BS ISO/IEC 24775-2:2021

BSI Standards Publication

Information technology — Storage management

Part 2: Common Architecture

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24775-2:2021

National foreword

This British Standard is the UK implementation of ISO/IEC 24775-2:2021. It supersedes BS ISO/IEC 24775-2:2014, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee ICT/1, Information systems co-ordination.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2021
Published by BSI Standards Limited 2021

ISBN 978 0 539 13973 0

ICS 35.200

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 April 2021.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24775-2:2021

INTERNATIONAL STANDARD

ISO/IEC 24775-2

Second edition
2021-03

Information technology — Storage management —

Part 2: Common Architecture

Reference number
ISO/IEC 24775-2:2021(E)

Documents
Document Sharing Hub
© ISO/IEC 2021

Full document details: BS ISO/IEC 24775-2:2021

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2021

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24775-2:2021

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see http://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by SNIA (as Storage Management Technical Specification, Part 2 Common Architecture, Version 1.8.0, Revision 5) and drafted in accordance with its editorial rules. It was adopted, under the JTC 1 PAS procedure, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*.

This second edition cancels and replaces the first edition (ISO/IEC 24775-2:2014), which has been technically revised.

The main changes compared to the previous edition are as follows:

— USAGE text was revised to address code (now included in the front matter for all SNIA specifications)

— All recipes and their references were deleted.

— Instances of subprofile were changed to profile. In the annex, instances of subprofile were changed to component profile (TSG meeting voice vote).

— Profile versions and related text were updated. (TSG meeting voice vote).

— Indications have been replaced by DMTF Indications, and all affected clauses updated. (TSG meeting voice vote).

— Instances of Experimental within profiles already labeled as Experimental were removed to avoid confusion and redundancy. (Editorial change)

— CIM/XML was changed to CIM-XML (Response to ballot comments).

Documents
Document Sharing Hub

© ISO/IEC 2021 – All rights reserved

Full document details: BS ISO/IEC 24775-2:2021

— Annex: SMI-S Information Model.

— The CIM schema version was changed to 2.51 for V1.8.0 Rev3.

— Health and Fault Management

  — Table 1: OperationalStatus for Disk Drive, revised re operational status.
  — Revised Array example and other text (CORE-SMIS-SCR-00084).

— Indications

  — Added as Clause 10, includes some material previously in Annex C (normative) Indication Filter Strings.
  — References the DMTF Indications Profile, DSP 1054, version 1.2.2.

— References

  — Five references were added to DMTF references (Final) section (to indicate most recent versions). One reference was added to References under development section.
  — Added link to the SNIA TLS Specification.
  — Deleted "V.1.0" from all references to the SNIA TLS Specification for Storage Systems in SMI-S v1.6.1 and later versions of SMI-S (TSG ballot).

— Security

  — Removed Experimental material in the Securityclause per voice vote in TSG.

— Standard Messages

  — Standard messages (in table format) remain in the document (after being removed in a previous revision, TSG meeting voice vote).
  — Changes applied to the Standard Message tables:
  — Promoted to experimental new alert standard messages for diagnostic tests on storage pools (SMIS-170-Draft-SCR00003).
  — Resolved duplicate use of standard messages in the Block Storage Messages section (TSG-SMISSCR00316.001).
  — Added alerts in Common Profile-Related Messages section (TSG-SMIS-SCR00315.001, SMIS-170-Draft-SCR00008).
  — Promoted the maturity level from DRAFT to EXPERIMENTAL for these revisions: Updated profiles to remove SNIA_ classes and use DMTF CIM_ classes. (TSG-SMIS-SCR00315.001, SMIS-170-Draft- SCR00008) in Common Profile-Related Messages section and Filesystem Messages section.

— Annex A (informative) Mapping CIM Objects to SNMP MIB Structure removed.

— Annex B (normative) Compliance with the SNIA SMI Specification changed to Annex A.

— Annex C (normative) Indication Filter Strings removed. Some material moved to new Indications profile.

A list of all parts in the ISO/IEC 24775 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Documents
Document Sharing Hub

© ISO/IEC 2021 – All rights reserved

Full document details: BS ISO/IEC 24775-2:2021

INTENDED AUDIENCE

This document is intended for use by individuals and companies engaged in developing, deploying, and promoting interoperable multi-vendor SANs through the Storage Networking Industry Association (SNIA) organization.

CHANGES TO THE SPECIFICATION

Each publication of this specification is uniquely identified by a three-level identifier, comprised of a version number, a release number and an update number. The current identifier for this specification is version 1.8.0. Future publications of this specification are subject to specific constraints on the scope of change that is permissible from one publication to the next and the degree of interoperability and backward compatibility that should be assumed between products designed to different publications of this standard. The SNIA has defined three levels of change to a specification:

- Major Revision: A major revision of the specification represents a substantial change to the underlying scope or architecture of the SMI-S API. A major revision results in an increase in the version number of the version identifier (e.g., from version 1.x.x to version 2.x.x). There is no assurance of interoperability or backward compatibility between releases with different version numbers.
- Minor Revision: A minor revision of the specification represents a technical change to existing content or an adjustment to the scope of the SMI-S API. A minor revision results in an increase in the release number of the specification's identifier (e.g., from x.1.x to x.2.x). Minor revisions with the same version number preserve interoperability and backward compatibility.
- Update: An update to the specification is limited to minor corrections or clarifications of existing specification content. An update will result in an increase in the third component of the release identifier (e.g., from x.x.1 to x.x.2). Updates with the same version and minor release levels preserve interoperability and backward compatibility.

TYPOGRAPHICAL CONVENTIONS

Maturity Level

In addition to informative and normative content, this specification includes guidance about the maturity of emerging material that has completed a rigorous design review but has limited implementation in commercial products. This material is clearly delineated as described in the following sections. The typographical convention is intended to provide a sense of the maturity of the affected material, without altering its normative content. By recognizing the relative maturity of different sections of the standard, an implementer should be able to make more informed decisions about the adoption and deployment of different portions of the standard in a commercial product.

This specification has been structured to convey both the formal requirements and assumptions of the SMI-S API and its emerging implementation and deployment lifecycle. Over time, the intent is that all content in the specification will represent a mature and stable design, be verified by extensive implementation experience, assure consistent support for backward compatibility, and rely solely on content material that has reached a similar level of maturity. Unless explicitly labeled with one of the subordinate maturity levels defined for this specification, content is assumed to satisfy these requirements and is referred to as "Finalized". Since much of the evolving specification

content in any given release will not have matured to that level, this specification defines three subordinate levels of implementation maturity that identify important aspects of the content's increasing maturity and stability. Each subordinate maturity level is defined by its level of implementation experience, its stability and its reliance on other emerging standards. Each subordinate maturity level is identified by a unique typographical tagging convention that clearly distinguishes content at one maturity model from content at another level.

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24775-2:2021

Experimental Maturity Level

No material is included in this document unless its initial architecture has been completed and reviewed. Some content included in this document has complete and reviewed design, but lacks implementation experience and the maturity gained through implementation experience. This content is included in order to gain wider review and to gain implementation experience. This material is referred to as "Experimental". It is presented here as an aid to implementers who are interested in likely future developments within the SMI specification. The contents of an Experimental profile may change as implementation experience is gained. There is a high likelihood that the changed content will be included in an upcoming revision of the specification. Experimental material can advance to a higher maturity level as soon as implementations are available. Figure 1 is a sample of the typographical convention for Experimental content.

EXPERIMENTAL

Experimental content appears here.

EXPERIMENTAL

Figure 1 - Experimental Maturity Level Tag

Implemented Maturity Level

Profiles for which initial implementations have been completed are classified as "Implemented". This indicates that at least two different vendors have implemented the profile, including at least one provider implementation. At this maturity level, the underlying architecture and modeling are stable, and changes in future revisions will be limited to the correction of deficiencies identified through additional implementation experience. Should the material become obsolete in the future, it must be deprecated in a minor revision of the specification prior to its removal from subsequent releases. Figure 2 is a sample of the typographical convention for Implemented content.

IMPLEMENTED

Implemented content appears here.

IMPLEMENTED

Figure 2 - Implemented Maturity Level Tag

Stable Maturity Level

Once content at the Implemented maturity level has garnered additional implementation experience, it can be tagged at the Stable maturity level. Material at this maturity level has been implemented by three different vendors, including both a provider and a client. Should material that has reached this maturity level become obsolete, it may only be deprecated as part of a minor revision to the specification. Material at this maturity level that has been deprecated may only be removed from the specification as part of a major revision. A profile that has reached this maturity level is guaranteed to preserve backward compatibility from one minor specification revision to the next. As a result, Profiles at or above the Stable

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24775-2:2021

maturity level shall not rely on any content that is Experimental. Figure 3 is a sample of the typographical convention for Implemented content.

STABLE

Stable content appears here.

STABLE

Figure 3 - Stable Maturity Level Tag

Finalized Maturity Level

Content that has reached the highest maturity level is referred to as “Finalized.” In addition to satisfying the requirements for the Stable maturity level, content at the Finalized maturity level must solely depend upon or refine material that has also reached the Finalized level. If specification content depends upon material that is not under the control of the SNIA, and therefore not subject to its maturity level definitions, then the external content is evaluated by the SNIA to assure that it has achieved a comparable level of completion, stability, and implementation experience. Should material that has reached this maturity level become obsolete, it may only be deprecated as part of a major revision to the specification. A profile that has reached this maturity level is guaranteed to preserve backward compatibility from one minor specification revision to the next. Over time, it is hoped that all specification content will attain this maturity level. Accordingly, there is no special typographical convention, as there is with the other, subordinate maturity levels. Unless content in the specification is marked with one of the typographical conventions defined for the subordinate maturity levels, it should be assumed to have reached the Finalized maturity level.

Deprecated Material

Non-Experimental material can be deprecated in a subsequent revision of the specification. Sections identified as “Deprecated” contain material that is obsolete and not recommended for use in new development efforts. Existing and new implementations may still use this material, but shall move to the newer approach as soon as possible. The maturity level of the material being deprecated determines how long it will continue to appear in the specification. Implemented content shall be retained at least until the next revision of the specialization, while Stable and Finalized material shall be retained until the next major revision of the specification. Providers shall implement the deprecated elements as long as it appears in the specification in order to achieve backward compatibility. Clients may rely on deprecated elements, but are encouraged to use non-deprecated alternatives when possible.

Deprecated sections are documented with a reference to the last published version to include the deprecated section as normative material and to the section in the current specification with the replacement. Figure 4 contains a sample of the typographical convention for deprecated content.

DEPRECATED

Content that has been deprecated appears here.

DEPRECATED

Figure 4 - Deprecated Tag

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24775-2:2021

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24775-2:2021

Contents

List of Figures 15
List of Tables 17
Foreword 23

1 Scope 25

2 Normative references 27
2.1 General 27
2.2 Approved references 27
2.3 DMTF references (Final) 27
2.4 IETF references 28
2.5 References under development 29
2.6 Other references 29

3 Terms, definitions, symbols, abbreviations, and conventions 31
3.1 Terms and definitions 31
3.2 Acronyms and abbreviations 37
3.3 Keywords 37
3.4 Conventions 38

4 Transport and Reference Model 41
4.1 Introduction 41
4.1.1 Overview 41
4.1.2 Language Requirements 41
4.1.3 Communications Requirements 41
4.1.4 XML Message Syntax and Semantics 41
4.2 Transport Stack 42
4.3 Reference Model 42
4.3.1 Overview 42
4.3.2 Roles for Interface Constituents 43
4.3.3 Cascaded Agents 43

5 Health and Fault Management 45
5.1 Objectives 45
5.2 Overview 45
5.3 Terms 45
5.4 Description of Health and Fault Management 46
5.4.1 Operational Status and Health State (Polling) 46
5.4.2 Standard Errors and Events 47
5.4.3 Indications 47
5.4.4 Event Correlation and Fault Containment 47
5.4.5 Fault Regions 50
5.4.6 Examples 52

6 Object Model General Information 55
6.1 Model Overview (Key Resources) 55
6.1.1 Overview 55
6.1.2 Introduction to CIM UML Notation 55
6.2 Techniques 56
6.2.1 CIM Fundamentals 56
6.2.2 Modeling Profiles 58
6.2.3 CIM Naming 58

7 Correlatable and Durable Names 59

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24775-2:2021

7.1 Overview ... 59
7.2 Guidelines for SCSI Logical Unit Names ... 60
7.3 Guidelines for FC-SB-2 Device Names ... 60
7.4 Guidelines for Port Names ... 61
7.5 Guidelines for Storage System Names ... 61
7.6 Standard Formats for Correlatable Names ... 62
7.6.1 General ... 62
7.6.2 Standard Formats for Logical Unit Names ... 63
7.6.3 Standard Formats for Port Names ... 64
7.6.4 Standard Formats for Fabric Names ... 65
7.6.5 Standard Formats for Storage System Names ... 65
7.6.6 Operating System Device Names ... 67
7.6.7 Case Sensitivity ... 68
7.7 Testing Equality of correlatable Names ... 68
7.8 iSCSI Names ... 69
8 Standard Messages ... 71
8.1 Overview ... 71
8.2 Registries for Standard Messages ... 71
8.3 SNIA Standard Messages ... 71
8.3.1 Common Profile-related Messages ... 71
8.3.2 Block Storage Messages ... 85
8.3.3 Fabric Messages ... 118
8.3.4 Filesystem Messages ... 123
8.3.5 Host Messages ... 135
8.3.6 Media Library Messages ... 138
9 Service Discovery ... 171
9.1 Objectives ... 171
9.2 Overview ... 171
9.3 SLP Messages ... 173
9.4 Scopes ... 174
9.5 Services Definition ... 175
9.5.1 SLP Terms ... 175
9.5.2 Service Type ... 175
9.5.3 Service Attributes ... 175
9.6 User Agents (UA) ... 175
9.7 Service Agents (SAs) ... 176
9.8 Directory Agents (DAs) ... 177
9.9 Service Agent Server (SA Server) ... 177
9.9.1 General Information ... 177
9.9.2 SA Server (SAS) Implementation ... 177
9.9.3 SA Server (SAS) Clients ... 178
9.9.4 SA Server Configuration ... 178
9.9.5 SA Server Discovery ... 180
9.9.6 SAS Client Registration ... 180
9.10 Configurations ... 180
9.10.1 Overview ... 180
9.10.2 Multicast Configurations ... 180
9.10.3 No Multicast configuration ... 181
9.10.4 Multicast Islands ... 182
10 Indications ... 185

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24775-2:2021

10.1 Indications profile ... 185
10.1.1 Profile Support ... 185
10.1.2 Creating a client defined indication and subscription ... 185
10.1.3 ListenerDestination ... 185
10.2 Indication Filter Strings ... 185
10.2.1 Definition Syntax ... 185
10.2.2 Instance Creation ... 186
10.2.3 Instance Deletion ... 186
10.2.4 Modification of any value in an array property ... 186
10.2.5 Modification to either of Two Specific values in an Array Property ... 186
10.2.6 Alert ... 187
11 SMI-S Roles ... 189
11.1 Introduction ... 189
11.2 SMI-S Client ... 190
11.2.1 Overview ... 190
11.2.2 SLP Functions ... 190
11.2.3 Generic Operations ... 190
11.2.4 Security Considerations ... 190
11.2.5 Lock Management Functions ... 190
11.3 Dedicated SMI-S Server ... 190
11.3.1 Overview ... 190
11.3.2 SLP Functions ... 191
11.3.3 Generic Operations ... 191
11.3.4 Security Considerations ... 192
11.3.5 Lock Management Functions ... 192
11.4 General Purpose SMI-S Server ... 192
11.4.1 Overview ... 192
11.4.2 SLP Functions ... 192
11.4.3 Generic Operations ... 193
11.4.4 Lock Management Functions ... 193
11.4.5 Provider Sub-role ... 193
11.5 Directory Server ... 193
11.5.1 SLP Functions ... 193
11.5.2 Generic Operations ... 193
11.5.3 Security Considerations ... 193
11.5.4 Lock Management Functions ... 194
11.6 Combined Roles on a Single System ... 194
11.6.1 Overview ... 194
11.6.2 General Purpose SMI-S Server as a Profile Aggregator ... 194
12 Installation and Upgrade ... 195
12.1 Introduction ... 195
12.2 Role of the Administrator ... 195
12.3 Goals ... 195
12.3.1 Non-Disruptive Installation and De-installation ... 195
12.3.2 Plug-and-Play ... 195
12.4 Server Deployment ... 196
12.4.1 General ... 196
12.4.2 Controlled Environment ... 196
12.4.3 Multiple WBEM Server systems ... 196
12.4.4 Shared WBEM Server ... 197
12.4.5 Uninstallation ... 198

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24775-2:2021

12.4.6 Update ... 198
12.4.7 Reconfiguration ... 198
12.5 WBEM Service Support & Related Functions ... 198
12.5.1 Installation ... 198
12.5.2 Multiple WBEM Servers on a Single Server System ... 199
12.5.3 Uninstallation/Upgrade ... 199
12.5.4 Reconfiguration ... 199
12.5.5 Failure ... 199
12.6 Client ... 199
12.6.1 Uninstallation ... 199
12.6.2 Reconfiguration ... 199
12.7 Directory Service ... 199
12.7.1 Installation ... 199
12.7.2 Uninstallation/Failure ... 200
12.8 Issues with Discovery Mechanisms ... 200
13 Security ... 201
13.1 Requirements ... 201
13.1.1 Overview ... 201
13.1.2 General Requirements for HTTP Implementations ... 202
13.2 Description of SMI-S Security ... 202
13.2.1 Security Scope ... 202
13.2.2 Transport Security ... 203
13.2.3 Authentication ... 203
13.2.4 Service Discovery ... 204
Annex A (informative) SMI-S Information Model ... 207
Annex B (normative) Compliance with the SNIA SMI Specification ... 209

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24775-2:2021

LIST OF FIGURES

Figure 1 - Experimental Maturity Level Tag 8
Figure 2 - Implemented Maturity Level Tag 8
Figure 3 - Stable Maturity Level Tag 9
Figure 4 - Deprecated Tag 9
Figure 5 - Reference Model. 42
Figure 6 - Basic Fault Detection 46
Figure 7 - Health Lifecycle 49
Figure 8 - Continuum 50
Figure 9 - Application Fault Region 51
Figure 10 - Switch Example 53
Figure 11 - Lines that Connect Classes 55
Figure 12 - iSCSI Qualified Names (iqn) Examples 69
Figure 13 - iSCSI EUI Name Example 69
Figure 14 - iSCSI 64-bit NAA Name Example 70
Figure 15 - iSCSI 128-bit NAA Name Example 70
Figure 16 - SA Server Configuration 180
Figure 17 - Multicast Configuration 181
Figure 18 - No Multicast configuration 182
Figure 19 - Multicast Islands 183
Figure 20 - SMI-S Roles 189
Figure B.1 Provider Migration 211

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24775-2:2021

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24775-2:2021

LIST OF TABLES

Table 1 - OperationalStatus for Disk Drive 46
Table 2 - Standard Formats for StorageVolume Names 63
Table 3 - Standard Formats for Port Names....64
Table 4 - Standard Formats for Storage System Names....66
Table 5 - Standard Operating System Names for Tape Devices....67
Table 6 - LogicalDisk.Name for disk partitions 68
Table 7 - GenericDiskParittion.Name for disk partitions 68
Table 8 - Standard Operating System Names for Unpartitioned DIsks 68
Table 9 - Redundancy Message Arguments 71
Table 10 - Redundancy Alert Information 72
Table 11 - Environmental Message Arguments....72
Table 12 - Environmental Alert Information 73
Table 13 - FRU Operation Message Arguments 73
Table 14 - FRU Operation Alert Information 74
Table 15 - Password change Message Arguments 74
Table 16 - Password change Alert Information....74
Table 17 - User or Account Operation Message Arguments 75
Table 18 - User or Account Operation Alert Information....75
Table 19 - User Login Message Arguments 76
Table 20 - User Login Alert Information....76
Table 21 - Proxy Agent Device Communication Message Arguments 76
Table 22 - Proxy Agent Device Communication Alert Information....77
Table 23 - Port Status Changed Message Arguments 77
Table 24 - Port Status Changed Alert Information....78
Table 25 - Datacheck Error Message Arguments....78
Table 26 - Datacheck Error Alert Information 78
Table 27 - User Login Failure Message Arguments 79
Table 28 - User Login Failure Alert Information....79
Table 29 - Drive not responding Message Arguments 80
Table 30 - Drive not responding Alert Information 80
Table 31 - Fan Failure Alert Information 80
Table 32 - Power Supply Failure Alert Information 81
Table 33 - Drive Power Consumption Alert Information 81
Table 34 - Drive Voltage Alert Information....81
Table 35 - Predictive Failure Alert Information 82
Table 36 - Diagnostics Required Alert Information 82
Table 37 - Drive is responding Message Arguments....82
Table 38 - Drive is responding Alert Information 83
Table 39 - Cooling Fan Issues Cleared Alert Information....83
Table 40 - Power Supply Issues Cleared Message Arguments 83
Table 41 - Power Supply Issues Cleared Alert Information 84
Table 42 - Controller Failure Message Arguments 84
Table 43 - Controller Failure Alert Information....84
Table 44 - Controller Issues Cleared Message Arguments 84
Table 45 - Controller Issues Cleared Alert Information....85
Table 46 - Device Not ready Message Arguments 85
Table 47 - Error Properties for Device Not ready 86
Table 48 - Error Properties for Internal Bus Error....86

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24775-2:2021

Table 49 - Error Properties for DMA Overflow 87
Table 50 - Error Properties for Firmware Logic Error 87
Table 51 - Front End Port Error Message Arguments 88
Table 52 - Front End Port Error Alert Information 88
Table 53 - Back End Port Error Message Arguments 88
Table 54 - Back End Port Error Alert Information 88
Table 55 - Remote Mirror Error Message Arguments 89
Table 56 - Error Properties for Remote Mirror Error 89
Table 57 - Remote Mirror Error Alert Information 89
Table 58 - Error Properties for Cache Memory Error 90
Table 59 - Error Properties for Unable to Access Remote Device 90
Table 60 - Error Reading Data Alert Information 91
Table 61 - Error Writing Data Alert Information 91
Table 62 - Error Validating Write (CRC) Alert Information 92
Table 63 - Error Properties for Copy Operation Failed 92
Table 64 - Error Properties for RAID Operation Failed 93
Table 65 - Error Properties for Invalid RAID Type 93
Table 66 - Error Properties for Invalid Storage Element Type 94
Table 67 - Error Properties for Configuration Change Failed 94
Table 68 - Error Properties for Buffer Overrun 95
Table 69 - Stolen Capacity Message Arguments 95
Table 70 - Error Properties for Stolen Capacity 95
Table 71 - Invalid Extent passed Message Arguments 96
Table 72 - Error Properties for Invalid Extent passed 96
Table 73 - Error Properties for Invalid Deletion Attempted 97
Table 74 - Error Properties for Job Failed to Start 97
Table 75 - Job was Halted Message Arguments 98
Table 76 - Invalid State Transition Message Arguments 98
Table 77 - Error Properties for Invalid State Transition 98
Table 78 - Invalid SAP for Method Message Arguments 99
Table 79 - Error Properties for Invalid SAP for Method 99
Table 80 - Resource Not Available Message Arguments 99
Table 81 - Error Properties for Resource Not Available 100
Table 82 - Resource Limit Exceeded Message Arguments 100
Table 83 - Error Properties for Resource Limit Exceeded 100
Table 84 - Thin Provision Capacity Warning Message Arguments 101
Table 85 - Thin Provision Capacity Warning Alert Information 101
Table 86 - Provision Capacity Critical Message Arguments 101
Table 87 - Provision Capacity Critical Alert Information 102
Table 88 - Thin Provision Capacity Okay Message Arguments 102
Table 89 - Thin Provision Capacity Okay Alert Information 102
Table 90 - Masking Group Membership Changed Message Arguments 103
Table 91 - Masking Group Membership Changed Alert Information 103
Table 92 - StorageVolume Relocation Starts Message Arguments 103
Table 93 - StorageVolume Relocation Starts Alert Information 103
Table 94 - StorageVolume Relocation Ends Message Arguments 104
Table 95 - StorageVolume Relocation Ends Alert Information 104
Table 96 - StoragePool Relocation Starts Message Arguments 104
Table 97 - StoragePool Relocation Starts Alert Information 104

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24775-2:2021

Table 98 - StoragePool Relocation Ends Message Arguments....105
Table 99 - StoragePool Relocation Ends Alert Information....105
Table 100 - LogicalDisk Relocation Starts Message Arguments....105
Table 101 - LogicalDisk Relocation Starts Alert Information....105
Table 102 - LogicalDisk Relocation Ends Message Arguments....106
Table 103 - LogicalDisk Relocation Ends Alert Information....106
Table 104 - Volume or pool degraded Message Arguments....106
Table 105 - Volume or pool degraded Alert Information....106
Table 106 - Volume or pool failed Message Arguments....107
Table 107 - Volume or pool failed Alert Information....107
Table 108 - Volume or pool issues cleared Message Arguments....107
Table 109 - Volume or pool issues cleared Alert Information....108
Table 110 - The StoragePool is healthy Message Arguments....108
Table 111 - The StoragePool is healthy Alert Information....108
Table 112 - StoragePool is dependent on an element with problems Message Arguments....109
Table 113 - StoragePool is dependent on an element with problems Alert Information....109
Table 114 - The StoragePool is being serviced Message Arguments....110
Table 115 - The StoragePool is being serviced Alert Information....110
Table 116 - The OperationalStatus of the Pool is impacting an element allocated from it Message Arguments111
Table 117 - The OperationalStatus of the Pool is impacting an element allocated from it Alert Information....111
Table 118 - The StoragePool OperationalStatus may be corrected by applying a spare Message Arguments112
Table 119 - The StoragePool OperationalStatus may be corrected by applying a spare Alert Information....112
Table 120 - The StoragePool OperationalStatus may be corrected by relocating the pool Message Arguments113
Table 121 - The StoragePool OperationalStatus may be corrected by relocating the pool Alert Information....113
Table 122 - Pool experiencing interference from system workload Message Arguments....114
Table 123 - Pool experiencing interference from system workload Alert Information....114
Table 124 - Pool performance degraded by component element Message Arguments....115
Table 125 - Pool performance degraded by component element Alert Information....115
Table 126 - Pool degraded due to loss of RAID protection Message Arguments....116
Table 127 - Pool degraded due to loss of RAID protection Alert Information....116
Table 128 - Pool degraded due to loss of port redundancy Message Arguments....117
Table 129 - Pool degraded due to loss of port redundancy Alert Information....117
Table 130 - Pool predicting failure due lack of available capacity Message Arguments....117
Table 131 - Pool predicting failure due lack of available capacity Alert Information....118
Table 132 - Zone Database Changed Message Arguments....118
Table 133 - Zone Database Changed Alert Information....118
Table 134 - ZoneSet Activated Message Arguments....119
Table 135 - ZoneSet Activated Alert Information....119
Table 136 - Error Properties for Session Locked....120
Table 137 - Error Properties for Session Aborted....120
Table 138 - Switch Status Changed Message Arguments....121
Table 139 - Switch Status Changed Alert Information....121
Table 140 - Fabric Merge/Segmentation Message Arguments....121
Table 141 - Fabric Merge/Segmentation Alert Information....121
Table 142 - Switch Added/Removed Message Arguments....122
Table 143 - Switch Added/Removed Alert Information....122
Table 144 - Fabric Added/Removed Message Arguments....122

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24775-2:2021

Table 145 - Fabric Added/Removed Alert Information....122
Table 146 - Security Policy change Message Arguments....123
Table 147 - Security Policy change Alert Information....123
Table 148 - System OperationalStatus Bellwether Message Arguments....124
Table 149 - System OperationalStatus Bellwether Alert Information....124
Table 150 - NetworkPort OperationalStatus Bellwether Message Arguments....124
Table 151 - NetworkPort OperationalStatus Bellwether Alert Information....125
Table 152 - LogicalDisk OperationalStatus Bellwether Message Arguments....125
Table 153 - LogicalDisk OperationalStatus Bellwether Alert Information....125
Table 154 - CopyState is set to Broken Message Arguments....126
Table 155 - CopyState is set to Broken Alert Information....126
Table 156 - Not Enough Space Message Arguments....127
Table 157 - Not Enough Space Alert Information....127
Table 158 - The changes in RemoteReplicationCollection Message Arguments....127
Table 159 - The changes in RemoteReplicationCollection Alert Information....128
Table 160 - The changes in ProtocolEndpoint Message Arguments....128
Table 161 - The changes in ProtocolEndpoint Alert Information....128
Table 162 - CopyState is set to Broken Message Arguments....129
Table 163 - CopyState is set to Broken Alert Information....129
Table 164 - CopyState is set to Invalid Message Arguments....129
Table 165 - CopyState is set to Invalid Alert Information....130
Table 166 - CopyState is set to Inactive Message Arguments....130
Table 167 - CopyState is set to Inactive Alert Information....130
Table 168 - CopyState is set to Split Message Arguments....131
Table 169 - CopyState is set to Split Alert Information....131
Table 170 - CopyState alert has been cleared Message Arguments....131
Table 171 - CopyState alert has been cleared Alert Information....132
Table 172 - Available Space Changed Message Arguments....132
Table 173 - Available Space Changed Alert Information....132
Table 174 - Filesystem Inaccessible Message Arguments....133
Table 175 - Filesystem Inaccessible Alert Information....133
Table 176 - Filesystem is Online Message Arguments....133
Table 177 - Filesystem is Online Alert Information....133
Table 178 - Fileshare is degraded Message Arguments....134
Table 179 - Fileshare is degraded Alert Information....134
Table 180 - Fileshare in normal state Message Arguments....134
Table 181 - Fileshare in normal state Alert Information....135
Table 182 - Required Firmware Version Message Arguments....135
Table 183 - Required Firmware Version Alert Information....135
Table 184 - Recommended Firmware Version Message Arguments....136
Table 185 - Recommended Firmware Version Alert Information....136
Table 186 - Controller OK Message Arguments....136
Table 187 - Controller OK Alert Information....136
Table 188 - Controller not OK Message Arguments....137
Table 189 - Controller not OK Alert Information....137
Table 190 - Bus rescan complete Alert Information....137
Table 191 - Disk initialize Failed Message Arguments....137
Table 192 - Disk initialize Failed Alert Information....138
Table 193 - Read Warning Alert Information....138

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24775-2:2021

Table 194 - Write Warning Alert Information....138
Table 195 - Hard Error Alert Information....139
Table 196 - Media Alert Information....139
Table 197 - Read Failure Alert Information....139
Table 198 - Write Failure Alert Information....140
Table 199 - Media Life Alert Information....140
Table 200 - Not Data Grade Alert Information....140
Table 201 - Write Protect Alert Information....141
Table 202 - No Removal Alert Information....141
Table 203 - Cleaning Media Alert Information....141
Table 204 - Unsupported Format Alert Information....142
Table 205 - Recoverable Snapped Tape Alert Information....142
Table 206 - Unrecoverable Snapped Tape Alert Information....142
Table 207 - Memory Chip In Cartridge Failure Alert Information....143
Table 208 - Forced Eject Alert Information....143
Table 209 - Read Only Format Alert Information....143
Table 210 - Directory Corrupted On Load Alert Information....144
Table 211 - Nearing Media Life Alert Information....144
Table 212 - Clean Now Alert Information....144
Table 213 - Clean Periodic Alert Information....145
Table 214 - Expired Cleaning Media Alert Information....145
Table 215 - Invalid Cleaning Media Alert Information....145
Table 216 - Retention Requested Alert Information....146
Table 217 - Dual-Port Interface Error Alert Information....146
Table 218 - Drive Maintenance Alert Information....146
Table 219 - Hardware A Alert Information....147
Table 220 - Hardware B Alert Information....147
Table 221 - Interface Alert Information....147
Table 222 - Eject Media Alert Information....148
Table 223 - Download Failure Alert Information....148
Table 224 - Loader Hardware A Alert Information....148
Table 225 - Loader Stray Media Alert Information....149
Table 226 - Loader Hardware B Alert Information....149
Table 227 - Loader Door Alert Information....149
Table 228 - Loader Hardware C Alert Information....150
Table 229 - Loader Magazine Alert Information....150
Table 230 - Loader Predictive Failure Alert Information....150
Table 231 - Load Statistics Alert Information....151
Table 232 - Media Directory Invalid at Unload Alert Information....151
Table 233 - Media System area Write Failure Alert Information....151
Table 234 - Media System Area Read Failure Alert Information....152
Table 235 - No Start of Data Alert Information....152
Table 236 - Loading Failure Alert Information....152
Table 237 - Library Hardware A Alert Information....153
Table 238 - Library Hardware B Alert Information....153
Table 239 - Library Hardware C Alert Information....153
Table 240 - Library Hardware D Alert Information....154
Table 241 - Library Diagnostic Required Alert Information....154
Table 242 - Library Interface Alert Information....154

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24775-2:2021

Table 243 - Failure Prediction Alert Information 155
Table 244 - Library Maintenance Alert Information....155
Table 245 - Library Humidity Limits Alert Information....155
Table 246 - Library Voltage Limits Alert Information....156
Table 247 - Library Stray Media Alert Information 156
Table 248 - Library Pick Retry Alert Information....156
Table 249 - Library Place Retry Alert Information....157
Table 250 - Library Load Retry Alert Information....157
Table 251 - Library Door Alert Information....157
Table 252 - Library Mailslot Alert Information 158
Table 253 - Library Magazine Alert Information....158
Table 254 - Library Security Alert Information 158
Table 255 - Library Security Mode Alert Information 159
Table 256 - Library Offline Alert Information....159
Table 257 - Library Drive Offline Alert Information....159
Table 258 - Library Scan Retry Alert Information....160
Table 259 - Library Inventory Alert Information....160
Table 260 - Library Illegal Operation Alert Information 160
Table 261 - Pass Through Mechanism Failure Alert Information....161
Table 262 - Cartridge in Pass-through Mechanism Alert Information....161
Table 263 - Unreadable barcode Labels Alert Information 161
Table 264 - Throughput Threshold Warning Alert Message Arguments....162
Table 265 - Throughput Threshold Warning Alert Alert Information 162
Table 266 - Throughput Threshold Critical Alert Message Arguments 162
Table 267 - Throughput Threshold Critical Alert Alert Information....163
Table 268 - Physical Capacity Threshold Warning Alert Message Arguments....163
Table 269 - Physical Capacity Threshold Warning Alert Alert Information 163
Table 270 - Physical Capacity Threshold Critical Alert Message Arguments 164
Table 271 - Physical Capacity Threshold Critical Alert Alert Information....164
Table 272 - Logical Capacity Threshold Warning Alert Message Arguments....165
Table 273 - Logical Capacity Threshold Warning Alert Alert Information 165
Table 274 - Logical Capacity Threshold Critical Alert Message Arguments 165
Table 275 - Logical Capacity Threshold Critical Alert Alert Information....166
Table 276 - System Ratio Threshold Warning Alert Message Arguments....166
Table 277 - System Ratio Threshold Warning Alert Alert Information 166
Table 278 - System Ratio Threshold Critical Alert Message Arguments 167
Table 279 - System Ratio Threshold Critical Alert Alert Information....167
Table 280 - Deduplication Ratio Threshold Warning Alert Message Arguments....168
Table 281 - Deduplication Ratio Threshold Warning Alert Alert Information 168
Table 282 - Deduplication Ratio Threshold Critical Alert Message Arguments 168
Table 283 - Deduplication Ratio Threshold Critical Alert Alert Information....169
Table 284 - Replication Traffic Threshold Warning Alert Message Arguments 169
Table 285 - Replication Traffic Threshold Warning Alert Alert Information....169
Table 286 - Replication Traffic Threshold Critical Alert Message Arguments....170
Table 287 - Replication Traffic Threshold Critical Alert Alert Information 170
Table 288 - Message Types 174
Table 289 - Required Configuration Properties for SA as DA....178
Table 290 - Required Configuration Properties for SA 179
Table 291 - Create an IndicationFilter and subscribe to it 185

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24775-2:2021

FOREWORD

Storage Management Technical Specification, Part 2 Common Architecture, 1.8.0 Rev 4 defines the core architecture of SMI-S. This includes the protocols (WBEM, SLP,...); the model is defined in the other specification parts.

Parts of this Standard

This standard is subdivided in the following parts:

- *Storage Management Technical Specification, Part 1 Overview, 1.8.0 Rev 4*
- *Storage Management Technical Specification, Part 2 Common Architecture, 1.8.0 Rev 4*
- *Storage Management Technical Specification, Part 3 Common Profiles, 1.8.0 Rev 4*
- *Storage Management Technical Specification, Part 4 Block Devices, 1.8.0 Rev 4*
- *Storage Management Technical Specification, Part 5 Filesystems, 1.8.0 Rev 4*
- *Storage Management Technical Specification, Part 6 Fabric, 1.8.0 Rev 4*
- *Storage Management Technical Specification, Part 7 Host Elements, 1.8.0 Rev 4*
- *Storage Management Technical Specification, Part 8 Media Libraries, 1.8.0 Rev 4*

SNIA Web Site

Current SNIA practice is to make updates and other information available through their web site at http://www.snia.org

SNIA Address

Requests for interpretation, suggestions for improvement and addenda, or defect reports are welcome. They should be sent via the SNIA Feedback Portal at http://www.snia.org/feedback/ or by mail to the Storage Networking Industry Association, 4360 ArrowsWest Drive, Colorado Springs, Colorado 80907, U.S.A.

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24775-2:2021

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24775-2:2021

1 Scope

Storage Management Technical Specification, Part 2 Common Architecture, 1.8.0 Rev 4 defines the core architecture and protocols in SMI-S. The components of SMI-S architecture include:

- Transport - communicating management information between constituents of the management system
- Health and fault management - detecting failures through monitoring the state of storage components
- General information about the object model
- Names - how SMI-S uses names to allow applications to correlate across SMI-S and to other standards
- Standard messages - how exceptions are presented to client applications
- Service discovery - techniques clients use to discover SMI-S services
- Installation and upgrade - recommendations for implementations
- Compliance - requirement for compliance to the standard

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24775-2:2021

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24775-2:2021

2 Normative references

2.1 General

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

2.2 Approved references

ISO/IEC 14776-413, SCSI Architecture Model - 3 (SAM-3) [ANSI INCITS 402-200x]

ISO/IEC 14776-452, SCSI Primary Commands - 3 (SPC-3) [ANSI INCITS.351-2005]

ANSI/INCITS 374:2003, Information technology - Fibre Channel Single - Byte Command Set-3 (FC-SB-3)

ISO/IEC 20648, Information technology — TLS specification for storage systems

SNIA TLS Specification for Storage Systems
http://www.snia.org/https://www.snia.org/tech_activities/standards/curr_standards/tls

2.3 DMTF references (Final)

DMTF Final documents are accepted as standards. For DMTF Draft or Preliminary documents, see 2.5.

DMTF DSP0004, CIM Infrastructure Specification 3.0.1
http://www.dmtf.org/sites/default/files/standards/documents/DSP0004_3.0.1.pdf

DMTF DSP0200, CIM Operations over HTTP 1.4
http://www.dmtf.org/sites/default/files/standards/documents/DSP0200_1.4.pdf

DMTF DSP0201 Representation of CIM in XML 2.4
http://www.dmtf.org/sites/default/files/standards/documents/DSP0201_2.4.pdf

DMTF DSP0202 CIM Query Language Specification 1.0
http://www.dmtf.org/standards/published_documents/DSP0202_1.0.0.pdf

DMTF DSP0205 WBEM Discovery Using the Service Location Protocol 1.0.1
http://dmtf.org/sites/default/files/standards/documents/DSP0205_1.0.1.pdf

DMTF DSP0206 WBEM SLP Template 1.0
http://www.dmtf.org/sites/default/files/standards/documents/wbem.1.0.en

DMTF DSP0207, 1.0.1 WBEM URI Mapping Specification
http://www.dmtf.org/sites/default/files/standards/documents/DSP0207_1.0.1.pdf

DMTF DSP0210 CIM-RS Protocol 1.0
http://www.dmtf.org/sites/default/files/standards/documents/DSP0210_1.0.pdf

DMTF DSP0211 CIM-RS Payload Representation in JSON 1.0
http://www.dmtf.org/sites/default/files/standards/documents/DSP0211_1.0.pdf

DMTF DSP0221 Managed Object Format (MOF) 3.0.1
http://www.dmtf.org/sites/default/files/standards/documents/DSP0221_3.0.1.pdf

DMTF DSP0223 Generic Operations 2.0.0
http://www.dmtf.org/sites/default/files/standards/documents/DSP0223_2.0.0.pdf

DMTF DSP0226, WS-Management Protocol Specification 1.1.1
http://www.dmtf.org/sites/default/files/standards/documents/DSP0226_1.1.1.pdf

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24775-2:2021

DMTF DSP0227, WS-Management CIM Binding Specification 1.2
http://www.dmtf.org/sites/default/files/standards/documents/DSP0227_1.2.pdf

DMTF DSP0228, Message Registry Schema, 1.1.0
http://schemas.dmtf.org/wbem/messageregistry/1/dsp0228_1.1.0.xsd

DMTF DSP2011, Standard Messages Whitepaper 1.0
http://www.dmtf.org/sites/default/files/standards/documents/DSP2011.pdf

DMTF DSP0230, WS-CIM Mapping Specification 1.1.0
http://www.dmtf.org/sites/default/files/standards/documents/DSP0230_1.1.0.pdf

DMTF DSP8000 1.2.0 Message Registry Print XSLT Stylesheet
http://schemas.dmtf.org/wbem/messageregistry/1/dsp8000_1.2.0.xsl

DMTF DSP8016 2.0.0 WBEM Operations Message Registry
http://schemas.dmtf.org/wbem/messageregistry/1/dsp8016_2.0.0.xml

2.4 IETF references

For IETF Informational documents and proposed standards, see 2.5.

IETF RFC 2045, Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies
http://www.ietf.org/rfc/rfc2045.txt

IETF RFC 2246, The TLS Protocol Version 1.0
http://www.ietf.org/rfc/rfc2246.txt

IETF RFC 4291, IP Version 6 Addressing Architecture

IETF RFC 2396, Uniform Resource Identifiers (URI)
http://www.ietf.org/rfc/rfc2396.txt

IETF RFC 2608, Service Location Protocol, Version 2
http://www.ietf.org/rfc/rfc2608.txt

IETF RFC 2609, Service Templates and Service: Schemes
http://www.ietf.org/rfc/rfc2609.txt

IETF RFC 2610, DHCP Options for Service Location Protocol
http://www.ietf.org/rfc/rfc2610.txt

IETF RFC 2616, Hypertext Transfer Protocol -- HTTP/1.1
http://www.ietf.org/rfc/rfc2616.txt

IETF RFC 2617, HTTP Authentication: Basic ad Digest Access Authentication
http://www.ietf.org/rfc/rfc2617.txt

IETF RFC 2445, Internet Calendaring and Scheduling Core Object Specification (iCalendar)
http://www.ietf.org/rfc/rfc2445.txt

IETF RFC 3280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
http://www.ietf.org/rfc/rfc3280.txt

IETF RFC 3723, Securing Block Storage Protocols over IP
http://www.ietf.org/rfc/rfc3723.txt

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24775-2:2021

IETF RFC 3986, Definitions of Managed Objects for the DS3/E3 Interface Type
http://www.ietf.org/rfc/rfc3986.txt

IETF RFC 4291, IP Version 6 Addressing Architecture
http://www.ietf.org/rfc/rfc4291.txt

IIETF RFC 4514, Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names
http://www.ietf.org/rfc/rfc4514.txt

2.5 References under development

The following documents (and their web addresses) are subject to change.

DMTF DSP8055 1.0.0d Diagnostic Message Registry
http://www.dmtf.org/sites/default/files/standards/documents/DSP8055_1.0.0d.xml

2.6 Other references

IETF RFC 1945 Hypertext Transfer Protocol -- HTTP/1.0
http://www.ietf.org/rfc/rfc1945.txt

IETF RFC 2614 An API for Service Location
http://www.ietf.org/rfc/rfc2614.txt

UML (Universal Modeling Language) Specifications
http://www.omg.org/technology/documents/modeling_spec_catalog.htm#UML

ITU-T Recommendation X.509 (1997 E): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework

PKCS #12, Personal Information Exchange Syntax
http://www.rsasecurity.com/rsalabs/node.asp?id=2138

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24775-2:2021

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24775-2:2021

3 Terms, definitions, symbols, abbreviations, and conventions

3.1 Terms and definitions

3.1.1
access control
means to ensure authorized access and to prevent unauthorized access to resources relevant to information security based on the business and security requirements

3.1.2
account
an established relationship between a user and a computer, network or information service

3.1.3
accountability
Information Security property that establishes responsibility for the effects of action taken by individuals, organizations or communities with an explanation as to how and why the action took place.
[SOURCE: ISO/IEC 27000]

3.1.4
administrator
a person charged with the installation, configuration, and management of a computer system, network, storage subsystem, database, or application

3.1.5
agent
an Object Manager that includes the provider service for a limited set of resources

3.1.6
aggregation
a strong form of an association

3.1.7
audit Log
logs collecting the evidence of selected user activities, exceptions, and information security events

3.1.8
authentication
the act of verifying the identity claimed by a party to a communication

3.1.9
authentication mechanism
process for determining and validating a user (or device) identity

3.1.10
authorization
the process of granting a right or permission to access a system resource

3.1.11
bidirectional authentication
See "mutual authentication"

3.1.12
CIM Server
See "WBEM Server".

client
a process that issues requests for service

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24775-2:2021

3.1.13
Common Information Model
an object-oriented description of the entities and relationships in a business' management environment maintained by the Distributed Management Task Force

3.1.14
dedicated SMI-S Server
a WBEM Server that is dedicated to supporting a single device or subsystem

3.1.15
digested password
the hashed form of a cleartext password

3.1.16
discovery
a process which provides information about what physical and logical storage entities have been found within the management domain

3.1.17
Distributed Management Task Force (DMTF)
an industry organization that develops management standards for computer system and enterprise environments

3.1.18
dynamic host control protocol (DHCP)
an Internet protocol that allows nodes to dynamically acquire ("lease") network addresses for periods of time rather than having to pre-configure them

3.1.19
embedded SMI-S Server
a WBEM Server that is embedded in the device or subsystem for which it provides management

3.1.20
enclosure
a box or cabinet

3.1.21
entity authentication
corroboration that an entity is the one claimed.
[SOURCE: ISO/IEC 9798]

3.1.22
enumerate
an operation used to enumerate subclasses, subclass names, instances and instance names

3.1.23
event
an occurrence of a phenomenon of interest.

3.1.24
eXtensible Markup Language
a universal format for structured documents and data on the World Wide Web

3.1.25
extent
a set of consecutively addressed disk blocks.

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24775-2:2021

3.1.26
external authentication
authentication which relies on an authentication service separate from (or external to) an entity

3.1.27
extrinsic method
A method defined as part of CIM Schema

3.1.28
fabric
Any interconnect between two or more Fibre Channel N_Ports, including point-to-point, loop, and Switched Fabric.

3.1.29
FICON™[1]
Fibre Channel storage protocol used in IBM mainframe computers and peripheral devices such as ECKD storage arrays and tape drives

3.1.30
general purpose SMI-S Server
an SMI-S Server that is not dedicated to supporting a single device or subsystem, and may support multiple devices or subsystems.

3.1.31
grammar
a formal definition of the syntactic structure of a language (see "syntax"), normally given in terms of production rules that specify the order of constituents and their sub-constituents in a sentence (a well-formed string in the language)

3.1.32
host bus adapter (HBA)
card that contains ports for host systems

3.1.33
Hypertext Transfer Protocol (HTTP)
request-reply protocol used for internet communications

3.1.34
identity
representation of an actual user (or application or service or device)

3.1.35
interconnect element
non-terminal network elements (Switches, hubs, routers, directors).

3.1.36
interface definition language (IDL)
high-level declarative language that provides the syntax for interface declarations

3.1.37
intrinsic method
operations made against a WBEM server and a CIM namespace independent of the implementation of the schema defined in the server

---

1.FICON™ is an example of a suitable product available commercially. This information is given for the convenience of users of this standard and does not constitute an endorsement of this product by SNIA or any standards organization.

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24775-2:2021

3.1.38
logical unit number
a SCSI logical unit or logical unit number.

3.1.39
mutual authentication
authentication that provides both parties (users or entities) with assurance of each other's identity.

3.1.40
Network Address Authority (NAA)
a four bit identifier to denote a network address authority (i.e., an organization such as CCITT or IEEE that administers network addresses)

3.1.41
non-repudiation
the ability to prove an action or event has taken place, so that this event or action cannot be repudiated later
[SOURCE: ISO/IEC 27000]

3.1.42
out-of-band
transmission of management information for storage components outside of the data path, typically over Ethernet.

Also: use of mechanisms other than the ones required on a communications channel to transmit information.
[SOURCE: ISO/IEC 24767]

3.1.43
partition
collection of contiguous block on a disk or virtual disk

3.1.44
password
a secret sequence of characters or a word that a user submits to a system for purposes of authentication, validation, or verification.

3.1.45
path
combination of initiator and target ports and logical unit

3.1.46
privacy
the right of an entity (normally an individual or an organization), acting on its own behalf, to determine the degree to which the confidentiality of their private information is maintained.

3.1.47
privileged user
a user who, by virtue of function, and/or seniority, has been allocated powers within a system, which are significantly greater than those available to the majority of users

3.1.48
protocol
a set of rules that define and constrain data, operations, or both

3.1.49
proxy SMI-S Server
an SMI-S Server that does not run on the device or subsystem which it supports

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24775-2:2021

3.1.50
public key infrastructure (PKI)
a framework established to issue, maintain, and revoke public key certificates accommodating a variety of security technologies.

3.1.51
SAN
a group of fabrics that have common leaf elements.

3.1.52
SCSI Parallel Interface (SPI)
The family of SCSI standards that define the characteristics of the parallel version of the SCSI interface.

3.1.53
Secure Sockets Layer (SSL)
A suite of cryptographic algorithms, protocols and procedures used to provide security for communications used to access the world wide web.

Note 1 to entry: More recent versions of SSL are known as TLS (Transport Level Security) and are standardized by the Internet Engineering Task Force (IETF).

3.1.54
Service Access Point
the network address of a process offering a service.

3.1.55
shared secret
a pre-shared key that has been allocated to communicating parties prior to the communication process starting.

3.1.56
Simple Network Management Protocol (SNMP)
an IETF protocol for monitoring and managing systems and devices in a network

3.1.57
SMI-S server
a WBEM Server that supports SMI-S (*Storage Management Initiative Specification)* profiles for management of a device or subsystem

3.1.58
SNMP trap
a type of SNMP message used to signal that an event has occurred

3.1.59
soft zone
a zone consisting of zone Members that are made visible to each other through Client Service requests

3.1.60
Storage Management Initiative Specification (SMI-S)
an interface between WBEM-capable clients and servers for the secure, extensible, and interoperable management of networked storage (this standard)

3.1.61
Storage Networking Industry Association (SNIA)
an association of producers and consumers of storage networking products whose goal is to further storage networking technology and applications

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24775-2:2021

3.1.62
storage resource management (SRM)
management of physical and logical storage resources, including storage elements, storage devices, appliances, virtual devices, disk volume and file resources

3.1.63
switch
fibre channel interconnect element that supports a mesh topology

3.1.64
switched fabric
a fabric comprised of one or more Switches

3.1.65
syntax
the structure of strings in some language. A language's syntax is described by a grammar

3.1.66
threat
a potential source of an incident that may result in adverse changes to an asset, a group of assets or an organization
[SOURCE: ISO/IEC 27000]

3.1.67
unidirectional authentication
authentication that provides one party (user or entity) with assurance of the other's identity

3.1.68
User Datagram Protocol
an Internet protocol that provides connectionless datagram delivery service to applications

3.1.69
vulnerability
weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat
[SOURCE: ISO/IEC 27000]

3.1.70
Web Based Enterprise Management (WBEM)
a set of management and Internet standard technologies from DMTF developed to unify the management of distributed computing environments

3.1.71
WBEM Server
a server that provides support for CIM requests and provides CIM responses using web protocols

3.1.72
web service
a software system designed to support interoperable machine-to-machine interaction over a network

3.1.73
zone
a group of ports and switches that allow access. Defined by a zone definition

3.1.74
zone set
one or more zones that may be activated or deactivated as a group

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24775-2:2021

3.2 Acronyms and abbreviations

AAA	Authentication, Authorization, and Accounting
ACL	Access Control List
API	application programming interface
CA	Certificate Authority
CIM	Common Information Model
CRL	Certificate Revocation List
DHCP	dynamic host control protocol
FC	Fibre Channel
HBA	host bus adapter
HMAC	keyed-Hash Message Authentication Code
HTTPS	Hypertext Transfer Protocol Secure
IDL	interface definition language
IETF	Internet Engineering Task Force
IMA	iSCSI Management API
IP	Internet Protocol
IPsec	Internet Protocol Security
iSCSI	Internet SCSI
LDAP	Lightweight Directory Access Protocol
MAC	Message Authentication Code
OS	operating system
PKI	Public Key Infrastructure
RADIUS	Remote Authentication Dial In User Service
RBAC	Role-base Access Control
RFC	Request for Comments
SAM-3	SCSI Architecture Model
SAN	storage area network
SB	Single Byte (command set)
SCSI	Small Computer System Interface
SES	SCSI Enclosure Services
SLP	Service Location Protocol
SMI-S	Storage Management Initiative - Specification
SNIA	Storage Networking Industry Association
SPC-3	SCSI Primary Commands-3
SSL	Secure Socket Layer
SSO	Single Sign-on
SSP	Storage Service Provider
TC	Technical Committee
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
URL	Uniform Resource Locator
WBEM	Web-Based Enterprise Management
XML	Extensible Markup Language

3.3 Keywords

expected
a keyword used to describe the behavior of the hardware or software in the design models presumed by this standard

Other hardware and software design models may also be implemented.

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24775-2:2021

3.3.1
invalid
a keyword used to describe an illegal or unsupported bit, byte, word, field or code value

Note 1 to entry: Receipt of an invalid bit, byte, word, field or code value shall be reported as an error.

3.3.2
mandatory
a keyword indicating an item that is required to be implemented as defined in this standard to claim compliance with this standard.

3.3.3
may
a keyword that indicates flexibility of choice with no implied preference

3.3.4
may not
keywords that indicates flexibility of choice with no implied preference

3.3.5
obsolete
a keyword indicating that an item was defined in prior standards but has been removed from this standard

3.3.6
opaque
a keyword indicating that value has no semantics or internal structure

3.3.7
optional
a keyword that describes features that are not required to be implemented by this standard

Note 1 to entry: However, if any optional feature defined by this standard is implemented, it shall be implemented as defined in this standard.

3.3.8
reserved
a keyword referring to bits, bytes, words, fields and code values that are set aside for future standardization

Note 1 to entry: Their use and interpretation may be specified by future extensions to this or other standards.

Note 2 to entry: A reserved bit, byte, word or field shall be set to zero, or in accordance with a future extension to this standard. Recipients are not required to check reserved bits, bytes, words or fields for zero values.

Note 3 to entry: Receipt of reserved code values in defined fields shall be reported as an error.

3.3.9
shall
a keyword indicating a mandatory requirement
Designers are required to implement all such requirements to ensure interoperability with other products that conform to this standard.

3.3.10
should
a keyword indicating flexibility of choice with a preferred alternative; equivalent to the phrase “it is recommended”

3.4 Conventions

Certain words and terms used in this American National Standard have a specific meaning beyond the normal English meaning. These words and terms are defined either in 3 Terms, definitions, symbols, abbreviations, and conventions or in the text where they first appear.

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24775-2:2021

Numbers that are not immediately followed by lower-case b or h are decimal values.

Numbers immediately followed by lower-case b (xxb) are binary values.

Numbers immediately followed by lower-case h (xxh) are hexadecimal values.

Hexadecimal digits that are alphabetic characters are upper case (i.e., ABCDEF, not abcdef).

Hexadecimal numbers may be separated into groups of four digits by spaces. If the number is not a multiple of four digits, the first group may have fewer than four digits (e.g., AB CDEF 1234 5678h)

Decimal fractions are initiated with a comma (e.g., two and one half is represented as 2,5).

Decimal numbers having a value exceeding 999 are separated with a space(s) (e.g., 24 255).

See also " Typographical Conventions "(in front matter) for typographical conventions.

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24775-2:2021

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24775-2:2021

4 Transport and Reference Model

4.1 Introduction

4.1.1 Overview

The interoperable management of storage devices and network elements in a distributed storage network requires a common transport for communicating management information between constituents of the management system. This section of the specification details the design of this transport, as well as the roles and responsibilities of constituents that use the common transport (i.e., a reference model).

4.1.2 Language Requirements

To express management information across the interface, a language is needed that:

- Can contain platform independent data structures,
- Is self describing and easy to debug,
- Can be extended easily for future needs.

4.1.3 Communications Requirements

Communications protocols to carry the XML based management information are needed that:

- Can take advantage of the existing ubiquitous IP protocol infrastructures,
- Can be made to traverse inter- and intra-organizational firewalls,
- Can easily be embedded in low cost devices.

The Hyper Text Transport Protocol (HTTP) was chosen for the messaging protocol and TCP was chosen for the base transfer protocol to carry the XML management information for this interface as they meet the requirements in 4.1.3.

4.1.4 XML Message Syntax and Semantics

In order to be successful, the expression of XML management information (messages) across this interface needs to follow consistent rules for semantics and syntax. These rules are detailed in this specification. They are of sufficient quality, extensibility, and completeness to allow their wide adoption by storage vendors and management software vendors in the industry. In addition, to facilitate rapid adoption, existing software that can parse, marshal, un-marshal, and interpret these XML messages should be widely available in the market such that vendor implementations of the interface are accelerated. The message syntax and semantics selected should:

- Be available on multiple platforms,
- Have software implementations that are Open source (i.e., collaborative code base),
- Have software implementations available in Java and C++,
- Leverage industry standards where applicable,
- Conform with W3C standards for XML use.
- Be object model independent (i.e., be able to express any object model).

Virtually the only existing industry standard in this area is the WBEM standards as developed and maintained by the DMTF.

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24775-2:2021

4.2 Transport Stack

It is the primary objective of this interface to drive seamless interoperability across vendors as communications technology and the object model underlying this interface evolves. Accordingly, the transport stack has been layered such that (if required) other protocols can be added as technology evolves. For example, should SOAP or IIOP become prominent, the content in the stack could be expanded with minimal changes to existing product implementations in the market.This specification relies on the DMTF WBEM Protocol Specifications.

To be compliant with this specification, CIM-XML shall be supported.

Optionally, other WBEM protocols, such as WS-Management or CIM-RS, may additionally be supported.

It should be noted that this specification places no restriction on the physical network selected to carry this transport stack. For example, a vendor can choose to use in-band communication over Fibre-channel as the backbone for this interface. Another vendor could exclusively (and wisely) choose out-of-band communication over Ethernet to implement this management interface. Additionally, select vendors could choose a mix of in-band and out-of-band physical network to carry this transport stack.

4.3 Reference Model

4.3.1 Overview

As shown in Figure 7, the Reference Model shows all possible constituents of the management environment in the presence of the transport stack for this interface.

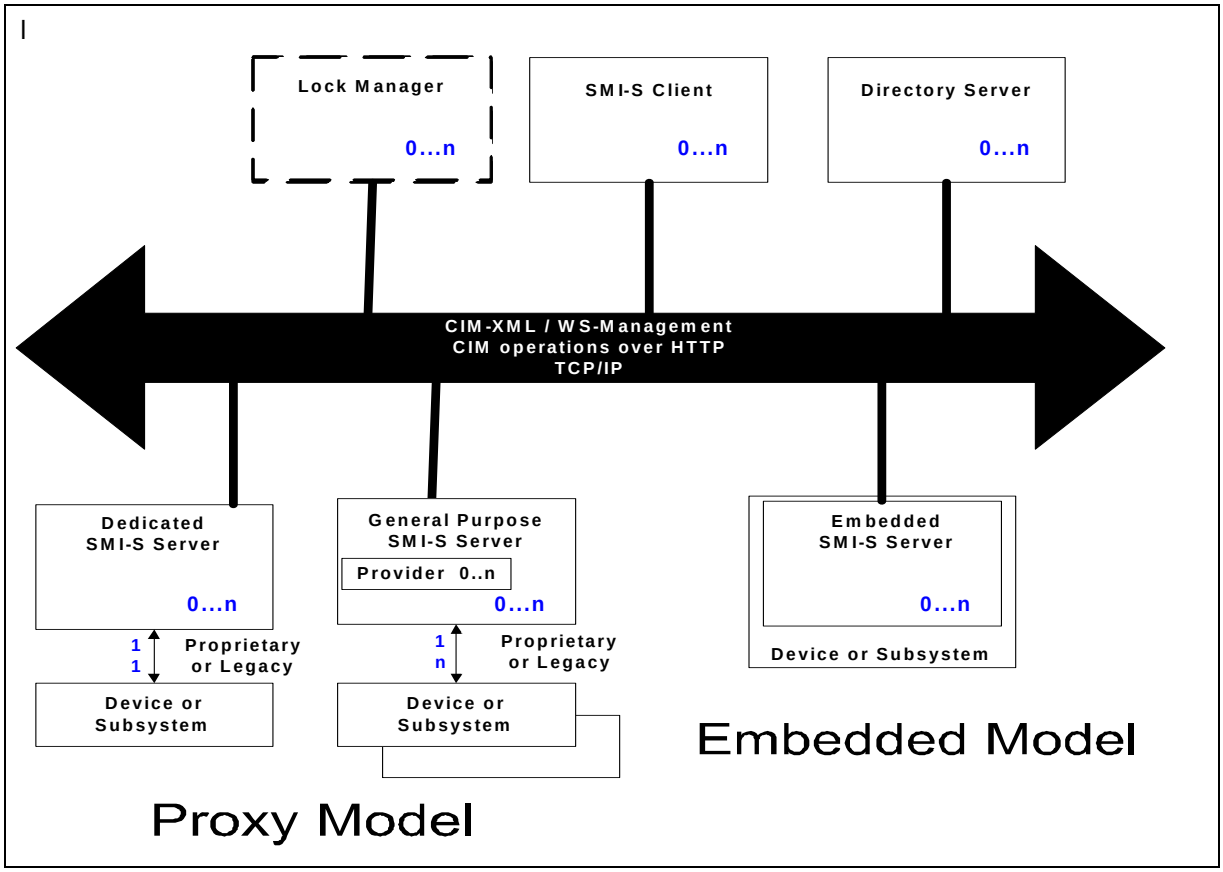

Figure 7 -Reference Model.

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24775-2:2021

Client

Figure 7 illustrates that the transport for this interface uses a WBEM Protocol to execute intrinsic and extrinsic methods against the schema for this interface.

NOTE It is envisioned that a more complete version of this reference model would include a Lock Manager. However, in this version of SMI-S, a Lock Manager is not specified. As a result, it is shown as a dotted box to illustrate where the role would fit.

4.3.2 Roles for Interface Constituents

4.3.2.1 Client

A Client is the consumer of the management information in the environment. It provides an API (language binding in Java or C++ for example) for overlying management applications (like backup engines, graphical presentation frameworks, and volume managers) to use.

4.3.2.2 SMI-S Server

An SMI-S Server is a WBEM Server. Often, an SMI-S Server controls only one device or subsystem, and is incapable of providing support for complex intrinsic methods like schema traversal. An SMI-S Server can be embedded in a device (like a Fibre Channel Switch) or provide a proxy on a host that communicates to a device over a legacy or proprietary interconnect (like a SCSI based array controller).

Embedding an SMI-S Server directly in a device or subsystem reduces the management overhead seen by a customer and eliminates the requirement for a stand-alone host (running the proxy agent) to support the device.

Embedded SMI-S Servers are the desired implementation for “plug and play” support in an SMI-S managed environment. However, proxy SMI-S Servers are a practical concession to the legacy devices that are already deployed in storage networked environments. In either case, the minimum CIM support for SMI-S Servers applies to either SMI-S Server deployments.

4.3.2.3 General Purpose SMI-S Server

A General Purpose SMI-S Server serves management information from one or more devices or underlying subsystems through providers. As such a General Purpose SMI-S Server is an aggregator that enables proxy access to devices/subsystems and can perform more complex operations like schema traversals. A General Purpose SMI-S Server typically includes a standard provider interface to which device vendors adapt legacy or proprietary product implementations.

4.3.2.4 Provider

A provider expresses management information for a given resource such as a storage device or subsystem exclusively to a WBEM Server. The resource may be local to the host that runs the Object Manager or may be remotely accessed through a distributed systems interconnect.

4.3.2.5 Lock Manager

This version of the specification does not support a lock manager.

4.3.2.6 Directory Server (SLP Directory Agent)

A directory server provides a common service for use by clients for locating services in the management environment.

4.3.3 Cascaded Agents

This specification discusses constituents in the SMI-S environment in the context of Clients and Servers. This version of the specification also allows constituents in a SMI-S management environment to function as both client and server.

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24775-2:2021

Directory Server (SLP Directory Agent)

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24775-2:2021

5 Health and Fault Management

5.1 Objectives

Health and Fault Management is the activity of anticipating or detecting failures through monitoring the state of the storage network and its components and intervening before services can be interrupted. A service in this case is the realization of storage through several interconnected devices connected, configured for a dedicated purpose. The purpose is the delivery of software application functionality in support of some business function.

5.2 Overview

- Express states and statuses with standard meanings.
- Define the use of comprehensive error reporting in determining the type, category, and source of failures.
- Define the quality associated with errors rather than qualities.
- Define explicit failure scopes rather than requiring HFM enabled application to construct them.

5.3 Terms

5.3.1 error

An unexpected condition, result, signal or datum. An error is usually caused by an underlying problem in the system such as a hardware fault or software defect. Errors can be classified as correctable (recoverable) or uncorrectable, detectable or undetectable.

5.3.2 fault

A problem that occurs when something is broken and therefore not functioning in the manner it was intended to function. A fault may cause an error to occur.

5.3.3 fault region

Many devices or applications can attempt to fix themselves upon encountering some adverse condition. The set of components which the device or application can attempt to fix is called the Fault Region. The set may include part or all of other devices or applications. Having the Fault Regions declared helps a HFM application, acting as a doctor, to do no harm by attempting to interfere and thereby adversely affect the corrective action being attempted.

5.3.4 Health and Fault Management (HFM)

Health and Fault Management is the activity of anticipating or detecting debilitating failures through monitoring the state of the storage network and its components and intervening in before services can be interrupted. A service in this case is the realization of storage utilization through several interconnected devices connected, configured for a dedicated purpose. The purpose is the delivery of software application functionality in support of some business function.

5.3.5 operational status

These values indicate the current status(es) of the element. Various operational statuses are defined (e.g., OK, starting, stopping, stopped, In Service, No Contact).

5.3.6 health state

These values indicate the current health of the element. This attribute expresses the health of this element but not necessarily that of its subcomponents.

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24775-2:2021

5.4 Description of Health and Fault Management

The goal of effective administration requires devices and applications that comprise storage services to report their status and the nature of their errors in standard terms. These terms need to be understandable by a client without device-specific knowledge.

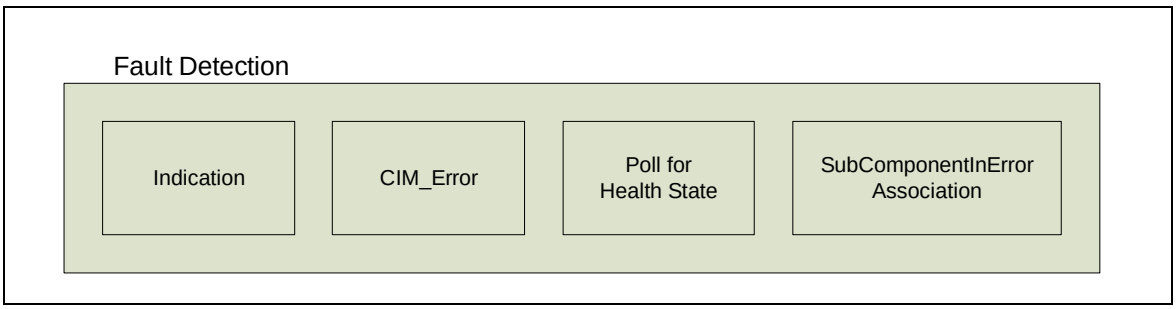

Figure 8 - Basic Fault Detection

There are four basic ways for a SMI-S client to detect an error or fault condition. Figure 8 lists the four basic methods for fault detection. These are:

- Health state and Operational status - Polling.
- Error - Standard errors returned from CIM operations.
- Indications - Subscribe for and receive asynchronous Indications.
- Fault Regions (experimental) - Walk the CIM model looking for RelatedElementCausingError associations.

5.4.1 Operational Status and Health State (Polling)

Operational Status and Health State are the two properties that will be used to monitor health. These two properties could convey very different statuses and may at times be related or independent of each other. For example, you may have a disk drive with the Operational Status of “Stopped” and the HealthState of 30 (Non-recoverable error) or 5 (OK). Now the reason the disk drive is stopped could vary from the fact that it had a head crash (HealthState = 30) to the situation where it was stopped for the routine maintenance (HealthState = 5).

Table 1 is an example of how HealthState can disambiguate health for a disk drive, various values for OperationalStatus and HealthState:

Table 1 shows, for a disk drive, various possible values for OperationalStatus and HealthState. Note that there are many cases not shown.:

Table 1 - OperationalStatus for Disk Drive

Operational Status	Description	HealthState	Description	Comment
2	OK	5	OK	Everything is fine
2	OK	10	Degraded/Warning	Some soft errors
3 or 5	Degraded or Predicted Failure	15	Minor Failure	Many soft errors
3 or 5	Degraded or Predicted Failure	20	Major Failure	Some hard errors
3	Degraded	10	Good	A subcomponent has failed (no data loss)

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24775-2:2021

Table 1 - OperationalStatus for Disk Drive (Continued)

Operational Status	Description	HealthState	Description	Comment
10	Stopped	5	OK	Drive spun down normally
10	Stopped	30	Non-recoverable Error	Head crash
8	Starting	10	Degraded/Warning	Will update HealthState once fully started
4	Stressed	5	OK	Too many I/O in progress, but the drive is fine.
15	Dormant	5	OK	The drive is not needed currently

The property OperationalStatus is multi-valued and more dynamic. It tends to emphasize the current status and potentially the immediate status leading to the current status; whereas, the property HealthState is less dynamic and tends to imply the health over a longer period of time. Again, in the disk drive example, the disk drive's operational status may change many times in a given time period. However, in the same time period, the health of the same drive may not change at all.

5.4.2 Standard Errors and Events

Standardization of error and events are required so that the meaning is unambiguous and is given to comparisons.

Error and Alert indications

HFM clients shall not be required to be embodied with specific knowledge of the devices and applications in order to derive the quality of the error from the datum. The device and application shall express the quality of the error rather than the quantity interpreted with *a priori* knowledge to determine that error condition is present. For example, a device needs to express that it is too hot rather than requiring the HFM enabled application to determine this from the temperature datum and device specific knowledge of acceptable operating conditions.

Standard errors are defined for each Profile. The definitions will be contained in the profiles. Standard errors are not the only error codes that can be returned, but are the only codes that a generic client will understand.

5.4.3 Indications

Indications are asynchronous messages from WBEM Servers to clients. A client must register for them. Each SMI-S profile contains lists of indication filters that clients use to indicate the information it is interested in. The message itself is defined in the SMI-S Indications Profile (in *Storage Management Technical Specification, Part 3 Common Profiles, 1.8.0 Rev 4*).

EXPERIMENTAL

5.4.4 Event Correlation and Fault Containment

Automation will require that an error arising through control and configuration activities, as a side effect of them, or by failures caused by defects can be directly correlatable. Error categories like network cabling failures or network transmission errors will help organize the types of error that can be produced. Standard errors, like impending disk media failure, will be required as well.

Once the errors have been collected and correlated, the HFM enabled application can produce an impact list sorted by likelihood. Some of the error correlation can be determined by the common affect through

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24775-2:2021

the manifestation of the RelatedElementCausingError association to be described later. The alerts themselves can report its correlation with other alerts.

Potential faults can then be derived from errors for each component. Deriving such a list may require a dialog between the HFM enabled application and the device or application in question such that the HFM enabled application is assisted in the production of the list.

If permitted, then control and configuration operations may be executed to contain the fault. The pallet of these operations will be those operations already available through SMI-S. However, special operations may arise from the HFM design work as well. Fault containment will include the reconfiguration of the storage service with alternative components, leaving failing components or interconnections isolated.

Much like a physician, the HFM enabled application is notified or consulted when symptoms appear. The HFM enabled application then develops a prognosis based on the manifestation of the ailment. At times, the HFM enabled application will perform diagnostic procedures. The end result of the process is to produce a list of possible causes, ranked by probability, and associated recommended procedures.

Also like a doctor, the HFM enabled application will settle for enabling the patients to heal themselves. That is the HFM enabled applications cannot be expected to heal the device in all cases. A significant portion of all possible corrective actions will require the intervention of people or device unique knowledge.

The simplified state diagram shown in Figure 9 follows the fault mitigation life cycle for HFM.

The device or application manifests an event, either by a state change, error returned from a WBEM operation, or an alert indication.

The event is recognized by the HFM enabled application and accessed by the HFM enabled application. It may be that the event indication does the represent the existence of an error. An error condition may be heralded by a single or multiple events occurring in some order. The process of examining and characterizing event as errors is called error handling.

Once it is determined that an error condition is present, then possible causes are sought and ranked by likelihood. The causes themselves describe a potential problem or fault with the component in question. Alternatively, the device or application may report the fault directly, through an alert indication, optionally with recommended actions.

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24775-2:2021

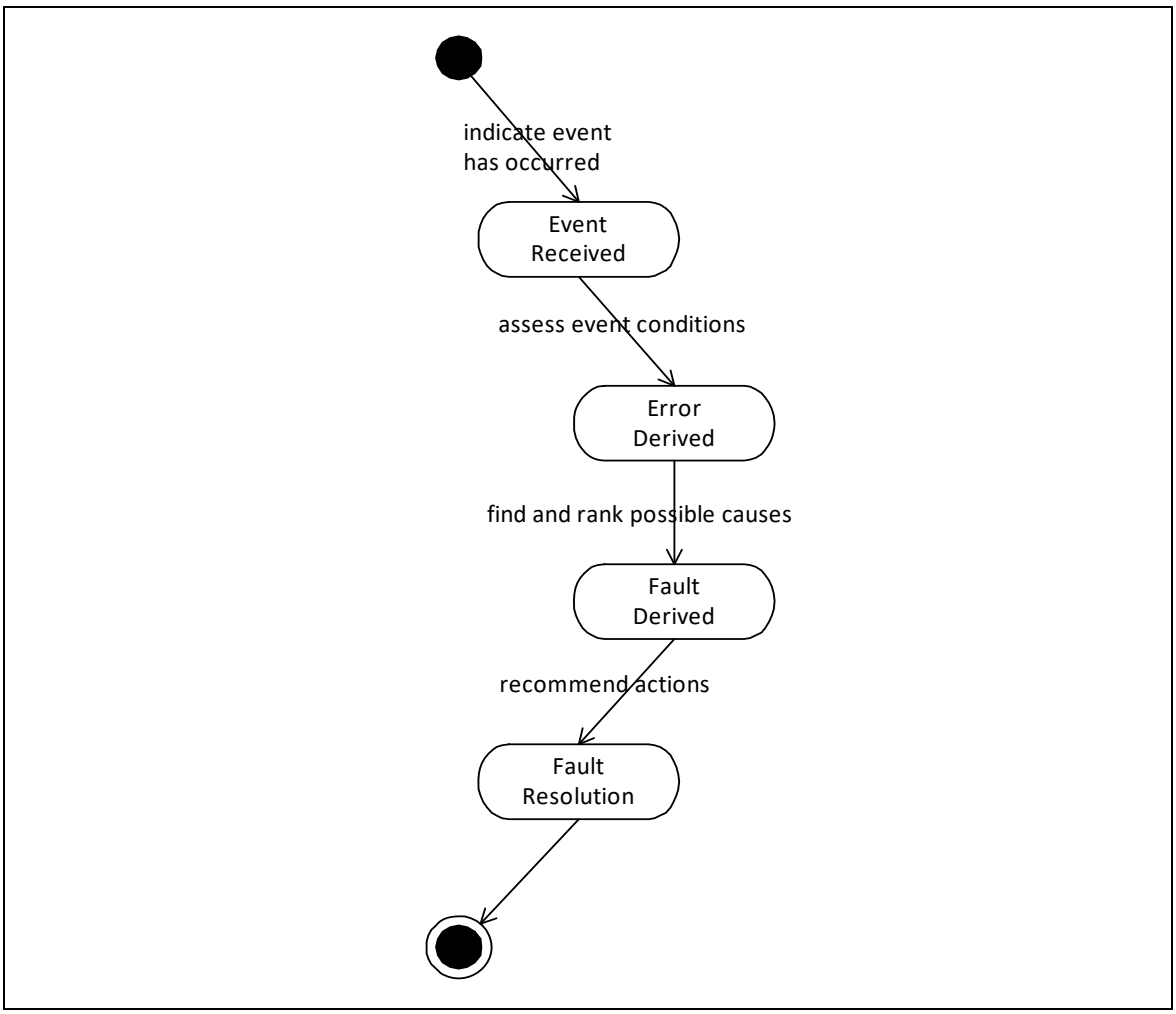

Figure 9 - Health Lifecycle

Fault resolution may not require the intervention of an operator or field technician. It is these faults that can be handled entirely by the HFM enabled application. Otherwise, the HFM enabled application cannot actively participate in whole fault resolution life cycle. In this case, the HFM enabled application would wait for the end state of fault resolution to come to being before ending its fault mitigation exercise.

Faults are contained and components repaired or replaced. The instructions to the HFM enabled application for what can be done to repair the fault are the recommended actions. Fault Containment includes fencing off the faulty component and maintaining the service. To be minimally effective, the HFM enabled application contains the fault. The repair may or may not be done with human intervention.

The devices and application that comprise a storage system have themselves some level of self diagnostics and report functionality.

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24775-2:2021

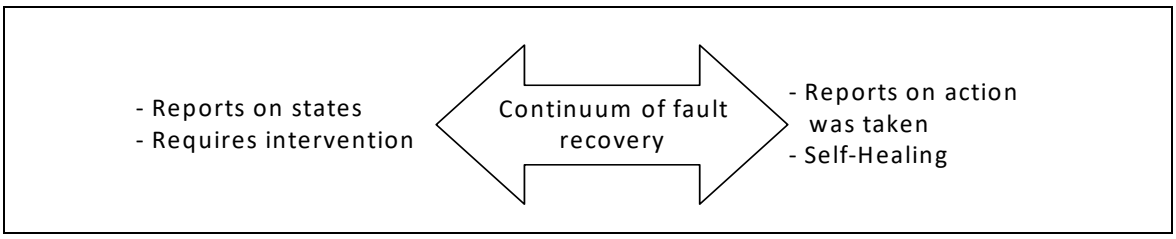

Figure 10 - Continuum

There is a range of ability of devices and applications to recover from failures and to report on the error recovery actions taken. See Figure 10. The variance of capabilities for device and applications can be plotted on a continuum. At one end of continuum, the device or application recognizes a fault condition and takes action, reporting on the action taken and any further action required to service it. At the other end of the continuum, the device can only report on that states and requires intervention both in the detection of fault conditions and taking corrective action.

There are limits to what an HFM enabled application can do. Obviously, if the device or application cannot report states, errors and alerts in a standard way or cannot report this data at all, then there is little an external implementation can do.

However, few, if any, of these devices and applications can monitor and correct the service as a whole. It is for this reason, the HFM implementation is needed to augment the effectiveness of the administrator.

5.4.5 Fault Regions

A scope can be applied to the effect of errors and the associated fault. A fault may affect a component, a device or application, storage service, or all the above. This scope defines the area of influence for fault containment. For example, the device itself may monitor its components and perform fault mitigation on its own. The plot of components whose errors are handled by a given fault mitigation entity is the fault region. The scope of effect of this fault region shall be defined.

Figure 11 illustrates the scope of fault regions in a simplified SAN example and how they may be recursive in nature. AN HFM application has the widest scope of concern in this example.

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24775-2:2021