.0c

5 Extended Capabilities

…

5.3 Sanitize Operations

A sanitize operation is performed as defined in the NVM Express Base Specification~~.~~, with the following exceptions:

- Namespaces associated with the Key Value command set are not accessible in the Media Verification state or the Post-Verification Deallocation state (refer to the Sanitize Operations section in the NVM Express Base Specification).
- Namespaces associated with the Key Value command set do not support additional media modification (refer to the NVM Express Base Specification).

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.