

BS ISO/IEC 24775-2:2014



BSI Standards Publication

Information technology – Storage management

Part 2: Common architecture

bsi.

...making excellence a habit.
AVA Documents™
Document Sharing Hub

National foreword

This British Standard is the UK implementation of ISO/IEC 24775-2:2014.

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 secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2014. Published by BSI Standards Limited 2014

ISBN 978 0 580 84209 2

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 November 2014.

Amendments issued since publication

Date	Text affected
------	---------------



ISO/IEC 24775-2

Edition 1.0 2014-10

INTERNATIONAL STANDARD



**Information technology – Storage management –
Part 2: Common architecture**





THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2014 ISO/IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about ISO/IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

IEC Central Office
3, rue de Varembe
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue

The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub

The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,...). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in 14 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary

More than 55 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.



ISO/IEC 24775-2

Edition 1.0 2014-10

INTERNATIONAL STANDARD



**Information technology – Storage management –
Part 2: Common architecture**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

PRICE CODE

H

ICS 35.200

ISBN 978-2-8322-1893-8

Warning! Make sure that you obtained this publication from an authorized distributor.

AVA Documents
Document Sharing Hub

FOREWORD.....	15
Introduction	17
1 Scope	19
2 Normative references	20
3 Terms, definitions, symbols, abbreviations, and conventions	22
3.1 Terms and definitions	22
3.2 Acronyms and abbreviations	29
3.3 Keywords	30
3.4 Conventions	31
4 Typographical Conventions.....	32
4.1 Maturity Model	32
4.2 Experimental Maturity Level	32
4.3 Implemented Maturity Level	32
4.4 Stable Maturity Level	33
4.5 Finalized Maturity Level	33
4.6 Deprecated Material	33
5 Transport and reference model	35
5.1 Introduction to transport and reference model	35
5.1.1 Overview	35
5.1.2 Language requirements	35
5.1.3 Communications requirements	35
5.1.4 XML Message Syntax and Semantics	35
5.2 Transport Stack	35
5.3 Reference model	37
5.3.1 Overview	37
5.3.2 Roles for Interface Constituents	37
5.3.3 Cascaded Agents	38
6 Health and Fault Management	39
6.1 Objectives	39
6.2 Overview	39
6.3 General concepts	39
6.4 Description of Health and Fault Management	40
6.4.1 General	40
6.4.2 Operational Status and Health State (Polling)	40
6.4.3 Standard Errors and Events	41
6.4.4 Error and Alert indications	41
6.4.5 Indications	41

6.4.6	Event Correlation and Fault Containment	41
6.4.7	Fault regions	44
6.4.8	Examples	46
7	Object Model General Information.....	50
7.1	Model overview (Key resources)	50
7.1.1	Overview	50
7.1.2	Introduction to CIM UML notation	50
7.2	Techniques	51
7.2.1	CIM fundamentals	51
7.2.2	Modeling profiles	53
7.2.3	CIM Naming	53
8	Correlatable and durable names	54
8.1	Overview	54
8.2	Guidelines for SCSI Logical Unit Names	55
8.3	Guidelines for FC-SB-2 device names	55
8.4	Guidelines for port names	56
8.5	Guidelines for storage system names	56
8.6	Standard formats for correlatable names	57
8.6.1	General	57
8.6.2	Standard formats for Logical Unit names	57
8.6.3	Standard formats for port names	59
8.6.4	Standard formats for fabric names	59
8.6.5	Standard formats for storage system names	59
8.6.6	Operating system device names	61
8.6.7	Case sensitivity	63
8.7	Testing equality of correlatable names	63
8.8	iSCSI names	63
9	Standard Messages.....	65
9.1	Overview	65
9.2	Required characteristics of Standard Messages	65
9.2.1	Declaring and producing Standard Messages	65
9.3	Message registry	67
9.3.1	Common Element Messages	67
9.3.2	Common Protocol Messages	77
9.3.3	Storage Messages	87
9.3.4	Fabric Messages	101
9.3.5	Host Messages	106
9.3.6	Media Library Messages	108

10	Service discovery	133
10.1	Objectives	133
10.2	Overview	133
10.3	SLP Messages	135
10.4	Scopes	136
10.5	Services Definition	137
10.5.1	General	137
10.5.2	Service Type	137
10.5.3	Service Attributes	137
10.6	User Agents (UA)	139
10.7	Service Agents (SAs)	140
10.8	Directory Agents (DAs)	140
10.9	Service Agent Server (SA Server)	140
10.9.1	General Information	140
10.9.2	SA Server (SAS) Implementation	141
10.9.3	SA Server (SAS) Clients	141
10.9.4	SA Server Configuration	142
10.9.5	SA Server Discovery	143
10.9.6	SAS Client Registration	143
10.10	Configurations	144
10.10.1	General	144
10.10.2	Multicast Configurations	144
10.10.3	No Multicast configuration	144
10.10.4	Multicast Islands	145
10.11	'Standard WBEM' Service Type Templates	146
11	Information Technology – Storage Management roles	150
11.1	Introduction to storage management roles	150
11.2	Information Technology – Storage Management Client	151
11.2.1	Overview	151
11.2.2	SLP functions	151
11.2.3	WBEM protocol functions	151
11.2.4	Security considerations	151
11.2.5	Lock management functions	151
11.3	Dedicated Information Technology – Storage Management Server	151
11.3.1	Overview	151
11.3.2	SLP functions	152
11.3.3	WBEM protocol functions	152
11.3.4	Security considerations	153
11.3.5	Lock management functions	153

11.4	General Purpose Information Technology – Storage Management Server	153
11.4.1	Overview	153
11.4.2	SLP functions	153
11.4.3	CIM-XML protocol functions	154
11.4.4	Lock management functions	154
11.4.5	Provider Subrole	154
11.5	Directory Server	154
11.5.1	General	154
11.5.2	SLP functions	154
11.5.3	CIM-XML protocol functions	155
11.5.4	Security considerations	155
11.5.5	Lock management functions	155
11.6	Combined roles on a single system	155
11.6.1	Overview	155
11.6.2	General Purpose Information Technology – Storage Management Server as a Profile Aggregator	155
12	Installation and upgrade	156
12.1	Overview	156
12.2	Role of the administrator	156
12.3	Goals	156
12.3.1	Non-disruptive installation and De-installation	156
12.3.2	Plug-and-Play	156
12.4	Server deployment	157
12.4.1	General	157
12.4.2	Controlled environment	157
12.4.3	Multiple CIMOM systems	157
12.4.4	Shared CIMOM	158
12.4.5	Uninstallation	159
12.4.6	Update	159
12.4.7	Reconfiguration	159
12.5	WBEM service support and related functions	159
12.5.1	Installation	159
12.5.2	Multiple CIM Servers on a Single Server System	160
12.5.3	Uninstallation/Upgrade	160
12.5.4	Reconfiguration	160
12.5.5	Failure	160
12.6	Client	160
12.6.1	Uninstallation	160
12.6.2	Reconfiguration	160
12.7	Directory Service	160

12.7.1 Installation	160
12.7.2 Uninstallation/Failure	161
12.8 Issues with Discovery mechanisms	161
13 Security.....	162
13.1 Objectives	162
13.2 Overview	162
13.2.1 General	162
13.2.2 General requirements for HTTP implementations	163
13.3 Description of SMI-S Security	164
13.3.1 General	164
13.3.2 Transport security	164
13.3.3 SSL 3.0 and TLS	165
13.3.4 Authentication	169
13.3.5 Indications	170
13.3.6 Service Discovery	171
13.3.7 HTTP Realms	172
13.4 Security Guidance	173
13.4.1 SSL 3.0 and TLS guidance	173
13.4.2 Authentication guidance	174
13.4.3 Authorization	178
13.4.4 Using IT Infrastructure Securely – Service Discovery	180
Annex A (informative) Mapping CIM objects to SNMP MIB structures	181
A.1 Purpose of this annex.....	181
A.2 CIM-to-MIB mapping overview	181
A.3 The SML MIB	181
Annex B (normative) Compliance with SMI-S.....	183
B.1 Compliance statement	183
B.2 How compliance of the architecture is declared.....	183
B.3 How compliance of the model is declared.....	183
B.4 The Server Profile and compliance	183
B.4.1 General	183
B.4.2 Example	183
B.5 Backward compatibility	184
B.5.1 General	184
B.5.2 Overview	185
B.5.3 Requirements	186
B.5.4 Implementation considerations.....	187
B.6 Rules for combining (autonomous) profiles.....	187
B.6.1 General	187

B.6.2	Backward Compatibility Rules for combining profiles	187
B.6.3	Conditions for a new profile	188
B.7	Rules for vendor extensions	188
B.7.1	General	188
B.7.2	Objectives for vendor extension rules.....	188
B.7.3	Vendor extensions and compliance rules.....	189
B.7.4	Vendor extensions and backward compatibility rules	189
B.7.5	Vendor extensions and SMI-S Nullification	190
B.7.6	Vendor Extensions that Avoid Client Confusion	190
Annex C (normative)	Indication filter strings	192
C.1	Overview.....	192
C.2	Instance creation.....	192
C.2.1	Filter string.....	192
C.2.2	Semantics	192
C.3	Instance deletion	192
C.3.1	Filter string.....	192
C.3.2	Semantics	192
C.4	Modification of any value in an array property	192
C.4.1	WQL string	192
C.4.2	CQL string.....	193
C.4.3	Semantics	193
C.5	Modification to either of two specific values in an array property.....	193
C.5.1	WQL string	193
C.5.2	CQL string.....	193
C.5.3	Semantics	193
C.6	Alert.....	193
C.6.1	Filter string.....	193
C.6.2	Semantic.....	193
Bibliography		194

Figure 1 – Experimental Maturity Level Tag	32
Figure 2 – Implemented Maturity Level Tag	33
Figure 3 – Stable Maturity Level Tag	33
Figure 4 – Deprecated Tag	34
Figure 5 – Transport Stack.....	36
Figure 6 – Reference Model.....	37
Figure 7 – Basic Fault Detection	40
Figure 8 – Health lifecycle.....	43
Figure 9 – Continuum	44
Figure 10 – Application Fault Region.....	45
Figure 11 – Array Instance.....	46
Figure 12 – Switch Example.....	48
Figure 13 – Lines that Connect Classes	50
Figure 14 – iSCSI Qualified Names (iqn) examples.....	64
Figure 15 – iSCSI EUI Name example	64
Figure 16 – iSCSI 64-bit NAA Name example	64
Figure 17 – iSCSI 128-bit NAA Name example	64
Figure 18 – SA Server Configuration	143
Figure 19 – Multicast Configuration	144
Figure 20 – No Multicast configuration	145
Figure 21 – Multicast Islands.....	146
Figure 22 – SMI_S Roles	150
Figure B.1 – Provider migration.....	185

Table 1 – OperationalStatus for Disk Drive	40
Table 2 – Standard formats for StorageVolume names	57
Table 3 – Standard formats for port names.....	59
Table 4 – Standard formats for storage system names.....	60
Table 5 – Standard operating system names for tape devices	62
Table 6 – LogicalDisk.Name for disk partitions	62
Table 7 – GenericDiskParittion.Name for disk partitions.....	62
Table 8 – Standard operating system names for unpartitioned disks.....	63
Table 9 – Example Standard Message Declaration	66
Table 10 – Example Standard Message Values	67
Table 11 – Redundancy Message Arguments	67
Table 12 – Redundancy Alert Information	68
Table 13 – Environmental Message Arguments	68
Table 14 – Environmental Alert Information	69
Table 15 – FRU Operation Message Arguments	69
Table 16 – FRU Operation Alert Information	69
Table 17 – Password change Message Arguments	70
Table 18 – Password change Alert Information	70
Table 19 – User or Account Operation Message Arguments.....	70
Table 20 – User or Account Operation Alert Information.....	71
Table 21 – User Login Message Arguments.....	71
Table 22 – User Login Alert Information	71
Table 23 – Proxy Agent Device Communication Message Arguments.....	72
Table 24 – Proxy Agent Device Communication Alert Information.....	72
Table 25 – Port Status Changed Message Arguments.....	72
Table 26 – Port Status Changed Alert Information	73
Table 27 – Datacheck Error Message Arguments.....	73
Table 28 – Datacheck Error Alert Information	73
Table 29 – User Login Failure Message Arguments	74
Table 30 – User Login Failure Alert Information	74
Table 31 – Drive not responding Message Arguments.....	74
Table 32 – Drive not responding Alert Information	75
Table 33 – Cooling Fan Failure Alert Information	75
Table 34 – Power Supply Failure Alert Information	75
Table 35 – Drive Power Consumption Alert Information	76
Table 36 – Drive Voltage Alert Information	76
Table 37 – Predictive Failure Alert Information	76
Table 38 – Diagnostics Required Alert Information	77
Table 39 – Authorization Failure Message Arguments.....	77
Table 40 – Error Properties for Authorization Failure	77

Table 41 – Operation Not Supported Message Arguments	78
Table 42 – Property Not Found Message Arguments	78
Table 43 – Invalid Query Message Arguments	79
Table 44 – Parameter Error Message Arguments.....	79
Table 45 – Error Properties for Parameter Error	79
Table 46 – Query Syntax Error Message Arguments	80
Table 47 – Error Properties for Query Syntax Error.....	80
Table 48 – Query Too Expensive Message Arguments	80
Table 49 – Error Properties for Query Too Expensive	80
Table 50 – Class or Property Invalid in Query Message Arguments.....	81
Table 51 – Error Properties for Class or Property Invalid in Query.....	81
Table 52 – Invalid Join in Query Message Arguments	81
Table 53 – Error Properties for Invalid Join in Query.....	82
Table 54 – Unexpected Hardware Fault Message Arguments.....	82
Table 55 – Error Properties for Unexpected Hardware Fault.....	82
Table 56 – Too busy to respond Message Arguments	82
Table 57 – Shutdown Started Message Arguments	83
Table 58 – Shutdown Started Alert Information.....	83
Table 59 – Component overheat Message Arguments	83
Table 60 – Error Properties for Component overheat	83
Table 61 – Component overheat Alert Information	84
Table 62 – Device Failover Message Arguments.....	84
Table 63 – Functionality is not licensed Message Arguments	84
Table 64 – Error Properties for Functionality is not licensed.....	84
Table 65 – Invalid Property Combination during instance creation or modification Message Arguments	85
Table 66 – Error Properties for Invalid Property Combination during instance creation or modification.....	85
Table 67 – Property Not Found Message Arguments	86
Table 68 – Error Properties for Property Not Found	86
Table 69 – Proxy Can Not Connect Message Arguments	86
Table 70 – Error Properties for Proxy Can Not Connect	86
Table 71 – Not Enough Memory Message Arguments	87
Table 72 – Error Properties for Not Enough Memory	87
Table 73 – Error Properties for Object Already Exists	87
Table 74 – Device Not ready Message Arguments	88
Table 75 – Error Properties for Device Not ready.....	88
Table 76 – Error Properties for Internal Bus Error	88
Table 77 – Error Properties for DMA Overflow	89
Table 78 – Error Properties for Firmware Logic Error	89

Table 79 – Front End Port Error Message Arguments	89
Table 80 – Front End Port Error Alert Information	89
Table 81 – Back End Port Error Message Arguments.....	90
Table 82 – Back End Port Error Alert Information.....	90
Table 83 – Remote Mirror Error Message Arguments.....	90
Table 84 – Error Properties for Remote Mirror Error.....	90
Table 85 – Remote Mirror Error Alert Information.....	91
Table 86 – Error Properties for Cache Memory Error	91
Table 87 – Error Properties for Unable to Access Remote Device	91
Table 88 – Error Reading Data Alert Information.....	92
Table 89 – Error Writing Data Alert Information	92
Table 90 – Error Validating Write (CRC) Alert Information.....	92
Table 91 – Error Properties for Copy Operation Failed.....	93
Table 92 – Error Properties for RAID Operation Failed.....	93
Table 93 – Error Properties for Invalid RAID Type	93
Table 94 – Error Properties for Invalid Storage Element Type	94
Table 95 – Error Properties for Configuration Change Failed	94
Table 96 – Error Properties for Buffer Overrun	94
Table 97 – Stolen Capacity Message Arguments	95
Table 98 – Error Properties for Stolen Capacity	95
Table 99 – Invalid Extent passed Message Arguments.....	95
Table 100 – Error Properties for Invalid Extent passed	95
Table 101 – Error Properties for Invalid Deletion Attempted	96
Table 102 – Error Properties for Job Failed to Start	96
Table 103 – Job was Halted Message Arguments	96
Table 104 – Invalid State Transition Message Arguments	97
Table 105 – Error Properties for Invalid State Transition	97
Table 106 – Invalid SAP for Method Message Arguments	97
Table 107 – Error Properties for Invalid SAP for Method	97
Table 108 – Resource Not Available Message Arguments.....	98
Table 109 – Error Properties for Resource Not Available	98
Table 110 – Resource Limit Exceeded Message Arguments.....	98
Table 111 – Error Properties for Resource Limit Exceeded	99
Table 112 – Thin Provision Capacity Warning Message Arguments.....	99
Table 113 – Thin Provision Capacity Warning Alert Information.....	99
Table 114 – Thin Provision Capacity Critical Message Arguments.....	100
Table 115 – Thin Provision Capacity Critical Alert Information	100
Table 116 – Thin Provision Capacity Okay Message Arguments	100
Table 117 – Thin Provision Capacity Okay Alert Information	100
Table 118 – Masking Group Membership Changed Message Arguments	101

Table 119 – Masking Group Membership Changed Alert Information.....	101
Table 120 – Zone Database Changed Message Arguments	101
Table 121 – Zone Database Changed Alert Information	102
Table 122 – ZoneSet Activated Message Arguments	102
Table 123 – ZoneSet Activated Alert Information	102
Table 124 – Error Properties for Session Locked	102
Table 125 – Error Properties for Session Aborted	103
Table 126 – Switch Status Changed Message Arguments	103
Table 127 – Switch Status Changed Alert Information.....	103
Table 128 – Fabric Merge/Segmentation Message Arguments	104
Table 129 – Fabric Merge/Segmentation Alert Information	104
Table 130 – Switch Added/Removed Message Arguments	104
Table 131 – Switch Added/Removed Alert Information	105
Table 132 – Fabric Added/Removed Message Arguments.....	105
Table 133 – Fabric Added/Removed Alert Information	105
Table 134 – Security Policy change Message Arguments.....	105
Table 135 – Security Policy change Alert Information	106
Table 136 – Required Firmware Version Message Arguments.....	106
Table 137 – Required Firmware Version Alert Information.....	106
Table 138 – Recommended Firmware Version Message Arguments.....	107
Table 139 – Recommended Firmware Version Alert Information	107
Table 140 – Controller OK Message Arguments.....	107
Table 141 – Controller OK Alert Information	107
Table 142 – Controller not OK Message Arguments.....	107
Table 143 – Controller not OK Alert Information.....	108
Table 144 – Bus rescan complete Alert Information	108
Table 145 – Disk initialize Failed Message Arguments.....	108
Table 146 – Disk initialize Failed Alert Information.....	108
Table 147 – Read Warning Alert Information	109
Table 148 – Write Warning Alert Information	109
Table 149 – Hard Error Alert Information	109
Table 150 – Media Alert Information.....	110
Table 151 – Read Failure Alert Information.....	110
Table 152 – Write Failure Alert Information.....	110
Table 153 – Media Life Alert Information	111
Table 154 – Not Data Grade Alert Information	111
Table 155 – Write Protect Alert Information	111
Table 156 – No Removal Alert Information	112
Table 157 – Cleaning Media Alert Information	112
Table 158 – Unsupported Format Alert Information	112

Table 159 – Recoverable Snapped Tape Alert Information.....	113
Table 160 – Unrecoverable Snapped Tape Alert Information.....	113
Table 161 – Memory Chip In Cartridge Failure Alert Information.....	113
Table 162 – Forced Eject Alert Information.....	114
Table 163 – Read Only Format Alert Information	114
Table 164 – Directory Corrupted On Load Alert Information	114
Table 165 – Nearing Media Life Alert Information	115
Table 166 – Clean Now Alert Information.....	115
Table 167 – Clean Periodic Alert Information.....	115
Table 168 – Expired Cleaning Media Alert Information.....	116
Table 169 – Invalid Cleaning Media Alert Information	116
Table 170 – Retention Requested Alert Information	116
Table 171 – Dual-Port Interface Error Alert Information.....	117
Table 172 – Drive Maintenance Alert Information.....	117
Table 173 – Hardware A Alert Information	117
Table 174 – Hardware B Alert Information	118
Table 175 – Interface Alert Information.....	118
Table 176 – Eject Media Alert Information	118
Table 177 – Download Failure Alert Information.....	119
Table 178 – Loader Hardware A Alert Information.....	119
Table 179 – Loader Stray Media Alert Information	119
Table 180 – Loader Hardware B Alert Information.....	120
Table 181 – Loader Door Alert Information	120
Table 182 – Loader Hardware C Alert Information	120
Table 183 – Loader Magazine Alert Information.....	121
Table 184 – Loader Predictive Failure Alert Information	121
Table 185 – Load Statistics Alert Information.....	121
Table 186 – Media Directory Invalid at Unload Alert Information.....	122
Table 187 – Media System area Write Failure Alert Information	122
Table 188 – Media System Area Read Failure Alert Information	122
Table 189 – No Start of Data Alert Information	123
Table 190 – Loading Failure Alert Information	123
Table 191 – Library Hardware A Alert Information.....	123
Table 192 – Library Hardware B Alert Information.....	124
Table 193 – Library Hardware C Alert Information	124
Table 194 – Library Hardware D Alert Information	124
Table 195 – Library Diagnostic Required Alert Information.....	125
Table 196 – Library Interface Alert Information	125
Table 197 – Failure Prediction Alert Information	125
Table 198 – Library Maintenance Alert Information	126

Table 199 – Library Humidity Limits Alert Information	126
Table 200 – Library Voltage Limits Alert Information	126
Table 201 – Library Stray Media Alert Information	127
Table 202 – Library Pick Retry Alert Information	127
Table 203 – Library Place Retry Alert Information	127
Table 204 – Library Load Retry Alert Information	128
Table 205 – Library Door Alert Information	128
Table 206 – Library Mailslot Alert Information	128
Table 207 – Library Magazine Alert Information	129
Table 208 – Library Security Alert Information	129
Table 209 – Library Security Mode Alert Information	129
Table 210 – Library Offline Alert Information	130
Table 211 – Library Drive Offline Alert Information	130
Table 212 – Library Scan Retry Alert Information	130
Table 213 – Library Inventory Alert Information	131
Table 214 – Library Illegal Operation Alert Information	131
Table 215 – Pass Through Mechanism Failure Alert Information	131
Table 216 – Cartridge in Pass-through Mechanism Alert Information	132
Table 217 – Unreadable barcode Labels Alert Information	132
Table 218 – Message Types	136
Table 219 – Required Configuration Properties for SA as DA	142
Table 220 – Required Configuration Properties for SA	142
Table 221 – ACL for File "XYZ"	179

INFORMATION TECHNOLOGY – STORAGE MANAGEMENT –

Part 2: Common architecture

FOREWORD

- 1) 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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.
- 2) The formal decisions or agreements of IEC and ISO on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees and ISO member bodies.
- 3) IEC, ISO and ISO/IEC publications have the form of recommendations for international use and are accepted by IEC National Committees and ISO member bodies in that sense. While all reasonable efforts are made to ensure that the technical content of IEC, ISO and ISO/IEC publications is accurate, IEC or ISO cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees and ISO member bodies undertake to apply IEC, ISO and ISO/IEC publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any ISO, IEC or ISO/IEC publication and the corresponding national or regional publication should be clearly indicated in the latter.
- 5) ISO and IEC do not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. ISO or IEC are not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or ISO or its directors, employees, servants or agents including individual experts and members of their technical committees and IEC National Committees or ISO member bodies for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication of, use of, or reliance upon, this ISO/IEC publication or any other IEC, ISO or ISO/IEC publications.
- 8) Attention is drawn to the normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this ISO/IEC publication may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

International Standard ISO/IEC 24775-2 was prepared by subcommittee 25: Interconnection of information technology equipment, of ISO/IEC joint technical committee 1: Information technology.

This International Standard, together with ISO/IEC 24775-1 and ISO/IEC 24775-3 to ISO/IEC 24775-8, replaces ISO/IEC 24775, second edition, published in 2011, and constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

- a) reorganization into eight parts;
- b) maturity identification using stages; and
- c) new profiles.

The introduction of ISO/IEC 24775-1 contains a detailed list of the technical changes.

The list of all currently available parts of the ISO/IEC 24775 series, under the general title *Information technology – Storage management*, can be found on the IEC web site.

This International Standard has been approved by vote of the member bodies, and the voting results may be obtained from the address given on the second title page.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

IMPORTANT – The “colour inside” logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this publication using a colour printer.

Introduction

Information Technology – Storage Management, Part 2 Common Architecture defines the core architecture of SMI-S. This includes the protocols (WBEM, SLP,...); the model is defined in the parts.

Parts of this Standard

This International Standard is subdivided into the following parts:

- *Information technology – Storage management – Part 1: Overview*
- *Information technology – Storage management – Part 2: Common architecture*
- *Information technology – Storage management – Part 3: Common profiles*
- *Information technology – Storage management – Part 4: Block devices*
- *Information technology – Storage management – Part 5: Filesystems*
- *Information technology – Storage management – Part 6: Fabric*
- *Information technology – Storage management – Part 7: Host elements*
- *Information technology – Storage management – Part 8: Media libraries*

Changes since the last edition

This first multipart edition cancels and replaces the second edition published in 2011 and constitutes a technical revision. This edition includes the following significant changes with respect to the previous edition. The changes fall into three broad categories:

- **Improved organization.** The International Standard has been reorganized into eight parts to provide more information more easily. The parts are:
 - *Part 1 Overview:* The overview book provides a high level overview of the standard.
 - *Part 2 Common Architecture:* This part covers general information about the interface, such as security and protocols.
 - *Part 3 Common Profiles:* This part covers component profiles that extend profiles in other books, such as target ports and job control.
 - *Part 4 Block Devices:* This part covers storage profiles that support various forms of disk storage.
 - *Part 5 Filesystems:* This part covers profiles that support filesystems, such as NAS (Network Attached Storage).
 - *Part 6 Fabric:* This part covers profiles that deal with interconnection of host servers and storage devices, such as switches.
 - *Part 7 Host Elements:* This part covers profiles for storage software on host servers, such as disk partitioning and Host Hardware RAID controllers.
 - *Part 8 Media Libraries:* This part covers profiles that deal with removable media such as tape libraries.
- **Maturity identification.** As material is added to the standard it goes through various stages of maturity. The initial stage is *Experimental*, which is material that has not yet been implemented and is subject to change. The other stages indicate the degree of implementations. The stages are:
 - **Experimental:** Full design review, no commercial implementations.
 - **Implemented:** Initial implementations available, may be removed at minor revision.
 - **Stable:** Three or more vendors have implemented the identified material, backward compatibility assured, removed only at major revision.

- **Finalized:** Relies solely on Finalized content, deprecated only at major revision.
- **Deprecated:** Obsolete material, may be removed in future revisions.

For a more detailed explanation of each maturity level and its typographical indication, see Clause 4 Typographical Conventions.

- **Expanded scope.** The range of SAN components modeled by the profiles defined in the parts has been greatly expanded.
 - New profiles include:
 - *Part 3 Common Profiles:* Serial Attached SCSI (SAS) Target Port, Serial ATA (SATA) Target Ports, SB Target Port, SAS Initiator Ports, ATA Initiator Ports, FC-SB-x Initiator Ports, FCoE Initiator Ports, Power Supply, Fan, Sensors, Base Server, Media Access Device, Storage Enclosure, Software Inventory, Profile Registration, Proxy Server System Management, Operational Power.
 - *Part 4 Block Devices:* Block Storage Views, CKD Block Services, Erasure, Storage Server Asymmetry, Volume Composition, Storage Element Protection, Replication Services, Pools from Volumes, Group Masking and Mapping, Thin Provisioning.
 - *Part 5 Filesystems:* File Export, File Server Manipulation, File Storage, Filesystem, Filesystem Copy Services, Filesystem Performance, Filesystem Quotas, NAS Network Port, Host Filesystem, Filesystem Remote Copy Services.
 - *Part 6 Fabric:* Fibre Channel Security, Fabric Views, Virtual Fabrics, Switch Partitioning, SAS Expander, N Port Virtualizer, Inter Fabric Routing.
 - *Part 7 Host Elements:* Storage HBA, Host Hardware RAID Controller.
 - *Part 8 Media Libraries:* Partitioned Tape Library, Virtual Tape Library, Virtual Tape Library Copy and Library Views.
 - The following experimental profiles were removed from the International Standard:
 - *Part 3 Common Profiles:* Security, 3rd Party Authentication, Authorization, Credential Management, Identity Management, Security Role Based Access Control and Security Resource Ownership.
 - *Part 4 Block Devices:* Pool Management Policy.
 - The following profiles were deprecated:
 - *Part 3 Common Profiles:* Cascading (replaced by direct use of cascading classes).
 - *Part 4 Block Devices:* Volume Management (and not replaced).
 - *Part 6 Fabric:* Router (and not replaced).
 - *Part 7 Host Elements:* FC HBA (replaced by Storage HBA), SB Multipath Management (and not replaced).
 - *Part 8 Media Libraries:* InterLibraryPort Connection (and not replaced).
 - In addition, many of the existing profiles have been enhanced.

This International Standard was prepared by the SNIA (Storage Networking Industry Association)¹. The standard is often referred to as **SMI-S** (*Storage Management Initiative Specification*).

1) Storage Networking Industry Association, 425 Market Street, Suite 1020, San Francisco, CA 94105, U.S.A.
<http://www.snia.org>

1 Scope

This part of ISO/IEC 24775 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.

2 Normative references

The following documents, in whole or in part, are normatively referenced in the document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document, including any amendments, applies.

ISO/IEC 14776-413, *SCSI Architecture Model - 3 (SAM-3)*

ISO/IEC 14776-453, *SCSI Primary Commands - 3 (SPC-3)*

ISO/IEC 24775-3, *Information Technology – Storage Management, Part 3 Common Profiles*

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

DMTF DSP0200, *CIM Operations over HTTP 1.3*

http://www.dmtf.org/standards/published_documents/DSP0200_1.3.0.pdf

DMTF DSP0202, *CIM Query Language Specification 1.0*

http://www.dmtf.org/standards/published_documents/DSP0202_1.0.0.pdf

DMTF DSP0226, *WS-Management Protocol Specification*

IETF RFC 2045, *Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies*

<http://www.ietf.org/rfc/rfc2045.txt>

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 and Digest Access Authentication*

<http://www.ietf.org/rfc/rfc2617.txt>

IETF RFC 2614, *An API for Service Location*

<http://www.ietf.org/rfc/rfc2614.txt>

IETF RFC 2869, *RADIUS Extensions*

<http://www.ietf.org/rfc/rfc2869.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>

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>

IETF RFC 4346, *The Transport Layer Security (TLS) Protocol Version 1.1*

<http://www.ietf.org/rfc/rfc4346.txt>

ISO/IEC 24775-2:2014 © ISO/IEC 2014 - 21 -

IETF RFC 5246, *The Transport Layer Security (TLS) Protocol Version 1.2*
<http://tools.ietf.org/rfc/rfc5246.txt>

3 Terms, definitions, symbols, abbreviations, and conventions

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

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

Note 1 to entry: Access controls may be logical, physical, technical, managerial or a combination. Access controls ensure that only the operations permitted are performed.

[SOURCE: ISO/IEC 27000:2014, 2.1, modified – Definition gives more details.]

3.1.2

account

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

3.1.4

administrator

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

3.1.5

agent

object manager that includes the provider service for a limited set of resources

Note 1 to entry: An agent may be embedded or hosted and can be an aggregator for multiple devices.

3.1.6

aggregation

strong form of association

EXAMPLE The containment relationship between a system and the components that make up the system can be called an aggregation.

Note 1 to entry: An aggregation is expressed as a Qualifier on the association class.

Note 2 to entry: Aggregation often implies, but does not require, that the aggregated objects have mutual dependencies.

3.1.7

audit log

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

Note 1 to entry: These logs are kept for an agreed period of time to assist in future investigations.

Note 2 to entry: Audit logs may be used to comply with legal requirements.

3.1.8

authentication

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**

process of granting a right or permission to access a system resource

3.1.11**CIM Server**

Server that provides support for CIM requests and provides CIM responses

3.1.12**client**

process that issues requests for service

Note 1 to entry: Formulating and issuing requests may involve multiple client processes distributed over one or more computer systems.

3.1.13**Common Information Model****CIM**

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

Note 1 to entry: A CIM is divided into a Core Model and Common Models.

Note 2 to entry: The Core Model addresses high-level concepts (such as systems and devices), as well as fundamental relationships (such as dependencies).

Note 3 to entry: The Common Models describe specific problem domains such as computer system, network, user or device management.

Note 4 to entry: The Common Models are subclasses of the Core Model and may also be subclasses of each other.

3.1.14**dedicated SMI-S Server**

CIM Server that is dedicated to supporting a single device or subsystem

3.1.15**digested password**

hashed form of a cleartext password

3.1.16**discovery**

information about physical and logical storage entities within the management domain

3.1.17**Distributed Management Task Force****DMTF**

industry organization that develops management standards for computer system and enterprise environments

Note 1 to entry: DMTF standards include WBEM, CIM, DMI, DEN and ARM.

3.1.18**dynamic host control protocol****DHCP**

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**

CIM Server embedded in the device or subsystem for which it provides management

3.1.20**enclosure**

box or cabinet

3.1.21**entity authentication**

corroboration that an entity is the one claimed

3.1.22**enumerate**

operation used to enumerate subclasses, subclass names, instances and instance names in the target Namespace

Note 1 to entry: If successful, the method returns zero or more requested elements that meet the required criteria.

3.1.23**event**

occurrence of a phenomenon of interest

3.1.24**extent**

set of consecutively addressed disk blocks

3.1.25**external authentication**

relying on an authentication service separate from (or external to) an entity

Note 1 to entry: For example, a device may pass the user name and password to a separate RADIUS server for validation.

3.1.26**extrinsic method**

method defined as part of CIM Schema

3.1.27**fabric**

any interconnect between two or more Fibre Channel N_Ports, including point-to-point, loop, and Switched Fabric

3.1.28**FICON™¹**

Fibre Channel storage protocol used in IBM mainframe computers and peripheral devices such as ECKD storage arrays and tape drives

3.1.29**general purpose SMI-S Server**

server that is not dedicated to supporting a single device or subsystem, and may support multiple devices or subsystems

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

3.1.30**grammar**

formal definition of the syntactic structure of a language (see 3.1.67, "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)

3.1.31**host bus adapter****HBA**

card that contains ports for host systems

3.1.32**Hypertext Transfer Protocol****HTTP**

request-reply protocol used for internet communications

3.1.33**identity**

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

Note 1 to entry: A common example is the assignment of the user name JoeJ (the identity) to represent the human user Joe Jones for purposes of authentication and authorization.

3.1.34**interconnect element**

non terminal network elements

EXAMPLES Switches, hubs, routers, directors

3.1.35**interface definition language****IDL**

high-level declarative language that provides the syntax for interface declarations

3.1.36**intrinsic method**

operations made against a CIM server and a CIM namespace independent of the implementation of the schema defined in the server

3.1.37**logical unit number****LUN**

abbreviation for a SCSI logical unit or logical unit number

3.1.38**mutual authentication****bidirectional authentication**

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

3.1.39**Network Address Authority****NAA**

four bit identifier to denote a network address authority

Note 1 to entry: i.e., an organization such as CCITT or IEEE that administers network addresses.

3.1.40**non-repudiation**

ability to prove an action or event has taken place, so that this event or action cannot be repudiated later

[SOURCE: ISO/IEC 27000:2014, 2.54]

3.1.41**out-of-band**

transmission of management information for storage components outside of the data path, typically over Ethernet

Note 1 to entry: Use of mechanisms other than the ones required on a communications channel to transmit information.

3.1.42**partition**

collection of contiguous block on a disk or virtual disk

3.1.43**password**

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

3.1.44**path**

combination of initiator and target ports and logical unit

3.1.45**privacy**

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

3.1.46**privileged user**

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

Note 1 to entry: Such persons will include, for example, the system administrator(s), storage administrator(s), and network administrator(s) who are responsible for keeping the system available and may need powers to create new user profiles as well as add to or amend the powers and access rights of existing users.

3.1.47**protocol**

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

Note 1 to entry: For example, xmlCIM uses XML as its transfer syntax, and HTTP as the request-reply protocol HTTP is layered over the TCP/IP network protocol.

3.1.48**proxy SMI-S Server**

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

Note 1 to entry: For example, a proxy SMI-S Server might run on a host system, but support a storage array.

3.1.49**public key infrastructure****PKI**

framework established to issue, maintain, and revoke public key certificates accommodating a variety of security technologies

3.1.50**SAN**

Storage Area Network

group of fabrics that have common leaf elements

3.1.51**SB**

Single-Byte Command Code Sets

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**

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**

network address and port number of a process offering a service

3.1.55**shared secret**

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

3.1.56**Simple Network Management Protocol****SNMP**

IETF protocol for monitoring and managing systems and devices in a network

Note 1 to entry: The data being monitored and managed is defined by a MIB.

Note 2 to entry: The functions supported by the protocol are the request and retrieval of data, the setting or writing of data, and traps that signal the occurrence of events.

3.1.57**SMI-S Server**

CIM Server that supports SMI-S (this International Standard, also known as the *Storage Management Initiative Specification*) Profiles for management of a device or subsystem

3.1.58**SNMP Trap**

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

3.1.59**Soft Zone**

Zone consisting of Zone Members that are made visible to each other through Client Service requests

Note 1 to entry: Typically, Soft Zones contain Zone Members that are visible to devices via Name Server exposure of Zone Members.

Note 2 to entry: The Fabric does not enforce a Soft Zone. Note that well known addresses are implicitly included in every Zone.

3.1.60**Storage Management Initiative Specification****SMI-S**

interface between WBEM-capable clients and servers for the secure, extensible, and interoperable management of networked storage

Note 1 to entry: This International Standard.

3.1.61**Storage Networking Industry Association****SNIA**

association of producers and consumers of storage networking products whose goal is to further storage networking technology and applications

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**

fabric comprised of one or more Switches

3.1.65**syntax**

structure of strings in any language

Note 1 to entry: A language's syntax is described by a grammar.

3.1.66**threat**

potential cause of an unwanted incident, which may result in harm to a system or organization

[SOURCE: ISO/IEC 27000:2014, 2.83]

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****UDP**

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, modified – Definition includes more details]

3.1.70**Web Based Enterprise Management****WBEM**

Web-Based Enterprise Management is an initiative in the DMTF.

Note 1 to entry: It is a set of technologies that enables interoperable management of an enterprise.

Note 2 to entry: WBEM consists of CIM, an XML DTD defining the tags (XML encodings) to describe the CIM Schema and its data, and a set of HTTP operations for exchanging the XML-based information.

3.1.71

web service

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

Note 1 to entry: It has an interface described in a machine-processable format (specifically WSDL).

Note 2 to entry: Other systems interact with the Web service in a manner prescribed by its description using SOAP messages, typically conveyed using HTTP with an XML serialization in conjunction with other Web-related standards. [W3C WS-Arch]

3.1.72

XML

eXtensible Markup Language

universal format for structured documents and data on the World Wide Web

3.1.73

zone

group of ports and switches that allow access

Note 1 to entry: Defined by a zone definition.

3.1.74

zone set

one or more Zones that may be activated or deactivated as a group

3.2 Acronyms and abbreviations

AAA	Authentication, Authorization, and Accounting
ACL	Access Control List
API	application programming interface
CA	Certificate Authority
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	<i>Storage Management Initiative Specification (this International Standard)</i>
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

3.3 Keywords

3.3.1

expected

A keyword used to describe the behavior of the hardware or software in the design models presumed by this International Standard.

Note 1 to entry: Other hardware and software design models may also be implemented.

3.3.2

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.

3.3.3

mandatory

A keyword indicating an item that is required to be implemented as defined in this International Standard to claim compliance with this International Standard.

3.3.4

may

A keyword that indicates flexibility of choice with no implied preference.

3.3.5

may not

Keywords that indicates flexibility of choice with no implied preference.

3.3.6

obsolete

A keyword indicating that an item was defined in prior standards but has been removed from this International Standard.

3.3.7**opaque**

A keyword indicating that value has no semantics or internal structure.

3.3.8**optional**

A keyword that describes features that are not required to be implemented by this International Standard.

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

3.3.9**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 International Standard.

Note 3 to entry: Recipients are not required to check reserved bits, bytes, words or fields for zero values.

Note 4 to entry: Receipt of reserved code values in defined fields shall be reported as an error.

3.3.10**shall**

A keyword indicating a mandatory requirement.

Note 1 to entry: Designers are required to implement all such requirements to ensure interoperability with other products that conform to this International Standard.

3.3.11**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 International Standard have a specific meaning beyond the normal English meaning. These words and terms are defined either in 3.1 or in the text where they first appear.

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).

4 Typographical Conventions

4.1 Maturity Model

In addition to informative and normative content, this International Standard 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 Clause 4. 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 International Standard, an implementer should be able to make more informed decisions about the adoption and deployment of different portions of the International Standard in a commercial product.

This International Standard has been structured to convey both the formal requirements and assumptions of the Information Technology – Storage Management API and its emerging implementation and deployment lifecycle. Over time, the intent is that all content in the International Standard 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 International Standard, content is assumed to satisfy these requirements and is referred to as “Finalized”. Since much of the evolving International Standard content in any given release will not have matured to that level, this International Standard 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.

4.2 Experimental Maturity Level

No material is included in this International Standard unless its initial architecture has been completed and reviewed. Some content included in this International Standard 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 International Standards. 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 International Standard. 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.

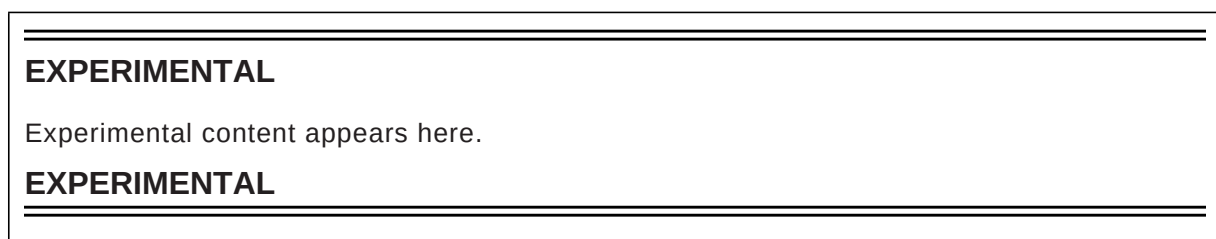


Figure 1 – Experimental Maturity Level Tag

4.3 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 shall be deprecated in a minor revision of the International Standard prior to its removal from subsequent releases. Figure 2 is a sample of the typographical convention for Implemented content.

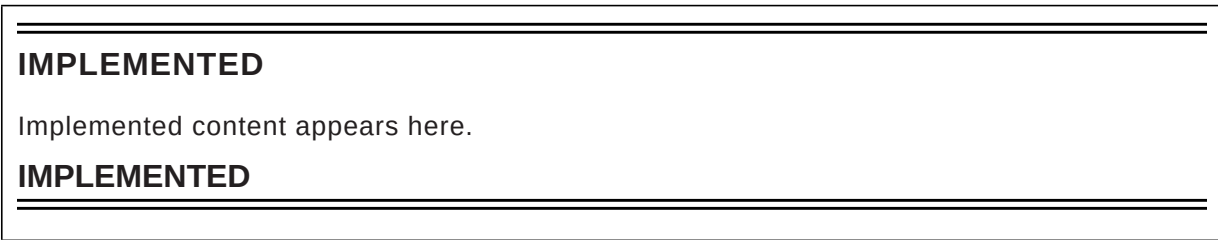


Figure 2 – Implemented Maturity Level Tag

4.4 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 International Standard. Material at this maturity level that has been deprecated may only be removed from the International Standard as part of a major revision. A profile that has reached this maturity level is guaranteed to preserve backward compatibility from one minor International Standard revision to the next. As a result, Profiles at or above the Stable maturity level shall not rely on any content that is Experimental. Figure 3 is a sample of the typographical convention for Implemented content.



Figure 3 – Stable Maturity Level Tag

4.5 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 shall solely depend upon or refine material that has also reached the Finalized level. If International Standard 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 International Standard. A profile that has reached this maturity level is guaranteed to preserve backward compatibility from one minor International Standard revision to the next. Over time, it is hoped that all International Standard 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 International Standard 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.

4.6 Deprecated Material

Non-Experimental material can be deprecated in a subsequent revision of the International Standard. Sections identified as “Deprecated” contain material that is obsolete and not recommended for use in new development efforts. Existing and new implementations are 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 International Standard. 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 International Standard. Providers shall implement the deprecated elements as long as it appears in the International Standard 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 International Standard with the replacement. Figure 4 contains a sample of the typographical convention for deprecated content.



Figure 4 – Deprecated Tag

5 Transport and reference model

5.1 Introduction to transport and reference model

5.1.1 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 clause 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).

5.1.2 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.

5.1.3 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 5.1.3.

5.1.4 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 International Standard. 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.

5.2 Transport Stack

The complete transport stack for this interface is illustrated in Figure 5. 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 IIOB become prominent, the content in the stack could be expanded with minimal changes to existing product implementations in the market.

EXPERIMENTAL

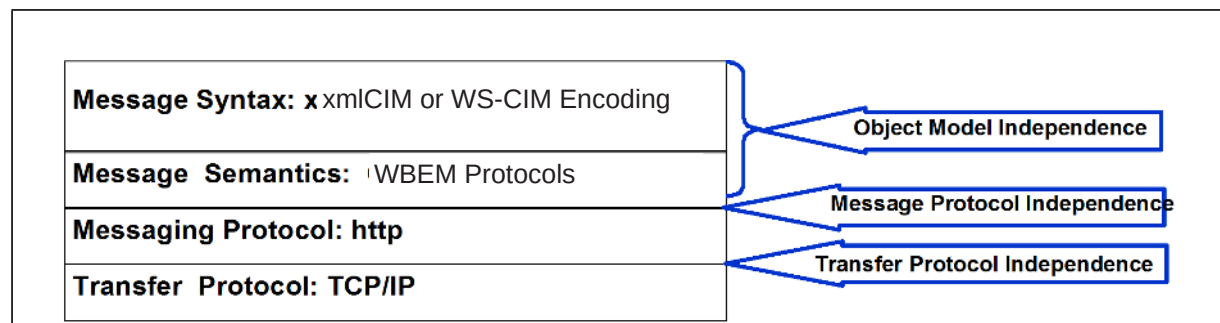


Figure 5 – Transport Stack

Implementers should be aware that an announced plan for converging web services standards is expected to cause changes to WS-Management, WSDM, and related protocols. SNIA intends to specify the resulting converged protocols for use with SMI-S, and hence use of web services protocols with SMI-S may remain Experimental until stable versions of the converged protocol specifications are available. Implementers are encouraged to experiment with web services protocols for SMI-S in the interim, but should consult the convergence plan to understand the potential protocol changes and possible impacts.

EXPERIMENTAL

This International Standard relies on the DMTF WBEM Protocol Specifications. Please refer to the DMTF WBEM Specification page for details on these specifications.

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

EXPERIMENTAL

Optionally, other protocols, such as WS-Management may also be supported.

EXPERIMENTAL

It should be noted that this International Standard 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.

5.3 Reference model

5.3.1 Overview

As shown in Figure 6, the Reference Model shows all possible constituents of the management environment in the presence of the transport stack for this interface.

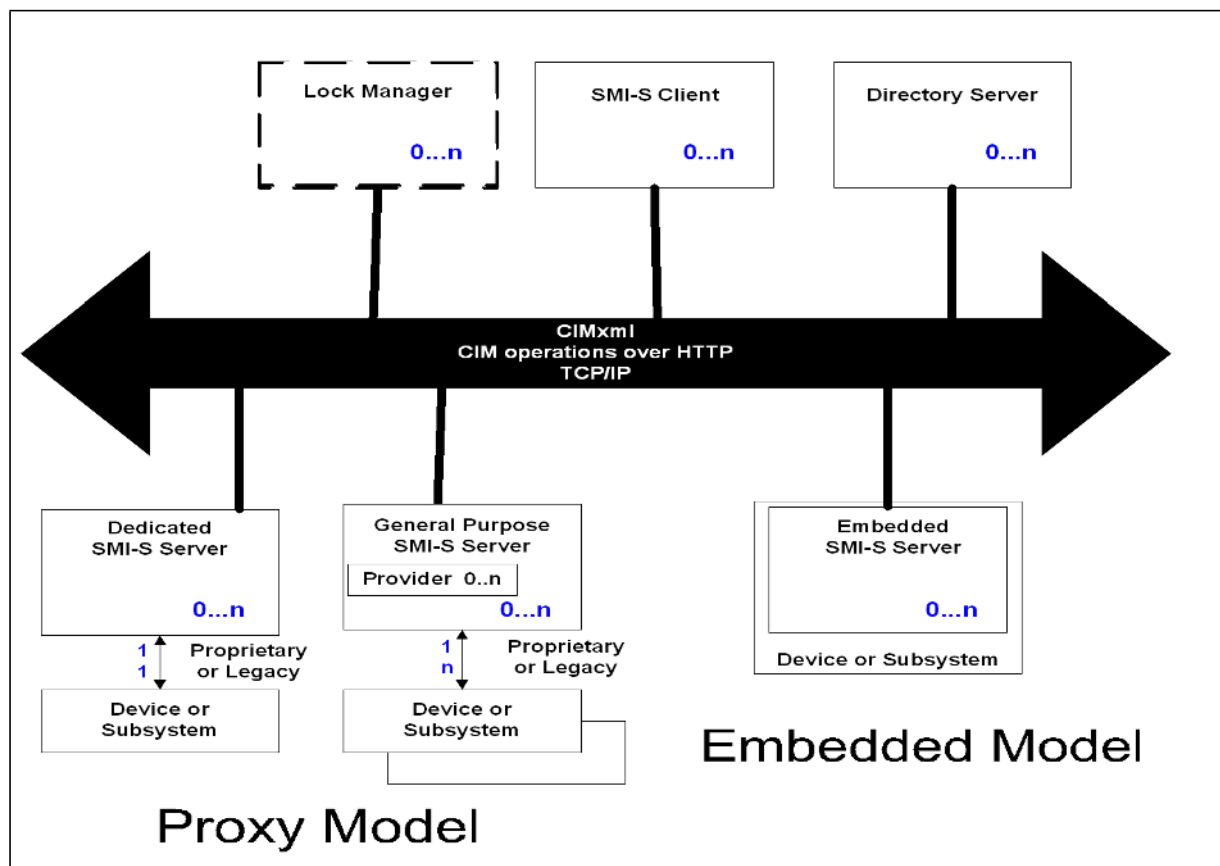


Figure 6 – Reference Model

Figure 6 illustrates that the transport for this interface uses a WBEM Protocol and HTTP/TCP/IP 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 Information Technology – Storage Management, a Lock Manager is not specified. As a result, it is shown as a dotted box to illustrate where the role would fit.

5.3.2 Roles for Interface Constituents

5.3.2.1 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.

5.3.2.2 SMI-S Server

An SMI-S Server is a CIM Server. It shall implement those functional profiles, as defined in the DMTF specifications, necessary to satisfy the Information Technology – Storage Management profile with which it conforms. 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 Information Technology – Storage Management 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.

5.3.2.3 General Purpose SMI-S Server

A General Purpose SMI-S Server is CIM Server that 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.

5.3.2.4 Provider

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

5.3.2.5 Lock Manager

This version of the International Standard does not support a lock manager.

5.3.2.6 Directory Server (SLP Directory Agent)

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

5.3.3 Cascaded Agents

This International Standard discusses constituents in the Information Technology – Storage Management environment in the context of Clients and Servers. This version of the International Standard also allows constituents in a Information Technology – Storage Management management environment to function as both client and server.

6 Health and Fault Management

6.1 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.

6.2 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.

6.3 General concepts

6.3.1 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.

6.3.2 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.

6.3.3 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.

6.3.4 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.

6.3.5 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).

6.3.6 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.

6.4 Description of Health and Fault Management

6.4.1 General

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.

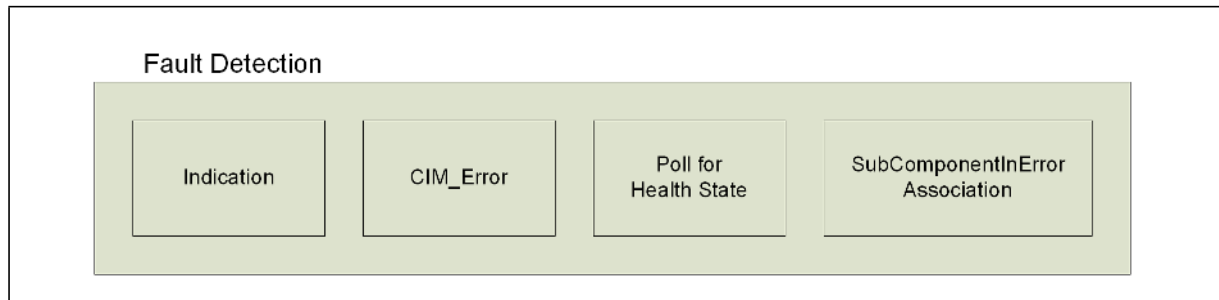


Figure 7 – Basic Fault Detection

There are four basic ways for a SMI-S client to detect an error or fault condition. Figure 7 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.

6.4.2 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

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

Table 1 – OperationalStatus for Disk Drive (Continued)

OperationalStatus	Description	HealthState	Description	Comment
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.

6.4.3 Standard Errors and Events

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

6.4.4 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/Subprofile. The definitions will be contained in the profiles/subprofiles. Standard errors are not the only error codes that can be returned, but are the only codes that a generic client will understand.

6.4.5 Indications

Indications are asynchronous messages from CIM servers to clients. A client must register for them. Each SMI-S profile/subprofile 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 indication subprofile.

EXPERIMENTAL

6.4.6 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 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 8 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.

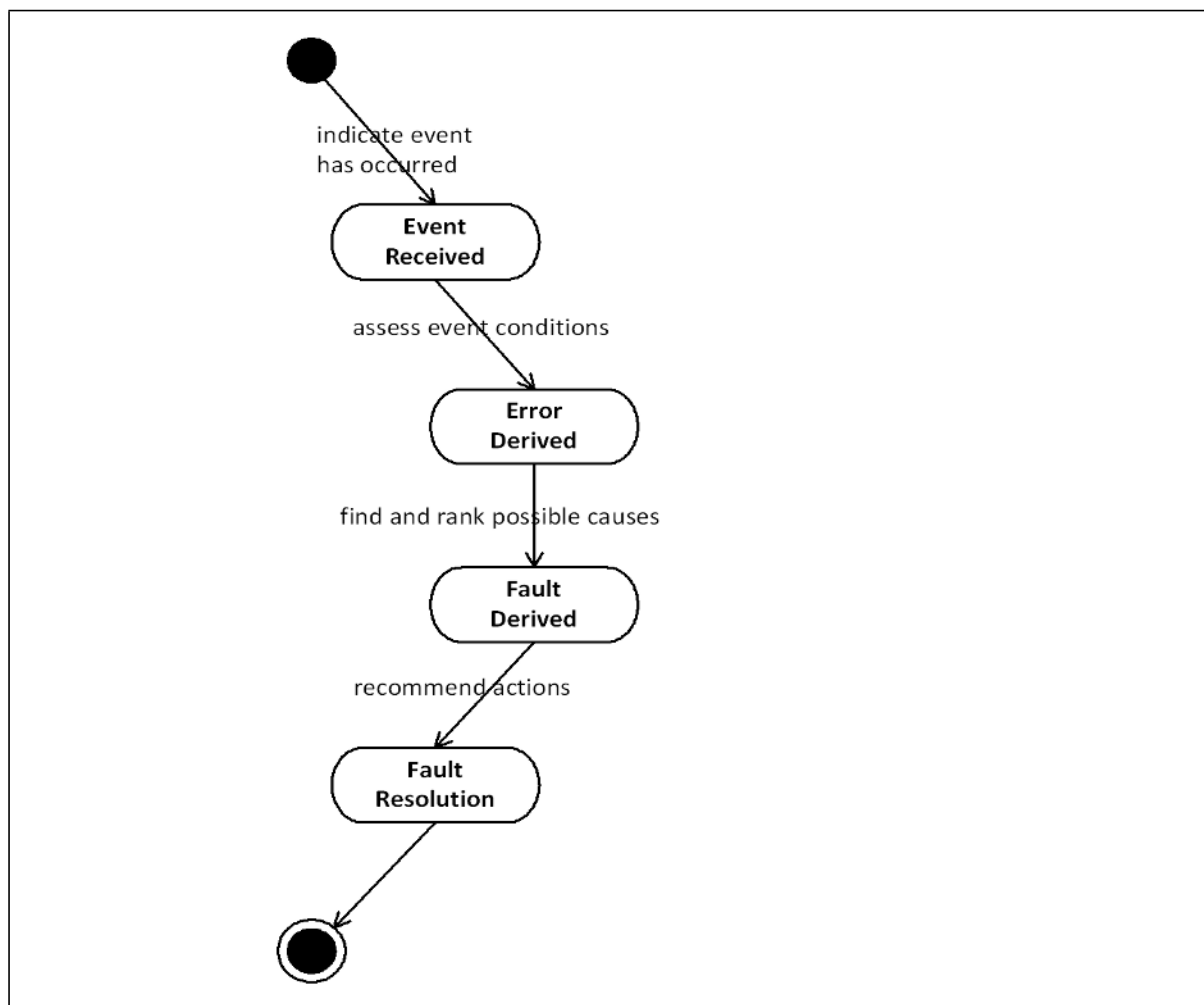


Figure 8 – Health lifecycle

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 can not 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.

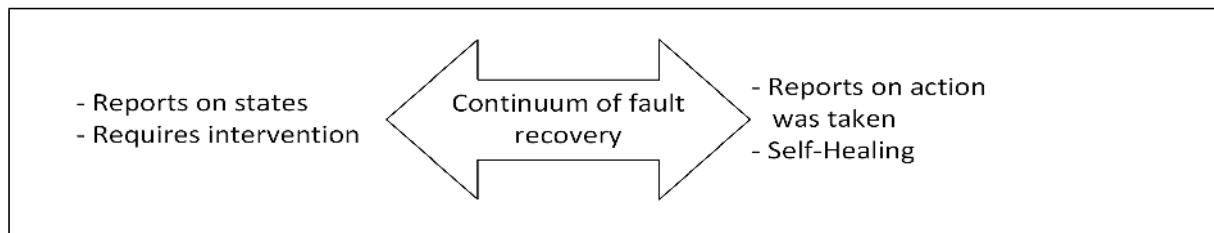


Figure 9 – Continuum

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 9. 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 can not report states, errors and alerts in a standard way or can not 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.

6.4.7 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 10 illustrates the scope of fault regions in a simplified SAN example and how the may be recursive in nature. AN HFM application has the widest scope of concern in this example.

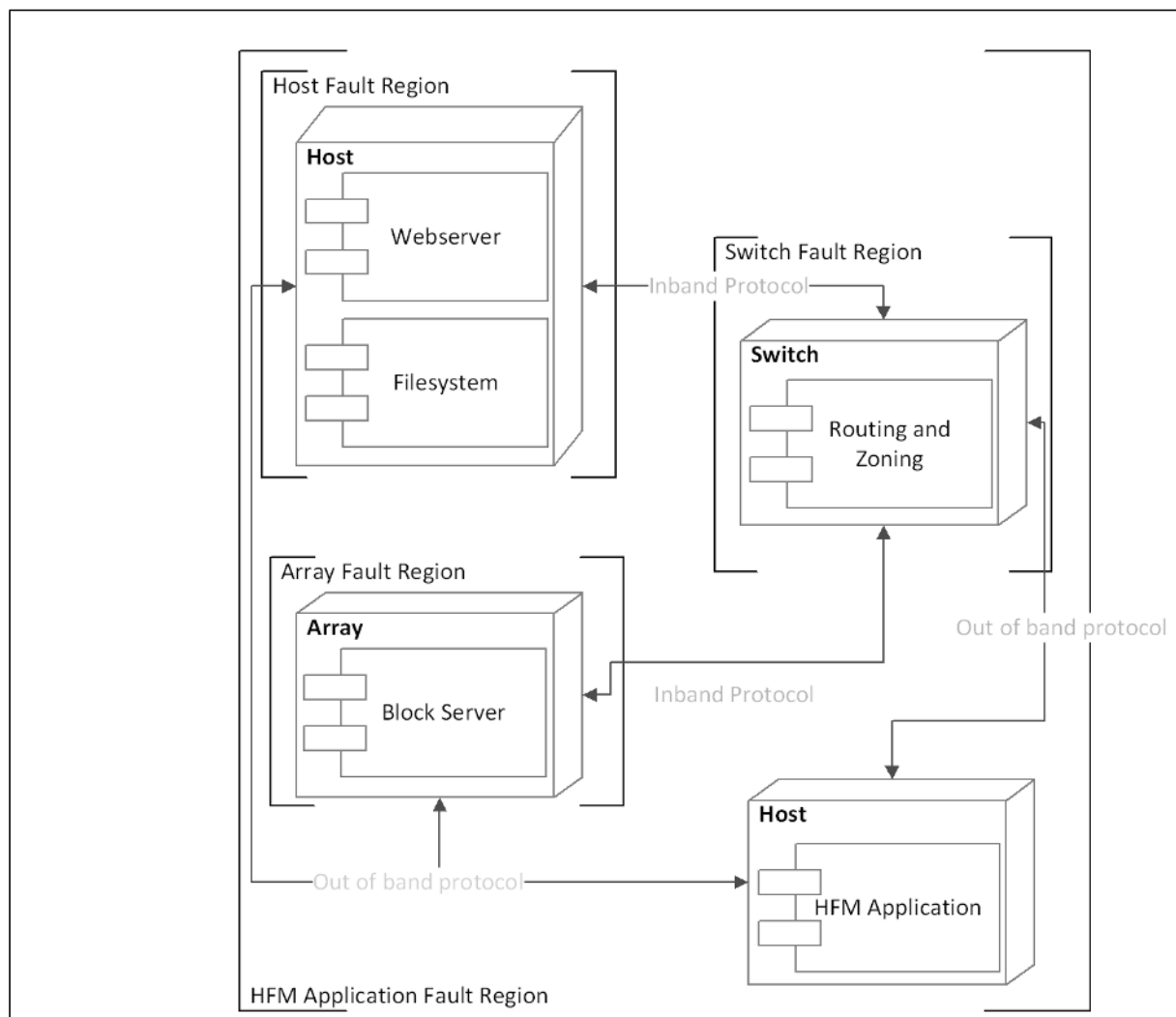


Figure 10 – Application Fault Region

Error handling is initiated by the interception of error events. For example, a switch may recognize the failure of one of its ports and reroute traffic to a working port. In this case, the fault region is defined as the switch itself. If the failure event is publicly consumable, other fault mitigation entities can also handle the error as well. The failure of a drive may be mitigated one way in the array fault region and mitigated differently in the HFM enabled application fault region. For example, the array fault mitigation entity can bring a volume off line if the failure of the disk brings the set of disks below the minimum required for quorum. At the same time, the HFM enabled application can reconfigure the storage service to create a replacement volume and then restore the failed volume's data from backup.

The HFM enabled application is one of the several possible storage network scope fault mitigation entities. As discussed previously, this broad scope is necessary to mitigate faults where the faults cannot be entirely mitigated by the storage device or application alone. It is necessary that fault mitigation entities like the HFM enabled application can observe the activities of the fault mitigation entities contained within their fault regions such that they do no harm. Device or application should express what error conditions are to be handled inside their own fault domain and how an HFM enabled application can detect that such fault containment is occurring. State changes on components may be sufficient representation of these activities.

In general, the HFM enabled application fault region mitigation may not necessarily include the same actions that the host, switch, or array may take to fix them.

EXPERIMENTAL

6.4.8 Examples

6.4.8.1 Array Example

6.4.8.1.1 General

The scenario presented is related to a storage array that contains one or many ports. See Figure 11. A port is off-line. This port effects the serving of a volume to a host.

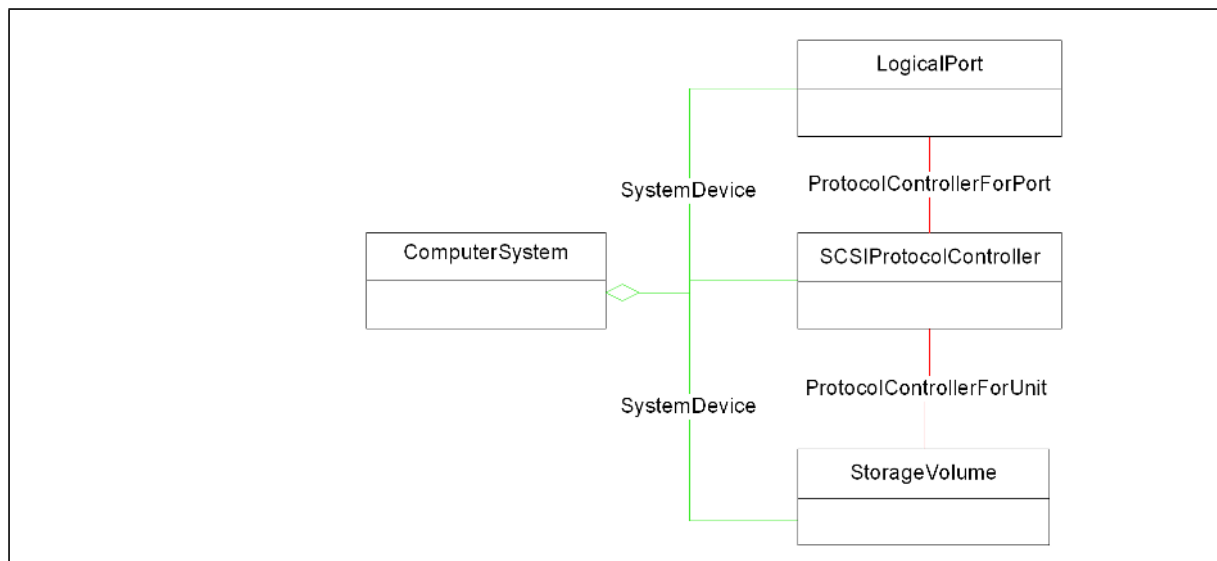


Figure 11 – Array Instance

6.4.8.1.2 Indication

An **AlertIndication** is produced by the array notifying the HFM enabled application of the failure. The indication reports the Object Name of the **ProtocolController** that has failed through its **AlertingManagedElement** property. When storage capacity configuration operations are attempted on storage related to the failed **ProtocolController**, an **Error** is reported. The error reports the Object Name of the **ProtocolController** that has failed through the **ErrorSource** property. **Error** is a class introduced in CIM 2.9 that provides a mechanism to express error number, category, recommended actions and the like.

6.4.8.1.3 Standard Errors

It is mandatory to report error conditions through both **AlertIndication** and **Error** in those cases where **Error** is returned when the method call failed for reasons other than the method call itself. For example, if the device port is down then a method call can fail because of this condition. It is expected that the device will report a port error **AlertIndication** to listening clients as well.

6.4.8.1.4 Operational status and Health State (Polling)

A client that gets the top **Computer** system instance should see an operational status of degraded and a health state of good if the data wasn't lost. At the same time, reading the instance of **Computer** system for the broken controller would see an operational status of "stopped" and a health state of "non-recoverable Error".