

IBM Systems



# **IBM Director Events Reference**

*Version 5.10*

---

**Note**

Before using this information and the product it supports, read the information in Appendix C, "Notices."

**Third Edition (October 2005)**

This edition applies to version 5.10 of IBM Director and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright International Business Machines Corporation 1999, 2005. All rights reserved.**  
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

---

# Contents

Figures . . . . .	19
<b>About this book</b> . . . . .	20
Conventions and terminology . . . . .	20
Related information . . . . .	20
How to send your comments . . . . .	23
<b>What's new in this release</b> . . . . .	24
New events in IBM Director 5.10 . . . . .	24
Changed events in IBM Director 5.10 . . . . .	28
Removed events from IBM Director 5.10 . . . . .	29
<hr/>	
<b>Part 1. Getting started</b> . . . . .	30

<b>Chapter 1. Introducing IBM Director</b> . . . . .	31
<b>Chapter 2. Event management</b> . . . . .	33
Monitoring operating-system specific events . . . . .	34
Processing an event in IBM Director . . . . .	35
Event-action plans. . . . .	36
Event filters . . . . .	37
Event-filter types . . . . .	38
Event-filter criteria . . . . .	40
Event actions . . . . .	44
Message Browser . . . . .	49
<b>Chapter 3. Event-action plan examples</b> . . . . .	50
Restarting Norton AntiVirus sample event-action plan. . . . .	50
Stopping the FreeCell program sample event-action plan. . . . .	52
Restarting a print spooler sample event-action plan. . . . .	54

Chapter 4. Event Action Plans	56
Chapter 5. Event Log	58
<hr/>	
<b>Part 2. Events</b>	<b>59</b>
<b>Chapter 6. Capacity Manager events</b>	<b>60</b>
<b>Chapter 7. CIM events</b>	<b>64</b>
CIM > Certificate	64
CIM > Storage > Array	66
CIM > System	68
CIM > System > Automatic Server Restart	69
CIM > System > DASD Backplane	70
CIM > System > Disk Space Low	71
CIM > System > Error Log	72
CIM > System > Fan	73
CIM > System > IP Change	73
CIM > System > IPMI Log	74
CIM > System > Lease Expiration	75
CIM > System > Life Cycle	76
CIM > System > Memory	77
CIM > System > Memory PFA	78
CIM > System > Network Adapter	79
CIM > System > PFA	81
CIM > System > Power State	82
CIM > System > Processor	84
CIM > System > Processor PFA	85
CIM > System > Redundant Network Adapter Switchback	86
CIM > System > Redundant Network Adapter Switchover	87
CIM > System > Remote Login	88
CIM > System > Server Power Supply	88

CIM > System > ServerRAID Array FlashCopy Complete . . . . .	89
CIM > System > ServerRAID Array FlashCopy Detected . . . . .	90
CIM > System > ServerRAID Array FlashCopy Fail . . . . .	90
CIM > System > ServerRAID Array Rebuild Complete. . . . .	91
CIM > System > ServerRAID Array Rebuild Detected . . . . .	92
CIM > System > ServerRAID Array Rebuild Fail. . . . .	92
CIM > System > ServerRAID Array Sync Complete . . . . .	93
CIM > System > ServerRAID Array Sync Detected . . . . .	94
CIM > System > ServerRAID Array Sync Fail . . . . .	94
CIM > System > ServerRAID Array Sync Fail . . . . .	94
CIM > System > ServerRAID Compaction Complete . . . . .	95
CIM > System > ServerRAID Compaction Detected. . . . .	96
CIM > System > ServerRAID Compaction Fail. . . . .	96
CIM > System > ServerRAID Compression Complete. . . . .	97
CIM > System > ServerRAID Compression Detected . . . . .	98
CIM > System > ServerRAID Compression Fail . . . . .	98
CIM > System > ServerRAID Config Fail . . . . .	99
CIM > System > ServerRAID Controller Added. . . . .	100
CIM > System > ServerRAID Controller Bad Stripes . . . . .	101
CIM > System > ServerRAID Controller Battery Overtemp. . . . .	102
CIM > System > ServerRAID Controller Battery Temp Normal . . . . .	103
CIM > System > ServerRAID Controller Fail . . . . .	103
CIM > System > ServerRAID Controller Failover. . . . .	104
CIM > System > ServerRAID Controller Mismatched Versions. . . . .	105
CIM > System > ServerRAID Controller Replaced . . . . .	106
CIM > System > ServerRAID Copyback Complete . . . . .	106
CIM > System > ServerRAID Copyback Detected . . . . .	107
CIM > System > ServerRAID Copyback Fail . . . . .	108
CIM > System > ServerRAID Dead Battery. . . . .	108
CIM > System > ServerRAID Dead Battery Cache . . . . .	109
CIM > System > ServerRAID Decompression Complete . . . . .	110
CIM > System > ServerRAID Decompression Detected . . . . .	110

CIM > System > ServerRAID Decompression Fail . . . . .	111
CIM > System > ServerRAID Defunct Drive . . . . .	112
CIM > System > ServerRAID Defunct Drive FRU . . . . .	112
CIM > System > ServerRAID Defunct Replaced . . . . .	113
CIM > System > ServerRAID Drive Added . . . . .	113
CIM > System > ServerRAID Drive Clear Complete . . . . .	114
CIM > System > ServerRAID Drive Clear Detected. . . . .	115
CIM > System > ServerRAID Drive Clear Fail . . . . .	115
CIM > System > ServerRAID Drive Removed . . . . .	116
CIM > System > ServerRAID Drive Verify Complete . . . . .	116
CIM > System > ServerRAID Drive Verify Detected . . . . .	117
CIM > System > ServerRAID Drive Verify Fail . . . . .	118
CIM > System > ServerRAID Enclosure Fail . . . . .	118
CIM > System > ServerRAID Enclosure Fan Fail. . . . .	119
CIM > System > ServerRAID Enclosure Fan Installed . . . . .	120
CIM > System > ServerRAID Enclosure Fan OK. . . . .	121
CIM > System > ServerRAID Enclosure Fan Removed . . . . .	121
CIM > System > ServerRAID Enclosure OK . . . . .	122
CIM > System > ServerRAID Enclosure Power Supply Fail . . . . .	123
CIM > System > ServerRAID Enclosure Power Supply Installed . . . . .	123
CIM > System > ServerRAID Enclosure Power Supply OK. . . . .	124
CIM > System > ServerRAID Enclosure Power Supply Removed . . . . .	125
CIM > System > ServerRAID Enclosure Temp Fail. . . . .	126
CIM > System > ServerRAID Enclosure Temp OK . . . . .	126
CIM > System > ServerRAID Expansion Complete. . . . .	127
CIM > System > ServerRAID Expansion Detected . . . . .	127
CIM > System > ServerRAID Expansion Fail. . . . .	128
CIM > System > ServerRAID FlashCopy Complete . . . . .	129
CIM > System > ServerRAID FlashCopy Detected. . . . .	129
CIM > System > ServerRAID FlashCopy Fail. . . . .	130
CIM > System > ServerRAID Health Event. . . . .	131

CIM > System > ServerRAID Init Complete . . . . .	132
CIM > System > ServerRAID Init Detected . . . . .	132
CIM > System > ServerRAID Init Fail. . . . .	133
CIM > System > ServerRAID Logical Drive Added . . . . .	134
CIM > System > ServerRAID Logical Drive Blocked . . . . .	134
CIM > System > ServerRAID Logical Drive Critical. . . . .	135
CIM > System > ServerRAID Logical Drive Critical Periodic . . . . .	136
CIM > System > ServerRAID Logical Drive Off Line . . . . .	136
CIM > System > ServerRAID Logical Drive OK. . . . .	137
CIM > System > ServerRAID Logical Drive Removed . . . . .	137
CIM > System > ServerRAID Logical Drive Unblocked. . . . .	138
CIM > System > ServerRAID Migration Complete . . . . .	138
CIM > System > ServerRAID Migration Detected. . . . .	139
CIM > System > ServerRAID Migration Fail . . . . .	139
CIM > System > ServerRAID No Controllers . . . . .	140
CIM > System > ServerRAID PFA Drive . . . . .	141
CIM > System > ServerRAID PFA Drive FRU . . . . .	141
CIM > System > ServerRAID Polling Fail. . . . .	142
CIM > System > ServerRAID Rebuild Complete . . . . .	143
CIM > System > ServerRAID Rebuild Detected . . . . .	143
CIM > System > ServerRAID Rebuild Fail . . . . .	144
CIM > System > ServerRAID Sync Complete . . . . .	145
CIM > System > ServerRAID Sync Detected. . . . .	145
CIM > System > ServerRAID Sync Fail. . . . .	146
CIM > System > ServerRAID Test Event . . . . .	147
CIM > System > ServerRAID Unsupported Drive. . . . .	147
CIM > System > SMART Drive . . . . .	148
CIM > System > System Enclosure . . . . .	148
CIM > System > System Event . . . . .	149
CIM > System > Temperature . . . . .	150
CIM > System > Voltage . . . . .	152

CIM > System > Warranty Expiration . . . . .	153
CIM > Windows NT Event Log . . . . .	154
CIM > Windows NT Service . . . . .	154
CIM > Windows Registry . . . . .	154
<b>Chapter 8. Configuration Manager events.</b> . . . . .	<b>155</b>
Configuration Manager > Profile . . . . .	155
<b>Chapter 9. Director events</b> . . . . .	<b>158</b>
Director > Console . . . . .	159
Director > Console > Logon Failure . . . . .	159
Director > Console > User Logoff . . . . .	162
Director > Console > User Logon . . . . .	163
Director > Database . . . . .	163
Director > Director Agent. . . . .	165
Director > Director Agent > MPA. . . . .	165
Director > Director Agent > Process Monitors . . . . .	166
Director > Director Agent > Resource Monitors . . . . .	169
Director > Inventory . . . . .	171
Director > Inventory > Custom Collection . . . . .	171
Director > Inventory > Inventory Monitor . . . . .	173
Director > mib . . . . .	174
Director > Scheduler . . . . .	178
Director > Scheduler > Job . . . . .	179
Director > Scheduler > System . . . . .	181
Director > Test . . . . .	183
Director > Topology . . . . .	184
<b>Chapter 10. Mass Configuration events</b> . . . . .	<b>185</b>
<b>Chapter 11. MPA events</b> . . . . .	<b>187</b>
MPA > Component . . . . .	189



MPA > Component > Blade Server . . . . .	190
MPA > Component > Bus . . . . .	192
MPA > Component > Chassis . . . . .	193
MPA > Component > CPU . . . . .	196
MPA > Component > DASD . . . . .	198
MPA > Component > DIMM . . . . .	200
MPA > Component > Fan . . . . .	201
MPA > Component > Hardware Information . . . . .	203
MPA > Component > I/O Module . . . . .	205
MPA > Component > KVM . . . . .	207
MPA > Component > OS Image . . . . .	208
MPA > Component > PFA . . . . .	210
MPA > Component > Power Subsystem . . . . .	211
MPA > Component > Power Supply . . . . .	214
MPA > Component > Server . . . . .	216
MPA > Component > Service Processor . . . . .	218
MPA > Component > SMP Expansion Module . . . . .	222
MPA > Component > USB . . . . .	224
MPA > Component > VRM . . . . .	225
MPA > Environmental . . . . .	226
MPA > Miscellaneous . . . . .	236
MPA > Platform . . . . .	237
MPA > Server WatchDog. . . . .	238
MPA > Unknown . . . . .	239
<b>Chapter 12. PET events . . . . .</b>	<b>241</b>
PET > Environmental . . . . .	242
PET > Environmental > Sensor . . . . .	242
PET > Firmware . . . . .	246
PET > Firmware > BIOS . . . . .	246
PET > Hardware . . . . .	248

PET > System . . . . .	252
PET > System > OS . . . . .	253
<b>Chapter 13. SNMP events . . . . .</b>	<b>255</b>
SNMP > Hardware . . . . .	256
ibmSystemMIB . . . . .	257
ibmSystemTrapChassis . . . . .	258
ibmSystemTrapDASDBackplane . . . . .	259
ibmSystemTrapErrorLog . . . . .	259
ibmSystemTrapFan . . . . .	260
ibmSystemTrapGenericFan . . . . .	261
ibmSystemTrapGenericVoltage . . . . .	262
ibmSystemTrapLeaseExpiration . . . . .	263
ibmSystemTrapMemoryPF . . . . .	264
ibmSystemTrapNetworkAdapterFailed . . . . .	265
ibmSystemTrapNetworkAdapterOffline . . . . .	266
ibmSystemTrapNetworkAdapterOnline . . . . .	266
ibmSystemTrapPFA . . . . .	267
ibmSystemTrapPowerSupply . . . . .	268
ibmSystemTrapProcessorPF . . . . .	269
ibmSystemTrapRedundantNIC . . . . .	270
ibmSystemTrapRedundantNICSwitchback . . . . .	270
ibmSystemTrapRedundantNICSwitchover . . . . .	271
ibmSystemTrapRemotelogin . . . . .	271
ibmSystemTrapsSMART . . . . .	272
ibmSystemTrapsPPowerSupply . . . . .	273
ibmSystemTrapStorage . . . . .	274
ibmSystemTrapTemperature . . . . .	275
ibmSystemTrapVoltage . . . . .	276
ibmSystemTrapWarrantyExpiration . . . . .	277
ibmServerRAIDMIB . . . . .	278

iBMServerRAIDArrayFlashCopyComplete . . . . .	279
iBMServerRAIDArrayFlashCopyDetected . . . . .	280
iBMServerRAIDArrayFlashCopyFail . . . . .	281
iBMServerRAIDArrayRebuildComplete . . . . .	282
iBMServerRAIDArrayRebuildDetected . . . . .	282
iBMServerRAIDArrayRebuildFail . . . . .	283
iBMServerRAIDArraySyncComplete . . . . .	284
iBMServerRAIDArraySyncDetected . . . . .	284
iBMServerRAIDArraySyncFail . . . . .	285
iBMServerRAIDCompactionComplete . . . . .	286
iBMServerRAIDCompactionDetected . . . . .	287
iBMServerRAIDCompactionFail . . . . .	287
iBMServerRAIDCompressionComplete . . . . .	288
iBMServerRAIDCompressionDetected . . . . .	289
iBMServerRAIDCompressionFail . . . . .	290
iBMServerRAIDConfigFail . . . . .	291
iBMServerRAIDControllerAdded . . . . .	291
iBMServerRAIDControllerBadStripes . . . . .	292
iBMServerRAIDControllerBatteryOvertemp . . . . .	294
iBMServerRAIDControllerBatteryTempNormal . . . . .	294
iBMServerRAIDControllerFail . . . . .	295
iBMServerRAIDControllerFailover . . . . .	296
iBMServerRAIDControllerReplaced . . . . .	296
iBMServerRAIDCopyBackComplete . . . . .	297
iBMServerRAIDCopyBackDetected . . . . .	298
iBMServerRAIDCopyBackFail . . . . .	299
iBMServerRAIDDeadBattery . . . . .	299
iBMServerRAIDDeadBatteryCache . . . . .	300
iBMServerRAIDDecompressionComplete . . . . .	301
iBMServerRAIDDecompressionDetected . . . . .	302
iBMServerRAIDDecompressionFail . . . . .	302

iBMServerRAIDDefunctDrive . . . . .	303
iBMServerRAIDDefunctDriveFRU . . . . .	304
iBMServerRAIDDefunctReplaced . . . . .	305
iBMServerRAIDDriveAdded . . . . .	306
iBMServerRAIDDriveClearComplete . . . . .	306
iBMServerRAIDDriveClearDetected. . . . .	307
iBMServerRAIDDriveClearFail . . . . .	308
iBMServerRAIDDriveRemoved . . . . .	309
iBMServerRAIDDriveVerifyComplete . . . . .	310
iBMServerRAIDDriveVerifyDetected . . . . .	310
iBMServerRAIDDriveVerifyFail . . . . .	311
iBMServerRAIDEnclosureFail . . . . .	312
iBMServerRAIDEnclosureFanOK . . . . .	313
iBMServerRAIDEnclosureOK . . . . .	314
iBMServerRAIDExpansionComplete . . . . .	315
iBMServerRAIDExpansionDetected. . . . .	315
iBMServerRAIDExpansionFail . . . . .	316
iBMServerRAIDFanFail . . . . .	317
iBMServerRAIDFanInstalled . . . . .	318
iBMServerRAIDFanRemoved . . . . .	319
iBMServerRAIDFlashCopyComplete . . . . .	320
iBMServerRAIDFlashCopyDetected . . . . .	320
iBMServerRAIDFlashCopyFail . . . . .	321
iBMServerRAIDInitComplete . . . . .	322
iBMServerRAIDInitDetected. . . . .	323
iBMServerRAIDInitFail . . . . .	323
iBMServerRAIDLogicalDriveAdded . . . . .	324
iBMServerRAIDLogicalDriveBlocked . . . . .	325
iBMServerRAIDLogicalDriveCritical . . . . .	326
iBMServerRAIDLogicalDriveCriticalPeriodic. . . . .	327
iBMServerRAIDLogicalDriveOffline. . . . .	328

iBMServerRAIDLlogicalDriveOK . . . . .	329
iBMServerRAIDLlogicalDriveRemoved . . . . .	329
iBMServerRAIDLlogicalDriveUnblocked . . . . .	330
iBMServerRAIDMigrationComplete . . . . .	331
iBMServerRAIDMigrationDetected . . . . .	331
iBMServerRAIDMigrationFail . . . . .	332
iBMServerRAIDNoControllers . . . . .	333
iBMServerRAIDPFADrive . . . . .	334
iBMServerRAIDPFADriveFRU . . . . .	334
iBMServerRAIDPollingFail . . . . .	335
iBMServerRAIDPowerSupplyFail . . . . .	336
iBMServerRAIDPowerSupplyInstalled. . . . .	337
iBMServerRAIDPowerSupplyOK . . . . .	338
iBMServerRAIDPowerSupplyRemoved . . . . .	339
iBMServerRAIDRebuildComplete . . . . .	339
iBMServerRAIDRebuildDetected . . . . .	340
iBMServerRAIDRebuildFail . . . . .	341
iBMServerRAIDSyncComplete . . . . .	341
iBMServerRAIDSyncDetected . . . . .	342
iBMServerRAIDSyncFail . . . . .	343
iBMServerRAIDTempFail . . . . .	344
iBMServerRAIDTempOK . . . . .	345
iBMServerRAIDTestEvent. . . . .	345
iBMServerRAIDUnsupportedDrive . . . . .	346
iBMServerRAIDVersionMismatch . . . . .	347
SNMP > Software . . . . .	347

<b>Chapter 14. Storage events . . . . .</b>	<b>349</b>
---	------------

<b>Chapter 15. System Availability events . . . . .</b>	<b>350</b>
---	------------

<b>Chapter 16. Windows Event Log events. . . . .</b>	<b>351</b>
--	------------

<b>Part 3. Events categorized by goal</b> . . . . .	<b>353</b>
Chapter 17. Events associated with BladeCenter products . . . . .	354
Chapter 18. Events associated with system environments . . . . .	358
Chapter 19. Events associated with hardware component failures . . . . .	359
Chapter 20. Events associated with ServeRAID products . . . . .	361
Chapter 21. Events associated with service processors . . . . .	369
<b>Part 4. Supplementary information</b> . . . . .	<b>371</b>
<b>Chapter 22. Extended attributes and variable-binding information</b> . . . . .	<b>372</b>
Extended attributes for CIM events . . . . .	372
Extended attributes for HMC CIM events . . . . .	372
Extended attributes for the Director > Director Agent events. . . . .	373
Extended attributes for the Director > Scheduler events. . . . .	373
Extended attributes for MPA events . . . . .	374
Extended attributes for PET events . . . . .	374
Variable-binding information for IBM Director SNMP events. . . . .	376
Variable-binding information for IBM Director SNMP ServeRAID events. . . . .	377
<b>Chapter 23. CIM indications in IBM Director</b> . . . . .	<b>378</b>
IBMPMSG_ChassisEvent CIM indication . . . . .	378
IBMPMSG_DASDBackplaneEvent CIM indication . . . . .	379
IBMPMSG_ErrorLogEvent CIM indication . . . . .	380
IBMPMSG_FanEvent CIM indication. . . . .	381
IBMPMSG_GenericFanEvent CIM indication . . . . .	382
IBMPMSG_GenericVoltageEvent CIM indication. . . . .	382
IBMPMSG_LeaseExpirationEvent CIM indication . . . . .	383
IBMPMSG_MemoryPFEEvent CIM indication . . . . .	384

IBMPSG_NetworkAdapterFailedEvent CIM indication . . . . .	385
IBMPSG_NetworkAdapterOfflineEvent CIM indication . . . . .	386
IBMPSG_NetworkAdapterOnlineEvent CIM indication . . . . .	386
IBMPSG_PFAEvent CIM indication . . . . .	387
IBMPSG_PowerSupplyEvent CIM indication . . . . .	388
IBMPSG_ProcessorPFEEvent CIM indication . . . . .	389
IBMPSG_RedundantNetworkAdapterEvent CIM indication. . . . .	390
IBMPSG_RedundantNetworkAdapterSwitchbackEvent CIM indication. . . . .	390
IBMPSG_RedundantNetworkAdapterSwitchoverEvent CIM indication . . . . .	391
IBMPSG_RemoteloginEvent CIM indication. . . . .	392
IBMPSG_ServerRAIDArrayFlashCopyComplete CIM indication . . . . .	393
IBMPSG_ServerRAIDArrayFlashCopyDetected CIM indication . . . . .	394
IBMPSG_ServerRAIDArrayFlashCopyFail CIM indication . . . . .	394
IBMPSG_ServerRAIDArrayRebuildComplete CIM indication . . . . .	395
IBMPSG_ServerRAIDArrayRebuildDetected CIM indication . . . . .	395
IBMPSG_ServerRAIDArrayRebuildFail CIM indication . . . . .	396
IBMPSG_ServerRAIDArraySyncComplete CIM indication . . . . .	396
IBMPSG_ServerRAIDArraySyncDetected CIM indication . . . . .	397
IBMPSG_ServerRAIDArraySyncFail CIM indication . . . . .	397
IBMPSG_ServerRAIDCompactionComplete CIM indication. . . . .	398
IBMPSG_ServerRAIDCompactionDetected CIM indication . . . . .	398
IBMPSG_ServerRAIDCompactionFail CIM indication. . . . .	399
IBMPSG_ServerRAIDCompressionComplete CIM indication . . . . .	400
IBMPSG_ServerRAIDCompressionDetected CIM indication . . . . .	400
IBMPSG_ServerRAIDCompressionFail CIM indication . . . . .	401
IBMPSG_ServerRAIDConfigFail CIM indication . . . . .	401
IBMPSG_ServerRAIDControllerAdded CIM indication . . . . .	402
IBMPSG_ServerRAIDControllerBadStripes CIM indication . . . . .	402
IBMPSG_ServerRAIDControllerBatteryOvertemp CIM indication . . . . .	403
IBMPSG_ServerRAIDControllerBatteryTempNormal CIM indication . . . . .	403
IBMPSG_ServerRAIDControllerFail CIM indication . . . . .	404

IBMPSG_ServerRAIDControllerFailover CIM indication . . . . .	404
IBMPSG_ServerRAIDControllerMismatchedVersions CIM indication . . . . .	405
IBMPSG_ServerRAIDControllerReplaced CIM indication . . . . .	405
IBMPSG_ServerRAIDCopyBackComplete CIM indication . . . . .	406
IBMPSG_ServerRAIDCopyBackDetected CIM indication . . . . .	406
IBMPSG_ServerRAIDCopyBackFail CIM indication . . . . .	407
IBMPSG_ServerRAIDDeadBattery CIM indication . . . . .	407
IBMPSG_ServerRAIDDeadBatteryCache CIM indication . . . . .	408
IBMPSG_ServerRAIDDecompressionComplete CIM indication . . . . .	408
IBMPSG_ServerRAIDDecompressionDetected CIM indication . . . . .	409
IBMPSG_ServerRAIDDecompressionFail CIM indication . . . . .	410
IBMPSG_ServerRAIDDefunctDrive CIM indication . . . . .	410
IBMPSG_ServerRAIDDefunctDriveFRU CIM indication . . . . .	411
IBMPSG_ServerRAIDDefunctReplaced CIM indication . . . . .	411
IBMPSG_ServerRAIDDriveAdded CIM indication . . . . .	412
IBMPSG_ServerRAIDDriveClearComplete CIM indication . . . . .	412
IBMPSG_ServerRAIDDriveClearDetected CIM indication . . . . .	413
IBMPSG_ServerRAIDDriveClearFail CIM indication . . . . .	413
IBMPSG_ServerRAIDDriveRemoved CIM indication . . . . .	414
IBMPSG_ServerRAIDDriveVerifyComplete CIM indication . . . . .	414
IBMPSG_ServerRAIDDriveVerifyDetected CIM indication . . . . .	415
IBMPSG_ServerRAIDDriveVerifyFail CIM indication . . . . .	415
IBMPSG_ServerRAIDEnclosureFail CIM indication . . . . .	416
IBMPSG_ServerRAIDEnclosureFanFail CIM indication . . . . .	416
IBMPSG_ServerRAIDEnclosureFanInstalled CIM indication . . . . .	417
IBMPSG_ServerRAIDEnclosureFanOK CIM indication . . . . .	418
IBMPSG_ServerRAIDEnclosureFanRemoved CIM indication . . . . .	418
IBMPSG_ServerRAIDEnclosureOK CIM indication . . . . .	419
IBMPSG_ServerRAIDEnclosurePowerSupplyFail CIM indication . . . . .	419
IBMPSG_ServerRAIDEnclosurePowerSupplyInstalled CIM indication . . . . .	420
IBMPSG_ServerRAIDEnclosurePowerSupplyOK CIM indication . . . . .	420



IBMPSSG_ServerRAIDEnclosurePowerSupplyRemoved CIM indication . . . . .	421
IBMPSSG_ServerRAIDEnclosureTempFail CIM indication . . . . .	421
IBMPSSG_ServerRAIDEnclosureTempOK CIM indication . . . . .	422
IBMPSSG_ServerRAIDExpansionComplete CIM indication . . . . .	422
IBMPSSG_ServerRAIDExpansionDetected CIM indication . . . . .	423
IBMPSSG_ServerRAIDExpansionFail CIM indication . . . . .	424
IBMPSSG_ServerRAIDFlashCopyComplete CIM indication . . . . .	424
IBMPSSG_ServerRAIDFlashCopyDetected CIM indication . . . . .	425
IBMPSSG_ServerRAIDFlashCopyFail CIM indication . . . . .	425
IBMPSSG_ServerRAIDInitComplete CIM indication . . . . .	426
IBMPSSG_ServerRAIDInitDetected CIM indication . . . . .	426
IBMPSSG_ServerRAIDInitFail CIM indication . . . . .	427
IBMPSSG_ServerRAIDLogicalDriveAdded CIM indication . . . . .	427
IBMPSSG_ServerRAIDLogicalDriveBlocked CIM indication . . . . .	428
IBMPSSG_ServerRAIDLogicalDriveCritical CIM indication . . . . .	428
IBMPSSG_ServerRAIDLogicalDriveCriticalPeriodic CIM indication . . . . .	429
IBMPSSG_ServerRAIDLogicalDriveOffline CIM indication . . . . .	429
IBMPSSG_ServerRAIDLogicalDriveOK CIM indication . . . . .	430
IBMPSSG_ServerRAIDLogicalDriveRemoved CIM indication . . . . .	430
IBMPSSG_ServerRAIDLogicalDriveUnblocked CIM indication . . . . .	431
IBMPSSG_ServerRAIDMigrationComplete CIM indication . . . . .	431
IBMPSSG_ServerRAIDMigrationDetected CIM indication . . . . .	432
IBMPSSG_ServerRAIDMigrationFail CIM indication . . . . .	433
IBMPSSG_ServerRAIDNoControllers CIM indication . . . . .	433
IBMPSSG_ServerRAIDPFADrive CIM indication . . . . .	434
IBMPSSG_ServerRAIDPFADriveFRU CIM indication . . . . .	434
IBMPSSG_ServerRAIDPollingFail CIM indication . . . . .	435
IBMPSSG_ServerRAIDRebuildComplete CIM indication . . . . .	435
IBMPSSG_ServerRAIDRebuildDetected CIM indication . . . . .	436
IBMPSSG_ServerRAIDRebuildFail CIM indication . . . . .	436
IBMPSSG_ServerRAIDSyncComplete CIM indication . . . . .	437

IBMPSG_ServerRAIDSyncDetected CIM indication . . . . .	437
IBMPSG_ServerRAIDSyncFail CIM indication . . . . .	438
IBMPSG_ServerRAIDTestEvent CIM indication. . . . .	438
IBMPSG_ServerRAIDUnsupportedDrive CIM indication . . . . .	439
IBMPSG_SMARTEvent CIM indication. . . . .	439
IBMPSG_SPPowerSupplyEvent CIM indication . . . . .	440
IBMPSG_StorageEvent CIM indication . . . . .	441
IBMPSG_TemperatureEvent CIM indication . . . . .	442
IBMPSG_VoltageEvent CIM indication. . . . .	443
IBMPSG_WarrantyExpirationEvent CIM indication. . . . .	443
<b>Appendix A. Configuring ASF . . . . .</b>	<b>445</b>
<b>Appendix B. Preparing to install IBM Director on an xSeries server . . . . .</b>	<b>447</b>
<b>Appendix C. Notices . . . . .</b>	<b>449</b>
Trademarks . . . . .	451
<b>Abbreviations, Acronyms, and Glossary . . . . .</b>	<b>454</b>
Abbreviation and acronym list . . . . .	454
Glossary . . . . .	460
<b>Index . . . . .</b>	<b>477</b>

# Figures

1. Hardware in an IBM Director environment . . . . .	32
2. SNMP string variable example . . . . .	176
3. SNMP integer variable example . . . . .	177

---

## About this book

This book provides information about IBM Director events. Depending on the event, this information can include:

- Event type
- Description
- Severity
- Whether it is an alert or resolution
- Extended attributes

This book also provides planning and implementation information for event management.

---

## Conventions and terminology

These notices are designed to highlight key information:

**Note:** These notices provide important tips, guidance, or advice.

**Important:** These notices provide information or advice that might help you avoid inconvenient or difficult situations.

**Attention:** These notices indicate possible damage to programs, devices, or data. An attention notice appears before the instruction or situation in which damage can occur.

---

## Related information

This topic provides links to additional information related to IBM Director.

### **IBM Director resources on the World Wide Web**

The following Web pages provide resources for understanding, using, and troubleshooting IBM Director and other systems-management tools.

## **IBM Director information center**

[publib.boulder.ibm.com/infocenter/eserver/v1r2/topic/dirinfo/fqm0\\_main.html](http://publib.boulder.ibm.com/infocenter/eserver/v1r2/topic/dirinfo/fqm0_main.html)

Updated periodically, the IBM Director information center contains the most up-to-date documentation available on a wide range of topics.

## **IBM Director Web site on ibm.com®**

[www.ibm.com/servers/eserver/xseries/systems\\_management/ibm\\_director/](http://www.ibm.com/servers/eserver/xseries/systems_management/ibm_director/)

The IBM Director Web site on [ibm.com](http://ibm.com) has links to downloads and documentation for all currently supported versions of IBM Director. Information on this site includes:

- IBM Director 5.10 - downloads and documentation
- IBM Director 4.22 - downloads and documentation
- IBM Director 4.22 Upward Integration Modules (UIMs) - downloads and documentation
- IBM Director 4.21 - downloads and documentation
- IBM Director 4.20 - downloads and documentation
- IBM Director Hardware and Software Compatibility document - lists supported ®server and IBM® xSeries® systems, as well as all supported operating systems. It is updated every 6 to 8 weeks.
- Printable documentation for IBM Director - available in Portable Document Format (PDF) in several languages

## **IBM Systems Software information center**

[www.ibm.com/servers/library/infocenter/](http://www.ibm.com/servers/library/infocenter/)

This Web page provides information about IBM Virtualization Engine™, IBM Director, and other topics.

## **IBM ServerProven® page**

[www.ibm.com/pc/us/compat/index.html](http://www.ibm.com/pc/us/compat/index.html)

This Web page provides information about IBM xSeries, BladeCenter®, and IntelliStation® hardware compatibility with IBM Director.

## **IBM Systems Management Software: Download/Electronic Support page**

[www.ibm.com/servers/eserver/xseries/systems\\_management/ibm\\_director/](http://www.ibm.com/servers/eserver/xseries/systems_management/ibm_director/)

Use this Web page to download IBM systems-management software, including IBM Director. Check this Web page regularly for new IBM Director releases and updates.

## **IBM Servers**

[www.ibm.com/servers/](http://www.ibm.com/servers/)

This Web page on [ibm.com](http://ibm.com) links to information, downloads, and IBM Director extensions such as Remote Deployment Manager, Capacity Manager, Systems Availability and Software Distribution (Premium Edition) for IBM servers:

- IBM BladeCenter
- IBM iSeries™
- IBM pSeries®
- IBM xSeries
- IBM zSeries®

## **IBM Redbooks™**

[www.ibm.com/redbooks/](http://www.ibm.com/redbooks/)

You can download the following documents from the IBM Redbooks Web page. You also might want to search this Web page for documents that focus on specific IBM hardware; such documents often contain systems-management material.

**Note:** Be sure to note the date of publication and to determine the level of IBM Director software to which the Redbooks publication refers.

- *Creating a Report of the Tables in the IBM Director 4.1 Database* (TIPS0185)
- *IBM Director Security* (REDP-0417-00)
- *IBM eServer™ BladeCenter Systems Management with IBM Director V4.1 and Remote Deployment Manager V4.1* (REDP-3776-00)
- *Implementing Systems Management Solutions using IBM Director* (SG24-6188)
- *Integrating IBM Director with Enterprise Management Solutions* (SG24-5388)
- *Managing IBM TotalStorage® NAS with IBM Director* (SG24-6830)

- *Monitoring Redundant Uninterruptible Power Supplies Using IBM Director (REDP-3827-00)*

## **Remote Supervisor Adapter**

### **Remote Supervisor Adapter overview**

[www.ibm.com/support/docview.wss?uid=psg1MIGR-4UKSML](http://www.ibm.com/support/docview.wss?uid=psg1MIGR-4UKSML)

This Web page includes links to the *Remote Supervisor Adapter User's Guide* and *Remote Supervisor Adapter Installation Guide*.

### **Remote Supervisor Adapter II overview**

[www.ibm.com/support/docview.wss?uid=psg1MIGR-50116](http://www.ibm.com/support/docview.wss?uid=psg1MIGR-50116)

This Web page includes information about the Remote Supervisor Adapter II.

## **Other documents**

For planning purposes, the following documents might be of interest:

- *Planning and installation guide - IBM eServer BladeCenter (Type 8677)*
- *IBM Management Processor Command-Line Utility User's Guide version 3.00*

---

## **How to send your comments**

Your feedback is important in helping to provide the most accurate and highest quality information. If you have any comments about this book or any other IBM Director publication, use the form for reader's comments is provided at the back of this publication. If the form has been removed, you may address your comments to:

International Business Machines Corporation  
Design & Information Development  
Department CGFA  
PO Box 12195  
Research Triangle Park, NC 27709-9990  
U.S.A.

---

## What's new in this release

In this release, a number of events have been added, changed, or removed.

---

### New events in IBM Director 5.10

IBM Director 5.10 provides new events to provide new or improved support for IBM hardware.

#### CIM > Certificate event

- “CIM > Certificate” on page 64

#### CIM > System events

- Automatic Server Restart
- IP Change
- IPMI Log
- Life Cycle
- Memory
- Power State
- ServerRAID™ Array FlashCopy® Complete
- ServerRAID Array FlashCopy Detected
- ServerRAID Array FlashCopy Fail
- ServerRAID Array Rebuild Complete
- ServerRAID Array Rebuild Detected
- ServerRAID Array Rebuild Fail
- ServerRAID Array Sync Complete
- ServerRAID Array Sync Detected
- ServerRAID Array Sync Fail
- ServerRAID Compaction Complete



- ServerRAID Compaction Detected
- ServerRAID Compaction Fail
- ServerRAID Compression Complete
- ServerRAID Compression Detected
- ServerRAID Compression Fail
- ServerRAID Config Fail
- ServerRAID Controller Added
- ServerRAID Controller Bad Stripes
- ServerRAID Controller Battery Overtemp
- ServerRAID Controller Battery Temp Normal
- ServerRAID Controller Fail
- ServerRAID Controller Failover
- ServerRAID Controller Mismatched Versions
- ServerRAID Controller Replaced
- ServerRAID Copyback Complete
- ServerRAID Copyback Detected
- ServerRAID Copyback Fail
- ServerRAID Dead Battery
- ServerRAID Dead Battery Cache
- ServerRAID Decompression Complete
- ServerRAID Decompression Detected
- ServerRAID Decompression Fail
- ServerRAID Defunct Drive
- ServerRAID Defunct Drive FRU
- ServerRAID Defunct Replaced
- ServerRAID Drive Added

- ServerRAID Drive Clear Complete
- ServerRAID Drive Clear Detected
- ServerRAID Drive Clear Fail
- ServerRAID Drive Removed
- ServerRAID Drive Verify Complete
- ServerRAID Drive Verify Detected
- ServerRAID Drive Verify Fail
- ServerRAID Enclosure Fail
- ServerRAID Enclosure Fan Fail
- ServerRAID Enclosure Fan Installed
- ServerRAID Enclosure Fan OK
- ServerRAID Enclosure Fan Removed
- ServerRAID Enclosure OK
- ServerRAID Enclosure Power Supply Fail
- ServerRAID Enclosure Power Supply Installed
- ServerRAID Enclosure Power Supply OK
- ServerRAID Enclosure Power Supply Removed
- ServerRAID Enclosure Temp Fail
- ServerRAID Enclosure Temp OK
- ServerRAID Expansion Complete
- ServerRAID Expansion Detected
- ServerRAID Expansion Fail
- ServerRAID FlashCopy Complete
- ServerRAID FlashCopy Detected
- ServerRAID FlashCopy Fail
- ServerRAID Init Complete

- ServerRAID Init Detected
- ServerRAID Init Fail
- ServerRAID Logical Drive Added
- ServerRAID Logical Drive Blocked
- ServerRAID Logical Drive Critical
- ServerRAID Logical Drive Critical Periodic
- ServerRAID Logical Drive Off Line
- ServerRAID Logical Drive OK
- ServerRAID Logical Drive Removed
- ServerRAID Logical Drive Unblocked
- ServerRAID Migration Complete
- ServerRAID Migration Detected
- ServerRAID Migration Fail
- ServerRAID No Controllers
- ServerRAID PFA Drive
- ServerRAID PFA Drive FRU
- ServerRAID Polling Fail
- ServerRAID Rebuild Complete
- ServerRAID Rebuild Detected
- ServerRAID Rebuild Fail
- ServerRAID Sync Complete
- ServerRAID Sync Detected
- ServerRAID Sync Fail
- ServerRAID Test Event
- ServerRAID Unsupported Drive
- System Event

## **Configuration Manager events**

- Configuration Manager

## **Director events**

- Director > Database
  - Director > Inventory
- 

## **Changed events in IBM Director 5.10**

IBM Director 5.10 provides events that have been changed from previous releases.

### **CIM > Director Agent Events**

The CIM > Director Agent Events events have been changed. They are now CIM > System events.

- DASD Backplane
- Disk Space Low
- Error Log
- Fan
- Lease Expiration
- Memory PFA
- Network Adapter
- PFA
- Processor
- Processor PFA
- Redundant Network Adapter SwitchBack
- Redundant Network Adapter SwitchOver
- Remote Login
- Server Power Supply
- ServerRAID Health Event

This event type has been retained to provide compatibility for previous supported versions of IBM Director Agent that might be present in an IBM Director Server 5.10 environment. For IBM Director Agent 5.10, use the new CIM > System > ServerRAID event types. Using the new event types, you can create event-action plans that can be triggered by a number of changes in the ServerRAID environment.

- SMART Drive
- System Enclosure
- Temperature
- Voltage
- Warranty Expiration

## **MPA events**

The MPA > Deployment events have been changed. They are now MPA > Server WatchDog events.

---

## **Removed events from IBM Director 5.10**

IBM Director 5.10 no longer supports some event types. This can be because of product withdrawal or a new implementation.

- BladeCenter Assistant > Component > Deployment wizard  
This event type has been replaced with the Configuration Manager event types.
- CIM > Director Agent Events > LAN Leash
- MPA > Component > Service Processor > Remote Login
- The SNMP trap event type IBMPSGLANLeashEvent

This SNMP trap is still present in the MIB file, but it is deprecated.

# **Part 1. Getting started**

---

# Chapter 1. Introducing IBM Director

This topic provides an overview of IBM Director.

IBM Director is an integrated, easy-to-use suite of tools that provide you with comprehensive systems-management capabilities to help realize maximum system availability and lower IT costs. Its open, industry-standard design enables heterogeneous-hardware management and broad operating-system support, including most Intel® microprocessor-based systems and certain IBM @SERVER System p5®, iSeries, pSeries, System z9®, and zSeries servers.

IBM Director automates many of the processes that are required to manage systems proactively, including capacity planning, asset tracking, preventive maintenance, diagnostic monitoring, troubleshooting, and more. It has a graphical user interface that provides easy access to both local and remote systems.

IBM Director can be used in environments with multiple operating systems and integrated with robust workgroup and enterprise management software from IBM (such as Tivoli® software), Computer Associates, Hewlett-Packard, Microsoft®, NetIQ, and BMC Software.

## IBM Director environment

IBM Director is designed to manage a complex environment that contains numerous servers, desktop computers, workstations, mobile computers (notebook computers), and assorted devices. IBM Director can manage up to 5000 Level-2 systems.

An IBM Director environment contains the following groups of hardware:

- One or more servers on which IBM Director Server is installed. Such servers are called *management servers*.
- Servers, workstations, desktop computers, and mobile computers that are managed by IBM Director. Such systems are called *managed systems*.
- Network devices, printers, or computers that have Simple Network Management Protocol (SNMP) agents installed or embedded. Such devices are called *SNMP devices*.

- Additional managed objects such as platforms and chassis. Collectively, all managed systems, devices, and objects are referred to as *managed objects*.

Figure 1 shows the hardware in an IBM Director environment.

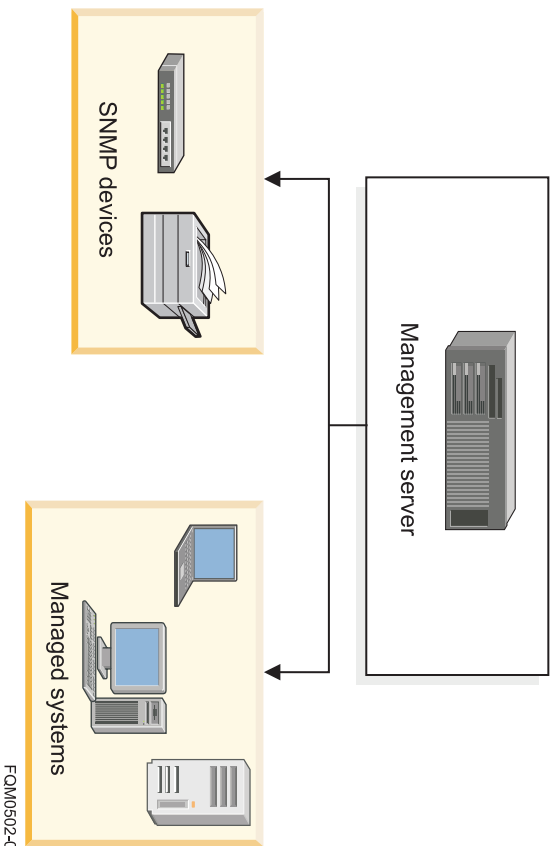


Figure 1. Hardware in an IBM Director environment



---

## Chapter 2. Event management

An *event* is an occurrence of significance to a task, system, or managed object, such as the completion or failure of an operation. In a system-management environment, IBM Director Server receives events, traps, and notifications from many sources.

These sources include, but are not limited to, the following programs and protocols:

- IBM Director native events generated by IBM Director Agent
- CIM indications from the CIMOM that is installed as part of IBM Director Agent and IBM Director Core Services
- Microsoft Windows® event log
- Windows Management Instrumentation (WMI)
- SNMP traps through out-of-band communication
- Platform Event Traps (PET) through out-of-band communication from Alert Standard Format (ASF)-capable systems and Intelligent Platform Management Interface (IPMI)-capable systems
- IBM service processors notifications through out-of-band communication

When IBM Director Server receives these events or notifications, it converts them into IBM Director events. For example, when IBM Director Server receives a CIM indication, it converts the CIM indication into an IBM Director event of the type CIM. When you view the Event Filter Builder tree, the CIM events are displayed under the CIM node in the tree.

**Note:** IBM Director can convert CIM indications into other event types, including event types that are used by enterprise-level system-management programs, such as SNMP events. Using these event types, IBM Director can provide system data to the by enterprise-level system-management programs through the IBM Director Upward Integration Modules. For more information, see the “CIM indications in IBM Director” section of the *IBM Director Events Reference*.

However, these SNMP events are not the same as SNMP traps that IBM Director Server receives out-of-band (that is, not through IBM Director Agent or IBM Director Core Services). Out-of-band SNMP

traps are generated by hardware products and other software programs. They are displayed under the SNMP node in the Event Filter Builder tree, but beneath a different subnode.

You can use the events in the Event Filter Builder tree when working with managed objects. To monitor one or more events, you must create an event filter that contains an event type from one of these sources, use the event filter as part of an event-action plan, and then apply the event-action plan to a managed object. Events from the Windows event log are displayed in the Windows event log tree in the Event Type Filter Builder. Events from WMI are displayed in the Common Information Model (CIM) tree.

## Alerts and resolutions

In IBM Director, an event can be in one of the following categories: alert and resolution. Typically, an *alert* is the occurrence of a problem relating to a managed object. A *resolution* is the occurrence of a correction or solution to a problem.

**Note:** In the IBM Director product, there are tasks and features that use the word *alert* in place of the word event. Also, ServeRAID Manager uses the word *notification* instead of event.

---

## Monitoring operating-system specific events

If you want to monitor Windows- or i5/OS-specific events in the IBM Director environment, you must create an event-action plan in order for IBM Director to process these events. The predefined active event-action plan in IBM Director, Log All Events, does not monitor these operating-system specific events.

Managed objects running Windows or i5/OS® can generate the following operating-system specific events:

<b>Window-specific event types</b>	<ul style="list-style-type: none"><li>• Windows event log</li><li>• (Optional) A subset of the following CIM events:<ul style="list-style-type: none"><li>– Windows event log</li><li>– Windows services</li><li>– Windows registry</li></ul></li></ul>
<b>i5/OS specific event types</b>	<ul style="list-style-type: none"><li>• Msgq</li></ul>

Even though these events are generated by their respective operating systems (or an optional layer that is installed on the operating system), IBM Director does not process these events unless you create an event-action plan to do so. When you install IBM Director, it has one predefined active event-action plan: Log All Events. However, this event-action plan does not log these Windows- or i5/OS-specific events. You must create an event-action plan with a simple-event filter that contains the event types for one or more of these events. Then, you must apply this event-action plan to the managed object running Windows or i5/OS.

When IBM Director Agent starts on a managed object running Windows, the twgescli.exe program starts, too. This program listens for IBM Director Server to send a message to IBM Director Agent that an event-action plan has been applied to that managed object. If the event-action plan includes a simple-event filter that contains the event types for any of the Windows-specific events, IBM Director appropriates these events for its own use. This is called *event subscription*. The twgescli.exe program subscribes to the event types that are specified in the event-action plan and translates the Windows-specific events into an IBM Director event type. Then, the program forwards the events to the management server from which the event-action plan was applied.

When IBM Director Agent starts on a managed object running i5/OS, the process is the same with comparable code to twgescli.exe that is included in IBM Director Agent for i5/OS.

---

## Processing an event in IBM Director

Understanding how IBM Director processes an event can help you build and troubleshoot event-action plans.

IBM Director completes the following steps to determine which event actions to execute:

1. The managed object generates an event and forwards the event to all the management servers that have discovered the managed object (except for some events, such as those that are generated through meeting or exceeding a resource-monitor threshold, which are sent only to the management server where the thresholds are configured and applied).
2. IBM Director Server processes the event and determines which managed object generated the event and which group or groups the managed object belongs to.
3. IBM Director Server determines whether any event-action plans are applied to the managed object or to any of the groups of which the managed object is a member.

4. If an event-action plan has been applied, IBM Director Server determines whether any event filters match the event that was generated.
  5. The management server performs any event actions for each matching event filter.
- 

## Event-action plans

When you create an event-action plan, you attach one or more event actions to a specified event filter. Then, you include one or more event filters in the event-action plan. Finally, you apply that event-action plan to a system or group of systems.

An event-action plan is composed of two types of components:

- Event filters, which specify event types and any related parameters
- Event actions, which occur in response to filtered events

You can apply an event-action plan to an individual managed object, several managed objects, or a group of managed objects.

By creating event-action plans and applying them to specific managed objects, you can be notified by e-mail or pager, for example, when a specified threshold is reached or a specified event occurs. Or you can configure an event-action plan to start a program on a managed object and change a managed-object variable when a specific event occurs. You can use process-monitor events and resource-monitor events to build an event-action plan.

Successful implementation of event-action plans requires planning and consideration of how you will implement them. In particular, developing and following strict naming conventions is important, so that you can easily identify what a specific plan does.

### Modifying an existing event-action plan

You can modify an existing event-action plan, even one that is already applied to managed objects or groups, using the Event Action Plan Builder.

If you modify an event filter or an event action that is used in an existing event-action plan, the changes are applied automatically to any event-action plans that use those filters or actions. If you add or delete a filter or an

action that is used in an existing event-action plan, the following warning is displayed.

---

## Event filters

An *event filter* specifies an instance of one or more events that you want IBM Director to process. IBM Director ignores any event instances that do not meet the specifications of the event filter. Because the event filter can specify possible values for the extended attributes that are included in an event type's definition, an event instance can be customized for very specific problems and occurrences. To permit users to quickly event filters, the extended attributes include default values; however, users can customize the extended attribute settings.

You can use an event filter to capture a single event or multiple events. The following list includes some of the criteria that you can use to determine whether to include an event with other events:

- All managed objects that are targeted for the filter are able to generate all events that are included in the filter. If the managed object does not generate the event for which the filter is defined, the filter will not be effective on that managed object.
- The event actions that will be used to respond to the event are the same for all targeted objects.
- The other event filter options besides the event type are common for all targeted objects. These settings include the times the event filter is active, the severity of the event, and other attributes.

Event-action plans can include event filters with event types that are not generated by all managed objects. In such instances, you can apply the event-action plan to those managed objects, but it will have no effect. For example, if an event filter is based on a ServeRAID event and that event-action plan is applied to managed objects that do not have a ServeRAID adapter installed, the event filter has no events to filter, and therefore, no actions are performed. If you understand this concept, you can create more complex event-action plans, and you can reduce the number of event-action plans you have to build and maintain.

All currently available event types are displayed in the tree on the Event Type page in the Event Filter Builder window. The currently installed tasks and extensions publish their events in the Event Type tree when IBM Director Server or IBM Director Agent or IBM Director Core Services starts.

**Note:** Whether the events are published when IBM Director Server or IBM Director Agent or IBM Director Core Services starts depends on the tasks or extensions and how they are implemented.

If you add an extension to your IBM Director installation, the extension might publish its events either when it is added to the installation or when the extension sends its first event. If the extension publishes when it sends its first event, only that event is published.

## **Event-filter types**

IBM Director provides four types of event filters.

In the Event Action Plan Builder window, the Event Filters pane provides the following event filters.

Event filter	Description
Simple Event	<p>Simple event filters are general-purpose filters; most event filters are this type. When you expand this tree, any customized simple event filters that you have created are displayed. Also, the following predefined, read-only event filters are displayed:</p> <ul style="list-style-type: none"><li>• All Events</li><li>• Critical Events</li><li>• Environmental Sensor Events</li><li>• Fatal Events</li><li>• Hardware Predictive Failure Events</li><li>• Harmless Events</li><li>• Minor Events</li><li>• Security Events</li><li>• Storage Events</li><li>• Unknown Events</li><li>• Warning Events</li></ul> <p>Some of these predefined filters use the severity of events to determine which events they will allow to pass through; other filters target a specific type of event. For example, the Critical Events filter processes only those events that have a Critical severity. The All Events filter processes any events that occur on any managed object, except for Windows-specific and i5/OS-specific events. Using one of these predefined event filters ensures that the correct event type or event severity is preselected.</p> <p>If you want to see what events are included in a predefined event filter, double-click that predefined event filter in the Event Filters pane. The “Simple Event Filter Builder” window opens, and the Event Filter Builder notebook is displayed. Select the applicable notebook page to view the selected event filters. For example, click the <b>Severity</b> tab to view the selections for the Critical Event filter. You cannot change predefined event filters; they are read-only. However, you can make changes and click <b>File</b> → <b>Save As</b> to save the modified event filter with another name.</p>

Event filter	Description
Duplication Event	<p>Duplication event filters ignore duplicate events, in addition to the options that are available in the simple event filters.</p> <p>To use this filter, you must specify the number of times (Count) that the same event is ignored during a specified time range (Interval). Then, this filter processes the first event that meets the criteria that are defined for this filter. Only the first event triggers the event actions that are associated with this event filter. For the associated event actions to be triggered again, one of the following conditions must be met:</p> <ul style="list-style-type: none"> <li>• The value that is specified in the <b>Count</b> field must be exceeded.</li> <li>• The time range that is specified in the <b>Interval</b> field must elapse.</li> <li>• The value that is specified in the <b>Count</b> field must be exceeded by 1 (Count+1) within the time range that is specified in the <b>Interval</b> field.</li> </ul> <p>For example, you can define a duplication event filter to filter on the occurrence of an offline event and define a corresponding event action to forward the event to IBM Director Server. Depending on the criteria that you define, only the first event announcing that the system is offline is processed, and all other instances in which an event meets the filtering criteria are discarded until the Count value is exceeded during the specified interval.</p>
Exclusion Event	<p>Exclusion event filters exclude certain event types, in addition to the simple event filter options. Using this filter, you define the criteria of the events to exclude.</p>
Threshold Event	<p>A threshold event filter processes an event after it has occurred a specified number of times within a specified interval, in addition to the simple event filter options.</p> <p>An event that meets the criteria that are defined in this filter triggers associated actions only after an event has met the criteria for the number of times that are specified in the <b>Count</b> field or only after the number of times specified in the <b>Count</b> field within the time range specified in the <b>Interval</b> field.</p> <p>For example, you can define a threshold event filter to monitor frequently occurring heartbeat events and forward the event to IBM Director Server only when the heartbeat event is received for the 100th time during a specified amount of time.</p>

## Event-filter criteria

Depending on the event-filter type, you set specific values for these types of criteria.



Criteria	Description
Event Type	<p>Use the Event Type page to specify the source or sources of the events that are to be processed. This tree is created dynamically; and entries are added by tasks and as new alerts are received. Entries in the tree can be expanded to display suboption events.</p> <p>Most event filters are created using only this page. It specifies the source or sources of the events that are to be processed by this filter.</p> <p>By default, the <b>Any</b> check box is selected, meaning that none of the events that are listed are filtered, except for Windows-specific and 15/OS-specific events. If you want to specify certain events on which to filter, clear the <b>Any</b> check box. You can highlight more than one event by pressing the Ctrl or Shift key.</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. When you select a root option in the Event Type tree, all suboption events are selected as well. For example, when you select <b>MPA</b> in the Simple Event Filter Builder window, all Component, Deployment, Environmental, and Platform suboption events are selected also. <p>If additional event types are published after you create the event filter, the newly available event types are included in your event filter only if the new event types are suboption events of an event type that you selected. However, if you want to include a newly published event type that is not a suboption event, you must update the event filter by selecting the new event type.</p> </li> <li>2. The event types for BladeCenter events are displayed under <b>MPA</b>, except for BladeCenter Configuration Management events, which are displayed under <b>Configuration Management</b>.</li> </ol>

<b>Criteria</b>	<b>Description</b>
Severity	<p>Use the Severity page to indicate the urgency of the events that are filtered. If an event is received whose severity level is not included in the event filter, the filter will not process that event. By default, the <b>Any</b> check box is selected, indicating that all event severities are processed by the filter.</p> <p>When you select more than one severity, they are joined together using logical OR. The source of the event determines what severity the event is. Generally, the severity levels have the following meanings:</p> <p><b>Fatal</b> The event caused a failure and must be resolved before the program or component is restarted.</p> <p><b>Critical</b> The event might cause a failure and must be resolved immediately.</p> <p><b>Minor</b> The event is not likely to cause immediate program failure but should be resolved.</p> <p><b>Warning</b> The event is not necessarily problematic but might warrant investigation.</p> <p><b>Harmless</b> The event is for information only. Most events of this severity do not indicate potential problems. However, offline events are categorized as harmless, and these events <i>can</i> indicate potential problems.</p> <p><b>Unknown</b> The application that generated the event did not assign a severity level.</p>

Criteria	Description
Day/Time	<p>Use the Day/Time page to set the filter to accept and ignore events on certain days and at certain times of the day. By default, the <b>Any</b> check box is selected, indicating that events that occur at any time are processed by the event filter.</p> <p>The time zone that applies to the specified time is the time zone in which the management server is located. If your management console is not in the same time zone as the management server, the difference in time zones is displayed above the Selections pane as an aid to determining the correct time.</p> <p>By default, all events are passed through all filters. This includes events that were queued by IBM Director Agent because the link between the managed object and the management server was unavailable. However, you can prevent these queued events from being processed by a filter by selecting the <b>Block queued events</b> check box. This option can be useful if the timing of the event is important or if you want to avoid filtering on multiple queued events that are sent all at once when IBM Director Server becomes accessible. However, you can block queued events only if you filter events at a specified time. To block queued events, you must clear the <b>Any</b> check box.</p>
Category	<p>Use the Category page to specify an event filter according to the status of an event (alert or resolution of a problem). However, not all events have resolutions.</p>
Sender Name	<p>Use the Sender Name page to specify the managed object to which the event filter will apply. Events that are generated by all other managed objects will be ignored. By default, the <b>Any</b> check box is selected, indicating that events from all managed objects (including IBM Director Server) are processed by the event filter.</p> <p>Initially, only IBM Director Server is shown in the list. As other managed objects generate events, such as when a threshold is exceeded, this list is added to dynamically. If you anticipate that other managed objects will generate events, you also can type managed-object names into the field and click <b>Add</b> to add them.</p>
Extended Attributes	<p>Use the Extended Attributes page to specify additional event-filter criteria using additional keywords and keyword values that you can associate with some categories of events, such as SNMP. This page is available only when you clear the <b>Any</b> check box on the Event Type page and select certain entries from that page.</p> <p>If the Extended Attributes page is available for a specific event type but no keywords are listed, IBM Director Server is not aware of any keywords that can be used for filtering.</p> <p>To view the extended attributes of specific event types, expand the <b>Event Log</b> task in the IBM Director Console Tasks pane and select an event of that type from the list. The extended attributes of the event, if any, are displayed at the bottom of the Event Details pane, below the Sender Name category.</p>

Criteria	Description
System Variables	Use the System Variables page to further qualify the filtering criteria by specifying a system variable. This page is available only if there are one or more system variables. A system variable consists of a user-defined pairing of a keyword and value that are known only to the local management server. <b>Note:</b> These user-defined system variables are not associated with the system variables of the Windows operating system.
Event Text	Use the Event Text page to specify event message text to associate with the event.

## Event actions

The *event action* specifies the actions that you want IBM Director to take as a result of the occurrence of an event.

### Event action types

IBM Director has several predefined event action types. With the exception of Add to Event Log, you must customize each event action type that you want to use.

#### Add/Remove “event” system to Static Group

Adds a managed object to or removes a managed object from a specified static group when the managed object logs a specific event.

#### Add/Remove source group members to target static group

Adds all specified managed objects in a source group to a target group or removes all specified managed objects from the target group.

#### Add a Message to the Console Ticker Tape

Displays a message in red type that scrolls from right to left at the bottom of IBM Director Console.

#### Add to the Event Log

Adds a description of the event to the IBM Director event log.

#### Define a Timed Alarm to Generate an Event

Generates an event only if IBM Director does not receive an associated event within the specified interval.

### **Define a Timed Alarm to Start a Program on the Server**

Starts a program on the management server if IBM Director does not receive an associated event within the specified interval.

### **Log to Textual Log File**

Generates a text log file for the event that triggers this action.

### **Post a News Group (NNTP)**

Sends a message to a newsgroup using the Network News Transfer Protocol (NNTP).

### **Resend Modified Event**

Creates or changes an event action that modifies and resends an original event.

### **Send an Alphanumeric Page (via TAP)**

Windows only) Sends a message to a pager using the Telocator Alphanumeric Protocol (TAP).

### **Send an Event Message to a Console User**

Displays a popup message on the management console of one or more specified users.

### **Send an Internet (SMTP) E-mail**

Sends a Simple Mail Transfer Protocol (SMTP) e-mail message.

### **Send an SNMP Inform to an IP host**

Sends an SNMP inform request to a specified IP host.

### **Send an SNMP Trap to a NetView® Host**

Generates an SNMP trap and sends it to a specified NetView host using a TCP/IP connection to the host. If delivery of the SNMP trap fails, a message is posted in the history log of the managed object.

### **Send an SNMP Trap to an IP Host**

Generates an SNMPv1 or SNMPv2c trap and sends it to a specified IP address or host name.

### **Send a Numeric Page**

(Windows only) Sends a numeric-only message to the specified pager.

### **Send a TEC Event to a TEC Server**

Generates a Tivoli Enterprise Console® event and sends it to a specified Tivoli Enterprise Console server.

### **Set an Event System Variable**

Sets the managed system variable to a new value or resets the value of an existing system variable.

### **Start a Program on a System**

Starts a program on any managed objects on which IBM Director Agent is installed.

### **Start a Program on the “event” System**

Starts a program on the managed object that generated the event.

### **Start a Program on the Server**

In response to an event, starts a program on the management server that received the event.

### **Start a Task on the “event” System**

In response to an event, starts a noninteractive task on the managed object that generated the event.

### **Update the Status of the “event” System**

When the selected resource status generates an event, causes a status indicator beside the icon of the managed object that is associated with the resource to be set or cleared according to your specification.

## **Event-data-substitution variables**

For some event-action types, you can include event-specific information as part of the text message. Including event information is referred to as *event-data substitution*. You can use these event-data-substitution variables to customize event actions.

### **&date**

The date the event occurred.

### **&time**

The time the event occurred.

### **&text**

The event details, if they are supplied by the event.

- &type**  
The event-type criteria that are used to trigger the event. For example, the event that is generated when a managed object goes offline is of type Director > Topology > Offline. This corresponds to the entry on the Event Type page.
- &severity**  
The severity level of the event.
- &system**  
The name of the managed object for which the event was generated. The system name is either the name of IBM Director Agent or, in the case of an SNMP device, the TCP/IP address.
- &sender**  
The name of the managed object from which the event was sent. This variable returns null if the name is unavailable.
- &group**  
The group to which the target object belongs and is being monitored. This variable returns null if the group is unavailable.
- &category**  
The category of the event, either Alert or Resolution. For example, if the managed object goes offline, the category is Alert. If the managed object goes online, the category is Resolution.
- &pgmtype**  
A dotted representation of the event type using internal type strings.
- &timestamp**  
The coordinated time of the event.
- &rawsev**  
The nonlocalized string of event severity (Fatal, Critical, Minor, Warning, Harmless, Unknown).
- &rawcat**  
The nonlocalized string of event category (Alert, Resolution).

**&corr**

The correlator string of the event. Related events, such as those from the same monitor-threshold activation, will match this.

**&snduid**

The unique ID of the event sender.

**&sysuid**

The unique ID of the managed object that is associated with the event.

**&prop:file\_name#property\_name**

The value of the property string *property\_name* from property file *file\_name* (relative to the IBM\Director\classes directory).

**Note:** For i5/OS, the absolute directory path must be used.

**&sysvar:variable\_name**

The event system variable *variable\_name*. This variable returns null if a value is unavailable.

**&slotid:slot\_id**

The value of the event detail slot with the nonlocalized ID *slot\_id*.

**&md5hash**

The MD5 (message digest 5) hash code, or cyclic redundancy check (CRC), of the event data (an event-specific unique ID).

**&hashtxt**

Provides a full replacement for the field with an MD5 hash code (32-character hex code) of the event text.

**&hashtxt16**

Provides a full replacement for the field with a short MD5 hash code (16-character hex code) of the event text.

**&otherstring**

The value of the detail slot that has a localized label that matches *otherstring*. A detail slot is a record in an event detail. For example, an event has one event detail that has an ID of *key1* and a value of *value1*. You can use the substitution variable **&slotid:key1** to obtain the value *value1*. You also can use **&key1** to obtain



the value *value1*. In the description above, *otherstring* is a placeholder for the user-defined event detail ID. However, if the passed ID is not found, “Not applicable” is returned.

---

## **Message Browser**

You can use the Message Browser to view events that are sent to IBM Director Console. The Message Browser is displayed automatically whenever an alert is sent to the management console.

You can choose to have events sent to the management console when an event occurs by configuring an event action plan with the Send an Event Message to a Console User event action.

The Message Browser displays all alerts, including management console ticker-tape alerts. However, the Message Browser does not display any ticker-tape messages. A ticker-tape message can display, for example, resource-monitor data.

---

## Chapter 3. Event-action plan examples

The following event-action plans have been exported from an IBM Director environment. They are examples of some common tasks that you can automate using an event-action plan.

---

### Restarting Norton AntiVirus sample event-action plan

A sample event-action plan that detects when Norton AntiVirus has been stopped before completing its scan on a Level-2 managed system. The plan includes event actions that display a message on the IT administrators' system and restart the Norton AntiVirus client.

#### Event Action Plan

*Monday, April 11, 2005 4:10:37 PM*

1. **Event Action Plan** : NAV Service Stopped
  - **Event Filter** : NAV Service Stopped
    - **Filter Type**
      - Simple Event Filter
    - **Event Type**
      - Director:Director.Agent.Windows Service Monitors.Norton AntiVirus Client.State.Error
    - **Extended Attributes**
      - **Action Name** : Add to the Event Log

Language	English (United States)
Time Zone...	

- **Action Name** : Generic Popup to IT Admins

Message	&Text on &System at &Time &Date
---------	---------------------------------

User(s)	davidf, mrstout, marcl
Delivery Criteria	Active Users Only
Language	English (United States)
Time Zone...	America/Los_Angeles

- **Action Name** : Start NAV Client

Task	[Process_Tasks][Process Management][Start NAV Client]
Language	English (United States)
Time Zone...	America/Los_Angeles

- **Action Name** : NAV Service Stopped

Message	Norton AntiVirus Service Stopped on &System
User(s)	*
Language	English (United States)
Time Zone...	America/Los_Angeles

- **Action Name** : Kirkland Problems

Target Group Name	Kirkland, We Have a Problem!
Add/Remove Option	Add system to target group
Language	English (United States)
Time Zone...	America/Los_Angeles

---

## Stopping the FreeCell program sample event-action plan

A sample event-action plan that detects when the game FreeCell has started on a Level-2 managed system. The plan includes event actions that start a ticker tape message on a specified system, display a message on the administrators' system, stop FreeCell, and display a message on the Level-2 managed system that was running FreeCell.

### Event Action Plan

**Monday, April 11, 2005 4:10:37 PM**

1. **Event Action Plan** : FreeCell Killer
  - **Event Filter** : Fiercely Started
    - **Filter Type**
      - Simple Event Filter
    - **Event Type**
      - Director:Director Agent.Process Monitors.Process Alert.Process Started.freecell.exe
    - **Extended Attributes**
      - **Action Name** : FreeCell Started Ticker Tape

Message	FreeCell has been started on &System
User(s)	*
Language	English (United States)
Time Zone...	America/Los_Angeles

- **Action Name** : Add to the Event Log

Language	English (United States)
Time Zone...	

- **Action Name** : Generic Popup to IT Admins

Message	&Text on &System at &Time &Date
User(s)	admin201, admin209, admin007
Delivery Criteria	Active Users Only
Language	English (United States)
Time Zone...	America/Los_Angeles

- **Action Name** : Kirkland Problems

Target Group Name	Control, We Have a Problem!
Add/Remove Option	Add system to target group
Language	English (United States)
Time Zone...	America/Los_Angeles

- **Action Name** : FreeCell Killer

Task	[Process Tasks][Process Management][FreeCell Killer]
Language	English (United States)
Time Zone...	America/Los_Angeles

- **Action Name** : Game Warning to HS20-EBC03

Program specification	net send HS20-EBC03 It is against company policy to play games on server hardware. Please pack up your personal belongings and report to Human Resources immediately. Game over. . . .
Working Directory	null
Language	English (United States)
Time Zone...	America/Los_Angeles

---

## Restarting a print spooler sample event-action plan

A sample event-action plan that detects when the print spooler has stopped on a Level-2 managed system. The plan includes event actions that restart the print spooler and send an e-mail.

### Event Action Plan

**Monday, April 11, 2005 4:10:37 PM**

1. **Event Action Plan** : Print Spooler Task

- **Event Filter** : Print Spooler Stopped - Simple
  - **Filter Type**
    - Simple Event Filter
  - **Event Type**
    - Director:Director Agent.NT Service Monitors.Print Spooler.Service State.Error
  - **Extended Attributes**
    - **Action Name** : Net Start Spooler

Task	[Process Tasks][Process Management][Net Start Spooler]
Language	English (United States)
Time Zone...	America/Chicago

- **Event Filter** : Print Spooler Stopped - Threshold
  - **Filter Type**
    - Threshold Event Filter
  - **Event Type**
    - Director:Director Agent.NT Service Monitors.Print Spooler.Service State.Error
  - **Extended Attributes**
    - **Interval**: 3600
    - **ConsoleUnit**: hour(s)

- **Count: 5**
- **Action Name : Send e-mail**

E-mail address (such as name@company.com)	User@company.com
Reply-To address	director@company.com
SMTP server	smtp@company.com
SMTP Port	25
Subject of Message	Event & Text received from &System at &Time on &Date
Body of Message	null
Language	English (United States)
Time Zone...	America/Chicago

---

## Chapter 4. Event Action Plans

Use Event Action Plans to specify actions that are performed in response to events that are generated by a managed object. Managed objects include, but are not limited to, Level-0, Level-1, Level-2 managed systems, SNMP devices, BladeCenter management modules, platforms, and switches.

An event action plan is composed of two types of components:


- One or more event filters, which specify event types and any related parameters
- One or more event actions, which occur in response to filtered events

You can apply an event action plan to an individual managed object, several managed objects, or a group of managed objects.

By creating event action plans and applying them to specific managed objects, you can be notified by e-mail or pager, for example, when a specified threshold is reached or a specified event occurs. Or you can configure an event action plan to start a program on a managed object and change a managed-object variable when a specific event occurs. You can use any event, including process-monitor and resource-monitor events, to build an event action plan.

When you install IBM Director, a single event action plan is already defined, in addition to any that you created using the Event Action Plan wizard. The Log All Events event action plan has the following characteristics:

- It uses the event filter named All Events, a simple event filter that processes all events from all managed objects.
- It performs the action Add to the Event Log, a standard event action that adds an entry to the IBM Director Server event log.


Icon	
Supported IBM Director objects	All managed objects



Supported operating systems	All operating systems supported by IBM Director. For detailed operating-system support information, see the IBM Director information center at <a href="http://publib.boulder.ibm.com/infocenter/eserver/v1r2/topic/dirinfo/fqm0_main.html">publib.boulder.ibm.com/infocenter/eserver/v1r2/topic/dirinfo/fqm0_main.html</a> .
Availability	Part of the standard IBM Director installation.
Required hardware or hardware limitations	None
Required software	None
Required protocols	None
Required device drivers	None
Mass Configuration support	No
Scheduler support	No
Files associated with this task	None
Events associated with this task	All events in an IBM Director environment are available for use in this task. For detailed events information, see the IBM Director information center on the Web at <a href="http://publib.boulder.ibm.com/infocenter/eserver/v1r2/topic/dirinfo/fqm0_main.html">publib.boulder.ibm.com/infocenter/eserver/v1r2/topic/dirinfo/fqm0_main.html</a> .

## Chapter 5. Event Log

Use Event Log to view details about all events or subsets of events that have been received and logged by IBM Director Server. You can view all events or view events for a managed object or by filter criteria.

Icon	
Supported IBM Director objects	All managed objects
Supported operating systems	All operating systems supported by IBM Director. For detailed operating-system support information, see the IBM Director information center at <a href="http://publib.boulder.ibm.com/infocenter/eserver/v1r2/topic/dirinfo/fqm0_main.html">publib.boulder.ibm.com/infocenter/eserver/v1r2/topic/dirinfo/fqm0_main.html</a> .
Availability	Part of the standard IBM Director installation.
Required hardware or hardware limitations	None
Required software	None
Required protocols	None
Required device drivers	None
Mass Configuration support	No
Scheduler support	No
Files associated with this task	None
Events associated with this task	This task displays all events generated by managed objects, software, and other IBM Director tasks. For detailed events information, see the IBM Director information center on the Web at <a href="http://publib.boulder.ibm.com/infocenter/eserver/v1r2/topic/dirinfo/fqm0_main.html">publib.boulder.ibm.com/infocenter/eserver/v1r2/topic/dirinfo/fqm0_main.html</a> .

## **Part 2. Events**

---

## Chapter 6. Capacity Manager events

The Capacity Manager events occur when Capacity Manager identifies a managed system that has a system capacity bottleneck. For the Capacity Manager Agent to generate these events, you must select the **Generate Bottleneck Events** check box when creating a Capacity Manager report definition.

### Event source

These event types are generated by the Capacity Manager Agent that is installed on a Level-2 managed system. A prerequisite for the Capacity Manager Agent is IBM Director Agent.

### Details

If you select the **Capacity Manager** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Capacity Manager subtree.

Event type	Event text	Severity	Category	Extended attributes
Capacity Manager	Not applicable	Not applicable	Not applicable	None

You can choose to select specific event types that are displayed under the Capacity Manager node in the Event Filter Builder tree. The event filter will process only the event types that you select.

Event type	Event text	Severity	Category	Extended attributes
Bottleneck	A system bottleneck has been detected.	Critical	Alert	<ul style="list-style-type: none"><li>• <i>CMR file</i> indicates that the Capacity Manager report is generated in the CMR format.</li><li>• <i>CMS file</i> indicates that the Capacity Manager report is generated in the CMS format.</li><li>• <i>Cluster node</i> indicates that a Capacity Manager report is generated about the Level-2 managed systems that are in a Microsoft cluster.</li></ul>

Event type	Event text	Severity	Category	Extended attributes
Bottleneck (continued)				<ul style="list-style-type: none"> <li>• <i>Days until bottleneck starts</i> indicates the number of days until the predicted bottleneck will start.</li> <li>• <i>HTML file</i> indicates that the Capacity Manager report is generated in the HTML format.</li> <li>• <i>Hours until bottleneck starts</i> indicates the number of hours until the predicted bottleneck will start.</li> <li>• <i>Involves CPUs</i> indicates that the predicted bottleneck involves the system microprocessor.</li> <li>• <i>Involves Disks</i> indicates that the predicted bottleneck involves the system hard disk drives.</li> <li>• <i>Involves LAN Adapters</i> indicates that the predicted bottleneck involves the system LAN adapter.</li> <li>• <i>Involves Memory</i> indicates that the predicted bottleneck involves the system memory.</li> <li>• <i>Minutes until bottleneck starts</i> indicates the number of minutes until the predicted bottleneck will start.</li> <li>• <i>TXT file</i> indicates that the Capacity Manager report is generated in the ASCII text format.</li> <li>• <i>XML file</i> indicates that the Capacity Manager report is generated in the XML format.</li> </ul>
Bottleneck > Recommendation	An event-enabled Capacity Manager report has been run and a system bottleneck was detected during performance analysis.	Critical	Alert	<ul style="list-style-type: none"> <li>• <i>CMR file</i> indicates that the Capacity Manager report is generated in the CMR format.</li> <li>• <i>CMS file</i> indicates that the Capacity Manager report is generated in the CMS format.</li> <li>• <i>Cluster node</i> indicates that a Capacity Manager report is generated about the Level-2 managed systems that are in a Microsoft cluster.</li> </ul>

Event type	Event text	Severity	Category	Extended attributes
Bottleneck > Recommendation (continued)				<ul style="list-style-type: none"> <li>• <i>Days since bottleneck first started</i> indicates the number of days since the bottleneck started.</li> <li>• <i>Days since bottleneck last stopped</i> indicates the number of days since the bottleneck stopped.</li> <li>• <i>Days until bottleneck starts</i> indicates the number of days until the predicted bottleneck will start.</li> <li>• <i>HTML file</i> indicates that the Capacity Manager report is generated in the HTML format.</li> <li>• <i>Hours in this bottleneck</i> indicates the number of hours in this bottleneck occurrence.</li> <li>• <i>Hours since bottleneck first started</i> indicates the number of hours since the bottleneck started.</li> <li>• <i>Hours since bottleneck last stopped</i> indicates the number of hours since the bottleneck stopped.</li> <li>• <i>Hours until bottleneck starts</i> indicates the number of hours until the predicted bottleneck will start.</li> <li>• <i>Involves CPUs</i> indicates that the predicted bottleneck involves the system microprocessor.</li> <li>• <i>Involves Disks</i> indicates that the predicted bottleneck involves the system hard disk drives.</li> <li>• <i>Involves LAN Adapters</i> indicates that the predicted bottleneck involves the system LAN adapter.</li> <li>• <i>Involves Memory</i> indicates that the predicted bottleneck involves the system memory.</li> <li>• <i>Minutes since bottleneck first started</i> indicates the number of minutes since the bottleneck started.</li> <li>• <i>Minutes since bottleneck last stopped</i> indicates the number of minutes since the bottleneck stopped.</li> <li>• <i>Minutes until bottleneck starts</i> indicates the number of minutes until the predicted bottleneck will start.</li> </ul>

Event type	Event text	Severity	Category	Extended attributes
Bottleneck > Recommendation (continued)				<ul style="list-style-type: none"> <li>• <i>TXT</i> file indicates that the Capacity Manager report is generated in the ASCII text format.</li> <li>• <i>When bottleneck first started</i> indicates the time when the bottleneck started.</li> <li>• <i>When bottleneck last stopped</i> indicates the time when the bottleneck stopped.</li> <li>• <i>XML</i> file indicates that the Capacity Manager report is generated in the XML format.</li> </ul>
No Response	Not applicable	Minor	Alert	None
No Response > No Monitors	No systems responded with monitor data when an event-enabled report was run.	Minor	Alert	None

---

## Chapter 7. CIM events

The CIM events occur when a change in state is detected for IBM Director components and features as well as hardware in an IBM Director environment. For detailed event types, expand the **CIM** node in the Event Filter Builder tree.

### Event source

CIM event types are generated by IBM Director components and features, hardware, and hardware options. See each event type for details about which IBM Director component or hardware generates that event.

### Details

If you select the **CIM** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the CIM subtree.

Event type	Event text	Severity	Category	Extended attributes
CIM	Not applicable	Not applicable	Not applicable	None

---

## CIM > Certificate

The Certificate events occur when the IBM Director security certificate is nearing expiration or has expired. This certificate is used by Level-1 managed systems to ensure security in communicating with IBM Director Server. Use these events to create an event-action plan to warn when a certificate is nearing expiration or has expired.

### Event source

IBM Director Server generates these events when a Level-1 managed system security certificate is nearing expiration or has expired. The certificate is generated by the IBM Director installation or with the **certmgr**



command and is valid for 365 days. The CertificateExpirationManager.properties file is located in the IBM Director data directory on the management server. This file contains two settings:

**advance\_notify\_in\_hours**

The number of hours before the expiration of a Level-1 certificate. This setting determines when an event will be generated providing notification of a nearing expiration. The default is 240 hours.

**polling\_interval**

The frequency that the validity of a Level-1 certificate is checked by IBM Director Server. The default is 86400 seconds (24 hours).

**Details**

**Note:** These events are new in IBM Director 5.10.

If you select the **Certificate** check box in the Event Filter Builder tree, the event filter will process all of the events that are specified in the Certificate subtree.

Event type	Event text	Severity	Category	Extended attributes
Certificate	Not applicable	Not applicable	Not applicable	None

You can choose to select specific event types that are displayed under the **Profile** node in the Event Filter Builder tree. The event filter will process only the event types that you select.

Event type	Event text	Severity	Category	Extended attributes
Expire	The certificate that is used for CIMOM authentication, located in the data\\cim\\keystore\\ibmd_cert.jks file, will expire soon.	Warning	Alert	<ul style="list-style-type: none"> <li>• <i>Certificate not valid after</i> is the date when the certificate will expire.</li> <li>• <i>Certificate not valid before</i> is the date when the certificate becomes valid.</li> <li>• <i>Certificate expires in (hours)</i> indicates the number of hours in which the certificate will expire.</li> </ul>

Event type	Event text	Severity	Category	Extended attributes
Expire	The certificate that is used for CIMOM authentication, located in the data\\cim\\keystore\\ibmrd_cert.jks file, has expired.	Critical	Alert	<ul style="list-style-type: none"> <li>• <i>Certificate not valid</i> after is the date when the certificate will expire.</li> <li>• <i>Certificate not valid before</i> is the date when the certificate becomes valid.</li> <li>• <i>Certificate expires in (hours)</i> indicates the number of hours in which the certificate will expire.</li> </ul>

## CIM > Storage > Array

The Array event types occur when storage hardware devices detect a change in their operational status or other environmental changes.

### Event source

The CIM > Storage > Array > Alert events are generated by the following storage hardware options:

- IBM System Storage DS300 and DS400 storage subsystems.
- IBM System Storage DS4000 Series. A proxy provider supplies Storage Management Initiative Specification (SMI-S) compliance for this device. The proxy SMI-S provider documentation is available at <http://www.engenio.com/default.aspx?pageID=362>.

The CIM > Storage > Array > Operational Category events are generated by IBM Director when it detects changes in the operational status of the storage hardware.

### Details

**Note:** These events are new in IBM Director 5.10.

If you select the **Array** check box in the Event Filter Builder tree, the event filter will process all of the events that are specified in the Array subtree.

<b>Event type</b>	<b>Event text</b>	<b>Severity</b>	<b>Category</b>	<b>Extended attributes</b>
Array	Not applicable	Not applicable	Not applicable	None

You can choose to select specific event types that are displayed under the **Array** node in the Event Filter Builder tree. The event filter will process only the events that you select.

<b>Event type</b>	<b>Event text</b>	<b>Severity</b>	<b>Category</b>	<b>Extended attributes</b>
Alert	<b>Note:</b> This text varies depending on the storage hardware option.	Varies depending on the storage hardware option.	Alert	None

Event type	Event text	Severity	Category	Extended attributes
Operational Category	Operational status changed	Minor	Alert	<ul style="list-style-type: none"> <li>• <i>CIM Class Name</i> is the CIM object model name of the class that generated in this event and is set to <i>CIM_Computersystem</i>.</li> <li>• <i>CIM Object Path</i> provides the following information: <ul style="list-style-type: none"> <li>– The host name of the CIM server</li> <li>– The port of CIM server</li> <li>– The CIM namespace where the object is found</li> <li>– A set of string properties that uniquely identify the instance.</li> </ul> </li> <li>• <i>Operational Category</i> is one of the following strings: <ul style="list-style-type: none"> <li>– OK</li> <li>– OK, Stressed</li> <li>– OK, Predictive Failure</li> <li>– OK, Supporting Entity in Error</li> <li>– Degraded</li> <li>– Error</li> <li>– Error, Non-recoverable</li> <li>– Error, Supporting Entity in Error</li> <li>– No contact</li> <li>– Lost Communication</li> <li>– Starting</li> <li>– Unknown</li> </ul> </li> </ul>

## CIM > System

The System events occur when a change in the state of a Level-1 or Level-2 managed system is detected. These events also occur when a change in the state of a Hardware Management Console (HMC) is detected.

## Event source

CIM indications are generated by managed systems that have either IBM Director Core Services (Level-1 managed systems) or IBM Director Agent (Level-2 managed systems) installed. IBM Director Server converts the CIM indications into the CIM event types. The HMC CIMOM also generates CIM indications that IBM Director Server converts into CIM event types.

## Details

The CIM > System event types use the following standard set of extended attributes:

- AlertingManagedElement
- Category
- EventID
- EventTime
- ProviderName

If you select the **System** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the System subtree.

Event type	Event text	Severity	Category	Extended attributes
System	Not applicable	Not applicable	Not applicable	None

## CIM > System > Automatic Server Restart

The Automatic Server Restart event occurs when the operating system locks up and no longer responds. Subsequently, a system restart (reboot) begins.

## Resolution

No resolution. This event is informative only.

## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
Automatic Server Restart	The last system restart was due to the automatic server restart hardware.	Warning	Alert	None
Automatic Server Restart	The last system restart was not due to the automatic server restart hardware.	Normal	Resolution	None

## CIM > System > DASD Backplane

The DASD Backplane event occurs when the Remote Supervisor Adapter detects that the state of the system hard disk drive changes with respect to its availability.

### Resolution

Replace the specified hard disk drive that has failed. If necessary, restore your data from a backup.

**Note:** After correcting the hardware error, you must clear this event manually.

### Details

Event type	Event text	Severity	Category	Additional extended attributes
DASD Backplane	Drive <i>drive</i> has reported a fault. This event must be cleared manually. where <i>drive</i> is the affected hard disk drive.	Critical	Alert	None

## CIM > System > Disk Space Low

The Disk Space Low event occurs when the state of system hard disk drive space changes with respect to user-defined levels of hard disk drive space remaining. By default, the warning level is 5% remaining and critical level is 3% remaining.

### Resolution

- If the severity is Critical or Warning: Remove files from the specified hard disk or lower the minimum threshold.
- If the severity is Normal: The error has been resolved. This event is informative only.

### Details

Event type	Event text	Severity	Category	Additional extended attributes
Disk Space Low	Logical drive <i>name</i> fell below threshold of <i>threshold</i> MB. The current value is <i>value</i> MB. where: <ul style="list-style-type: none"><li>• <i>name</i> is the affected logical drive.</li><li>• <i>threshold</i> is the critical threshold value.</li><li>• <i>value</i> is the amount of current disk space available.</li></ul>	Critical	Alert	None
Disk Space Low	Logical drive <i>name</i> fell below threshold of <i>threshold</i> MB. The current value is <i>value</i> MB. where: <ul style="list-style-type: none"><li>• <i>name</i> is the affected logical drive.</li><li>• <i>threshold</i> is the warning threshold value.</li><li>• <i>value</i> is the amount of current disk space available.</li></ul>	Warning	Alert	None

Event type	Event text	Severity	Category	Additional extended attributes
Disk Space Low	Logical drive <i>name</i> free space is normal. The current value is <i>value</i> MB. where <i>name</i> is the affected logical drive and <i>value</i> is the amount of current disk space available.	Normal	Resolution	None
Disk Space Low	Logical drive <i>name</i> status could not be determined. where <i>name</i> is the affected logical drive.	Unknown	Resolution	None

## CIM > System > Error Log

The Error Log event occurs when the Remote Supervisor Adapter detects that its error log is at 75% or 100% of its capacity.

### Resolution

If the severity is Warning: Back up and clear the system-management processor event log.

**Note:** After correcting the hardware error, you must clear this event manually.

### Details

Event type	Event text	Severity	Category	Additional extended attributes
Error Log	The system management processor error log is 75% full. This event must be cleared manually.	Warning	Alert	None
Error Log	The system management processor error log is full. This event must be cleared manually.	Warning	Alert	None



## CIM > System > Fan

The Fan event occurs when the state of a system fan has changed with respect to the manufacturer-defined RPM values. If a Remote Supervisor Adapter is installed in a system, this event is sent when a fan stops, is removed, or is not performing optimally. If a Remote Supervisor Adapter is not installed, an event is sent when the fan stops or is removed.

### Resolution

- If the severity is Critical: Replace the specified fan that has failed.
- If the severity is Normal: The error has been resolved. This event is informative only.

### Details

Event type	Event text	Severity	Category	Additional extended attributes
Fan	Fan Sensor <i>number</i> fell below threshold of <i>threshold</i> RPM. The current value is <i>speed</i> RPM.  where: <ul style="list-style-type: none"><li>• <i>number</i> is the affected fan sensor.</li><li>• <i>threshold</i> is the critical fan threshold value.</li><li>• <i>speed</i> is the current fan speed.</li></ul> <b>Note:</b> This event must be cleared manually.	Critical	Alert	None
Fan	Fan Sensor <i>number</i> reports normal.  where <i>number</i> is the affected fan sensor.	Normal	Resolution	None

## CIM > System > IP Change

The IP Change event occurs when a change in an IP address used by the HMC is detected.

## Resolution

No resolution. This event is informative only.

## Event source

CIM event types for HMC are generated by the CIMOM running on the HMC.

## Details

**Note:** This event is new in IBM Director 5.10.

The CIM > System event types for HMC use the following standard set of extended attributes:

- AlertingManagedElement
- EventID
- EventTime
- SenderUUID

Event type	Event text	Severity	Category	Additional extended attributes
IP Change	The IP Address associated with HMC <i>number</i> has changed. where <i>number</i> identifies the HMC.	Harmless	Alert	<ul style="list-style-type: none"><li>• <i>Description</i> indicates the type of event.</li><li>• <i>OldIPAddress</i> indicates the previous IP address used by the HMC.</li><li>• <i>NewIPAddress</i> indicates the new IP address used by the HMC.</li></ul>

## CIM > System > IPMI Log

The IPMI Log event occurs when the system-management processor error log is 75% full or full.

## Resolution

To correct this problem, reduce the number of events in the event log.

## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
IPMI Log	The system management processor error log is 75% full. This event must be cleared manually.	Normal	Alert	None
IPMI Log	The system management processor error log is full. This event must be cleared manually.	Normal	Alert	None

## CIM > System > Lease Expiration

The Lease Expiration event occurs when the system lease expiration date has been reached with respect to the value configured for the date in the Asset ID task.

## Resolution

- If the severity is Warning: The lease has expired.
- If the severity is Normal: The error has been resolved. This event is informative only.

## Details

The date value is provided by the Asset ID™ task. The Lease page in the Asset ID task includes the **End Date** field where you can set the lease expiration date. The date is stored in the IBMPSG\_Lease.LeaseEndDate CIM property that is monitored at regular poll intervals. A CIM indication is generated when the system CIMOM starts and when a state change is detected relative to the internal poll interval.

Event type	Event text	Severity	Category	Additional extended attributes
Lease Expiration	The lease on <i>system</i> has expired. It expired on <i>date</i> . where <i>system</i> is the affected system and <i>date</i> is the lease expiration date.	Warning	Alert	None
Lease Expiration	The lease on <i>system</i> is normal. It will expire on <i>date</i> . where <i>system</i> is the affected system and <i>date</i> is the lease expiration date.	Normal	Resolution	None

## CIM > System > Life Cycle

The Life Cycle event occurs when an LPAR is created or deleted on a system managed by the Hardware Management Console (HMC). The event also occurs when a CEC is managed by the HMC or removed from management by the HMC.

### Resolution

No resolution. This event is informative only.

### Event source

CIM event types for HMC are generated by the CIMOM running on the HMC.

### Details

**Note:** This event is new in IBM Director 5.10.

The CIM > System event types for HMC use the following standard set of extended attributes:

- AlertingManagedElement
- EventID
- EventTime
- SenderUUID

Event type	Event text	Severity	Category	Additional extended attributes
Life Cycle	LPAR <i>name</i> has been created. where <i>name</i> identifies the LPAR created.	Minor	Alert	<i>LifeCycleEvent</i> indicates whether the CEC was added or removed from management by the HMC.
Life Cycle	LPAR <i>name</i> has been deleted. where <i>name</i> identifies the deleted LPAR.	Minor	Alert	<i>LifeCycleEvent</i> indicates whether the CEC was added or removed from management by the HMC.
Life Cycle	CEC <i>cec</i> is now managed by HMC <i>hmc</i> . where <i>cec</i> identifies the CEC and <i>hmc</i> identifies the HMC.	Minor	Alert	<i>LifeCycleEvent</i> indicates whether the CEC was added or removed from management by the HMC.
Life Cycle	CEC <i>cec</i> is no longer managed by HMC <i>hmc</i> . where <i>cec</i> identifies the CEC and <i>hmc</i> identifies the HMC.	Minor	Alert	<i>LifeCycleEvent</i> indicates whether the CEC was added or removed from management by the HMC.

## CIM > System > Memory

The Memory event occurs when the currently available memory in a system changes with respect to availability due to a modification during a system shut down.

### Resolution

- If the severity is Critical: Replace the specified DIMM that is failing or has failed.
- If the severity is Normal: The error has been resolved. This event is informative only.

## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
Memory	Memory configuration reduced from <i>previous</i> MB to <i>current</i> MB. where <i>previous</i> is the previous memory size and <i>current</i> is the current memory size.	Critical	Alert	None
Memory	Memory configuration increased from <i>previous</i> MB to <i>current</i> MB. where <i>previous</i> is the previous memory size and <i>current</i> is the current memory size.	Normal	Resolution	None

## CIM > System > Memory PFA

The Memory PFA event occurs when a dual inline memory module (DIMM) in a system changes with respect to its availability.

### Resolution

- If the severity is Critical: Replace the specified DIMM that is failing or has failed.
- If the severity is Normal: The error has been resolved. This event is informative only.

### Details

Event type	Event text	Severity	Category	Additional extended attributes
Memory PFA	Memory device identified as memory in bank <i>slot</i> is predicting an imminent failure. where <i>slot</i> is the affected memory slot.	Critical	Alert	None

Event type	Event text	Severity	Category	Additional extended attributes
Memory PFA	Memory device identified as memory in bank <i>slot</i> is not predicting a failure. where <i>slot</i> is the affected memory slot.	Normal	Resolution	None

## CIM > System > Network Adapter

The Network Adapter events occur when a network interface card (NIC) in a system fails, goes offline, or goes online.

### Resolution

- If the severity is Critical or Warning: Replace the specified NIC that has failed.
- If the severity is Normal: The error has been resolved. This event is informative only.

### Details

If you select the **Network Adapter** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Network Adapter subtree.

Event type	Event text	Severity	Category	Additional extended attributes
Network Adapter	Not applicable	Not applicable	Not applicable	<ul style="list-style-type: none"> <li>• <i>DeviceID</i> is the ID for the component if there are more than one of the same component and you are trying to fix a particular instance.</li> <li>• <i>Resolution</i> provides information that can help resolve a hardware problem in the server.</li> </ul>

You can choose to select specific event types that are displayed under the **Network Adapter** node in the Event Filter Builder tree. The event filter will process only the event types that you select.

Event type	Event text	Severity	Category	Additional extended attributes
Failed	The network adapter failed.	Critical	Alert	<ul style="list-style-type: none"> <li>• <i>DeviceID</i> is the ID for the component if there are more than one of the same component and you are trying to fix a particular instance.</li> <li>• <i>Resolution</i> provides information that can help resolve a hardware problem in the server.</li> </ul>
Offline	The network adapter is offline.	Warning	Alert	<ul style="list-style-type: none"> <li>• <i>DeviceID</i> is the ID for the component if there are more than one of the same component and you are trying to fix a particular instance.</li> <li>• <i>Resolution</i> provides information that can help resolve a hardware problem in the server.</li> </ul>



Event type	Event text	Severity	Category	Additional extended attributes
Online	The network adapter is online.	Normal	Resolution	<ul style="list-style-type: none"> <li>• <i>DeviceID</i> is the ID for the component if there are more than one of the same component and you are trying to fix a particular instance.</li> <li>• <i>Resolution</i> provides information that can help resolve a hardware problem in the server.</li> </ul>

## CIM > System > PFA

The PFA event occurs when the Remote Supervisor Adapter detects that a component in a system is about to fail.

### Resolution

Identify and replace the component that is generating the Predictive Failure Analysis event.

**Note:** After correcting the hardware error, you must clear this event manually.

### Details

Event type	Event text	Severity	Category	Additional extended attributes
PFA	Predictive Failure Detected. Please check the system management processor error log for more information. This event must be cleared manually.	Critical	Alert	None

## **CIM > System > Power State**

The Power State event occurs when a change in the power state of a CEC or LPAR is detected.

### **Resolution**

No resolution. This event is informative only.

### **Event source**

CIM event types for HMC are generated by the CIMOM running on the HMC.

### **Details**

**Note:** This event is new in IBM Director 5.10.

The CIM > System event types for HMC use the following standard set of extended attributes:

- AlertingManagedElement
- EventID
- EventTime
- SenderUUID

**Note:** For this event, the AlertingManagedElement attribute is set to the object path of the ComputerSystem instance.

Event type	Event text	Severity	Category	Additional extended attributes
Power State	LPAR name has been powered on. where <i>name</i> identifies the affected LPAR.	Minor	Alert	<p><i>PowerState</i> identifies the power state of the system using one of the following values:</p> <ul style="list-style-type: none"> <li>• 1 = Full Power</li> <li>• 2 = Power Save - Low Power Mode</li> <li>• 3 = Power Save - Standby</li> <li>• 4 = Power Save - Other</li> <li>• 5 = Power Cycle</li> <li>• 6 = Power Off</li> <li>• 7 = Hibernate</li> <li>• 8 = Soft Off</li> </ul>
Power State	LPAR name has been powered off. where <i>name</i> identifies the affected LPAR.	Minor	Alert	<p><i>PowerState</i> identifies the power state of the system using one of the following values:</p> <ul style="list-style-type: none"> <li>• 1 = Full Power</li> <li>• 2 = Power Save - Low Power Mode</li> <li>• 3 = Power Save - Standby</li> <li>• 4 = Power Save - Other</li> <li>• 5 = Power Cycle</li> <li>• 6 = Power Off</li> <li>• 7 = Hibernate</li> <li>• 8 = Soft Off</li> </ul>

Event type	Event text	Severity	Category	Additional extended attributes
Power State	CEC <i>name</i> has been powered on.  where <i>name</i> identifies the affected LPAR.	Minor	Alert	<p><i>PowerState</i> identifies the power state of the system using one of the following values:</p> <ul style="list-style-type: none"> <li>• 1 = Full Power</li> <li>• 2 = Power Save - Low Power Mode</li> <li>• 3 = Power Save - Standby</li> <li>• 4 = Power Save - Other</li> <li>• 5 = Power Cycle</li> <li>• 6 = Power Off</li> <li>• 7 = Hibernate</li> <li>• 8 = Soft Off</li> </ul>
Power State	CEC <i>name</i> has been powered off.  where <i>name</i> identifies the affected LPAR.	Minor	Alert	<p><i>PowerState</i> identifies the power state of the system using one of the following values:</p> <ul style="list-style-type: none"> <li>• 1 = Full Power</li> <li>• 2 = Power Save - Low Power Mode</li> <li>• 3 = Power Save - Standby</li> <li>• 4 = Power Save - Other</li> <li>• 5 = Power Cycle</li> <li>• 6 = Power Off</li> <li>• 7 = Hibernate</li> <li>• 8 = Soft Off</li> </ul>

## CIM > System > Processor

The Processor event occurs when microprocessors were removed or added during the last system shut down

## Resolution

- If the severity is Critical: Replace the specified processor that is failing or has failed.
- If the severity is Normal: The error has been resolved. This event is informative only.

## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
Processor	Processor configuration reduced from <i>previous</i> CPU to <i>current</i> CPU.  where <i>previous</i> is the previous number of microprocessors (CPUs) and <i>current</i> is the current number of microprocessors.	Critical	Alert	None
Processor	Processor configuration increased from <i>previous</i> CPU to <i>current</i> CPU.  where <i>previous</i> is the previous number of microprocessors (CPUs) and <i>current</i> is the current number of microprocessors.	Normal	Resolution	None

## CIM > System > Processor PFA

The Processor PFA event occurs when the state of a system processor changes with respect to its availability.

## Resolution

- If the severity is Critical: Replace the specified processor that is failing or has failed.
- If the severity is Normal: The error has been resolved. This event is informative only.

## Details

Event type	Event text	Severity	Category	Additional extended attributes
Processor PFA	Processor device identified as processor in slot <i>slot</i> is predicting an imminent failure. where <i>slot</i> is the affected processor slot.	Critical	Alert	None
Processor PFA	Processor device identified as processor in slot <i>slot</i> is not predicting a failure. where <i>slot</i> is the affected processor slot.	Normal	Resolution	None

## CIM > System > Redundant Network Adapter Switchback

The Redundant Network Adapter Switchback event occurs when the primary network interface card (NIC) is restored in a teamed NIC configuration.

### Resolution

The error has been resolved. This event is informative only.

### Details

Event type	Event text	Severity	Category	Additional extended attributes
Redundant Network Adapter Switchback	Onboard NIC has Switched Back	Normal	Alert	None
Redundant Network Adapter Switchback	NIC in PCI Bus bus Slot <i>slot</i> has Switched Back where <i>bus</i> is the affected bus and <i>slot</i> is the affected slot.	Normal	Alert	None

Event type	Event text	Severity	Category	Additional extended attributes
Redundant Network Adapter Switchback	NIC in PCI Slot <i>slot</i> has Switched Back where <i>slot</i> is the affected slot.	Normal	Alert	None
Redundant Network Adapter Switchback	NIC has Switched Back	Normal	Alert	None

## CIM > System > Redundant Network Adapter Switchover

The Redundant Network Adapter Switchover event occurs when the primary network interface card (NIC) fails in a teamed NIC configuration and the standby NIC becomes the active NIC.

### Resolution

Check the network connection.

### Details

Event type	Event text	Severity	Category	Additional extended attributes
Redundant Network Adapter Switchover	Onboard NIC has Switched Over	Warning	Alert	None
Redundant Network Adapter Switchover	NIC in PCI Bus <i>bus</i> Slot <i>slot</i> has Switched Over where <i>bus</i> is the affected bus and <i>slot</i> is the affected slot.	Warning	Alert	None
Redundant Network Adapter Switchover	NIC in PCI Slot <i>slot</i> has Switched Over where <i>slot</i> is the affected slot.	Warning	Alert	None
Redundant Network Adapter Switchover	NIC has Switched Over	Warning	Alert	None

## CIM > System > Remote Login

The Remote Login event occurs when an end-user or application has logged in to the Web interface of the Remote Supervisor Adapter.

### Resolution

No resolution. This event is informative only.

**Note:** After correcting the hardware error, you must clear this event manually.

### Details

Event type	Event text	Severity	Category	Additional extended attributes
Remote Login	The system management processor has been accessed via a remote login. This event must be cleared manually.	Warning	Alert	None

## CIM > System > Server Power Supply

The Server Power Supply event occurs when the state of a system power supply changes with respect to its availability.

### Resolution

- If the severity is Critical or Warning: Check the power supply and line cord. Replace the power supply if required.
- If the severity is Normal: The error has been resolved. This event is informative only.



## Details

Event type	Event text	Severity	Category	Additional extended attributes
Server Power Supply	PowerSupply device identified as PowerSupply <i>number</i> reports critical state with possible loss of redundancy. where <i>number</i> is the affected power supply.	Critical	Alert	None
Server Power Supply	PowerSupply device identified as PowerSupply <i>number</i> has failed. This event must be cleared manually. where <i>number</i> is the affected power supply.	Critical	Alert	None
Server Power Supply	PowerSupply device identified as PowerSupply <i>number</i> has lost AC power and loss of standby power is imminent. where <i>number</i> is the affected power supply.	Warning	Alert	None
Server Power Supply	PowerSupply device identified as PowerSupply <i>number</i> reports normal. where <i>number</i> is the affected power supply.	Normal	Resolution	None

## CIM > System > ServerRAID Array FlashCopy Complete

The ServerRAID Array FlashCopy Complete event occurs when a ServerRAID FlashCopy operation is completed on a specified array in a ServerRAID configuration.

### Resolution

No resolution. This event is informative only.

## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Array FlashCopy Complete	FlashCopy with backup complete: <i>array</i> . where <i>array</i> is the affected array.	Harmless	Alert	None

## CIM > System > ServerRAID Array FlashCopy Detected

The ServerRAID Array FlashCopy Detected event occurs when a ServerRAID FlashCopy operation is in progress on a specified array in a ServerRAID configuration.

### Resolution

No resolution. This event is informative only.

### Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Array FlashCopy Detected	FlashCopy in progress: <i>array</i> . where <i>array</i> is the affected array.	Harmless	Alert	None

## CIM > System > ServerRAID Array FlashCopy Fail

The ServerRAID Array FlashCopy Fail event occurs when a ServerRAID FlashCopy operation fails on a specified array in a ServerRAID configuration.

## Resolution

The FlashCopy operation failed because a hardware error occurred. The specified logical drive might be offline.

If the source logical drive is offline, replace the failed hard disk drives and restore the data from tape backup. If the target logical drive is offline, replace the failed hard disk drives. FlashCopy operations will not work when the source or target logical drives are offline.

If the source or target logical drives are not offline, complete the following steps:

1. Verify that the controller, cables, and hard disk drives are installed correctly.
2. Verify that there is power to the hard disk drives.
3. Retry the command.
4. If the command still fails, restart the server and retry the command.
5. If the problem persists, contact your service representative.

## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Array FlashCopy Fail	FlashCopy with backup failed: <i>array [error]</i> where <i>array</i> is the affected array and <i>error</i> is the error code.	Critical	Alert	None

## CIM > System > ServerRAID Array Rebuild Complete

The ServerRAID Array Rebuild Complete event occurs when a ServerRAID rebuild operation is completed on a specified array in a ServerRAID configuration.

## Resolution

No resolution. This event is informative only.

## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Array Rebuild Complete	Rebuild complete: <i>array</i> . where <i>array</i> is the affected array.	Harmless	Alert	None

## CIM > System > ServerRAID Array Rebuild Detected

The ServerRAID Array Rebuild Detected event occurs when a ServerRAID rebuild operation is in progress on a specified array in a ServerRAID configuration.

### Resolution

No resolution. This event is informative only.

### Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Array Rebuild Detected	Rebuilding: <i>array</i> . where <i>array</i> is the affected array.	Harmless	Alert	None

## CIM > System > ServerRAID Array Rebuild Fail

The ServerRAID Array Rebuild Fail event occurs when a ServerRAID rebuild operation fails on a specified array in a ServerRAID configuration.

## Resolution

A hardware error occurred. To correct the error, complete the following steps:

1. Verify that the controller, cables, and hard disk drives are installed correctly.
2. Verify that there is power to the hard disk drives.
3. Retry the command.
4. If the command still fails, restart the server and retry the command.
5. If the problem persists, contact your service representative.

## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Array Rebuild Fail	Rebuild failed: <i>array [error]</i> where <i>array</i> is the affected array and <i>error</i> is the error code.	Critical	Alert	None

## CIM > System > ServerRAID Array Sync Complete

The ServerRAID Array Sync Complete event occurs when a ServerRAID synchronization operation is completed on a specified array in a ServerRAID configuration.

## Resolution

No resolution. This event is informative only.

## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Array Sync Complete	Synchronize complete: <i>array</i> . where <i>array</i> is the affected array.	Harmless	Alert	None

## CIM > System > ServerRAID Array Sync Detected

The ServerRAID Array Sync Detected event occurs when a ServerRAID synchronization operation is in progress on a specified array in a ServerRAID configuration.

### Resolution

No resolution. This event is informative only.

### Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Array Sync Detected	Synchronizing: <i>array</i> . where <i>array</i> is the affected array..	Harmless	Alert	None

## CIM > System > ServerRAID Array Sync Fail

The ServerRAID Array Sync Fail event occurs when a ServerRAID synchronization operation fails on a specified array in a ServerRAID configuration.

## Resolution

A hardware error occurred. Verify that the specified logical drive is not offline or critical (that is, one hard disk drive that is offline in a RAID level-1, 1E, 5, 5E, 10, 1E0, or 50 logical drive). If the logical drive is critical, replace the failed hard disk drive. If the logical drive is offline, replace the failed hard disk drives and restore the data from tape backup.

If the source or target logical drives are *not* offline or critical, complete the following steps:

1. Verify that the controller, cables, and hard disk drives are installed correctly.
2. Verify that there is power to the hard disk drives.
3. Retry the command.
4. If the command still fails, restart the server and retry the command.
5. If the problem persists, contact your service representative.

## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Array Sync Fail	Synchronize failed: <i>array [error]</i> where <i>array</i> is the affected array and <i>error</i> is the error code.	Critical	Alert	None

## CIM > System > ServerRAID Compaction Complete

The ServerRAID Compaction Complete event occurs when a ServerRAID compaction operation is completed on a specified logical drive in a ServerRAID configuration.

## Resolution

No resolution. This event is informative only.

## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Compaction Complete	Compaction complete: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Harmless	Alert	None

## CIM > System > ServerRAID Compaction Detected

The ServerRAID Compaction Detected event occurs when a ServerRAID compaction operation is in progress on a specified logical drive in a ServerRAID configuration.

### Resolution

No resolution. This event is informative only.

### Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Compaction Detected	Compacting: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Harmless	Alert	None

## CIM > System > ServerRAID Compaction Fail

The ServerRAID Compaction Fail event occurs when a ServerRAID compaction operation fails on a specified logical drive in a ServerRAID configuration.



## Resolution

A hardware error occurred. Determine if one or more hard disk drives that are part of the specified logical drive have failed. If such a failure has occurred, restore the data from a tape backup. Otherwise, complete the following steps:

1. Verify that the controller, cables, and hard disk drives are installed correctly.
2. Verify that there is power to the hard disk drives.
3. Retry the command.
4. If the command still fails, restart the server and retry the command.

## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Compaction Fail	Compaction failed: <i>drive [error]</i> where <i>drive</i> is the affected logical drive and <i>error</i> is the error code.	Critical	Alert	None

## CIM > System > ServerRAID Compression Complete

The ServerRAID Compression Complete event occurs when a ServerRAID compression operation is completed on a specified logical drive in a ServerRAID configuration.

## Resolution

No resolution. This event is informative only.

## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Compression Complete	Compression complete: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Harmless	Alert	None

## CIM > System > ServerRAID Compression Detected

The ServerRAID Compression Detected event occurs when a ServerRAID compression operation is in progress on a specified logical drive in a ServerRAID configuration.

### Resolution

No resolution. This event is informative only.

### Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Compression Detected	Compressing: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Harmless	Alert	None

## CIM > System > ServerRAID Compression Fail

The ServerRAID Compression Fail event occurs when a ServerRAID compression operation fails on a specified logical drive in a ServerRAID configuration.

## Resolution

A hardware error occurred. Determine if one or more hard disk drives that are part of the specified logical drive have failed. If such a failure has occurred, restore the data from a tape backup. Otherwise, complete the following steps:

1. Verify that the controller, cables, and hard disk drives are installed correctly.
2. Verify that there is power to the hard disk drives.
3. Retry the command.
4. If the command still fails, restart the server and retry the command.

## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Compression Fail	Compression failed: <i>drive [error]</i> . where <i>drive</i> is the affected logical drive and <i>error</i> is the error code.	Critical	Alert	None

## CIM > System > ServerRAID Config Fail

The ServerRAID Config Fail event occurs when a ServerRAID controller configuration cannot be read.

## Resolution

A hardware error occurred. To correct the error, complete the following steps:

1. Verify that the controller, cables, and hard disk drives are installed correctly.
2. Verify that there is power to the hard disk drives.
3. Retry the command.
4. If the command still fails, restart the server and retry the command.

5. If the problem persists, complete the following steps:
  - a. Restore to factory-default settings.
  - b. Recreate the configuration.

### Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Config Fail	Error getting controller configuration.	Critical	Alert	None

## CIM > System > ServerRAID Controller Added

The ServerRAID Controller Added event occurs when a specified ServerRAID controller is added to a system.

### Resolution

No resolution. This event is informative only.

### Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Controller Added	A controller has been added to the system: <i>controller</i> where <i>controller</i> is the added controller.	Harmless	Alert	None

## CIM > System > ServerRAID Controller Bad Stripes

The ServerRAID Controller Bad Stripes event occurs when one or more logical drives contain at least one bad stripe.

### Resolution

The Bad Stripe Table (BST) provides a means of recovering most data on a logical drive after multiple hardware errors prevent access to a logical drive stripe. An entry in the BST indicates that the data contained in a stripe has been lost.

While many conditions can produce a Bad Stripe Table entry, the most common cause is an error accessing one of the stripe units within a stripe of a critical logical drive. A single stripe unit failure is correctable and recoverable but two or more failures within the same redundant RAID stripe are not.

For example, in a critical RAID-5 array, in which one of the drives in the array is defunct, a stripe will be marked bad with an entry in the BST if a non-recoverable media error occurs when accessing one of the other drives of the array.

After an entry is logged in the BST, the controller will return an error code to the driver whenever the host system tries to access a Logical Block Address (LBA) within the affected stripe. This is one immediate indication that some part of the logical drive is unusable.

**Note:** It is not possible to correlate the bad stripe with a specific file in the operating system.

To resolve this error, complete the following steps:

- Check the ServerRAID Manager event logs to identify the affected logical drive(s).
- Because the data has been lost, the only way to recover from this condition is to complete the following steps:
  1. Delete the array.
  2. Recreate the array and its logical drives.
  3. Restore the data from backup media.

**Note:** The alternative is to take the entire logical drive offline, thus resulting in the loss of all data contained on that logical drive.

To minimize the risk of lost data, schedule frequent periodic backups.

## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Controller Bad Stripes	One or more logical drives contain a bad stripe: <i>controller</i> where <i>controller</i> is the controller for the affected logical drives.	Warning	Alert	None

## CIM > System > ServerRAID Controller Battery Overtemp

The ServerRAID Controller Battery Overtemp event occurs when the battery on a specified ServerRAID controller has exceeded its temperature threshold.

### Resolution

Battery temperature has exceeded 50 degrees Celsius. To resolve this error, complete the following steps:

1. Verify that the controller is installed correctly.
2. Verify that the server has adequate ventilation.
3. If the problem persists, the battery might have failed or the server might require service. Contact your service representative.

## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Controller Battery Overtemp	The battery has exceeded normal operating temperature: <i>controller</i> where <i>controller</i> is the affected controller.	Warning	Alert	None

## CIM > System > ServerRAID Controller Battery Temp Normal

The ServerRAID Controller Battery Temp Normal event occurs when the battery on a specified ServerRAID controller has a normal temperature.

### Resolution

No resolution. This event is informative only.

### Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Controller Battery Temp Normal	The battery operating temperature is normal: <i>controller</i> where <i>controller</i> is the affected controller.	Harmless	Alert	None

## CIM > System > ServerRAID Controller Fail

The ServerRAID Controller Fail event occurs when a specified ServerRAID controller fails.

## Resolution

A hardware error occurred. To correct the error, complete the following steps:

1. Verify that the controller, cables, and hard disk drives are installed correctly.
2. Verify that there is power to the hard disk drives.
3. Retry the command.
4. If the command still fails, restart the server and retry the command.
5. If the problem persists, contact your service representative.

## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Controller Fail	Commands are not responding: <i>controller</i> where <i>controller</i> is the affected controller.	Critical	Alert	None

## CIM > System > ServerRAID Controller Failover

The ServerRAID Controller Failover event occurs when a specified ServerRAID controller fails over and the passive controller in the failover pairing is now active.

## Resolution

No resolution. This event is informative only.



## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Controller Failover	A controller failover was detected: <i>controller</i> where <i>controller</i> is the controller that failed.	Critical	Alert	None

## CIM > System > ServerRAID Controller Mismatched Versions

The ServerRAID Controller Mismatched Versions event occurs when the versions of the BIOS, firmware, and driver for a specified ServerRAID controller do not match.

### Resolution

Upgrade to the latest version of the ServerRAID BIOS, firmware, and device driver.

### Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Controller Mismatched Versions	Version mismatch detected: <i>controller</i> . The BIOS ( <i>version version</i> ), Firmware ( <i>version version</i> ), and Driver ( <i>version version</i> ) are not a matched set and are not compatible.  where <i>controller</i> is the affected controller and <i>version</i> is the version of the affected ServerRAID code.	Warning	Alert	None

## CIM > System > ServerRAID Controller Replaced

The ServerRAID Controller Replaced event occurs when a specified controller is replaced in a ServerRAID configuration.

### Resolution

No resolution. This event is informative only.

### Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Controller Replaced	A controller has been replaced in the system: <i>controller</i> where <i>controller</i> is the affected controller.	Harmless	Alert	None

## CIM > System > ServerRAID Copyback Complete

The ServerRAID Copyback Complete event occurs when a copy-back operation is completed on a specified logical drive in a ServerRAID configuration.

### Resolution

No resolution. This event is informative only.

## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Copyback Complete	Copy back complete: <i>location</i> . where <i>location</i> is the affected controller and array.	Harmless	Alert	None

## CIM > System > ServerRAID Copyback Detected

The ServerRAID Copyback Detected event occurs when a copy-back operation is in progress on a specified logical drive in a ServerRAID configuration.

### Resolution

No resolution. This event is informative only.

### Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Copyback Detected	Copy back in progress: <i>location</i> . Source: Channel <i>channel</i> , SCSI ID <i>id</i> . Target: Channel <i>channel</i> , SCSI ID <i>id</i> . where <ul style="list-style-type: none"><li>• <i>location</i> is the affected controller and array</li><li>• <i>channel</i> is the specified channel</li><li>• <i>id</i> is the specified SCSI ID</li></ul>	Harmless	Alert	None

## CIM > System > ServerRAID Copyback Fail

The ServerRAID Copyback Fail event occurs when a copy-back operation fails on a specified logical drive in a ServerRAID configuration.

### Resolution

A hardware error occurred. To resolve this error, complete the following steps:

1. Verify that the controller, cables, and hard disk drives are installed correctly.
2. Verify that there is power to the hard disk drives.
3. If the command still fails, restart the server and retry the command.
4. If the problem persists, replace the specified drive.

### Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Copyback Fail	Copy back failed: <i>location [error]</i> where <i>location</i> is the affected controller and array and <i>error</i> is the error code.	Critical	Alert	None

## CIM > System > ServerRAID Dead Battery

The ServerRAID Dead Battery event occurs when the battery fails on a specified controller.

### Resolution

To resolve this problem, complete the following steps:

1. Verify that the battery on the battery-backup cache device is installed properly.
2. If the problem persists, replace the battery.

## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Dead Battery	The battery-backup cache device needs a new battery: <i>controller</i> where <i>controller</i> is the affected controller.	Critical	Alert	None

## CIM > System > ServerRAID Dead Battery Cache

The ServerRAID Dead Battery Cache event occurs when the battery-backup cache fails on a specified controller.

### Resolution

The battery-backup cache device is installed improperly or is defective. To resolve this error, complete the following steps:

1. Verify that the battery-backup cache device is installed properly.
2. If the battery-backup cache device is installed properly but is defective, contact your service representative.

### Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Dead Battery Cache	The battery-backup cache device is defective: <i>controller</i> . Error code: <i>error</i> where <i>controller</i> is the affected controller and <i>error</i> is the error code.	Critical	Alert	None

## CIM > System > ServerRAID Decompression Complete

The ServerRAID Decompression Complete event occurs when a ServerRAID decompression operation is completed on a specified logical drive in a ServerRAID configuration.

### Resolution

No resolution. This event is informative only.

### Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Decompression Complete	Decompression complete: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Harmless	Alert	None

## CIM > System > ServerRAID Decompression Detected

The ServerRAID Decompression Detected event occurs when a ServerRAID decompression operation is in progress on a specified logical drive in a ServerRAID configuration.

### Resolution

No resolution. This event is informative only.

## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Decompression Detected	Decompressing: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Harmless	Alert	None

## CIM > System > ServerRAID Decompression Fail

The ServerRAID Decompression Fail event occurs when a ServerRAID decompression operation fails on a specified logical drive in a ServerRAID configuration.

### Resolution

A hardware error occurred. Determine if one or more hard disk drives that are part of the specified logical drive have failed. If such a failure has occurred, restore the data from a tape backup. Otherwise, complete the following steps:

1. Verify that the controller, cables, and hard disk drives are installed correctly.
2. Verify that there is power to the hard disk drives.
3. Retry the command.
4. If the command still fails, restart the server and retry the command.

### Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Decompression Fail	Decompression failed: <i>drive</i> [ <i>error</i> ] where <i>drive</i> is the affected logical drive and <i>error</i> is the error code.	Critical	Alert	None

## CIM > System > ServerRAID Defunct Drive

The ServerRAID Defunct Drive event occurs when a specified hard disk drive fails in a ServerRAID configuration.

### Resolution

A hardware error occurred. To resolve the error, complete one of the following steps:

- If the specified hard disk drive is part of an array, refer to the event pertaining to the logical drives in that array for additional information.
- If the specified hard disk drive is not part of an array, contact your service representative.

### Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Defunct Drive	Defunct drive: <i>location</i> . where <i>location</i> is the affected controller and port.	Critical	Alert	None

## CIM > System > ServerRAID Defunct Drive FRU

The ServerRAID Defunct Drive FRU event occurs when a specified hard disk drive with the provided field-replaceable unit (FRU) number fails in a ServerRAID configuration.

### Resolution

A hardware error occurred. To resolve the error, complete one of the following steps:

- If the specified hard disk drive is part of an array, refer to the event pertaining to the logical drives in that array for additional information.
- If the specified hard disk drive is not part of an array, contact your service representative.



## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Defunct Drive FRU	Defunct drive: <i>location</i> (FRU Part # <i>FRU</i> ). where <i>location</i> is the affected controller and port and <i>FRU</i> is the FRU number of the hard disk drive.	Critical	Alert	None

## CIM > System > ServerRAID Defunct Replaced

The ServerRAID Defunct Replaced event occurs when a specified defunct hard disk drive has been set to the hot-spare state in a ServerRAID configuration.

### Resolution

No resolution. This event is informative only.

### Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Defunct Replaced	Defunct drive: <i>location</i> ( <i>error</i> ). where <i>location</i> is the affected controller and port and <i>error</i> is the error code.	Harmless	Alert	None

## CIM > System > ServerRAID Drive Added

The ServerRAID Drive Added event occurs when a specified hard disk drive is added to a ServerRAID configuration.

## Resolution

No resolution. This event is informative only.

## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Drive Added	Physical drive added: <i>location</i> where <i>location</i> is the affected controller and port.	Harmless	Alert	None

## CIM > System > ServerRAID Drive Clear Complete

The ServerRAID Drive Clear Complete event occurs when a ServerRAID clear operation is completed on a specified hard disk drive in a ServerRAID configuration.

## Resolution

No resolution. This event is informative only.

## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Drive Clear Complete	Clear complete: <i>drive</i> . where <i>drive</i> is the affected hard disk drive.	Harmless	Alert	None

## CIM > System > ServerRAID Drive Clear Detected

The ServerRAID Drive Clear Detected event occurs when a ServerRAID clear operation is in progress on a specified hard disk drive in a ServerRAID configuration.

### Resolution

No resolution. This event is informative only.

### Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Drive Clear Detected	Clearing: <i>drive</i> . where <i>drive</i> is the affected hard disk drive.	Harmless	Alert	None

## CIM > System > ServerRAID Drive Clear Fail

The ServerRAID Drive Clear Fail event occurs when a ServerRAID clear operation fails on a specified hard disk drive in a ServerRAID configuration.

### Resolution

A hardware error occurred. To resolve the error, complete the following steps:

1. Verify that the controller, cables, and hard disk drives are installed correctly.
2. Verify that there is power to the hard disk drives.
3. Retry the command.
4. If the command still fails, restart the server and retry the command.
5. If the command still fails, replace the specified drive.
6. If the problem persists, contact your service representative.

## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Drive Clear Fail	Clear failed: <i>drive [error]</i> where <i>drive</i> is the affected hard disk drive and <i>error</i> is the error code.	Critical	Alert	None

## CIM > System > ServerRAID Drive Removed

The ServerRAID Drive Removed event occurs when a specified hard disk drive is removed from a ServerRAID configuration.

### Resolution

No resolution. This event is informative only.

### Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Drive Removed	Physical drive removed: <i>location</i> . where <i>location</i> is the affected controller and port.	Harmless	Alert	None

## CIM > System > ServerRAID Drive Verify Complete

The ServerRAID Drive Verify Complete event occurs when a ServerRAID verify operation is completed on a specified hard disk drive in a ServerRAID configuration.

## Resolution

No resolution. This event is informative only.

## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Drive Verify Complete	Verify complete: <i>drive</i> . where <i>drive</i> is the affected hard disk drive..	Harmless	Alert	None

## CIM > System > ServerRAID Drive Verify Detected

The ServerRAID Drive Verify Detected event occurs when a ServerRAID verify operation is in progress on a specified hard disk drive in a ServerRAID configuration.

## Resolution

No resolution. This event is informative only.

## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Drive Verify Detected	Verifying: <i>drive</i> . where <i>drive</i> is the affected hard disk drive.	Harmless	Alert	None

## CIM > System > ServerRAID Drive Verify Fail

The ServerRAID Drive Verify Fail event occurs when a ServerRAID verify operation fails on a specified hard disk drive in a ServerRAID configuration.

### Resolution

A hardware error occurred. Verify that the specified logical drive is not offline or critical (that is, one hard disk drive that is offline in a RAID level-1, 1E, 5, 5E, 10, 1E0, or 50 logical drive). If the logical drive is critical, replace the failed hard disk drive. If the logical drive is offline, replace the failed hard disk drives and restore the data from tape backup.

If the source or target logical drives are *not* offline or critical, complete the following steps:

1. Verify that the controller, cables, and hard disk drives are installed correctly.
2. Verify that there is power to the hard disk drives.
3. Retry the command.
4. If the command still fails, restart the server and retry the command.
5. If the problem persists, contact your service representative.

### Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Drive Verify Fail	Verify failed: <i>drive</i> . where <i>drive</i> is the affected hard disk drive.	Critical	Alert	None

## CIM > System > ServerRAID Enclosure Fail

The ServerRAID Enclosure Fail event occurs when an enclosure has failed on a specified controller and channel in a ServerRAID configuration.

## Resolution

A hardware error occurred. To resolve the error, complete the following steps:

1. Verify that the controller, cables, and hard disk drives are installed correctly.
2. Verify that there is power to the hard disk drives.
3. Retry the command.
4. If the command still fails, restart the server and retry the command.
5. If the problem persists, contact your service representative.

## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Enclosure Fail	Enclosure device is not responding: <i>location</i> where <i>location</i> is the controller and channel that the affected enclosure is attached to.	Critical	Alert	None

## CIM > System > ServerRAID Enclosure Fan Fail

The ServerRAID Enclosure Fan Fail event occurs when a specified enclosure fan fails on a specified controller and channel in a ServerRAID configuration.

## Resolution

A hardware error occurred. Verify that the fan in the enclosure device is installed correctly. If it is, complete the following steps:

1. Verify that the controller, cables, and hard disk drives are installed correctly.
2. Verify that there is power to the hard disk drives.
3. Retry the command.

4. If the command still fails, restart the server and retry the command.
5. If the problem persists, replace the specified fan.

## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Enclosure Fan Fail	Enclosure fan <i>fan</i> is malfunctioning: <i>location</i> where <i>fan</i> is the affected fan and <i>location</i> is the controller and channel that the affected enclosure is attached to.	Critical	Alert	None

## CIM > System > ServerRAID Enclosure Fan Installed

The ServerRAID Enclosure Fan Installed event occurs when a specified enclosure fan is installed on a specified controller and channel in a ServerRAID configuration.

## Resolution

No resolution. This event is informative only.

## Details

**Note:** This event is new in IBM Director 5.10.

The ServerRAID Agent sends these events for IBM Director to indicate that a change has occurred in the ServerRAID subsystem.



Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Enclosure Fan Installed	Enclosure fan <i>fan</i> has been installed: <i>location</i> where <i>fan</i> is the affected fan and <i>location</i> is the controller and channel that the affected enclosure is attached to.	Harmless	Alert	None

## CIM > System > ServerRAID Enclosure Fan OK

The ServerRAID Enclosure Fan OK event occurs when a specified enclosure fan is functioning correctly on a specified controller and channel in a ServerRAID configuration.

### Resolution

No resolution. This event is informative only.

### Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Enclosure Fan OK	Enclosure fan <i>fan</i> is now operational: <i>location</i> where <i>fan</i> is the affected fan and <i>location</i> is the controller and channel that the affected enclosure is attached to.	Harmless	Alert	None

## CIM > System > ServerRAID Enclosure Fan Removed

The ServerRAID Enclosure Fan Removed event occurs when a specified enclosure fan is removed on a specified controller and channel in a ServerRAID configuration.

## Resolution

No resolution. This event is informative only.

## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Enclosure Fan Removed	Enclosure fan <i>fan</i> has been removed: <i>location</i> where <i>fan</i> is the affected fan and <i>location</i> is the controller and channel that the affected enclosure is attached to.	Warning	Alert	None

## CIM > System > ServerRAID Enclosure OK

The ServerRAID Enclosure OK event occurs when an enclosure is functioning correctly on a specified controller and channel in a ServerRAID configuration.

## Resolution

No resolution. This event is informative only.

## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Enclosure OK	Enclosure device is responding: <i>location</i> where <i>location</i> is the controller and channel that the affected enclosure is attached to.	Harmless	Alert	None

## CIM > System > ServerRAID Enclosure Power Supply Fail

The ServerRAID Enclosure Power Supply Fail event occurs when the specified enclosure power supply fails in a ServerRAID configuration.

### Resolution

A hardware error occurred. Verify that the power supply in the enclosure device is installed correctly. If it is, complete the following steps:

1. Verify that the controller, cables, and hard disk drives are installed correctly.
2. Verify that there is power to the hard disk drives.
3. Retry the command.
4. If the command still fails, restart the server and retry the command.
5. If the problem persists, replace the specified power supply.

### Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Enclosure Power Supply Fail	Enclosure power supply <i>supply</i> is malfunctioning: <i>location</i>  where <i>supply</i> is the affected power supply and <i>location</i> is the controller and channel that the affected enclosure is attached to.	Critical	Alert	None

## CIM > System > ServerRAID Enclosure Power Supply Installed

The ServerRAID Enclosure Power Supply Installed event occurs when a specified enclosure power supply is installed in a ServerRAID configuration.

## Resolution

No resolution. This event is informative only.

## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Enclosure Power Supply Installed	Enclosure power supply <i>supply</i> has been installed: <i>location</i> where <i>supply</i> is the affected power supply and <i>location</i> is the controller and channel that the affected enclosure is attached to.	Harmless	Alert	None

## CIM > System > ServerRAID Enclosure Power Supply OK

The ServerRAID Enclosure Power Supply OK event occurs when a specified enclosure power supply is functioning correctly in a ServerRAID configuration.

## Resolution

No resolution. This event is informative only.

## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Enclosure Power Supply OK	Enclosure power supply <i>supply</i> is now operational: <i>location</i> where <i>supply</i> is the affected power supply and <i>location</i> is the controller and channel that the affected enclosure is attached to.	Harmless	Alert	None

## CIM > System > ServerRAID Enclosure Power Supply Removed

The ServerRAID Enclosure Power Supply Removed event occurs when a specified enclosure power supply is removed from a ServerRAID configuration.

### Resolution

No resolution. This event is informative only.

### Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Enclosure Power Supply Removed	Enclosure power supply <i>supply</i> has been removed: <i>location</i> where <i>supply</i> is the affected power supply and <i>location</i> is the controller and channel that the affected enclosure is attached to.	Warning	Alert	None

## CIM > System > ServerRAID Enclosure Temp Fail

The ServerRAID Enclosure Fan Fail event occurs when an enclosure temperature exceeds a normal range on a specified controller in a ServerRAID configuration.

### Resolution

A hardware error occurred. Verify that the fans in the enclosure device are installed correctly and working. If they are, complete the following steps:

1. Verify that the controller, cables, and hard disk drives are installed correctly.
2. Retry the command.
3. If the command still fails, restart the server and retry the command.
4. If the problem persists, contact your service representative.

### Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Enclosure Temp Fail	Enclosure temperature is out of the normal range: <i>location</i> where <i>location</i> is the controller and channel that the affected enclosure is attached to.	Critical	Alert	None

## CIM > System > ServerRAID Enclosure Temp OK

The ServerRAID Enclosure Temp OK event occurs when an enclosure temperature is within a normal range on a specified controller in a ServerRAID configuration.

### Resolution

No resolution. This event is informative only.

## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Enclosure Temp OK	Enclosure temperature is in the normal range: <i>location</i> where <i>location</i> is the controller and channel that the affected enclosure is attached to.	Harmless	Alert	None

## CIM > System > ServerRAID Expansion Complete

The ServerRAID Expansion Complete event occurs when a ServerRAID expansion operation is completed on a specified logical drive in a ServerRAID configuration.

### Resolution

No resolution. This event is informative only.

### Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Expansion Complete	Expansion complete: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Harmless	Alert	None

## CIM > System > ServerRAID Expansion Detected

The ServerRAID Expansion Detected event occurs when a ServerRAID expansion operation is in progress on a specified logical drive in a ServerRAID configuration.

## Resolution

No resolution. This event is informative only.

## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Expansion Detected	Expanding: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Harmless	Alert	None

## CIM > System > ServerRAID Expansion Fail

The ServerRAID Expansion Fail event occurs when a ServerRAID expansion operation fails on a specified logical drive in a ServerRAID configuration.

## Resolution

A hardware error occurred. Determine if one or more hard disk drives that are part of the specified logical drive have failed. If such a failure has occurred, restore the data from a tape backup. Otherwise, complete the following steps:

1. Verify that the controller, cables, and hard disk drives are installed correctly.
2. Verify that there is power to the hard disk drives.
3. Retry the command.
4. If the command still fails, restart the server and retry the command.



## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Expansion Fail	Expansion failed: <i>drive [error]</i> . where <i>drive</i> is the affected logical drive and <i>error</i> is the error code.	Critical	Alert	None

## CIM > System > ServerRAID FlashCopy Complete

The ServerRAID FlashCopy Complete event occurs when a ServerRAID FlashCopy operation is completed on a specified logical drive in a ServerRAID configuration.

### Resolution

No resolution. This event is informative only.

### Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID FlashCopy Complete	FlashCopy with backup complete: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Harmless	Alert	None

## CIM > System > ServerRAID FlashCopy Detected

The ServerRAID FlashCopy Detected event occurs when a ServerRAID FlashCopy operation is in progress on a specified logical drive in a ServerRAID configuration.

## Resolution

No resolution. This event is informative only.

## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID FlashCopy Detected	FlashCopy in progress: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Harmless	Alert	None

## CIM > System > ServerRAID FlashCopy Fail

The ServerRAID FlashCopy Fail event occurs when a ServerRAID FlashCopy operation fails on a specified logical drive in a ServerRAID configuration.

## Resolution

The FlashCopy operation failed because a hardware error occurred. The specified logical drive might be offline. If the source logical drive is offline, replace the failed hard disk drives and restore the data from tape backup. If the target logical drive is offline, replace the failed hard disk drives. FlashCopy operations will not work when the source or target logical drives are offline.

If the source or target logical drives are not offline, complete the following steps:

1. Verify that the controller, cables, and hard disk drives are installed correctly.
2. Verify that there is power to the hard disk drives.
3. Retry the command.
4. If the command still fails, restart the server and retry the command.
5. If the problem persists, contact your service representative.

## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID FlashCopy Fail	FlashCopy with backup failed: <i>drive [error]</i> . where <i>drive</i> is the affected logical drive and <i>error</i> is the error code.	Critical	Alert	None

## CIM > System > ServerRAID Health Event

The ServerRAID Health Event event occurs on managed systems installed with IBM Director Agent 4.1, 4.10.2, 4.11, 4.12, 4.20, 4.20.2, 4.21, and 4.22 as well as the ServerRAID Agent feature.

### Event source

This event is generated by managed systems installed with the following versions of IBM Director Agent:

- 4.1
- 4.10.2
- 4.11
- 4.12
- 4.20
- 4.20.2
- 4.21
- 4.22

These managed systems also must have the ServerRAID Manager Agent feature installed.

**Note:** These events are not generated by the ServerRAID Manager (Standalone Edition).

## Details

**Note:** This event is deprecated and not supported by IBM Director Core Services or IBM Director Agent 5.10. The event is provided for compatibility with previous supported versions of IBM Director Agent.

For detailed information about this event, see the *IBM Director 4.20 Events Reference*.

## CIM > System > ServerRAID Init Complete

The ServerRAID Init Complete event occurs when a ServerRAID initialization operation is completed on a specified logical drive in a ServerRAID configuration.

### Resolution

No resolution. This event is informative only.

### Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Init Complete	Clear complete: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Harmless	Alert	None

## CIM > System > ServerRAID Init Detected

The ServerRAID Init Detected event occurs when a ServerRAID initialization operation is in progress on a specified logical drive in a ServerRAID configuration.

### Resolution

No resolution. This event is informative only.

## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Init Detected	Clearing: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Harmless	Alert	None

## CIM > System > ServerRAID Init Fail

The ServerRAID Init-Fail event occurs when a ServerRAID initialization operation fails on a specified logical drive in a ServerRAID configuration.

### Resolution

A hardware error occurred. Verify that the specified logical drive is not offline. If the logical drive is offline, replace the failed hard disk drives and restore the data from tape backup. If the specified logical drive is not offline, complete the following steps:

1. Verify that the controller, cables, and hard disk drives are installed correctly.
2. Verify that there is power to the hard disk drives.
3. Retry the command.
4. If the command still fails, restart the server and retry the command.
5. If the problem persists, contact your service representative.

### Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Init Fail	Initialize failed: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Critical	Alert	None

## CIM > System > ServerRAID Logical Drive Added

The ServerRAID Logical Drive Added event occurs when a specified logical drive is added in a ServerRAID configuration.

### Resolution

No resolution. This event is informative only.

### Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Logical Drive Added	Added logical drive: <i>drive</i> . Size <i>data</i> . where <i>drive</i> is the affected logical drive and <i>data</i> is the size and RAID level of that logical drive.	Harmless	Alert	None

## CIM > System > ServerRAID Logical Drive Blocked

The ServerRAID Logical Drive Blocked event occurs when a specified logical drive is in the blocked state.

### Resolution

When the ServerRAID controller performs a rebuild operation on an array, it reconstructs the data that was stored in RAID level-1 and RAID level-5 logical drives. However, the ServerRAID controller cannot reconstruct the data that was stored in any RAID level-0 logical drives in that array. The data in the RAID level-0 logical drives is blocked when the ServerRAID controller detects that the array is valid, but the data might be damaged.

To resolve this error, unblock the logical drive after the rebuild is complete. Restore the data from tape.

## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Logical Drive Blocked	Logical drive is blocked: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Critical	Alert	None

## CIM > System > ServerRAID Logical Drive Critical

The ServerRAID Logical Drive Critical event occurs when a specified logical drive is in the critical state.

### Resolution

A hard disk drive is defunct in the specified logical drive. The data on this logical drive is at risk. If another hard disk drive fails, the data might be lost.

Complete one of the following actions:

- If a rebuild operation is in progress, wait until the rebuild is complete.
- If a rebuild operation is not in progress, replace the failed hard disk drive with a new hard disk drive. After the hard disk drive is replaced, a rebuild operation will start automatically. See the troubleshooting chapter of the *IBM ServerRAID User's Reference*.

### Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Logical Drive Critical	Logical drive is critical: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Warning	Alert	None

## CIM > System > ServerRAID Logical Drive Critical Periodic

The ServerRAID Logical Drive Critical Periodic event occurs when a periodic scan detects that one or more logical drives are in a critical state.

### Resolution

A hard disk drive is defunct in the specified logical drive. The data on this logical drive is at risk. If another hard disk drive fails, the data might be lost.

Complete one of the following actions:

- If a rebuild operation is in progress, wait until the rebuild is complete.
- If a rebuild operation is not in progress, replace the failed hard disk drive with a new hard disk drive. After the hard disk drive is replaced, a rebuild operation will start automatically. See the troubleshooting chapter of the *IBM ServerRAID User's Reference*.

### Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Logical Drive Critical Periodic	Periodic scan found one or more critical logical drives: <i>drive</i> . Repair as soon as possible to avoid data loss. where <i>drive</i> is the affected logical drive.	Warning	Alert	None

## CIM > System > ServerRAID Logical Drive Off Line

The ServerRAID Logical Drive Off Line event occurs when a specified logical drive is in the offline state.

### Resolution

A hardware error occurred. Contact your service representative.



## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Logical Drive Off Line	Logical drive is offline: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Critical	Alert	None

## CIM > System > ServerRAID Logical Drive OK

The ServerRAID Logical Drive OK event occurs when a specified logical drive is functioning correctly.

### Resolution

No resolution. This event is informative only.

### Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Logical Drive OK	Logical drive is normal: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Harmless	Alert	None

## CIM > System > ServerRAID Logical Drive Removed

The ServerRAID Logical Drive Removed event occurs when a specified logical drive has been removed from a ServerRAID configuration.

### Resolution

No resolution. This event is informative only.

## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Logical Drive Removed	Deleted logical drive: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Harmless	Alert	None

## CIM > System > ServerRAID Logical Drive Unblocked

The ServerRAID Logical Drive Unblocked event occurs . when a specified logical drive is in the unblocked state.

### Resolution

No resolution. This event is informative only.

### Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Logical Drive Unblocked	Unblocked logical drive: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Harmless	Alert	None

## CIM > System > ServerRAID Migration Complete

The ServerRAID Migration Complete event occurs when a ServerRAID logical-drive migration is completed on a specified logical drive in a ServerRAID configuration.

### Resolution

No resolution. This event is informative only.

## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Migration Complete	Migration complete: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Harmless	Alert	None

## CIM > System > ServerRAID Migration Detected

The ServerRAID Migration Detected event occurs when a ServerRAID logical-drive migration is in progress on a specified logical drive in a ServerRAID configuration.

### Resolution

No resolution. This event is informative only.

### Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Migration Detected	Migrating: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Harmless	Alert	None

## CIM > System > ServerRAID Migration Fail

The ServerRAID Migration Fail event occurs when a ServerRAID logical-drive migration fails on a specified logical drive in a ServerRAID configuration.

## Resolution

A hardware error occurred. Determine if one or more hard disk drives that are part of the specified logical drive have failed. If such a failure has occurred, restore the data from a tape backup. Otherwise, complete the following steps:

1. Verify that the controller, cables, and hard disk drives are installed correctly.
2. Verify that there is power to the hard disk drives.
3. Retry the command.
4. If the command still fails, restart the server and retry the command.

## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Migration Fail	Migration failed: <i>drive [error]</i> where <i>drive</i> is the affected logical drive and <i>error</i> is the error code.	Critical	Alert	None

## CIM > System > ServerRAID No Controllers

The ServerRAID No Controllers event occurs when no ServerRAID controllers are detected.

## Resolution

No resolution. This event is informative only.

## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID No Controllers	No controllers were found in this system	Harmless	Alert	None

## CIM > System > ServerRAID PFA Drive

The ServerRAID PFA Drive event occurs when a Predictive Failure Analysis (PFA) is detected on a specified hard disk drive in a ServerRAID configuration.

### Resolution

The hard disk drive is going to fail. Contact your service representative.

### Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID PFA Drive	PFA detected for drive: <i>drive</i> . where <i>drive</i> is the affected hard disk drive.	Warning	Alert	None

## CIM > System > ServerRAID PFA Drive FRU

The ServerRAID PFA Drive FRU event occurs when a Predictive Failure Analysis (PFA) is detected on a specified hard disk drive with a specified field-replaceable unit (FRU) number in a ServerRAID configuration.

### Resolution

The hard disk drive is going to fail. Contact your service representative.

## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID PFA Drive FRU	PFA detected for drive: <i>drive (FRU)</i> . where <i>drive</i> is the affected hard disk drive and <i>FRU</i> is the FRU number of that drive.	Warning	Alert	None

## CIM > System > ServerRAID Polling Fail

The ServerRAID Polling Fail event occurs when a specified controller fails to respond to background polling commands.

### Resolution

A hardware error occurred. To resolve this error, complete the following steps:

1. Verify that the controller, cables, and hard disk drives are installed correctly.
2. Verify that there is power to the hard disk drives.
3. Retry the command.
4. If the problem persists, contact your service representative.

### Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Polling Fail	Background polling commands are not responding: <i>controller</i> . Result codes: <i>error</i> where <i>controller</i> is the affected controller and <i>error</i> is the error code.	Warning	Alert	None

## CIM > System > ServerRAID Rebuild Complete

The ServerRAID Rebuild Complete event occurs when a ServerRAID rebuild operation is completed on a specified logical drive in a ServerRAID configuration.

### Resolution

No resolution. This event is informative only.

### Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Rebuild Complete	Rebuild complete: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Harmless	Alert	None

## CIM > System > ServerRAID Rebuild Detected

The ServerRAID Rebuild Detected event occurs when a ServerRAID rebuild operation is in progress on a specified logical drive in a ServerRAID configuration.

### Resolution

No resolution. This event is informative only.

## Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Rebuild Detected	Rebuilding: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Harmless	Alert	None

## CIM > System > ServerRAID Rebuild Fail

The ServerRAID event occurs when a ServerRAID rebuild operation fails on a specified logical drive in a ServerRAID configuration.

### Resolution

A hardware error occurred. To resolve the error, complete the following steps:

1. Verify that the controller, cables, and hard disk drives are installed correctly.
2. Verify that there is power to the hard disk drives.
3. If the command still fails, restart the server and retry the command.
4. If the problem persists, replace the specified drive.

### Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Rebuild Fail	Rebuild failed: <i>drive</i> [ <i>error</i> ]. where <i>drive</i> is the affected logical drive and <i>error</i> is the error code.	Critical	Alert	None



## CIM > System > ServerRAID Sync Complete

The ServerRAID Sync Complete event occurs when a ServerRAID synchronization operation is completed on a specified logical drive in a ServerRAID configuration.

### Resolution

No resolution. This event is informative only.

### Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Sync Complete	Synchronize complete: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Harmless	Alert	None

## CIM > System > ServerRAID Sync Detected

The ServerRAID Sync Detected event occurs when a ServerRAID synchronization operation is in progress on a specified logical drive in a ServerRAID configuration.

### Resolution

No resolution. This event is informative only.

### Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Sync Detected	Synchronizing: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Harmless	Alert	None

## CIM > System > ServerRAID Sync Fail

The ServerRAID Sync Fail event occurs when a ServerRAID synchronization operation fails on a specified logical drive in a ServerRAID configuration.

### Resolution

A hardware error occurred. Verify that the specified logical drive is not offline or critical (that is, one hard disk drive that is offline in a RAID level-1, 1E, 5, 5E, 10, 1E0, or 50 logical drive). If the logical drive is critical, replace the failed hard disk drive. If the logical drive is offline, replace the failed hard disk drives and restore the data from tape backup.

If the specified logical drive is *not* offline or critical, complete the following steps:

1. Verify that the controller, cables, and hard disk drives are installed correctly.
2. Verify that there is power to the hard disk drives.
3. Retry the command.
4. If the command still fails, restart the server and retry the command.
5. If the problem persists, contact your service representative.

### Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Sync Fail	Synchronize failed: <i>drive [error]</i> where <i>drive</i> is the affected logical drive and <i>error</i> is the error code.	Critical	Alert	None

## CIM > System > ServerRAID Test Event

The ServerRAID Test Event event occurs when a ServerRAID test event is generated.

### Resolution

No resolution. This event is informative only.

### Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Test Event	This is a test event.	Harmless	Alert	None

## CIM > System > ServerRAID Unsupported Drive

The ServerRAID Unsupported Drive event occurs when an unsupported hard disk drive is detected in a ServerRAID configuration.

### Resolution

Replace the specified hard disk drive with a hard disk drive model that is supported by IBM ServerRAID controllers.

### Details

**Note:** This event is new in IBM Director 5.10.

Event type	Event text	Severity	Category	Additional extended attributes
ServerRAID Unsupported Drive	Possible non-warranted physical drive found: <i>drive</i> . where <i>drive</i> is the affected hard disk drive.	Warning	Alert	None

## CIM > System > SMART Drive

The SMART Drive event occurs when the state of an IDE or SCSI hard disk drive that complies with the self-monitoring, analysis, and reporting technology (SMART) changes with respect to its availability.

### Resolution

- If the severity is Critical: Replace the specified hard disk drive that is failing or has failed.
- If the severity is Normal: The error has been resolved. This event is informative only.

### Details

Event type	Event text	Severity	Category	Additional extended attributes
SMART Drive	<i>Device</i> device identified as physical drive <i>drive</i> is predicting an imminent failure. where <i>Device</i> is IDE, SCSI, or Unknown and <i>drive</i> is the affected SMART drive.	Critical	Alert	None
SMART Drive	<i>Device</i> device identified as physical drive <i>drive</i> is not predicting a failure. where <i>Device</i> is IDE, SCSI, or Unknown and <i>drive</i> is the affected SMART drive.	Normal	Resolution	None

## CIM > System > System Enclosure

The System Enclosure event occurs when the state of a system chassis (enclosure) changes, such as when the cover is removed from the system.

### Resolution

- If the severity is Critical: Make sure that the chassis cover is closed.
- If the severity is Normal: The error has been resolved. This event is informative only.

## Details

Event type	Event text	Severity	Category	Additional extended attributes
System Enclosure	System Enclosure Sensor reported intrusion detection.	Critical	Alert	None
System Enclosure	System Enclosure Sensor reports normal.	Normal	Resolution	None

### CIM > System > System Event

The System Event event occurs when a change in the hardware status of a CEC or LPAR managed by the HMC is detected.

#### Resolution

No resolution. This event is informative only.

#### Event source

CIM event types for HMC are generated by the CIMOM running on the HMC.

#### Details

**Note:** This event is new in IBM Director 5.10.

The CIM > System event types for HMC use the following standard set of extended attributes:

- AlertingManagedElement
- EventID
- EventTime
- SenderUUID

Event type	Event text	Severity	Category	Additional extended attributes
System Event	<b>Note:</b> This text varies depending on the System event that is received on the HMC. The provided text is a description of that System event occurrence.	Warning	Alert	None

## CIM > System > Temperature

The Temperature event occurs when the state of a system temperature sensor changes with respect to a manufacturer-defined or user-defined threshold.

### Resolution

- If the severity is Critical or Warning: Identify the cause of the temperature increase. If necessary, increase the cooling capacity.
- If the severity is Normal: The error has been resolved. This event is informative only.

### Details

Event type	Event text	Severity	Category	Additional extended attributes
Temperature	Temperature Sensor <i>number</i> exceeded the manufacturer defined threshold of <i>threshold</i> Celsius. The current value is <i>current</i> Celsius. where: <ul style="list-style-type: none"> <li>• <i>number</i> is the affected temperature sensor.</li> <li>• <i>threshold</i> is the manufacturer-defined threshold value.</li> <li>• <i>current</i> is the current temperature reading.</li> </ul>	Critical	Alert	None

Event type	Event text	Severity	Category	Additional extended attributes
Temperature	<p>Temperature Sensor <i>number</i> exceeded the user defined threshold of <i>threshold</i> Celsius. The current value is <i>current</i> Celsius.</p> <p>where:</p> <ul style="list-style-type: none"> <li>• <i>number</i> is the affected temperature sensor.</li> <li>• <i>threshold</i> is the user-defined threshold value.</li> <li>• <i>current</i> is the current temperature reading.</li> </ul>	Critical	Alert	None
Temperature	<p>Temperature Sensor <i>number</i> exceeded the manufacturer defined threshold of <i>threshold</i> Celsius. The current value is <i>current</i> Celsius.</p> <p>where:</p> <ul style="list-style-type: none"> <li>• <i>number</i> is the affected temperature sensor.</li> <li>• <i>threshold</i> is the manufacturer-defined threshold value.</li> <li>• <i>current</i> is the current temperature reading.</li> </ul>	Warning	Alert	None
Temperature	<p>Temperature Sensor <i>number</i> exceeded the user defined threshold of <i>threshold</i> Celsius. The current value is <i>current</i> Celsius.</p> <p>where:</p> <ul style="list-style-type: none"> <li>• <i>number</i> is the affected temperature sensor.</li> <li>• <i>threshold</i> is the user-defined threshold value.</li> <li>• <i>current</i> is the current temperature reading.</li> </ul>	Warning	Alert	None
Temperature	<p>Temperature Sensor <i>number</i> reports normal. where <i>number</i> is the affected temperature sensor.</p>	Normal	Resolution	None

## CIM > System > Voltage

The Voltage event occurs when the state of a system voltage sensor changes with respect to a manufacturer-defined threshold.

### Resolution

- If the severity is Critical: Identify the cause of the voltage problem. Make sure that the power supply is working. If necessary, replace the power supply.
- If the severity is Normal: The error has been resolved. This event is informative only.

**Note:** After correcting the hardware error, you must clear this event manually.

### Details

Event type	Event text	Severity	Category	Additional extended attributes
Voltage	Voltage Sensor <i>number</i> fell below threshold of <i>threshold</i> Volts. The current value is <i>current</i> Volts.  where: <ul style="list-style-type: none"><li>• <i>number</i> is the affected voltage sensor.</li><li>• <i>threshold</i> is the threshold value.</li><li>• <i>current</i> is the current voltage reading.</li></ul>	Critical	Alert	None
Voltage	Voltage Sensor <i>number</i> exceeded threshold of <i>threshold</i> Volts. The current value is <i>current</i> Volts.  where: <ul style="list-style-type: none"><li>• <i>number</i> is the affected voltage sensor.</li><li>• <i>threshold</i> is the threshold value.</li><li>• <i>current</i> is the current voltage reading.</li></ul>	Critical	Alert	None
Voltage	Voltage Sensor <i>number</i> reports normal.  where <i>number</i> is the affected voltage sensor.	Normal	Resolution	None



## CIM > System > Warranty Expiration

The Warranty Expiration event occurs when the system warranty expiration date has been reached with respect to the value configured for the date while using the Asset ID task.

### Resolution

- If the severity is Warning: The warranty has expired.
- If the severity is Normal: The error has been resolved. This event is informative only.

### Details

The date value in the event text is provided by the Asset ID task. The Warranty page in the Asset ID task includes the **End Date** field where you can set the lease expiration date. The date is stored in the IBMPSG\_Warranty.EndDate CIM property that is monitored at regular poll intervals. A CIM indication is generated when the system CIMOM starts and when a state change is detected relative to the internal poll interval.

Event type	Event text	Severity	Category	Additional extended attributes
Warranty Expiration	The warranty on <i>system</i> has expired. It expired on <i>date</i> . where <i>system</i> is the affected system and <i>date</i> is the warranty expiration date.	Warning	Alert	None
Warranty Expiration	The warranty on <i>system</i> is normal. It will expire on <i>date</i> . where <i>system</i> is the affected system and <i>date</i> is the warranty expiration date.	Normal	Resolution	None

---

## **CIM > Windows NT Event Log**

The Windows NT<sup>®</sup> Event Log events are generated by IBM Director Server when it receives events from the Windows operating system. If an IBM Director environment does not include any systems running Windows, these events are not available.

These CIM event types map to the Windows Event Log events in the IBM Director Event Filter Builder tree. For more information about the Windows event log, see the Windows event log documentation.

---

## **CIM > Windows NT Service**

The Windows NT Service events are generated by IBM Director Server when it receives events from the Windows operating system. If an IBM Director environment does not include any systems running Windows, these events are not available.

These CIM event types map to the Windows Event Log events in the IBM Director Event Filter Builder tree. For more information about the Windows event log, see the Windows event log documentation.

---

## **CIM > Windows Registry**

The Windows Registry events are generated by IBM Director Server when it receives events from the Windows operating system. If an IBM Director environment does not include any systems running Windows, these events are not available.

These CIM event types map to the Windows Event Log events in the IBM Director Event Filter Builder tree. For more information about the Windows event log, see the Windows event log documentation.

---

## Chapter 8. Configuration Manager events

The Configuration Manager event types occur when a profile is executed. For detailed Configuration Manager event types, expand the **Configuration Manager** node in the Event Filter Builder tree.

### Event source

These event types are generated by the Configuration Manager task from IBM Director Server.

### Details

If you select the **Configuration Manager** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Configuration Manager subtree. You can choose to select specific event types that are displayed under the **Configuration Manager** node in the Event Filter Builder tree. The event filter will process only the event types that you select.

Event type	Event text	Severity	Category	Extended attributes
Configuration Manager	Not applicable	Not applicable	Not applicable	None

---

## Configuration Manager > Profile

The Profile events occur when executing a profile.

### Details

If you select the **Profile** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Profile subtree.

Event type	Event text	Severity	Category	Extended attributes
Profile	Not applicable	Not applicable	Not applicable	None

You can choose to select specific event types that are displayed under the **Profile** node in the Event Filter Builder tree. The event filter will process only the event types that you select.

These event types use the following extended attributes:

- *Profile Name* is the name of the profile that is being applied to the target managed object.
- *Failed Components* identifies the components that failed the configuration. The attribute provides a list of one or more affected components separated by commas.
- *Empty Components* identifies the components for which the profile did not provide configuration information. The attribute provides a list of one or more affected components separated by commas.
- *Configured Components* identifies the components that were configured successfully by the profile. The attribute provides a list of one or more affected components separated by commas.

Event type	Event text	Severity	Category	Additional extended attributes
Execution	The Configuration Manager profile was applied successfully.	Harmless	Alert	None
Execution	The Configuration Manager profile was applied, but the settings for one or more components failed.	Warning	Alert	None
Execution	The Configuration Manager profile failed to be applied.	Critical	Alert	None
Execution	The Configuration Manager profile does not contain any configuration information to apply.	Harmless	Alert	None

<b>Event type</b>	<b>Event text</b>	<b>Severity</b>	<b>Category</b>	<b>Additional extended attributes</b>
Execution	Configuration Manager general failure: see the TWGRas.log file.	Critical	Alert	None
Execution	The Configuration Manager could not find the specified profile.	Critical	Alert	None
Execution	The target for the Configuration Manager profile is locked.	Critical	Alert	None
Execution	The target for the Configuration Manager profile is offline.	Critical	Alert	None

---

## Chapter 9. Director events

The Director events occur when a change in the state of IBM Director Console, IBM Director Agent, database, inventory, scheduled jobs, or monitored resources and application processes is detected. For detailed event types, expand the **Director** node in the Event Filter Builder tree.

### Event source

Director event types are generated by IBM Director Server or IBM Director Agent. See each event type for details about which IBM Director component generates that event.

### Details

For the Director events that are generated by IBM Director Agent, when these events are generated by a Level-2 managed system, they are automatically sent to all of the management servers that have discovered that managed system. For the Director events that are generated by IBM Director Server, when these events are generated by a management server, they are sent to that management server.

The Director events are processed by the Log All Events event-action plan. The Log All Events event-action plan adds the event to the IBM Director event log, and can be modified to include additional event actions for these event types. In contrast, other event types on which you want to filter on must be added to an event-action plan manually.

If you select the **Director** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Director subtree.

Event type	Event text	Severity	Category	Extended attributes
Director	Not applicable	Not applicable	Not applicable	None

---

## Director > Console

The Console events occur when a change in the state of IBM Director Console (a management console) is detected. For detailed event types, expand the **Console** node in the Event Filter Builder tree.

### Event source

These event types are generated by IBM Director Server.

### Details

If you select the **Console** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Console subtree.

Event type	Event text	Severity	Category	Extended attributes
Console	Not applicable	Not applicable	Not applicable	None

## Director > Console > Logon Failure

The Logon Failure events occur when IBM Director Console fails to logon to IBM Director Server. Failure to logon can include providing an incorrect user ID or password, using a user ID that has been disabled, using an incorrect version of IBM Director Console, attempting to logon using a user ID or management console that is already logged on.

### Details

These event types use the following set of extended attributes:

- *Address* is the TC/PIP address or host name for the management console that failed to logon.
- *User ID* is the user ID of the user who failed to logon.

If you select the **Logon Failure** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Logon Failure subtree.

<b>Event type</b>	<b>Event text</b>	<b>Severity</b>	<b>Category</b>	<b>Additional extended attributes</b>
Logon Failure	Not applicable	Not applicable	Not applicable	None

You can choose to select specific event types that are displayed under the **Logon Failure** node in the Event Filter Builder tree. The event filter will process only the event types that you select.

<b>Event type</b>	<b>Event text</b>	<b>Severity</b>	<b>Category</b>	<b>Additional extended attributes</b>
Bad Password	Logon to server by User ID <i>User ID</i> from <i>Address</i> failed (Bad Password)  Where <i>User ID</i> and <i>Address</i> are the values provided by the extended attributes.	Warning	Alert	None
Bad User ID	Logon to server by User ID <i>User ID</i> from <i>Address</i> failed (Bad User ID)  Where <i>User ID</i> and <i>Address</i> are the values provided by the extended attributes.	Warning	Alert	None
Disabled User ID	Logon to server by User ID <i>User ID</i> from <i>Address</i> failed (Disabled User ID)  Where <i>User ID</i> and <i>Address</i> are the values provided by the extended attributes.	Warning	Alert	None



<b>Event type</b>	<b>Event text</b>	<b>Severity</b>	<b>Category</b>	<b>Additional extended attributes</b>
Downlevel Console	Logon to server by User ID <i>User ID</i> from <i>Address</i> failed (Downlevel Console)  Where <i>User ID</i> and <i>Address</i> are the values provided by the extended attributes.	Warning	Alert	None
Expired Password	Logon to server by User ID <i>User ID</i> from <i>Address</i> failed (Expired Password)  Where <i>User ID</i> and <i>Address</i> are the values provided by the extended attributes.	Warning	Alert	None
Too Many Active IDs	Logon to server by User ID <i>User ID</i> from <i>Address</i> failed (Too Many Active IDs)  Where <i>User ID</i> and <i>Address</i> are the values provided by the extended attributes.	Warning	Alert	None
Too Many Active Logons	Logon to server by User ID <i>User ID</i> from <i>Address</i> failed (Too Many Active Logons)  Where <i>User ID</i> and <i>Address</i> are the values provided by the extended attributes.	Warning	Alert	None

Event type	Event text	Severity	Category	Additional extended attributes
Uplevel Console	Logon to server by User ID <i>User ID</i> from <i>Address</i> failed (Uplevel Console)	Warning	Alert	None
	Where <i>User ID</i> and <i>Address</i> are the values provided by the extended attributes.			

## Director > Console > User Logoff

The User Logoff event occurs when an IBM Director Console user ID logs off from IBM Director Server.

### Details

These event types use the following set of extended attributes:

- *Address* is the TC/PIP address or host name for the management console that failed to logon.
- *User ID* is the user ID of the user who failed to logon.

Select the **User Logoff** node in the Event Filter Builder tree to create an event filter that will process this event type.

Event type	Event text	Severity	Category	Additional extended attributes
User Logoff	User logged off.	Harmless	Alert	<ul style="list-style-type: none"> <li>• <i>Description</i> is the long name of the user ID. For example, if a user ID is "maddie", then the description is "systemname\Madison Lucas" where <i>systemname</i> is the name of the system.</li> <li>• <i>Locale</i> is the locale of the system where IBM Director Console was started.</li> <li>• <i>User Name</i> is the user name of the user who logged off.</li> </ul>

## Director > Console > User Logon

The User Logon event occurs when an IBM Director Console user ID logs on to IBM Director Server.

### Details

These event types use the following set of extended attributes:

- *Address* is the TC/PIP address or host name for the management console that failed to logon.
- *User ID* is the user ID of the user who failed to logon.

Select the **User Logon** node in the Event Filter Builder tree to create an event filter that will process this event type.

Event type	Event text	Severity	Category	Additional extended attributes
User Logon	User logged on.	Harmless	Alert	<ul style="list-style-type: none"><li>• <i>Description</i> is the long name of the user ID. For example, if a user ID is "maddie", then the description is "systemname\\Madison Lucas" where <i>systemname</i> is the name of the system.</li><li>• <i>Locale</i> is the locale of the system where IBM Director Console was started.</li><li>• <i>User Name</i> is the user name of the user who logged off.</li></ul>

## Director > Database

The Database events occur when the database connection between IBM Director Server and its database (the management database) is broken or restored.

### Event source

These event types are generated by IBM Director Server.

## Details

**Note:** These events are new in IBM Director 5.10.

The events occur only when IBM Director Server is running. If the database connection is interrupted, a critical event is generated and IBM Director Server attempts to recover. When the database connection is restored, a harmless event is generated. These events are not generated for a database connection failure when IBM Director Server is starting. If the management database is not available when IBM Director Server starts, IBM Director Server fails to start, unless you have disabled the database.

If you select the **Database** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Database subtree.

Event type	Event text	Severity	Category	Extended attributes
Database	Not applicable	Not applicable	Not applicable	None

You can choose to select specific event types that are displayed under the **Database** node in the Event Filter Builder tree. The event filter will process only the event types that you select.

Event type	Event text	Severity	Category	Extended attributes
Server Connection Not Available	<b>Note:</b> The event text is supplied by the database application. The text varies depending on the database application and the reason for the connection loss.	Critical	Alert	None
Server Connection Available	The database server is now available for connection.	Harmless	Resolution	None

---

## Director > Director Agent

The Director Agent event occurs when a change in the state of IBM Director Agent (a Level-2 managed system) is detected. For detailed event types, expand the **Director Agent** node in the Event Filter Builder tree.

### Event source

These event types are generated by IBM Director Agent (Level-2 managed systems).

### Details

The Director > Director Agent event types and the mib event types use the following standard set of extended attributes:

- Duration
- Monitor Resource
- Threshold Name

Some Director > Director Agent event types have additional extended attributes. These event types list the attributes in the Additional extended attributes column.

If you select the **Director Agent** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Director Agent subtree. You can choose to select specific event types that are displayed under the **Director Agent** node in the Event Filter Builder tree. The event filter will process only the event types that you select.

Event type	Event text	Severity	Category	Additional extended attributes
Director Agent	Not applicable	Not applicable	Not applicable	None

## Director > Director Agent > MPA

The MPA events occur when the IBM Director subagent for MPA fails to load because it cannot communicate with a service processor on the system.

## Event Source

These events are generated by the following versions of IBM Director Agent:

- 4.1
- 4.10.2
- 4.11
- 4.12
- 4.20
- 4.20.2
- 4.21
- 4.22

## Details

The Director > Director Agent event types and the mib event types use the following standard set of extended attributes:

- Duration
- Monitor Resource
- Threshold Name

Some Director > Director Agent event types have additional extended attributes. These event types list the attributes in the Additional extended attributes column.

Event type	Event text	Severity	Category	Additional extended attributes
MPA	Management Processor Assistant Agent failed to load.	Critical	Alert	None

## Director > Director Agent > Process Monitors

The Process Monitors events occur when an application process that you are monitoring has failed; a scheduled job has been completed successfully or with errors; or a target system has completed a job successfully or with errors.

## Event source

These event types are generated by IBM Director Agent (Level-2 managed systems).

## Details

Process Monitor event types are published and then displayed dynamically in the Event Filter Builder window when you:

- Configure a process monitor and specify event generation in the Process Monitors window.
- Schedule a job and specify event generation on the Options page in the New Scheduled Job window.

The Director > Director Agent event types and the mib event types use the following standard set of extended attributes:

- Duration
- Monitor Resource
- Threshold Name

Some Director > Director Agent event types have additional extended attributes. These event types list the attributes in the Additional extended attributes column.

Event type	Event text	Severity	Category	Additional extended attributes
Process Monitors	<b>Note:</b> The event text varies depending on the monitor that you create.	Varies depending on the threshold set for the monitor.	Alert	<ul style="list-style-type: none"><li>• <i>Actual Value</i> is the current reading of the monitored resource at the time the event is sent.</li><li>• <i>Threshold Value</i> is the configured value you assigned in the <b>Above or Equal</b> or <b>Below or Equal</b> field of the Threshold Configuration window.</li></ul>

## Director > Director Agent > Process Monitors > Process Alert

The Process Alert events occur when an application process that you are monitoring has started, stopped, or failed to start; a scheduled job has been completed successfully or with errors; or a target system has completed a job successfully or with errors.

## Event source

These event types are generated by IBM Director Agent (Level-2 managed systems).

### Details

The Director > Director Agent event types and the mib event types use the following standard set of extended attributes:

- Duration
- Monitor Resource
- Threshold Name

Some Director > Director Agent event types have additional extended attributes. These event types list the attributes in the Additional extended attributes column.

If you select the **Process Alert** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Process Alert subtree, including the dynamically created events that you selected to generate in the Scheduler or Process Monitor task.

Event type	Event text	Severity	Category	Additional extended attributes
Process Alert	<b>Note:</b> The event text varies depending on the monitor that you create.	Varies depending on the threshold set for the monitor.	Alert	<ul style="list-style-type: none"><li>• <i>Actual Value</i> is the current reading of the monitored resource at the time the event is sent.</li><li>• <i>Threshold Value</i> is the configured value you assigned in the <b>Above or Equal</b> or <b>Below or Equal</b> field of the Threshold Configuration window.</li></ul>

You can choose to select specific event types that are displayed under the **Process Alert** node in the Event Filter Builder tree. The event filter will process only the event types that you select.



Event type	Event text	Severity	Category	Additional extended attributes
Process Failed to Start	Process Failed to Start → Monitor 'PMON:process_name Fail' Changed:'process_name' has changed values for 0:00:00. New value reported is "1".	Critical	Alert	<ul style="list-style-type: none"> <li><i>Actual Value</i> is the current reading of the monitored resource at the time the event is sent.</li> <li><i>Threshold Value</i> is the configured value you assigned in the <b>Above or Equal or Below or Equal</b> field of the Threshold Configuration window.</li> </ul>
Process Started	Process Start → Monitor 'PMON:process_name Start' Changed:'process_name' has changed values for 0:00:00. New value reported is "1".	Harmless	Alert	<ul style="list-style-type: none"> <li><i>Actual Value</i> is the current reading of the monitored resource at the time the event is sent.</li> <li><i>Threshold Value</i> is the configured value you assigned in the <b>Above or Equal or Below or Equal</b> field of the Threshold Configuration window.</li> </ul>
Process Terminated	Process Terminated → Monitor 'PMON:process_name Stop' Changed:'process_name' has changed values for 0:00:00. New value reported is "1".	Warning	Alert	<ul style="list-style-type: none"> <li><i>Actual Value</i> is the current reading of the monitored resource at the time the event is sent.</li> <li><i>Threshold Value</i> is the configured value you assigned in the <b>Above or Equal or Below or Equal</b> field of the Threshold Configuration window.</li> </ul>

## Director > Director Agent > Resource Monitors

The Resource Monitors events occur when the state of a resource that you are monitoring has changed in respect to the settings you selected when creating the resource monitor; a scheduled job has been completed successfully or with errors; or a target system has completed a job successfully or with errors.

## Event source

These event types are generated by IBM Director Agent (Level-2 managed systems).

### Details

Resource Monitor event types are published and then displayed dynamically in the Event Filter Builder window when you:

- Configure a resource monitor and specify event generation in the System Threshold window.
- Schedule a job and specify event generation on the Options page in the New Scheduled Job window.

**Note:** If you configure a resource monitor for an SNMP device, the event types are not published under the Resource Monitor node. See Director > mib for information about these event types.

The Director > Director Agent event types and the mib event types use the following standard set of extended attributes:

- Duration
- Monitor Resource
- Threshold Name

Some Director > Director Agent event types have additional extended attributes. These event types list the attributes in the Additional extended attributes column.

Event type	Event text	Severity	Category	Additional extended attributes
Resource Monitors	<b>Note:</b> The event text varies depending on the monitor that you create.	Varies depending on the threshold set for the monitor.	Alert	<ul style="list-style-type: none"><li>• <i>Actual Value</i> is the current reading of the monitored resource at the time the event is sent.</li><li>• <i>Threshold Value</i> is the configured value you assigned in the <b>Above or Equal</b> or <b>Below or Equal</b> field of the Threshold Configuration window.</li></ul>

---

## Director > Inventory

The Inventory events occur when a change in the state of IBM Director inventory is detected. For detailed event types, expand the **Inventory** node in the Event Filter Builder tree.

### Event source

These event types are generated by IBM Director Server.

### Details

**Note:** This event is new in IBM Director 5.10.

If you select the **Inventory** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Inventory subtree. You can choose to select specific event types that are displayed under the **Inventory** node in the Event Filter Builder tree. The event filter will process only the event types that you select.

Event type	Event text	Severity	Category	Extended attributes
Inventory	Not applicable	Not applicable	Not applicable	None

## Director > Inventory > Custom Collection

The Custom Collection events occur when a custom inventory collection has succeeded or failed. Reasons for failure can include incorrect authorization to access the management database, a communication error with the management database, a hardware or software failure, or a timeout.

### Details

**Note:** These events are new in IBM Director 5.10.

If you select the **Custom Collection** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Custom Collection subtree.

Event type	Event text	Severity	Category	Extended attributes
Custom Collection	Not applicable	Not applicable	Not applicable	None

You can choose to select specific event types that are displayed under the **Custom Collection** node in the Event Filter Builder tree. The event filter will process only the event types that you select.

Event type	Event text	Severity	Category	Extended attributes
Authorization Failure	Inventory failed with an authorization failure.	Harmless	Alert	None
Communication Error	Inventory failed with a communications error.	Harmless	Alert	None
General Failure	Inventory failed with a general failure.	Harmless	Alert	None
Hardware Failure	Inventory failed with a hardware failure.	Harmless	Alert	None
No Data Found	Inventory failed with no data.	Harmless	Alert	None
Software Failure	Inventory failed with a software failure.	Harmless	Alert	None
Successful	Inventory was successful.	Harmless	Alert	None
Timeout Failure	Inventory failed with a timeout.	Harmless	Alert	None

## Director > Inventory > Inventory Monitor

The Inventory Monitor events occur when a change has been detected in the IBM Director database and you have set a monitor to communicate that change. An event is generated if a database row has been changed, added, or removed.

### Details

**Note:** These events are new in IBM Director 5.10.

The following table provides examples of the output generated by these events:

Row Added	Table: Partition, Row added: [CREOSOTE32, Index: 5, Name (i.e. Drive Letter): G:\, Total Size (KB): 18426552, Free Space (KB): 18360000, Label: New Volume, File System Type: NTFS]
Row Changed	Table: Partition, Row changed from [CREOSOTE32, Index: 2, Name (i.e. Drive Letter): D:\, Total Size (KB): 10241404, Free Space (KB): 7676176, Label: New Volume, File System Type: NTFS] to [CREOSOTE32, Index: 2, Name (i.e. Drive Letter): D:\, Total Size (KB): 10241404, Free Space (KB): 7691660, Label: New Volume, File System Type: NTFS]

If you select the **Inventory Monitor** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Inventory Monitor subtree.

Event type	Event text	Severity	Category	Extended attributes
Inventory Monitor	Not applicable	Not applicable	Not applicable	None

You can choose to select specific event types that are displayed under the **Inventory Monitor** node in the Event Filter Builder tree. The event filter will process only the event types that you select.

Event type	Event text	Severity	Category	Extended attributes
Row Added	Table: <i>Table</i> , Row added: <i>Row</i> where <i>Table</i> is the name of the affected table and <i>Row</i> is the row description of the added row.	Harmless	Alert	None
Row Changed	Table: <i>Table</i> , Row changed from <i>Previous</i> to <i>New</i> where: <ul style="list-style-type: none"> <li><i>Table</i> is the name of the affected table</li> <li><i>Previous</i> is the previous description of the affected row.</li> <li><i>New</i> is the new description of the affected row.</li> </ul>	Harmless	Alert	None
Row Removed	Table: <i>Table</i> , Row removed: <i>Row</i> where <i>Table</i> is the name of the affected table and <i>Row</i> is the row description of the removed row.	Harmless	Alert	None

## Director > mib

The mib event occurs when the state of an SNMP device resource that you are monitoring has changed in respect to the settings you selected when creating the resource monitor.

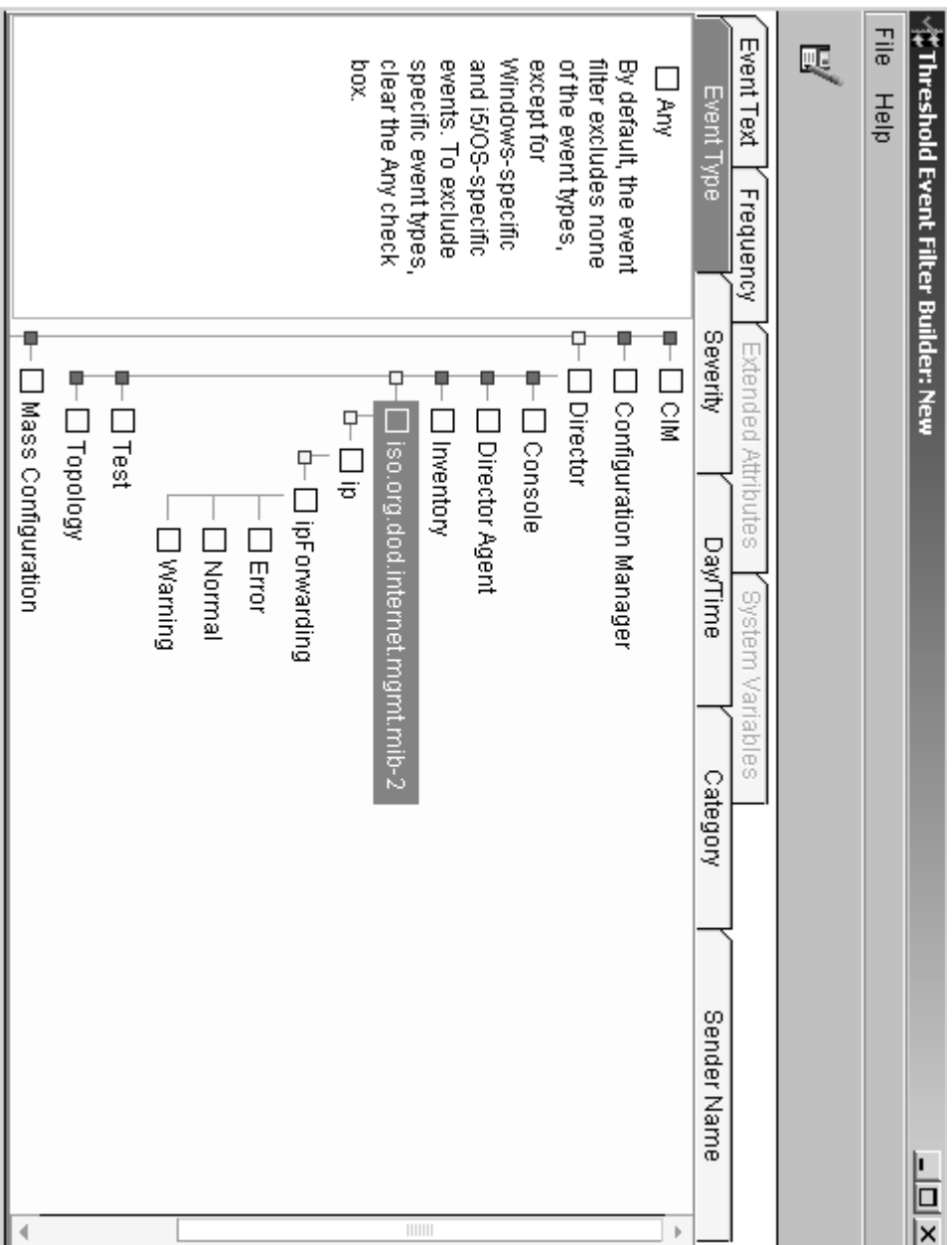
### Event source

These event types are generated by IBM Director Agent (Level-2 managed systems).

## Details

If you configure a resource monitor for an SNMP device, an event type is created using the path to the SNMP variable in its Management Information Base (MIB) file. This event type is displayed in place of the “mib” node. The format of the event type displayed in the tree uses a different template depending on whether the SNMP variable is a string or a numeric value.

For example, if a resource monitor is configured against the ipForwarding string variable that is defined in the SMI version 2 MIB file, the following event type is displayed under the Director node:



*Figure 2. SNMP string variable example*

The string variables Error, Normal, and Warning are displayed under the monitored variable.

The following example contains a resource monitor configured against the private Microsoft MIB. This MIB variable is an integer, not a string. The template for non-string variables (when configuring a resource monitor) is to put the



threshold levels that were defined in the monitor underneath the variable along with the state. This example is configured for a high-error and high-warning threshold.

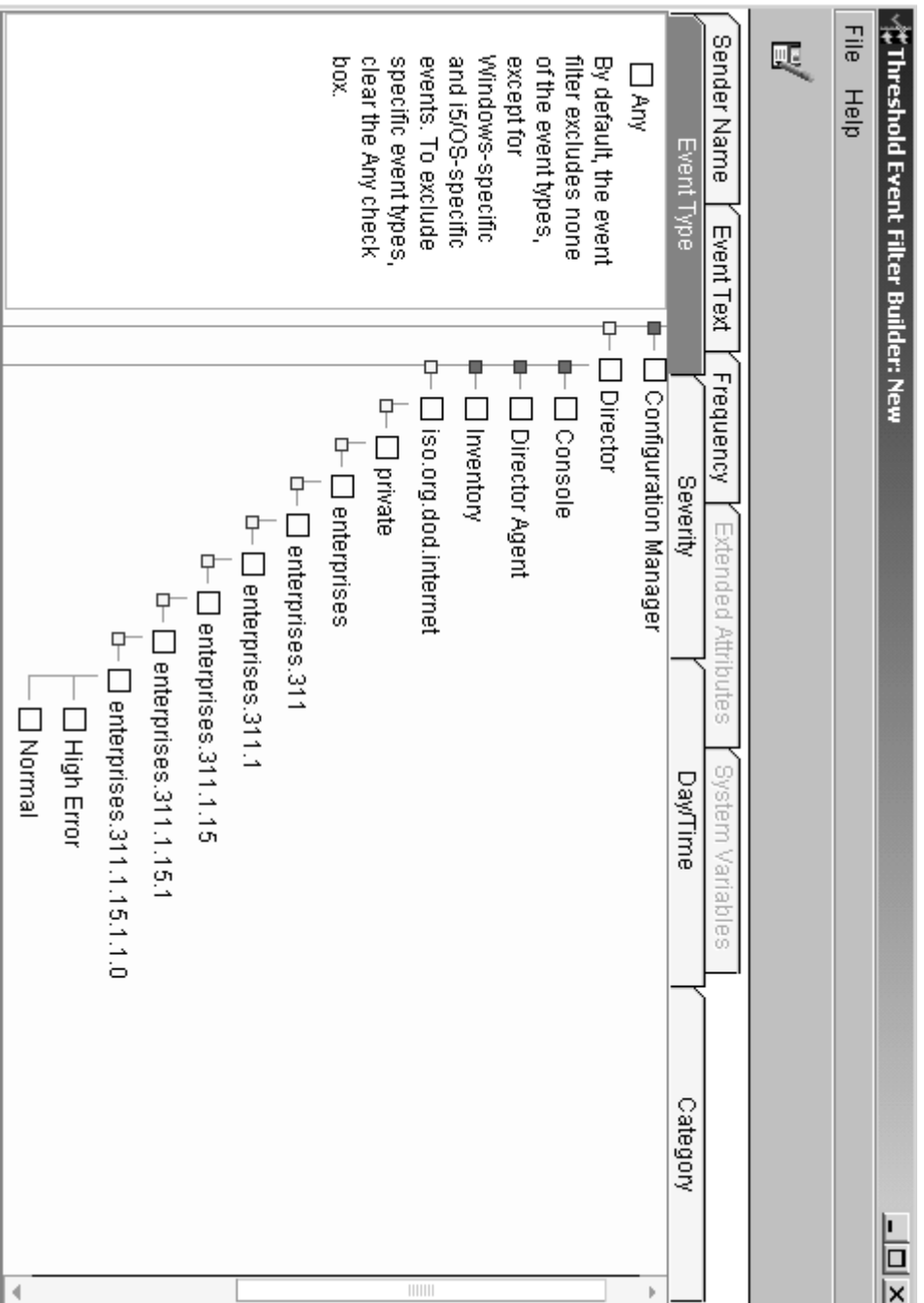


Figure 3. *SNMP integer variable example*

The Director > Director Agent event types and the mib event types use the following standard set of extended attributes:

- Duration
- Monitor Resource
- Threshold Name

Some Director > Director Agent event types have additional extended attributes. These event types list the attributes in the Additional extended attributes column.

Event type	Event text	Severity	Category	Additional extended attributes
<b>Note:</b> Path to the SNMP variable in its MIB file.	<b>Note:</b> The event text varies depending on the monitor that you create.	Varies depending on the threshold set for the monitor.	Alert	<ul style="list-style-type: none"> <li>• <i>Actual Value</i> is the current reading of the monitored resource at the time the event is sent.</li> <li>• <i>Threshold Value</i> is the configured value you assigned in the <b>Above or Equal</b> or <b>Below or Equal</b> field of the Threshold Configuration window.</li> </ul>

## Director > Scheduler

The Scheduler events occur when a scheduled job succeeds or fails; or a scheduled job is completed or fails on a target system. For detailed event types, expand the **Scheduler** node in the Event Filter Builder tree.

### Event source

These event types are generated by IBM Director Server.

### Details

The Director > Scheduler > Scheduler > System event types use the following standard set of extended attributes:

- Client Status
- Job Activation Time
- Job Current Task ID
- Job Current Subtask ID
- Job Current Task Name
- Job ID

If you select the **Scheduler** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Scheduler subtree. You can choose to select specific event types that are displayed under the **Scheduler** node in the Event Filter Builder tree. The event filter will process only the event types that you select.

Event type	Event text	Severity	Category	Additional extended attributes
Scheduler	<b>Note:</b> The event text varies depending on the job that you schedule.	Not applicable	Not applicable	None

## Director > Scheduler > Job

The Job events occur when a scheduled job is successful or if it fails. For detailed event types, expand the **Job** node in the Event Filter Builder tree.

### Details

The Director > Scheduler > Job event types use the following standard set of extended attributes:

- Job Activation Time
- Job ID

If you select the **Job** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Job subtree. You can choose to select specific event types that are displayed under the **Job** node in the Event Filter Builder tree. The event filter will process only the event types that you select.

Event type	Event text	Severity	Category	Additional extended attributes
Job	Not applicable	Not applicable	Not applicable	None

## Director > Scheduler > Job > Error

The Error events occur when a scheduled job has failed.

## Details

If you select the **Error** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Error subtree.

Event type	Event text	Severity	Category	Additional extended attributes
Error	Not applicable	Not applicable	Not applicable	None

You can choose to select specific event types that are displayed under the **Error** node in the Event Filter Builder tree. The event filter will process only the event types that you select.

Event type	Event text	Severity	Category	Additional extended attributes
<b>Note:</b> The name of the scheduled job.	<b>Note:</b> The name of the scheduled job.	Warning	Alert	None

## Director > Scheduler > Job > Success

The Success events occur when a scheduled job has succeeded.

## Details

If you select the **Success** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Success subtree.

Event type	Event text	Severity	Category	Additional extended attributes
Success	Not applicable	Not applicable	Not applicable	None

You can choose to select specific event types that are displayed under the **Success** node in the Event Filter Builder tree. The event filter will process only the event types that you select.

Event type	Event text	Severity	Category	Additional extended attributes
<b>Note:</b> The name of the scheduled job.	<b>Note:</b> The name of the scheduled job.	Harmless	Resolution	None

## Director > Scheduler > System

The System events occur when a scheduled job is completed or fails on a target system. For detailed event types, expand the **System** node in the Event Filter Builder tree.

### Details

The Director > Scheduler > System event types use the following standard set of extended attributes:

- Client Status
- Job Activation Time
- Job Current Task ID
- Job Current Subtask ID
- Job Current Task Name
- Job ID

If you select the **System** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the System subtree. You can choose to select specific event types that are displayed under the **System** node in the Event Filter Builder tree. The event filter will process only the event types that you select.

Event type	Event text	Severity	Category	Additional extended attributes
System	Not applicable	Not applicable	Not applicable	None

## Director > Scheduler > System > Error

The Error events occur when a scheduled job fails on a target system.

## Details

If you select the **Error** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Error subtree.

Event type	Event text	Severity	Category	Additional extended attributes
Error	Not applicable	Not applicable	Not applicable	None

You can choose to select specific event types that are displayed under the **Error** node in the Event Filter Builder tree. The event filter will process only the event types that you select.

Event type	Event text	Severity	Category	Additional extended attributes
<b>Note:</b> The name of the scheduled job.	<b>Note:</b> The name of the scheduled job.	Warning	Alert	None

## Director > Scheduler > System > Success

The Success events occur when a scheduled job is completed on a target system.

## Details

If you select the **Success** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Success subtree.

Event type	Event text	Severity	Category	Additional extended attributes
Success	Not applicable	Not applicable	Not applicable	None

You can choose to select specific event types that are displayed under the **Success** node in the Event Filter Builder tree. The event filter will process only the event types that you select.

Event type	Event text	Severity	Category	Additional extended attributes
<b>Note:</b> The name of the scheduled job.	<b>Note:</b> The name of the scheduled job.	Harmless	Alert	None

## Director > Test

The Test events occur when you test an event action. When you create an event action, you can verify that it works as you intended by testing it. Locate the event action under the corresponding event-action type in the Actions pane of the Event Action Plan Builder window. Right-click the event action, and then click **Test**. The event action occurs and generates a test event.

### Event source

These event types are generated by IBM Director Server.

### Details

If you select the **Test** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Test subtree.

Event type	Event text	Severity	Category	Extended attributes
Test	Not applicable	Not applicable	Not applicable	None

You can choose to select specific event types that are displayed under the **Test** node in the Event Filter Builder tree. The event filter will process only the event types that you select.

Event type	Event text	Severity	Category	Extended attributes
Action	<b>Note:</b> The name of the event action that you are testing is displayed.	Harmless	Alert	None

## Director > Topology

The Topology events occur when IBM Director Agent changes from an online or offline state.

### Event source

These event types are generated by IBM Director Server.

### Details

If you select the **Topology** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Topology subtree.

Event type	Event text	Severity	Category	Extended attributes
Topology	Not applicable	Not applicable	Not applicable	None

You can choose to select specific event types that are displayed under the **Topology** node in the Event Filter Builder tree. The event filter will process only the event types that you select.

Event type	Event text	Severity	Category	Extended attributes
Offline	IBM Director Agent is offline.	Harmless	Alert	None
Online	IBM Director Agent is online.	Harmless	Resolution	None



---

## Chapter 10. Mass Configuration events

The Mass Configuration events occur when more than one profile affecting the same value has been applied to a system or when more than one management server has sent profiles to a system.

### Event source

These event types are generated by the Mass Configuration feature in IBM Director.

### Details

These event types are sent by the Mass Configuration feature that you can use with the following tasks:

- Asset ID
- Configure ASF
- Configure SNMP Agent
- Network Configuration

When creating the Mass Configuration profiles for these tasks, an **Enable Changes** check box is provided. You must select this check box to enable access for other administrators to change the configured values. If the check box is selected and an administrator without access attempts to change a value, the Mass Configuration > Overwritten event is sent.

If you select the **Mass Configuration** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Mass Configuration subtree.

Event type	Event text	Severity	Category	Extended attributes
Mass Configuration	Not applicable	Not applicable	Not applicable	None

You can choose to select specific event types that are displayed under the **Mass Configuration** node in the Event Filter Builder tree. The event filter will process only the event types that you select.

<b>Event type</b>	<b>Event text</b>	<b>Severity</b>	<b>Category</b>	<b>Extended attributes</b>
Conflict	More than one profile that has a value for the same field has been applied to a system.	Warning	Alert	None
Overwritten	More than one server has sent mass configuration profiles to a system.	Warning	Alert	None

---

## Chapter 11. MPA events

MPA event types occur when a service processor or management module detect a change in the system state. The event types can indicate a change in the state of the system components, the system environmental values, system configuration, system startup, or the scalable platforms and nodes. For detailed event types, expand the MPA node in the Event Filter Builder tree.

### The MPA event source in IBM Director 5.10

**Note:** The following information does not include IBM Director Agent for NetWare, version 5.10. For information about this version of IBM Director Agent, the following section “The MPA event source in IBM Director, version 4.22 and earlier”

MPA events are not generated by IBM Director Core Services or IBM Director Agent as they were in previous versions of IBM Director. MPA events are generated only by IBM Director Server when it receives out-of-band notifications from IBM service processors and BladeCenter management modules. These event types are displayed in the MPA node of the Event Filter Builder tree. You must configure the service processors and management modules in your system-management environment to send notifications to IBM Director Server.

### The MPA event source in IBM Director, versions 4.22 and earlier

The following versions of IBM Director Agent include an MPA Agent:

- Version 5.10 on NetWare only.
- Versions 4.22 and earlier on Linux<sup>®</sup> and Windows, if you enabled in-band events for the managed system.

This MPA Agent generates MPA events in response to notifications sent from an in-band service processor.

Service processors that have been correctly configured (by selecting Director over LAN) will forward events over the LAN (out-of-band) to IBM Director Server. IBM Director Server maps each of these events to an event type that is displayed in the MPA node of the Event Filter Builder tree.

## Service processors and managed-object types

Any xSeries server and BladeCenter unit that has a supported service processor or management module can forward events to IBM Director Server. When IBM Director Server generates event types in response to an event, the target managed object of the specific event type can vary. The following table lists the service processor type and its associated target managed-object type.

**Note:** For all service processors, if IBM Director cannot determine the managed object type for a service processor notification, IBM Director instead will identify the source of the notification by the IP address of the service processor that sent the notification to IBM Director Server. An example of this is a managed system that is configured to send notifications to IBM Director Server, but IBM Director Server currently doesn't have a managed object representing that system.

Service processor type	Target managed-object type
BladeCenter management module	BladeCenter chassis
RXE-100 Remote Expansion Enclosure	RIOEnclosure
System with one of the following service processors: <ul style="list-style-type: none"><li>• ISMP</li><li>• Remote Supervisor Adapter</li><li>• Remote Supervisor Adapter II</li><li>• Advanced System Management processor (ASM processor)</li><li>• Advanced System Management PCI adapter (ASM PCI adapter)</li></ul>	Physical Platform and associated IBM Director System
System running the MPA Agent with one of the following service processors: <ul style="list-style-type: none"><li>• ASM processor</li><li>• ASM PCI adapter</li></ul>	Physical Platform and associated IBM Director System

**Note:** IBM Director cannot map events that are generated by ASM processors and ASM PCI adapters to a managed object unless the MPA Agent 4.22 or earlier is installed. The MPA agent is a feature of the IBM Director Agent, version 4.22 or earlier, installation.

## Details

If you select the **MPA** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the MPA subtree.

Event type	Event text	Severity	Category	Extended attributes
MPA	Not applicable	Not applicable	Not applicable	None

---

## MPA > Component

The Component event types occur when a service processor or management module detects that the state of a system component has changed. For detailed event types for system components, expand the **Component** node in the Event Filter Builder tree.

### Details

These MPA event types use the following set of extended attributes:

- Firmware code
- Sender UUID
- Sensor Label
- Sensor Number
- Source UUID

Some MPA event types have additional extended attributes. These event types list the attributes in the Additional extended attributes column.

If you select the **Component** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Component subtree.

Event type	Event text	Severity	Category	Additional extended attributes
Component	Not applicable	Not applicable	Not applicable	None

## MPA > Component > Blade Server

The Blade Server events occur when a management module detects that the state of a blade server has changed.

### Details

**Note:** These events are generated by BladeCenter management modules only.

These MPA event types use the following set of extended attributes:

- Firmware code
- Sender UUID
- Source UUID

Some event types have additional extended attributes. These event types list the attributes in the Additional extended attributes column.

If you select the **Blade Server** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Blade Server subtree.

Event type	Event text	Severity	Category	Additional extended attributes
Blade Server	Not applicable	Not applicable	Not applicable	None

You can choose to select specific event types that are displayed under the **Blade Server** node in the Event Filter Builder tree. The event filter will process only the event types that you select.

<b>Event type</b>	<b>Event text</b>	<b>Severity</b>	<b>Category</b>	<b>Additional extended attributes</b>
Communication	The management module failed to communicate with a blade server.	Critical	Alert	<i>Unit</i> identifies the affected blade server.
Communication	The management module successfully communicated with a blade server after a previous failure.	Harmless	Resolution	<i>Unit</i> identifies the affected blade server.
Inserted	A blade server was inserted.	Harmless	Alert	<i>Unit</i> identifies the affected blade server.
Insufficient Power	A blade server cannot power on because there is insufficient power.	Critical	Alert	<i>Unit</i> identifies the affected blade server.
Insufficient Power	A blade server has sufficient power to power on.	Harmless	Resolution	<i>Unit</i> identifies the affected blade server.
Over Power Budget	The management module instructed a blade server to power off because it exceeded the power budget.	Minor	Alert	<i>Unit</i> identifies the affected blade server.
Over Power Budget	A blade server was allowed to power on because it no longer exceeds the power budget.	Harmless	Resolution	<i>Unit</i> identifies the affected blade server.
Removed	A blade server was removed.	Warning	Alert	<i>Unit</i> identifies the affected blade server.
Throttled	A blade server is throttled.	Harmless	Alert	<i>Unit</i> identifies the affected blade server.
Throttled	A blade server is no longer throttled.	Harmless	Resolution	<i>Unit</i> identifies the affected blade server.
VPD	The blade server vital product data (VPD) could not be read. The blade server will not be allowed to power on.	Critical	Alert	<i>Unit</i> identifies the affected blade server.

Event type	Event text	Severity	Category	Additional extended attributes
VPD	The blade server vital product data (VPD) was read successfully.	Harmless	Resolution	<i>Unit</i> identifies the affected blade server.
Capacity on Demand	Not applicable	Not applicable	Not applicable	None
Capacity on Demand > Enabled	A blade server with a Standby Capacity on Demand feature was enabled.	Harmless	Alert	None

## MPA > Component > Bus

The Bus events occur when a service processor detects that the state of a bus has changed.

### Details

**Note:** These events are generated by service processors and BladeCenter management modules.

These MPA event types use the following set of extended attributes:

- Firmware code
- Sender UUID
- Source UUID

Some event types have additional extended attributes. These event types list the attributes in the Additional extended attributes column.

If you select the **Bus** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Bus subtree.



Event type	Event text	Severity	Category	Additional extended attributes
Bus	Not applicable	Not applicable	Not applicable	<i>Bus</i> identifies the affected bus.

You can choose to select specific event types that are displayed under the **Bus** node in the Event Filter Builder tree. The event filter will process only the event types that you select.

Event type	Event text	Severity	Category	Additional extended attributes
Communication	A failure occurred while attempting to communicate with a device.	Critical	Alert	<i>Bus</i> identifies the affected bus.
Communication	Successfully communicated with a device after a previous failure.	Harmless	Resolution	<i>Bus</i> identifies the affected bus.

## MPA > Component > Chassis

The Chassis events occur when a management module detects that the state of a BladeCenter chassis has changed. For detailed event types, expand the **Chassis** node in the Event Filter Builder tree.

### Details

**Note:** These events are generated by BladeCenter management modules only.

These MPA event types use the following set of extended attributes:

- Firmware code
- Sender UUID
- Source UUID

Some event types have additional extended attributes. These event types list the attributes in the Additional extended attributes column.

If you select the **Chassis** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Chassis subtree.

Event type	Event text	Severity	Category	Additional extended attributes
Chassis	Not applicable	Not applicable	Not applicable	<ul style="list-style-type: none"> <li>• <i>Issue</i> is one of the following strings:               <ul style="list-style-type: none"> <li>– <i>all_ps_over_temp</i> indicates that all of the power supplies have exceeded their temperature thresholds and the fans are running at full speed.</li> <li>– <i>blade_power</i> indicates that a blade server was inserted into a bay that is not receiving power.</li> <li>– <i>no_fans</i> indicates that none of the fans are functional.</li> </ul> </li> </ul>

## MPA > Component > Chassis > Configuration

The Configuration events occur when a management module detects that the state of a BladeCenter chassis configuration has changed.

### Details

**Note:** These events are generated by BladeCenter management modules only.

These MPA event types use the following set of extended attributes:

- Firmware code
- Sender UUID
- Source UUID

Some event types have additional extended attributes. These event types list the attributes in the Additional extended attributes column.

If you select the **Configuration** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Configuration subtree.

Event type	Event text	Severity	Category	Additional extended attributes
Configuration	A blade server was inserted into a bay that is not receiving power.	Minor	Alert	<ul style="list-style-type: none"> <li>Issue is set to blade_power.</li> <li>Power Domain identifies the BladeCenter chassis power domain into which the blade server was inserted. A BladeCenter chassis is divided into two power domains. Power supplies 1 and 2 provide power to the first domain; Power supplies 3 and 4 provide power to the second domain.</li> </ul>
Configuration	A chassis configuration issue was resolved.	Harmless	Resolution	<ul style="list-style-type: none"> <li>Issue is set to blade_power.</li> <li>Power Domain identifies the BladeCenter chassis power domain into which the blade server was inserted. A BladeCenter chassis is divided into two power domains. Power supplies 1 and 2 provide power to the first domain; Power supplies 3 and 4 provide power to the second domain.</li> </ul>
Configuration	A blade server is not compatible with the I/O module configuration.	Minor	Alert	<ul style="list-style-type: none"> <li>Component is set to processor_blade.</li> <li>Unit identifies the affected blade server.</li> </ul>
Configuration	A chassis configuration issue was resolved.	Harmless	Resolution	<ul style="list-style-type: none"> <li>Component is set to processor_blade.</li> <li>Unit identifies the affected blade server.</li> </ul>
Configuration	An I/O module is not compatible with the blade server configuration.	Minor	Alert	<ul style="list-style-type: none"> <li>Component is set to switch_module.</li> <li>Unit identifies the affected I/O module.</li> </ul>
Configuration	A chassis configuration issue was resolved.	Harmless	Resolution	<ul style="list-style-type: none"> <li>Component is set to switch_module.</li> <li>Unit identifies the affected I/O module.</li> </ul>

## MPA > Component > Chassis > Failed

The Failed events occur when a management module detects that a BladeCenter chassis has failed.

## Details

**Note:** These events are generated by BladeCenter management modules only.

These MPA event types use the following set of extended attributes:

- Firmware code
- Sender UUID
- Source UUID

Some event types have additional extended attributes. These event types list the attributes in the Additional extended attributes column.

If you select the **Failed** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Failed subtree.

Event type	Event text	Severity	Category	Additional extended attributes
Failed	There are no working fans.	Critical	Alert	<i>Issue</i> is set to no_fans.
Failed	All power supplies have exceeded the temperature thresholds and the fans are running at full speed.	Critical	Alert	<i>Issue</i> is set to all_ps_over_temp.

## MPA > Component > CPU

The CPU events occur when a service processor or management module detects that the state of a microprocessor (CPU) has changed.

### Details

**Note:** These events are generated by service processors and BladeCenter management modules.

These MPA event types use the following set of extended attributes:

- Firmware code

- Sender UUID
- Sensor Label
- Sensor Number
- Source UUID

Some MPA event types have additional extended attributes. These event types list the attributes in the Additional extended attributes column.

If you select the **CPU** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the CPU subtree.

Event type	Event text	Severity	Category	Additional extended attributes
CPU	Not applicable	Not applicable	Not applicable	<i>Unit</i> identifies the affected microprocessor.

You can choose to select specific event types that are displayed under the **CPU** node in the Event Filter Builder tree. The event filter will process only the event types that you select.

Event type	Event text	Severity	Category	Additional extended attributes
Configuration	The CPU configuration prohibits CPU from operating at maximum speed.	Warning	Alert	<i>Unit</i> identifies the affected microprocessor.
Configuration	The CPU configuration no longer prohibits CPU from operating at maximum speed.	Harmless	Resolution	<i>Unit</i> identifies the affected microprocessor.
Configuration	The CPU configuration is invalid.	Critical	Alert	<i>Unit</i> identifies the affected microprocessor.
Configuration	The CPU configuration is valid.	Harmless	Resolution	<i>Unit</i> identifies the affected microprocessor.
Failed	A CPU fault occurred.	Critical	Alert	<i>Unit</i> identifies the affected microprocessor.

<b>Event type</b>	<b>Event text</b>	<b>Severity</b>	<b>Category</b>	<b>Additional extended attributes</b>
Failed	A CPU internal error was detected and the CPU has been disabled. The system has been restarted.	Critical	Alert	<i>Unit</i> identifies the affected microprocessor.
Failed	A CPU internal error was detected, probably due to a bus timeout. The system has been restarted. You must manually clear this event.	Critical	Alert	<i>Unit</i> identifies the affected microprocessor.
Failed	A CPU internal error was detected and the CPU has been disabled. The system has been restarted. You must manually clear this event.	Critical	Alert	<i>Unit</i> identifies the affected microprocessor.
Failed	A CPU internal error was detected. The system has been restarted. You must manually clear this event.	Critical	Alert	<i>Unit</i> identifies the affected microprocessor.
Failed	A CPU is now operating normally.	Harmless	Resolution	<i>Unit</i> identifies the affected microprocessor.

## **MPA > Component > DASD**

The hard disk drive (DASD) events occur when a service processor or management module detects that the state of a hard disk drive has changed.

### **Details**

**Note:** These events are generated by service processors and BladeCenter management modules.

These MPA event types use the following set of extended attributes:

- Firmware code
- Sender UUID
- Sensor Label
- Sensor Number
- Source UUID

Some MPA event types have additional extended attributes. These event types list the attributes in the Additional extended attributes column.

If you select the **DASD** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the DASD subtree.

Event type	Event text	Severity	Category	Additional extended attributes
DASD	Not applicable	Not applicable	Not applicable	<ul style="list-style-type: none"> <li>• <i>SCSI /ID</i> identifies the target hard disk drive by SCSI ID.</li> <li>• <i>Unit</i> identifies the target hard disk drive by physical location.</li> </ul>

You can choose to select specific event types that are displayed under the **DASD** node in the Event Filter Builder tree. The event filter will process only the event types that you select.

Event type	Event text	Severity	Category	Additional extended attributes
Failed	A hard disk drive failed.	Minor	Alert	<ul style="list-style-type: none"> <li>• <i>SCSI /ID</i> identifies the target hard disk drive by SCSI ID.</li> <li>• <i>Unit</i> identifies the target hard disk drive by physical location.</li> </ul>
Failed	A hard disk drive failed. You must manually clear this event.	Critical	Alert	<ul style="list-style-type: none"> <li>• <i>SCSI /ID</i> identifies the target hard disk drive by SCSI ID.</li> <li>• <i>Unit</i> identifies the target hard disk drive by physical location.</li> </ul>

Event type	Event text	Severity	Category	Additional extended attributes
Failed	A hard disk drive is now operating normally.	Harmless	Resolution	<ul style="list-style-type: none"> <li>SCSI <i>ID</i> identifies the target hard disk drive by SCSI <i>ID</i>.</li> <li><i>Unit</i> identifies the target hard disk drive by physical location.</li> </ul>
Inserted	A hard disk drive was inserted.	Harmless	Resolution	<ul style="list-style-type: none"> <li>SCSI <i>ID</i> identifies the target hard disk drive by SCSI <i>ID</i>.</li> <li><i>Unit</i> identifies the target hard disk drive by physical location.</li> </ul>
Removed	A hard disk drive was removed.	Warning	Alert	<ul style="list-style-type: none"> <li>SCSI <i>ID</i> identifies the target hard disk drive by SCSI <i>ID</i>.</li> <li><i>Unit</i> identifies the target hard disk drive by physical location.</li> </ul>

## MPA > Component > DIMM

The DIMM events occur when a service processor or management module detects that the state of a dual inline memory module (DIMM) has changed.

### Details

**Note:** These events are generated by service processors and BladeCenter management modules.

These MPA event types use the following set of extended attributes:

- Firmware code
- Sender UUID
- Sensor Label
- Sensor Number
- Source UUID



Some MPA event types have additional extended attributes. These event types list the attributes in the Additional extended attributes column.

If you select the **DIMM** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the DIMM subtree.

Event type	Event text	Severity	Category	Additional extended attributes
DIMM	Not applicable	Not applicable	Not applicable	None

You can choose to select specific event types that are displayed under the **DIMM** node in the Event Filter Builder tree. The event filter will process only the event types that you select.

Event type	Event text	Severity	Category	Additional extended attributes
Failed	A DIMM failed.	Minor	Alert	None

## MPA > Component > Fan

The Fan events occur when a service processor or management module detects that the state of a fan has changed.

### Details

**Note:** These events are generated by service processors and BladeCenter management modules.

These MPA event types use the following set of extended attributes:

- Firmware code
- Sender UUID
- Sensor Label
- Sensor Number
- Source UUID

Some MPA event types have additional extended attributes. These event types list the attributes in the Additional extended attributes column.

If you select the **Fan** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Fan subtree.

Event type	Event text	Severity	Category	Additional extended attributes
Fan	Not applicable	Not applicable	Not applicable	None

You can choose to select specific event types that are displayed under the **Fan** node in the Event Filter Builder tree. The event filter will process only the event types that you select.

Event type	Event text	Severity	Category	Additional extended attributes
Configuration	The fan configuration is invalid.	Critical	Alert	None
Configuration	The fan configuration is valid.	Harmless	Resolution	None
Failed	A fan failed.	Critical	Alert	<ul style="list-style-type: none"> <li><i>Component</i> identifies the affected component, such as a power supply, with which the affected fan is associated. This attribute provides information only if the fan is associated with a component.</li> <li><i>Unit</i> identifies the affected fan.</li> </ul>
Failed	A fan failed. You must manually clear this event.	Critical	Alert	None
Failed	A fan is now functioning correctly.	Harmless	Resolution	<ul style="list-style-type: none"> <li><i>Component</i> identifies the affected component, such as a power supply, with which the affected fan is associated. This attribute provides information only if the fan is associated with a component.</li> <li><i>Unit</i> identifies the affected fan.</li> </ul>

Event type	Event text	Severity	Category	Additional extended attributes
Inserted	A fan was inserted.	Harmless	Resolution	<i>Unit</i> identifies the affected fan.
PFA	A PFA alert associated with a fan occurred.	Warning	Alert	<i>Unit</i> identifies the affected fan.
PFA	A fan is now functioning correctly.	Harmless	Resolution	<i>Unit</i> identifies the affected fan.
Removed	A fan was removed.	Warning	Alert	<i>Unit</i> identifies the affected fan.

## MPA > Component > Hardware Information

The Hardware Information events occur when a service processor detects that the state of the operating system has changed and the hardware can provide information about the change, such as crash dump information. For detailed Hardware Information event types, expand the **Hardware Information** node in the Event Filter Builder tree.

### Details

**Note:** This event is generated by service processors only.

These MPA event types use the following set of extended attributes:

- Firmware code
- Sender UUID
- Source UUID

Some event types have additional extended attributes. These event types list the attributes in the Additional extended attributes column.

If you select the **Hardware Information** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Hardware Information subtree.

Event type	Event text	Severity	Category	Additional extended attributes
Hardware Information	Not applicable	Not applicable	Not applicable	None

## MPA > Component > Hardware Information > Crash Dump

The Crash Dump events occur when a service processor detects that the state of the operating system has changed and the hardware can provide crash dump information.

### Details

**Note:** This event is generated by service processors only.

These MPA event types use the following set of extended attributes:

- Firmware code
- Sender UUID
- Source UUID

Some event types have additional extended attributes. These event types list the attributes in the Additional extended attributes column.

If you select the **Crash Dump** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Crash Dump subtree.

Event type	Event text	Severity	Category	Additional extended attributes
Crash Dump	Not applicable	Not applicable	Not applicable	None

You can choose to select specific event types that are displayed under the **Crash Dump** node in the Event Filter Builder tree. The event filter will process only the event types that you select.

Event type	Event text	Severity	Category	Additional extended attributes
Initiated	Hardware information related to an OS crash is available.	Critical	Alert	None
Aborted	An attempt to collect hardware information after an OS crash failed.	Fatal	Alert	None
Completed	Successfully collected hardware information after an OS crash.	Harmless	Alert	None

## MPA > Component > I/O Module

The I/O Module events occur when a management module detects that the state of an I/O module (such as a switch) has changed.

### Details

**Note:** These events are generated by BladeCenter management modules only.

These MPA event types use the following set of extended attributes:

- Firmware code
- Sender UUID
- Source UUID

Some event types have additional extended attributes. These event types list the attributes in the Additional extended attributes column.

If you select the **I/O Module** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the I/O Module subtree.

Event type	Event text	Severity	Category	Additional extended attributes
I/O Module	Not applicable	Not applicable	Not applicable	<i>Unit</i> identifies the affected I/O module.

You can choose to select specific event types that are displayed under the **I/O Module** node in the Event Filter Builder tree. The event filter will process only the event types that you select.

Event type	Event text	Severity	Category	Additional extended attributes
Configuration	The I/O module IP configuration changed.	Harmless	Alert	<ul style="list-style-type: none"> <li><i>IP Address 1</i> is the IP address being used by the BladeCenter I/O module.</li> <li><i>Unit</i> identifies the affected I/O module.</li> </ul>
Failed	An I/O module failed.	Critical	Alert	<i>Unit</i> identifies the affected I/O module.
Failed	An I/O module recovered from a failure.	Harmless	Resolution	<i>Unit</i> identifies the affected I/O module.
Inserted	An I/O module was inserted.	Harmless	Alert	<i>Unit</i> identifies the affected I/O module.
Insufficient Power	An I/O module cannot power on because there is insufficient power.	Critical	Alert	<i>Unit</i> identifies the affected I/O module.
Insufficient Power	An I/O module has sufficient power to power on.	Harmless	Resolution	<i>Unit</i> identifies the affected I/O module.
POST	I/O module POST completed with errors.	Warning	Alert	<i>Unit</i> identifies the affected I/O module.
POST	I/O module POST completed without errors after a previous failure.	Harmless	Resolution	<i>Unit</i> identifies the affected I/O module.
POST	I/O module POST timed out.	Critical	Alert	<i>Unit</i> identifies the affected I/O module.
POST	I/O module POST completed after a previous timeout.	Harmless	Resolution	<i>Unit</i> identifies the affected I/O module.

Event type	Event text	Severity	Category	Additional extended attributes
Power	Not applicable	Not applicable	Not applicable	<i>Unit</i> identifies the affected I/O module.
Power > Off	An I/O module was powered off.	Warning	Alert	<i>Unit</i> identifies the affected I/O module.
Power > On	An I/O module was powered on.	Harmless	Alert	<i>Unit</i> identifies the affected I/O module.
Redundancy	I/O module redundancy was lost.	Minor	Alert	<i>Unit</i> identifies the affected I/O module.
Redundancy	I/O module redundancy was restored.	Harmless	Resolution	<i>Unit</i> identifies the affected I/O module.
Removed	An I/O module was removed.	Warning	Alert	<i>Unit</i> identifies the affected I/O module.

## MPA > Component > KVM

The KVM events occur when a service processor or management module detects that the state of the keyboard, video, and mouse (KVM) has changed.

### Details

**Note:** These events are generated by service processors and BladeCenter management modules.

These MPA event types use the following set of extended attributes:

- Firmware code
- Sender UUID
- Source UUID

Some event types have additional extended attributes. These event types list the attributes in the Additional extended attributes column.

If you select the **KVM** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the KVM subtree.

Event type	Event text	Severity	Category	Additional extended attributes
KVM	Not applicable	Not applicable	Not applicable	None

You can choose to select specific event types that are displayed under the **KVM** node in the Event Filter Builder tree. The event filter will process only the event types that you select.

Event type	Event text	Severity	Category	Additional extended attributes
Owner	An attempt to switch the KVM owner failed.	Minor	Alert	None

## MPA > Component > OS Image

The OS Image events occur when a service processor detects that the state of the operating system has changed and that an operating system image is available. For detailed OS Image event types, expand the **OS Image** node in the Event Filter Builder tree.

### Details

**Note:** This event is generated by service processors only.

These MPA event types use the following set of extended attributes:

- Firmware code
- Sender UUID
- Source UUID

Some event types have additional extended attributes. These event types list the attributes in the Additional extended attributes column.



If you select the **OS Image** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the OS Image subtree.

Event type	Event text	Severity	Category	Additional extended attributes
OS Image	Not applicable	Not applicable	Not applicable	None

### MPA > Component > OS Image > Crash Dump

The Crash Dump events occur when a service processor detects that the state of the operating system has changed and that an operating system image is available.

#### Details

**Note:** This event is generated by service processors only.

These MPA event types use the following set of extended attributes:

- Firmware code
- Sender UUID
- Source UUID

Some event types have additional extended attributes. These event types list the attributes in the Additional extended attributes column.

If you select the **Crash Dump** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Crash Dump subtree.

Event type	Event text	Severity	Category	Additional extended attributes
Crash Dump	Not applicable	Not applicable	Not applicable	None

You can choose to select specific event types that are displayed under the **Crash Dump** node in the Event Filter Builder tree. The event filter will process only the event types that you select.

Event type	Event text	Severity	Category	Additional extended attributes
Initiated	An OS crash image is available.	Critical	Alert	None
Aborted	An attempt to collect an OS crash image failed.	Fatal	Alert	None
Completed	An attempt to collect an OS crash image succeeded.	Harmless	Alert	None

## MPA > Component > PFA

The PFA events occur when a service processor or management module detects a Predictive Failure Analysis<sup>®</sup> (PFA) alert. The service processor event log provides more information about the PFA alert.

### Details

**Note:** These events are generated by service processors and BladeCenter management modules.

These MPA event types use the following set of extended attributes:

- Firmware code
- Sender UUID
- Sensor Label
- Sensor Number
- Source UUID

Some MPA event types have additional extended attributes. These event types list the attributes in the Additional extended attributes column.

Event type	Event text	Severity	Category	Additional extended attributes
PFA	A PFA alert occurred. Check the service processor event log for more information.	Warning	Alert	None
PFA	A PFA alert occurred. Check the service processor event log for more information. You must manually clear this event.	Warning	Alert	None
PFA	The problem that generated a PFA alert was resolved. Check the service processor event log for more information.	Harmless	Resolution	None

## MPA > Component > Power Subsystem

The Power Subsystem events occur when a service processor or management module detects that the state of a power subsystem has changed.

### Details

**Note:** These events are generated by service processors and BladeCenter management modules.

These MPA event types use the following set of extended attributes:

- Firmware code
- Sender UUID
- Sensor Label
- Sensor Number
- Source UUID

Some MPA event types have additional extended attributes. These event types list the attributes in the Additional extended attributes column.

If you select the **Power Subsystem** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Power Subsystem subtree.

Event type	Event text	Severity	Category	Additional extended attributes
Power Subsystem	Not applicable	Not applicable	Not applicable	None

You can choose to select specific event types that are displayed under the **Power Subsystem** node in the Event Filter Builder tree. The event filter will process only the event types that you select.

Event type	Event text	Severity	Category	Additional extended attributes
Low Fuel	The server is in a low-fuel state.	Minor	Alert	None
Low Fuel	The server recovered from a low-fuel state.	Harmless	Resolution	None
Mismatched Power Supplies	Mismatched power supplies were detected.	Minor	Alert	<i>Power Domain</i> identifies the affected BladeCenter chassis power domain. A BladeCenter chassis is divided into two power domains. Power supplies 1 and 2 provide power to the first domain; Power supplies 3 and 4 provide power to the second domain.
Mismatched Power Supplies	No mismatched power supplies were detected.	Harmless	Resolution	<i>Power Domain</i> identifies the affected BladeCenter chassis power domain. A BladeCenter chassis is divided into two power domains. Power supplies 1 and 2 provide power to the first domain; Power supplies 3 and 4 provide power to the second domain.
Over Current	The server load exceeded the capacity of the power subsystem. You must manually clear this event.	Minor	Alert	None

<b>Event type</b>	<b>Event text</b>	<b>Severity</b>	<b>Category</b>	<b>Additional extended attributes</b>
Over Power	A power bus has exceeded 240 voltage amps. You must manually clear this event.	Critical	Alert	<ul style="list-style-type: none"> <li>• <i>Bus</i> identifies the affected bus.</li> <li>• <i>Voltage Sensor</i> identifies the affected voltage sensor.</li> </ul>
Over Subscription	One power supply is not sufficient to power all blade servers at peak performance. Throttling might occur.	Warning	Alert	<i>Power Domain</i> identifies the affected BladeCenter chassis power domain. A BladeCenter chassis is divided into two power domains. Power supplies 1 and 2 provide power to the first domain; Power supplies 3 and 4 provide power to the second domain.
Over Subscription	One power supply is sufficient to power all blade servers at peak performance.	Harmless	Resolution	<i>Power Domain</i> identifies the affected BladeCenter chassis power domain. A BladeCenter chassis is divided into two power domains. Power supplies 1 and 2 provide power to the first domain; Power supplies 3 and 4 provide power to the second domain.
Over Subscription	One power supply is not sufficient to power all blade servers. A power failure might result in an immediate shutdown.	Minor	Alert	<i>Power Domain</i> identifies the affected BladeCenter chassis power domain. A BladeCenter chassis is divided into two power domains. Power supplies 1 and 2 provide power to the first domain; Power supplies 3 and 4 provide power to the second domain.
Over Subscription	One power supply is sufficient to power all blade servers.	Harmless	Resolution	<i>Power Domain</i> identifies the affected BladeCenter chassis power domain. A BladeCenter chassis is divided into two power domains. Power supplies 1 and 2 provide power to the first domain; Power supplies 3 and 4 provide power to the second domain.

Event type	Event text	Severity	Category	Additional extended attributes
Redundancy	Power redundancy was lost.	Minor	Alert	<i>Power Domain</i> identifies the affected BladeCenter chassis power domain. A BladeCenter chassis is divided into two power domains. Power supplies 1 and 2 provide power to the first domain; Power supplies 3 and 4 provide power to the second domain.
Redundancy	Power redundancy was lost. You must manually clear this event.	Minor	Alert	There are no extended attributes for this event type.
Redundancy	Power redundancy was restored.	Harmless	Resolution	<i>Power Domain</i> identifies the affected BladeCenter chassis power domain. A BladeCenter chassis is divided into two power domains. Power supplies 1 and 2 provide power to the first domain; Power supplies 3 and 4 provide power to the second domain.

## MPA > Component > Power Supply

The Power Supply events occur when a service processor or management module detects that the state of a power supply has changed.

### Details

**Note:** These events are generated by service processors and BladeCenter management modules.

These MPA event types use the following set of extended attributes:

- Firmware code
- Sender UUID
- Sensor Label
- Sensor Number
- Source UUID

Some MPA event types have additional extended attributes. These event types list the attributes in the Additional extended attributes column.

If you select the **Power Supply** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Power Supply subtree.

Event type	Event text	Severity	Category	Additional extended attributes
Power Supply	Not applicable	Not applicable	Not applicable	<i>Unit</i> identifies the affected power supply.

You can choose to select specific event types that are displayed under the **Power Supply** node in the Event Filter Builder tree. The event filter will process only the event types that you select.

Event type	Event text	Severity	Category	Additional extended attributes
Failed	A power supply failed.	Critical	Alert	<ul style="list-style-type: none"> <li>• <i>Reason</i> is one of the following strings:               <ul style="list-style-type: none"> <li>– current</li> <li>– dc</li> <li>– epow</li> <li>– voltage</li> <li>– voltage_over</li> <li>– voltage_under</li> </ul> </li> <li>• <i>Unit</i> identifies the affected power supply.</li> <li>• <i>Voltage Sensor</i> identifies the faulty voltage sensor by voltage.</li> </ul>
Failed	A power supply failed. You must manually clear this event.	Critical	Alert	<ul style="list-style-type: none"> <li>• <i>Unit</i> identifies the affected power supply.</li> </ul>

Event type	Event text	Severity	Category	Additional extended attributes
Failed	A power supply is now functioning properly.	Harmless	Resolution	<ul style="list-style-type: none"> <li>Reason is one of the following strings: <ul style="list-style-type: none"> <li>– current</li> <li>– dc</li> <li>– epow</li> <li>– voltage</li> <li>– voltage_over</li> <li>– voltage_under</li> </ul> </li> <li>Unit identifies the affected power supply.</li> <li>Voltage Sensor identifies the faulty voltage sensor by voltage.</li> </ul>
Inserted	A power supply was inserted.	Harmless	Resolution	Unit identifies the affected power supply.
Removed	A power supply was removed.	Warning	Alert	Unit identifies the affected power supply.

## MPA > Component > Server

The Server events occur when a service processor or management module detects that the state of a server has changed.

### Details

**Note:** Unless stated otherwise, the following events are generated by service processors and BladeCenter management modules.

These MPA event types use the following set of extended attributes:

- Firmware code
- Sender UUID
- Sensor Label
- Sensor Number
- Source UUID



Some MPA event types have additional extended attributes. These event types list the attributes in the Additional extended attributes column.

If you select the **Server** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Server subtree.

Event type	Event text	Severity	Category	Additional extended attributes
Server	Not applicable	Not applicable	Not applicable	None

You can choose to select specific event types that are displayed under the **Server** node in the Event Filter Builder tree. The event filter will process only the event types that you select.

Event type	Event text	Severity	Category	Additional extended attributes
Configuration	The ASM interconnect configuration is invalid. <b>Note:</b> This event is generated by service processors only.	Minor	Alert	<i>Issue</i> is set to rs485.
Configuration	The PCI Planar/ASM interconnect configuration is invalid. <b>Note:</b> This event is generated by service processors only.	Minor	Alert	<i>Issue</i> is set to pci/rs485.
Configuration	A server configuration issue was resolved. <b>Note:</b> This event is generated by service processors only.	Harmless	Resolution	<ul style="list-style-type: none"> <li>• <i>Issue</i> is one of the following strings: <ul style="list-style-type: none"> <li>– rs485</li> <li>– pci/rs485</li> </ul> </li> </ul>
Power	Not applicable	Not applicable	Not applicable	None
Power > Off	The server is powering off.	Warning	Alert	None
Power > On	The server is powering on.	Harmless	Alert	None

Event type	Event text	Severity	Category	Additional extended attributes
State	A server changed state. <b>Note:</b> This event is generated by service processors only.	Harmless	Alert	<p><i>New State</i> is one of the following strings:</p> <ul style="list-style-type: none"> <li>• off</li> <li>• in_post</li> <li>• post_error</li> <li>• flash</li> <li>• booting_os</li> <li>• in_os</li> <li>• reset</li> <li>• on</li> </ul>

## MPA > Component > Service Processor

The Service Processor events occur when a service processor detects that its state has changed or a management module detects that its state, or the state of another management module in the same chassis, has changed.

### Details

**Note:** Unless stated otherwise, the following events are generated by service processors and BladeCenter management modules.

These MPA event types use the following set of extended attributes:

- Firmware code
- Sender UUID
- Sensor Label
- Sensor Number
- Source UUID

Some MPA event types have additional extended attributes. These event types list the attributes in the Additional extended attributes column.

If you select the **Service Processor** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Service Processor subtree.

Event type	Event text	Severity	Category	Additional extended attributes
Service Processor	Not applicable	Not applicable	Not applicable	None

You can choose to select specific event types that are displayed under the **Service Processor** node in the Event Filter Builder tree. The event filter will process only the event types that you select.

Event type	Event text	Severity	Category	Additional extended attributes
Active	A management module assumed control of the chassis. <b>Note:</b> These events are generated by BladeCenter management modules only.	Warning	Alert	<i>Unit</i> identifies the affected management module.
Communication	The management module cannot communicate with a blade server baseboard management controller (BMC). <b>Note:</b> These events are generated by BladeCenter management modules only.	Critical	Alert	None
Configuration	IBM Director Server failed to assign a default alert configuration to the service processor.	Warning	Alert	None

Event type	Event text	Severity	Category	Additional extended attributes
Failover	A network loss caused a failover to the redundant management module. You must manually clear this event. <b>Note:</b> These events are generated by BladeCenter management modules only.	Minor	Alert	None
Failover	An I2C bus failure caused a failover to the redundant management module. <b>Note:</b> These events are generated by BladeCenter management modules only.	Minor	Alert	None
Failover	A management module failover event was reset by a management module reset or by removal of the failed management module. <b>Note:</b> These events are generated by BladeCenter management modules only.	Harmless	Resolution	None
Inserted	A service processor was inserted.	Harmless	Alert	<i>Unit</i> identifies the affected service processor.
Log	The service processor event log is full.	Minor	Alert	None
Log	The service processor event log is full. You must manually clear this event.	Minor	Alert	None
Log	The service processor event log is 75% full.	Warning	Alert	None

Event type	Event text	Severity	Category	Additional extended attributes
Log	The service processor event log is 75% full. You must manually clear this event.	Warning	Alert	None
Log	The service processor event log was cleared.	Harmless	Resolution	None
Network Stack	The service processor network stack started.	Harmless	Alert	<ul style="list-style-type: none"> <li><i>IP Address 1</i> is the IP address used by network interface 1 (external interface on the BladeCenter management module).</li> <li><i>IP Address 2</i> is the IP address used by network interface 2 (external interface on the BladeCenter management module).</li> </ul>
Out-of-band	Not applicable	Not applicable	Not applicable	None
Out-of-band > Disabled	The service processor out-of-band connection was disabled.	Harmless	Alert	None
Out-of-band > Enabled	The service processor out-of-band connection was enabled.	Harmless	Alert	None
Out-of-band > Port	The port number changed for the service processor out-of-band connection. <b>Note:</b> This event is generated by service processors only.	Harmless	Alert	<i>Port</i> identifies the new port number.
Redundancy	Service processor redundancy was lost.	Minor	Alert	None
Redundancy	Service processor redundancy was restored.	Harmless	Resolution	None

Event type	Event text	Severity	Category	Additional extended attributes
Removed	A service processor was removed.	Warning	Alert	<i>Unit</i> identifies the affected service processor.
Restart	The service processor restarted. <b>Note:</b> This event is generated by service processors only.	Harmless	Alert	None
Secure Out-of-band	Not applicable	Not applicable	Not applicable	None
Secure Out-of-band > Disabled	The service processor secure out-of-band connection was disabled.	Harmless	Alert	None
Secure Out-of-band > Enabled	The service processor secure out-of-band connection was enabled.	Harmless	Alert	None
Secure Out-of-band > Port	The port number changed for the service processor secure out-of-band connection. <b>Note:</b> This event is generated by service processors only.	Harmless	Alert	<i>Port</i> identifies the new port number.
Test	The service processor sent a test event.	Harmless	Alert	None

## MPA > Component > SMP Expansion Module

The SMP Expansion Module events occur when a service processor detects that the state of an SMP Expansion Module has changed.

## Details

**Note:** This event is generated by service processors only.

These MPA event types use the following set of extended attributes:

- Firmware code
- Sender UUID
- Source UUID

Some event types have additional extended attributes. These event types list the attributes in the Additional extended attributes column.

If you select the **SMP Expansion Module** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the SMP Expansion Module subtree.

Event type	Event text	Severity	Category	Extended attributes
SMP Expansion Module	Not applicable	Not applicable	Not applicable	<i>Unit</i> identifies the affected SMP expansion module.

You can choose to select specific event types that are displayed under the **SMP Expansion Module** node in the Event Filter Builder tree. The event filter will process only the event types that you select.

Event type	Event text	Severity	Category	Extended attributes
Disabled	An SMP Expansion Module was disabled.	Critical	Alert	<i>Unit</i> identifies the affected SMP expansion module.
Disabled	An SMP Expansion Module recovered after being disabled.	Harmless	Resolution	<i>Unit</i> identifies the affected SMP expansion module.

## MPA > Component > USB

The USB events occur when a service processor or management module detects that the state of a USB device has changed.

### Details

**Note:** These events are generated by service processors and BladeCenter management modules.

These MPA event types use the following set of extended attributes:

- Firmware code
- Sender UUID
- Source UUID

Some event types have additional extended attributes. These event types list the attributes in the Additional extended attributes column.

If you select the **USB** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the USB subtree.

Event type	Event text	Severity	Category	Additional extended attributes
USB	Not applicable	Not applicable	Not applicable	None

You can choose to select specific event types that are displayed under the **USB** node in the Event Filter Builder tree. The event filter will process only the event types that you select.

Event type	Event text	Severity	Category	Additional extended attributes
Inserted	A USB device was inserted.	Harmless	Resolution	None
Owner	An attempt to switch the USB device owner failed.	Minor	Alert	None



Event type	Event text	Severity	Category	Additional extended attributes
Removed	A USB device was removed.	Warning	Alert	None

## MPA > Component > VRM

The VRM events occur when a service processor or management module detects that the state of a voltage regulator module (VRM) has changed.

### Details

**Note:** Unless stated otherwise, the following events are generated by service processors and BladeCenter management modules.

These MPA event types use the following set of extended attributes:

- Firmware code
- Sender UUID
- Sensor Label
- Sensor Number
- Source UUID

Some MPA event types have additional extended attributes. These event types list the attributes in the Additional extended attributes column.

If you select the **VRM** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the VRM subtree.

Event type	Event text	Severity	Category	Additional extended attributes
VRM	Not applicable	Not applicable	Not applicable	None

You can choose to select specific event types that are displayed under the **VRM** node in the Event Filter Builder tree. The event filter will process only the event types that you select.

Event type	Event text	Severity	Category	Additional extended attributes
Configuration	The voltage regulator module configuration is invalid. <b>Note:</b> This event is generated by service processors only.	Critical	Alert	None
Configuration	The voltage regulator module configuration is valid. <b>Note:</b> This event is generated by service processors only.	Harmless	Resolution	None
Failed	A voltage regulator module failed.	Critical	Alert	<i>Unit</i> identifies the affected voltage regulator module.
Failed	A voltage regulator module failed. You must manually clear this event.	Critical	Alert	None
Failed	A voltage regulator module is now working properly.	Harmless	Resolution	<i>Unit</i> identifies the affected voltage regulator module.

## MPA > Environmental

The Environmental events occur when a service processor or management module detects that the state of a system temperature or voltage sensor has changed with respect to a manufacturer-defined or user-defined threshold. For detailed event types, expand the **Environmental** node in the Event Filter Builder tree.

### Details

**Note:** Unless stated otherwise, the following events are generated by service processors and BladeCenter management modules.

These MPA event types use the following set of extended attributes:

- Firmware code
- Sender UUID
- Sensor Label
- Sensor Number
- Source UUID

Some MPA event types have additional extended attributes. These event types list the attributes in the Additional extended attributes column.

If you select the **Environmental** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Environmental subtree.

Event type	Event text	Severity	Category	Additional extended attributes
Environmental	Not applicable	Not applicable	Not applicable	Side identifies the affected side of an RXE-100 Remote Expansion Enclosure. This extended attribute is present only with event types that are generated for this enclosure. The enclosure contains twelve PCI slots that are divided into two sets of six. Each set can be configured to belong to the same server or two different servers.

You can choose to select specific event types that are displayed under the **Environmental** node in the Event Filter Builder tree. The event filter will process only the event types that you select.

Event type	Event text	Severity	Category	Additional extended attributes
Temperature	A monitored temperature has exceeded the threshold.	Critical	Alert	<ul style="list-style-type: none"> <li>• <i>Side</i> identifies the affected side of an RXE-100 Remote Expansion Enclosure. This extended attribute is present only with event types that are generated for this enclosure. The enclosure contains twelve PCI slots that are divided into two sets of six. Each set can be configured to belong to the same server or two different servers.</li> <li>• <i>Temperature Sensor</i> is one of the following strings: <ul style="list-style-type: none"> <li>– ambient</li> <li>– Blade Expansion Module</li> <li>– management processor</li> <li>– CPU</li> <li>– DASD</li> <li>– power supply</li> <li>– I/O module</li> <li>– memory</li> </ul> </li> <li>• <i>Unit</i> identifies the affected sensor. This attribute is applicable if the sensor is associated with a component that includes multiple sensors. For example, if the server has two sensors, Unit identifies whether the event information is for sensor 1 or sensor 2.</li> </ul>

Event type	Event text	Severity	Category	Additional extended attributes
Temperature	<p>A monitored temperature has exceeded the threshold. You must manually clear this event.</p> <p><b>Note:</b> This event type can be generated by:</p> <ul style="list-style-type: none"> <li>• IBM Director Agent for NetWare, version 5.10.</li> <li>• IBM Director Agent, versions 4.10, 4.10.2, 4.11, 4.12, 4.20, 4.20.2, 4.21, 4.22.</li> <li>• Service processors that are configured to send out-of-band events using the IBM Director over LAN selection.</li> </ul>	Critical	Alert	There are no extended attributes for this event type.

Event type	Event text	Severity	Category	Additional extended attributes
Temperature	A monitored temperature has exceeded the threshold.	Minor	Alert	<ul style="list-style-type: none"> <li>• <i>Side</i> identifies the affected side of an RXE-100 Remote Expansion Enclosure. This extended attribute is present only with event types that are generated for this enclosure. The enclosure contains twelve PCI slots that are divided into two sets of six. Each set can be configured to belong to the same server or two different servers.</li> <li>• <i>Temperature Sensor</i> is one of the following strings: <ul style="list-style-type: none"> <li>– ambient</li> <li>– Blade Expansion Module</li> <li>– management processor</li> <li>– CPU</li> <li>– DASD</li> <li>– power supply</li> <li>– I/O module</li> <li>– memory</li> </ul> </li> <li>• <i>Unit</i> identifies the affected sensor. This attribute is applicable if the sensor is associated with a component that includes multiple sensors. For example, if the server has two sensors, Unit identifies whether the event information is for sensor 1 or sensor 2.</li> </ul>

Event type	Event text	Severity	Category	Additional extended attributes
Temperature	A monitored temperature is now within the applicable range.	Harmless	Resolution	<ul style="list-style-type: none"> <li>• <i>Side</i> identifies the affected side of an RXE-100 Remote Expansion Enclosure. This extended attribute is present only with event types that are generated for this enclosure. The enclosure contains twelve PCI slots that are divided into two sets of six. Each set can be configured to belong to the same server or two different servers.</li> <li>• <i>Temperature Sensor</i> is one of the following strings: <ul style="list-style-type: none"> <li>– ambient</li> <li>– Blade Expansion Module</li> <li>– management processor</li> <li>– CPU</li> <li>– DASD</li> <li>– power supply</li> <li>– I/O module</li> <li>– memory</li> </ul> </li> <li>• <i>Unit</i> identifies the affected sensor. This attribute is applicable if the sensor is associated with a component that includes multiple sensors. For example, if the server has two sensors, <i>Unit</i> identifies whether the event information is for sensor 1 or sensor 2.</li> </ul>

Event type	Event text	Severity	Category	Additional extended attributes
Voltage	A monitored voltage is operating outside the applicable range.	Critical	Alert	<ul style="list-style-type: none"> <li>• <i>Component</i> is one of the following strings: <ul style="list-style-type: none"> <li>– Blade Expansion Module</li> <li>– IO card</li> <li>– system</li> <li>– voltage regulator module</li> </ul> </li> <li>• <i>Side</i> identifies the affected side of an RXE-100 Remote Expansion Enclosure. This extended attribute is present only with event types that are generated for this enclosure. The enclosure contains twelve PCI slots that are divided into two sets of six. Each set can be configured to belong to the same server or two different servers.</li> <li>• <i>Threshold</i> is one of the following values: high or low. The value identifies whether the voltage exceeded a high threshold or fell below a low threshold.</li> <li>• <i>Voltage Sensor</i> identifies the faulty voltage sensor: <ul style="list-style-type: none"> <li>– 12V Standby</li> <li>– 5V Standby</li> <li>– 3.3V Standby</li> <li>– 2.5 Standby</li> <li>– 1.8V Standby</li> <li>– 1.5V Standby</li> <li>– 1.2V Standby</li> <li>– 5V PCI</li> <li>– 3.3V PCI</li> <li>– 18V</li> <li>– 12V</li> <li>– 5V</li> <li>– 3.3V</li> <li>– 2.5V</li> <li>– 1.6V</li> <li>– 1.8V</li> </ul> </li> </ul>



Event type	Event text	Severity	Category	Additional extended attributes
Voltage (continued)				<ul style="list-style-type: none"> <li>• 1.5V</li> <li>• 1.3V</li> <li>• 1.25V</li> <li>• 1.2V</li> <li>• -5V</li> <li>• -12V</li> </ul>
Voltage	<p>A monitored voltage is operating outside the applicable range. You must manually clear this event.</p> <p><b>Note:</b> This event type can be generated by:</p> <ul style="list-style-type: none"> <li>• IBM Director Agent for NetWare, version 5.10.</li> <li>• IBM Director Agent, versions 4.10, 4.10.2, 4.11, 4.12, 4.20, 4.20.2, 4.21, 4.22.</li> <li>• Service processors that are configured to send out-of-band events using the IBM Director over LAN selection.</li> </ul>	Critical	Alert	There are no extended attributes for this event type.

Event type	Event text	Severity	Category	Additional extended attributes
Voltage	A monitored voltage is operating outside the applicable range.	Minor	Alert	<ul style="list-style-type: none"> <li>• <i>Component</i> is one of the following strings: <ul style="list-style-type: none"> <li>– Blade Expansion Module</li> <li>– IO card</li> <li>– system</li> <li>– voltage regulator module</li> </ul> </li> <li>• <i>Side</i> identifies the affected side of an RXE-100 Remote Expansion Enclosure. This extended attribute is present only with event types that are generated for this enclosure. The enclosure contains twelve PCI slots that are divided into two sets of six. Each set can be configured to belong to the same server or two different servers.</li> <li>• <i>Threshold</i> is one of the following values: high or low. The value identifies whether the voltage exceeded a high threshold or fell below a low threshold.</li> <li>• <i>Voltage Sensor</i> identifies the faulty voltage sensor: <ul style="list-style-type: none"> <li>– 12V Standby</li> <li>– 5V Standby</li> <li>– 3.3V Standby</li> <li>– 2.5 Standby</li> <li>– 1.8V Standby</li> <li>– 1.5V Standby</li> <li>– 1.2V Standby</li> <li>– 5V PCI</li> <li>– 3.3V PCI</li> <li>– 18V</li> <li>– 12V</li> <li>– 5V</li> <li>– 3.3V</li> <li>– 2.5V</li> <li>– 1.6V</li> <li>– 1.8V</li> </ul> </li> </ul>

Event type	Event text	Severity	Category	Additional extended attributes
Voltage (continued)				<ul style="list-style-type: none"> <li>• 1.5V</li> <li>• 1.3V</li> <li>• 1.25V</li> <li>• 1.2V</li> <li>• -5V</li> <li>• -12V</li> </ul>
Voltage	A monitored voltage is now within the applicable range.	Harmless	Resolution	<ul style="list-style-type: none"> <li>• <i>Component</i> is one of the following strings: <ul style="list-style-type: none"> <li>– Blade Expansion Module</li> <li>– IO card</li> <li>– system</li> <li>– voltage regulator module</li> </ul> </li> <li>• <i>Side</i> identifies the affected side of an RXE-100 Remote Expansion Enclosure. This extended attribute is present only with event types that are generated for this enclosure. The enclosure contains twelve PCI slots that are divided into two sets of six. Each set can be configured to belong to the same server or two different servers.</li> <li>• <i>Threshold</i> is one of the following values: high or low. The value identifies whether the voltage exceeded a high threshold or fell below a low threshold.</li> </ul>

Event type	Event text	Severity	Category	Additional extended attributes
Voltage (continued)				<ul style="list-style-type: none"> <li>• <i>Voltage Sensor</i> identifies the faulty voltage sensor:               <ul style="list-style-type: none"> <li>– 12V Standby</li> <li>– 5V Standby</li> <li>– 3.3V Standby</li> <li>– 2.5 Standby</li> <li>– 1.8V Standby</li> <li>– 1.5V Standby</li> <li>– 1.2V Standby</li> <li>– 5V PCI</li> <li>– 3.3V PCI</li> <li>– 18V</li> <li>– 12V</li> <li>– 5V</li> <li>– 3.3V</li> <li>– 2.5V</li> <li>– 1.6V</li> <li>– 1.8V</li> <li>– 1.5V</li> <li>– 1.3V</li> <li>– 1.25V</li> <li>– 1.2V</li> <li>– -5V</li> <li>– -12V</li> </ul> </li> </ul>

## MPA > Miscellaneous

The Miscellaneous events occur when an IPMI baseboard management controller reports a problem or information that IBM Director does not associate with another MPA event type.

## Details

**Note:** This event is generated by service processors only.

These MPA event types use the following set of extended attributes:

- Sensor Label
- Sensor Number
- Source UUID

Some event types have additional extended attributes. These event types list the attributes in the Additional extended attributes column.

Event type	Event text	Severity	Category	Additional extended attributes
Miscellaneous	Miscellaneous event occurred.	Varies depending on the service processor that sends the event.	Alert	None
Miscellaneous	Miscellaneous event occurred.	Varies depending on the service processor that sends the event.	Resolution	None

---

## MPA > Platform

The Platform events occur when a service processor detects that the state of the scalable nodes that are part of a scalable partition or scalable node has changed.

## Details

For detailed information about these events, see the *IBM Scalable Systems Manager version 4.20 Installation and User's Guide*.

---

### MPA > Server WatchDog

The Server WatchDog events occur when a service processor or management module detects that a system has failed to power on and start from the network, the bootstrap loader program failed to run, operating system timeout settings were exceeded, or system POST has failed.

#### Details

These MPA event types use the following set of extended attributes:

- Firmware code
- Sender UUID
- Sensor Label
- Sensor Number
- Source UUID

Some MPA event types have additional extended attributes. These event types list the attributes in the Additional extended attributes column.

If you select the **Server WatchDog** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Server WatchDog subtree.

Event type	Event text	Severity	Category	Additional extended attributes
Server WatchDog	Not applicable	Not applicable	Not applicable	None

You can choose to select specific event types that are displayed under the **Server WatchDog** node in the Event Filter Builder tree. The event filter will process only the event types that you select.

**Note:** Unless stated otherwise, the following events are generated by service processors and BladeCenter management modules.

Event type	Event text	Severity	Category	Additional extended attributes
Boot	The server failed to start.	Critical	Alert	None
Boot	The server failed to start. You must manually clear this event.	Critical	Alert	None
Boot	The server started successfully after a previous failure.	Harmless	Resolution	None
Loader	The loader timeout was exceeded. You must manually clear this event. <b>Note:</b> This event is generated by service processors only.	Critical	Alert	None
OS	The OS timeout was exceeded. You must manually clear this event.	Critical	Alert	None
POST	The system POST failed. You must manually clear this event.	Critical	Alert	None

## MPA > Unknown

The Unknown events occur when a service processor detects an unknown problem. Typically, the service processor event log provides more information.

## Details

**Note:** This event is generated by service processors only.

These MPA event types use the following set of extended attributes:

- Firmware code
- Sender UUID
- Source UUID

Some event types have additional extended attributes. These event types list the attributes in the Additional extended attributes column.

Event type	Event text	Severity	Category	Additional extended attributes
Unknown	Unknown event. Check the service processor event log for more information.	Warning	Alert	None
Unknown	Unknown recovery event. Check the service processor event log for more information.	Harmless	Resolution	None



---

## Chapter 12. PET events

Platform Event Trap (PET) events are generated by systems with Alert Standard Format (ASF) or an IPMI baseboard management controller. The PET events provide advance warning of possible system failures.

### Event source

PET events are not generated by IBM Director Core Services or IBM Director Agent. PET events are out-of-band events received by IBM Director Server from systems with Alert Standard Format (ASF) or an IPMI baseboard management controller.

**Note:** Not all ASF systems generate all of the PET events.

You must configure such systems in your system-management environment in order for IBM Director Server to receive PET events. Use the Configure Alert Standard Format task to configure ASF systems. For systems with an IPMI baseboard management controller, see Preparing to install IBM Director on an xSeries server for information about configuring the controller to send notifications to IBM Director Server.

### Details

**Note:** For detailed information about Platform Event Traps, see the following documentation:

- *Intel Intelligent Platform Management Interface Specification Version 1.5*, dated June 1, 2004.
- *Intel IPMI Platform Event Trap Specification Version 1.0*, dated December 7, 1998.

If a system has an IPMI baseboard management controller, both a PET event and an equivalent MPA event are sent to IBM Director Server. Because the MPA event provides more information and is easier to read, it is recommended that you create event-action plans with event filters for the MPA event types. However, if the system has Alert Standard Format (ASF), only a PET is generated and you must create event-action plans with event filters for the PET event types.

If you select the **PET** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the PET subtree.

Event type	Event text	Severity	Category	Extended attributes
PET	Not applicable	Not applicable	Not applicable	None

## PET > Environmental

The Environmental event occurs when a change in the state of the system environment is detected. In the IBM Director environment, the Environmental event types are associated with the state of the sensors that detect changes in a system environment. For detailed event types, expand the **Environmental** node in the Event Filter Builder tree.

### Details

If you select the **Environmental** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Environmental subtree. You can choose to select specific event types that are displayed under the Environmental node in the Event Filter Builder tree. The event filter will process only the event types that you select.

Event type	Event text	Severity	Category	Extended attributes
Environmental	Not applicable	Not applicable	Not applicable	Standard set of PET event type extended attributes

## PET > Environmental > Sensor

The Sensor events occur when a change in the state of an environmental sensor is detected.

### Details

If you select the **Sensor** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Sensor subtree.

Event type	Event text	Severity	Category	Extended attributes
Sensor	Not applicable	Not applicable	Not applicable	Standard set of PET event type extended attributes

You can choose to select specific event types that are displayed under the **Sensor** node in the Event Filter Builder tree. The event filter will process only the event types that you select.

**Note:** The severity for some of these event types is determined by the Event Severity extended attribute.

Event type	Event text	Severity	Category	Extended attributes
Case Intrusion	Case intrusion information	Set by the Event Severity attribute.	Alert	Standard set of PET event type extended attributes
Case Intrusion	Case intrusion information	Harmless	Resolution	Standard set of PET event type extended attributes
Current	Current information	Set by the Event Severity attribute.	Alert	Standard set of PET event type extended attributes
Current	Current information	Harmless	Resolution	Standard set of PET event type extended attributes
Fan	Fan information for device <i>device</i> .	Set by the Event Severity attribute.	Alert	Standard set of PET event type extended attributes
	where <i>device</i> is the value provided by the Entity Instance extended attribute.			

<b>Event type</b>	<b>Event text</b>	<b>Severity</b>	<b>Category</b>	<b>Extended attributes</b>
Fan	Fan information for device <i>device</i> .	Harmless	Resolution	Standard set of PET event type extended attributes
	where <i>device</i> is the value provided by the Entity Instance extended attribute.			
Fan	Device <i>device</i> inserted.	Set by the Event Severity attribute.	Alert	Standard set of PET event type extended attributes
	where <i>device</i> is the value provided by the Entity Instance extended attribute.			
Fan	Device <i>device</i> has been inserted.	Harmless	Resolution	Standard set of PET event type extended attributes
	where <i>device</i> is the value provided by the Entity Instance extended attribute.			
Fan	Device <i>device</i> has been removed.	Set by the Event Severity attribute.	Alert	Standard set of PET event type extended attributes
	where <i>device</i> is the value provided by the Entity Instance extended attribute.			
Fan	Device <i>device</i> has been removed.	Harmless	Resolution	Standard set of PET event type extended attributes
	where <i>device</i> is the value provided by the Entity Instance extended attribute.			
Power Supply	Power supply information	Set by the Event Severity attribute.	Alert	Standard set of PET event type extended attributes

<b>Event type</b>	<b>Event text</b>	<b>Severity</b>	<b>Category</b>	<b>Extended attributes</b>
Power Supply	Power supply information	Harmless	Resolution	Standard set of PET event type extended attributes
Power Supply	Redundancy has been lost.	Set by the Event Severity attribute.	Alert	Standard set of PET event type extended attributes
Power Supply	Redundancy has been lost.	Harmless	Resolution	Standard set of PET event type extended attributes
Power Supply	Redundancy has been degraded.	Set by the Event Severity attribute.	Alert	Standard set of PET event type extended attributes
Power Supply	Redundancy has been degraded.	Harmless	Resolution	Standard set of PET event type extended attributes
Power Supply	Redundancy has been regained.	Set by the Event Severity attribute.	Alert	Standard set of PET event type extended attributes
Power Supply	Redundancy has been regained.	Harmless	Resolution	Standard set of PET event type extended attributes
Temperature	Temperature information	Set by the Event Severity attribute.	Alert	Standard set of PET event type extended attributes
Temperature	Temperature information	Harmless	Resolution	Standard set of PET event type extended attributes
Voltage	Voltage information for device <i>device</i> .	Set by the Event Severity attribute.	Alert	Standard set of PET event type extended attributes
	where <i>device</i> is the value provided by the Entity Instance extended attribute.			

Event type	Event text	Severity	Category	Extended attributes
Voltage	Voltage information for device <i>device</i> .	Harmless	Resolution	Standard set of PET event type extended attributes
	where <i>device</i> is the value provided by the Entity Instance extended attribute.			

## PET > Firmware

The Firmware events occur when a change in the state of the system firmware is detected. In the IBM Director environment, the Firmware event types are associated with the state of the BIOS. For detailed event types, expand the **Firmware** node in the Event Filter Builder tree.

### Details

If you select the **Firmware** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Firmware subtree. You can choose to select specific event types that are displayed under the Firmware node in the Event Filter Builder tree. The event filter will process only the event types that you select.

Event type	Event text	Severity	Category	Extended attributes
Firmware	Not applicable	Not applicable	Not applicable	Standard set of PET event type extended attributes

## PET > Firmware > BIOS

The BIOS events occur when a change in the state of the system BIOS is detected.

## Details

If you select the **BIOS** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the BIOS subtree.

Event type	Event text	Severity	Category	Extended attributes
BIOS	Not applicable	Not applicable	Not applicable	Standard set of PET event type extended attributes

You can choose to select specific event types that are displayed under the **BIOS** node in the Event Filter Builder tree. The event filter will process only the event types that you select.

**Note:** The severity for some of these event types is determined by the Event Severity extended attribute.

Event type	Event text	Severity	Category	Extended attributes
Progress	System firmware progress information	Set by the Event Severity attribute.	Alert	Standard set of PET event type extended attributes
Progress	System firmware progress information	Harmless	Resolution	Standard set of PET event type extended attributes
Progress	The system firmware encountered an error in POST.	Set by the Event Severity attribute.	Alert	Standard set of PET event type extended attributes
Progress	The system firmware encountered an error in POST.	Harmless	Resolution	Standard set of PET event type extended attributes
Progress	The system boot has started.	Set by the Event Severity attribute.	Alert	Standard set of PET event type extended attributes

Event type	Event text	Severity	Category	Extended attributes
Progress	The system boot has started.	Harmless	Resolution	Standard set of PET event type extended attributes
Progress	The system firmware has hung.	Set by the Event Severity attribute.	Alert	Standard set of PET event type extended attributes
Progress	The system firmware has hung.	Harmless	Resolution	Standard set of PET event type extended attributes

## PET > Hardware

The Hardware events occur when a change in the state of a hardware component is detected. Hardware components include cables and interconnects, network connections, hard disk drives, timers, and other modules.

### Details

If you select the **Hardware** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Hardware subtree.

Event type	Event text	Severity	Category	Extended attributes
Hardware	Not applicable	Not applicable	Not applicable	Standard set of PET event type extended attributes

You can choose to select specific event types that are displayed under the **Hardware** node in the Event Filter Builder tree. The event filter will process only the event types that you select.



**Note:** The severity for some of these event types is determined by the Event Severity extended attribute.

Event type	Event text	Severity	Category	Extended attributes
Cable/Interconnect	The device is not present.	Set by the Event Severity attribute.	Alert	Standard set of PET event type extended attributes
Cable/Interconnect	The device is not present.	Harmless	Resolution	Standard set of PET event type extended attributes
Cable/Interconnect	The device is present.	Set by the Event Severity attribute.	Alert	Standard set of PET event type extended attributes
Cable/Interconnect	The device is present.	Harmless	Resolution	Standard set of PET event type extended attributes
Drivebay	Device <i>device</i> has been removed.	Set by the Event Severity attribute.	Alert	Standard set of PET event type extended attributes
	where <i>device</i> is the value provided by the Entity Instance extended attribute.			
Drivebay	Device <i>device</i> has been removed.	Harmless	Resolution	Standard set of PET event type extended attributes
	where <i>device</i> is the value provided by the Entity Instance extended attribute.			
Drivebay	The state of device <i>device</i> has changed to critical.	Set by the Event Severity attribute.	Alert	Standard set of PET event type extended attributes
	where <i>device</i> is the value provided by the Entity Instance extended attribute.			

<b>Event type</b>	<b>Event text</b>	<b>Severity</b>	<b>Category</b>	<b>Extended attributes</b>
Drivebay	The state of device <i>device</i> has changed to critical. where <i>device</i> is the value provided by the Entity Instance extended attribute.	Harmless	Resolution	Standard set of PET event type extended attributes
Drivebay	Device <i>device</i> has been inserted. where <i>device</i> is the value provided by the Entity Instance extended attribute.	Set by the Event Severity attribute.	Alert	Standard set of PET event type extended attributes
Drivebay	Device <i>device</i> has been inserted. where <i>device</i> is the value provided by the Entity Instance extended attribute.	Harmless	Resolution	Standard set of PET event type extended attributes
Drivebay	The state of device <i>device</i> has changed to OK. where <i>device</i> is the value provided by the Entity Instance extended attribute.	Set by the Event Severity attribute.	Alert	Standard set of PET event type extended attributes
Drivebay	The state of device <i>device</i> has changed to OK. where <i>device</i> is the value provided by the Entity Instance extended attribute.	Harmless	Resolution	Standard set of PET event type extended attributes

<b>Event type</b>	<b>Event text</b>	<b>Severity</b>	<b>Category</b>	<b>Extended attributes</b>
Module/Board	The device is not present.	Set by the Event Severity attribute.	Alert	Standard set of PET event type extended attributes
Module/Board	The device is not present.	Harmless	Resolution	Standard set of PET event type extended attributes
Module/Board	The device is present.	Set by the Event Severity attribute.	Alert	Standard set of PET event type extended attributes
Module/Board	The device is present.	Harmless	Resolution	Standard set of PET event type extended attributes
Monitor ASIC/IC	The state of the system-management module has changed to critical.	Set by the Event Severity attribute.	Alert	Standard set of PET event type extended attributes
Monitor ASIC/IC	The state of the system-management module has changed to critical.	Harmless	Resolution	Standard set of PET event type extended attributes
Network	The network connection is offline.	Set by the Event Severity attribute.	Alert	Standard set of PET event type extended attributes
Network	The network connection is offline.	Harmless	Resolution	Standard set of PET event type extended attributes
Network	The network connection has degraded.	Set by the Event Severity attribute.	Alert	Standard set of PET event type extended attributes
Network	The network connection has degraded.	Harmless	Resolution	Standard set of PET event type extended attributes

Event type	Event text	Severity	Category	Extended attributes
Network	The network connection is online.	Set by the Event Severity attribute.	Alert	Standard set of PET event type extended attributes
Network	The network connection is online.	Harmless	Resolution	Standard set of PET event type extended attributes
Watchdog 1	The watchdog timer has expired.	Set by the Event Severity attribute.	Alert	Standard set of PET event type extended attributes
Watchdog 1	The watchdog timer has expired.	Harmless	Resolution	Standard set of PET event type extended attributes
Watchdog 2	The timer has expired.	Set by the Event Severity attribute.	Alert	Standard set of PET event type extended attributes
Watchdog 2	The timer has expired.	Harmless	Resolution	Standard set of PET event type extended attributes

## PET > System

The System events occur when a change in the state of a system is detected. In the IBM Director environment, the System event types are associated with the state of the operating system. For detailed event types, expand the **System** node in the Event Filter Builder tree.

### Details

If you select the **System** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the System subtree. You can choose to select specific event types that are displayed under the System node in the Event Filter Builder tree. The event filter will process only the event types that you

select.

Event type	Event text	Severity	Category	Extended attributes
System	Not applicable	Not applicable	Not applicable	Standard set of PET event type extended attributes

## PET > System > OS

The OS events occur when a change in the state of the operating system is detected.

### Details

If you select the **OS** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the OS subtree.

Event type	Event text	Severity	Category	Extended attributes
OS	Not applicable	Not applicable	Not applicable	Standard set of PET event type extended attributes

You can choose to select specific event types that are displayed under the **OS** node in the Event Filter Builder tree. The event filter will process only the event types that you select.

**Note:** The severity for some of these event types is determined by the Event Severity extended attribute.

Event type	Event text	Severity	Category	Extended attributes
Boot	The operating system has failed to start (boot).	Set by the Event Severity attribute.	Alert	Standard set of PET event type extended attributes
Boot	The operating system has failed to start (boot).	Harmless	Resolution	Standard set of PET event type extended attributes

<b>Event type</b>	<b>Event text</b>	<b>Severity</b>	<b>Category</b>	<b>Extended attributes</b>
Boot	No media or device can be started (booted).	Set by the Event Severity attribute.	Alert	Standard set of PET event type extended attributes
Boot	No media or device can be started (booted).	Harmless	Resolution	Standard set of PET event type extended attributes
Operation	The operating system has hung.	Set by the Event Severity attribute.	Alert	Standard set of PET event type extended attributes
Operation	The operating system has hung.	Harmless	Resolution	Standard set of PET event type extended attributes
Operation > Heartbeat	Heartbeat information	Harmless	Resolution	Standard set of PET event type extended attributes

---

## Chapter 13. SNMP events

The SNMP events represent SNMP traps that are generated by the SNMP agents, software programs, and IBM hardware. A subset of the SNMP events are generated by IBM Director Core Services and IBM Director Agent.

### Event source

SNMP traps are generated by the SNMP agents that are installed on the SNMP devices being managed by IBM Director Server. IBM Director receives the SNMP traps and converts them into the SNMP event types that are displayed in the Event Filter Builder tree. See each event type for details about its source.

### Details

When you compile MIB files, they contain the trap definition of the traps that are displayed in the Event Filter Builder.

**Note:** For IBM Director 5.10, you must load the MIB files into memory in order to view the SNMP event types in the Event Filter Builder tree. To load a MIB file, complete the following steps:

1. Using the SNMP Browser task, click **File Select MIB to Load**.
2. In the Available MIB pane, click the MIB files that you want to load and then click **Add**.
3. When you have completed selecting MIB files, click **Apply** and then **OK**.

The event types available in the Event Filter Builder tree can vary depending on which MIB files you have loaded into memory and what products provided the MIB file. The IBM Director 5.10 information center provides information about the `ibmSystemMIB` and `ibmServerRAIDMIB` event types. For other SNMP event types under the iso node, see the MIB file that contains these SNMP traps.

The trap definitions can conform to either SNMP v1 or SNMP v2. The exact subnode under which the traps are displayed depends on which branch of the standard MIB the traps' MIB is under: experimental, mgmt, private, or

snmpV2. Trap definitions from most MIBs, are displayed under the private subnode (SNMP.iso.internet.private). Traps defined in the standard MIBs, such as MIB II, are displayed under the mgmt subnode (SNMP.iso.internet.mgmt).

If you select the **SNMP** check box in the Event Filter Builder tree, the event filter will process all of the events that are specified in the SNMP subtree. You can choose to select specific event types that are displayed under the **SNMP** node in the Event Filter Builder tree. The event filter will process only the events that you select.

---

## SNMP > Hardware

The Hardware events occur when IBM hardware components send SNMP traps in the IBM Director environment. For more information about these SNMP traps, see the documentation for the associated IBM hardware.

### Event source

SNMP traps are generated by the following IBM hardware that are installed in the IBM Director environment:

- Alert on LAN™ network interface cards (NICs)
- BladeCenter Fibre Channel expansion cards
- ServerRAID controllers

**Note:** These SNMP traps are generated by the ServerRAID Manager (Standalone Edition). For information about SNMP events generated by the ServerRAID Manager extension, see `SNMP > iso > ibmServerRAIDMIB`.

- Tape drives
- UPS devices

IBM Director receives the SNMP traps and converts them into the SNMP event types that are displayed in the Event Filter Builder tree.

### Details

If you select the **Hardware** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Hardware subtree. You can choose to select specific event types that are displayed



under the **Hardware** node in the Event Filter Builder tree. The event filter will process only the event types that you select.

---

## **ibmSystemMIB**

The `ibmSystemMIB` events provide information about system subcomponent failures and warranty and lease status. For detailed events, expand the **ibmSystemMIB** node in the Event Filter Builder tree.

### **Event source**

`ibmSystemMIB` event types are generated by IBM Director Agent. IBM Director uses CIM indications to communicate hardware information. If you have configured your IBM Director environment to use SNMP traps, IBM Director converts the CIM indications into the `ibmSystemMIB` SNMP traps. For information about configuring your IBM Director environment to use SNMP traps, see “Configuring SNMP trap forwarding.”

To support SNMP, the IBM Director Agent includes a CIM client that is called the IBM Director Agent SNMP agent. It translates the CIM-indication data into SNMP format and exports the SNMP data to SNMP clients, such as HP OpenView and Tivoli NetView Upward Integration Modules (UIMs). When you configure your IBM Director environment to use SNMP traps, the IBM Director Agent SNMP agent is registered with the operating system and any queries involving the IBM Director Agent enterprise OID are forwarded to the IBM Director Agent SNMP agent for processing.

When an SNMP client sends a Get request, the IBM Director Agent SNMP agent receives the request and queries the CIM server on the target managed system. Then, the CIM server performs the following steps:

1. Translates the SNMP request to a CIM client request
2. Converts the SNMP variable that is the subject of the request to a CIM instance and property
3. Translates the CIM response to an SNMP response
4. Returns the response to the SNMP client

While the IBM Director Agent SNMP agent is installed and registered, it creates and forwards SNMP traps to any configured alert destinations, and you cannot stop the forwarding of the SNMP traps. Unwanted SNMP traps must be filtered out by the listening event server.

## Event Filter Builder tree path

The full path for this event type in the Event Filter Builder tree is:

```
SNMP > iso > org > dod > internet > private > enterprises > ibm > ibmProd > ibmServer > ibmSystem >
ibmSystemMIB
```

## SNMP variables

This IBM Director SNMP event type uses the following set of variables:

- OID
- Identifier
- SourceObjectPath
- TargetObjectPath
- Severity
- Description
- TimeStamp

For the values that are bound to these variables for this event type, see the IBM-SYSTEM-TRAP-MIB.mib file in the *c:/Director/proddata/snmp* directory, where *c* is the hard disk drive and *Director* is the directory where you installed IBM Director. This MIB file also is contained in the IBM Director MIB file package that you can download from [www.ibm.com/servers/eserver/xseries/systems/\\_management/ibm\\_director/](http://www.ibm.com/servers/eserver/xseries/systems/_management/ibm_director/).

## Details

If you select the **ibmSystemMIB** check box in the Event Filter Builder tree, the event filter will process all of the events that are specified in the **ibmSystemMIB** subtree. You can choose to select specific event types that are displayed under the **ibmSystemMIB** node in the Event Filter Builder tree. The event filter will process only the events that you select.

## ibmSystemTrapChassis

The **ibmSystemTrapChassis** event occurs when the state of a system chassis (enclosure) changes, such as when the cover is removed from the system.

## Resolution

- If the severity is Critical: Make sure that the chassis cover is closed.
- If the severity is Normal: The error has been resolved. This event is informative only.

## Details

Event type	Event text	Severity
ibmSystemTrapChassis	System Enclosure Sensor reported intrusion detection.	Critical
ibmSystemTrapChassis	System Enclosure Sensor reports normal.	Normal

## ibmSystemTrapDASDBackplane

The `ibmSystemTrapDASDBackplane` event occurs when the Remote Supervisor Adapter detects that the state of the system hard disk drive changes with respect to its availability.

## Resolution

Replace the specified hard disk drive that has failed. If necessary, restore your data from a backup.

**Note:** After correcting the hardware error, you must clear this event manually.

## Details

Event type	Event text	Severity
ibmSystemTrapDASDBackplane	Drive <i>drive</i> has reported a fault. This event must be cleared manually. where <i>drive</i> is the affected hard disk drive.	Critical

## ibmSystemTrapErrorLog

The `ibmSystemTrapErrorLog` event occurs when the Remote Supervisor Adapter detects that its error log is at 75% or 100% of its capacity.

## Resolution

If the severity is Warning: Back up and clear the system-management processor event log.

**Note:** After correcting the hardware error, you must clear this event manually.

## Details

Event type	Event text	Severity
ibmSystemTrapErrorLog	The system management processor error log is 75% full. This event must be cleared manually.	Warning
ibmSystemTrapErrorLog	The system management processor error log is full. This event must be cleared manually.	Warning

## ibmSystemTrapFan

The `ibmSystemTrapFan` event occurs when the state of a system fan has changed with respect to the manufacturer-defined RPM values. If a Remote Supervisor Adapter is installed in a system, this event is sent when a fan stops, is removed, or is not performing optimally. If a Remote Supervisor Adapter is not installed, an event is sent when the fan stops or is removed.

## Resolution

- If the severity is Critical: Replace the specified fan that has failed.
- If the severity is Normal: The error has been resolved. This event is informative only.

## Details

Event type	Event text	Severity
ibmSystemTrapFan	Fan Sensor <i>number</i> fell below threshold of <i>threshold</i> RPM. The current value is <i>speed</i> RPM. where: <ul style="list-style-type: none"><li>• <i>number</i> is the affected fan sensor.</li><li>• <i>threshold</i> is the critical fan threshold value.</li><li>• <i>speed</i> is the current fan speed.</li></ul> <b>Note:</b> This event must be cleared manually.	Critical
ibmSystemTrapFan	Fan Sensor <i>number</i> reports normal. where <i>number</i> is the affected fan sensor.	Normal

### ibmSystemTrapGenericFan

The ibmSystemTrapGenericFan event occurs when the Remote Supervisor Adapter or ASM processor detects that the state of a system fan has changed with respect to its manufacturer-defined RPM thresholds but the precise fan instance cannot be determined.

#### Resolution

Replace the failed fan.

**Note:** After correcting the hardware error, you must clear this event manually.

## Details

Event type	Event text	Severity
ibmSystemTrapGenericFan	Fan Sensor <i>number</i> fell below threshold of <i>threshold</i> RPM. The current value is <i>speed</i> RPM. where: <ul style="list-style-type: none"><li>• <i>number</i> is the affected fan sensor.</li><li>• <i>threshold</i> is the critical fan threshold value.</li><li>• <i>speed</i> is the current fan speed.</li></ul> <b>Note:</b> This event must be cleared manually.	Critical
ibmSystemTrapGenericFan	Fan Sensor <i>number</i> reports normal. where <i>number</i> is the affected fan sensor.	Normal

### ibmSystemTrapGenericVoltage

The ibmSystemTrapGenericVoltage event occurs when the Remote Supervisor Adapter or the ASM processor detects that the state of a system voltage sensor has changed with respect to a manufacturer-defined threshold but the precise voltage sensor cannot be determined.

#### Resolution

Identify the cause of the voltage problem. Make sure that the power supply is working. If necessary, replace the power supply.

**Note:** After correcting the hardware error, you must clear this event manually.

## Details

Event type	Event text	Severity
ibmSystemTrapGenericVoltage	Voltage Sensor <i>number</i> fell below threshold of <i>threshold</i> Volts. The current value is <i>current</i> Volts.  where: <ul style="list-style-type: none"><li>• <i>number</i> is the affected voltage sensor.</li><li>• <i>threshold</i> is the threshold value.</li><li>• <i>current</i> is the current voltage reading.</li></ul>	Critical
ibmSystemTrapGenericVoltage	Voltage Sensor <i>number</i> exceeded threshold of <i>threshold</i> Volts. The current value is <i>current</i> Volts.  where: <ul style="list-style-type: none"><li>• <i>number</i> is the affected voltage sensor.</li><li>• <i>threshold</i> is the threshold value.</li><li>• <i>current</i> is the current voltage reading.</li></ul>	Critical
ibmSystemTrapGenericVoltage	Voltage Sensor <i>number</i> reports normal.  where <i>number</i> is the affected voltage sensor.	Normal

### ibmSystemTrapLeaseExpiration

The `ibmSystemTrapLeaseExpiration` event occurs when the system lease expiration date has been reached with respect to the value configured for the date in the Asset ID task.

#### Resolution

- If the severity is Warning: The lease has expired.
- If the severity is Normal: The error has been resolved. This event is informative only.

#### Details

The date value is provided by the Asset ID task. The Lease page in the Asset ID task includes the **End Date** field where you can set the lease expiration date. The date is stored in the `IBMPSG_Lease.LeaseEndDate` CIM

property that is monitored at regular poll intervals. A CIM indication is generated when the system CIMOM starts and when a state change is detected relative to the internal poll interval. If you have set SNMP trap forwarding, the CIM indication is converted to an SNMP event.

Event type	Event text	Severity
ibmSystemTrapLeaseExpiration	The lease on <i>system</i> has expired. It expired on <i>date</i> . where <i>system</i> is the affected system and <i>date</i> is the lease expiration date.	Warning
ibmSystemTrapLeaseExpiration	The lease on <i>system</i> is normal. It will expire on <i>date</i> . where <i>system</i> is the affected system and <i>date</i> is the lease expiration date.	Normal

## ibmSystemTrapMemoryPF

The `ibmSystemTrapMemoryPF` event occurs when a dual inline memory module (DIMM) in a system changes with respect to its availability.

### Resolution

- If the severity is Critical: Replace the specified DIMM that is failing or has failed.
- If the severity is Normal: The error has been resolved. This event is informative only.

### Details

Event type	Event text	Severity
ibmSystemTrapMemoryPF	Memory device identified as memory in bank <i>slot</i> is predicting an imminent failure. where <i>slot</i> is the affected memory slot.	Critical
ibmSystemTrapMemoryPF	Memory device identified as memory in bank <i>slot</i> is not predicting a failure. where <i>slot</i> is the affected memory slot.	Normal



## ibmSystemTrapNetworkAdapterFailed

The `ibmSystemTrapNetworkAdapterFailed` event occurs when a network interface card (NIC) in a system has failed.

### Resolution

Replace the specified NIC that has failed.

### Details

Event type	Event text	Severity
<code>ibmSystemTrapNetworkAdapterFailed</code>	The network adapter failed.	Critical

This IBM Director SNMP event type uses the following set of variables:

- `OID`
- `Identifier`
- `SourceObjectPath`
- `TargetObjectPath`
- `Severity`
- `Description`
- `TimeStamp`
- `Component`

For the values that are bound to these variables for this event type, see the `IBM-SYSTEM-TRAP-MIB.mib` file in the `c:/Director/proddata/snmp` directory, where `c` is the hard disk drive and `Director` is the directory where you installed IBM Director. This MIB file also is contained in the IBM Director MIB file package that you can download from [www.ibm.com/servers/eserver/xseries/systems\\_management/ibm\\_director/](http://www.ibm.com/servers/eserver/xseries/systems_management/ibm_director/).

## ibmSystemTrapNetworkAdapterOffline

The `ibmSystemTrapNetworkAdapterOffline` event occurs when a network interface card (NIC) in a system goes offline.

### Resolution

Check the network connection.

### Details

Event type	Event text	Severity
<code>ibmSystemTrapNetworkAdapterOffline</code>	The network adapter is offline.	Warning

This IBM Director SNMP event type uses the following set of variables:

- OID
- Identifier
- SourceObjectPath
- TargetObjectPath
- Severity
- Description
- TimeStamp
- Component

For the values that are bound to these variables for this event type, see the `IBM-SYSTEM-TRAP-MIB.mib` file in the `c:/Director/proddata/snmp` directory, where `c` is the hard disk drive and `Director` is the directory where you installed IBM Director. This MIB file also is contained in the IBM Director MIB file package that you can download from [www.ibm.com/servers/eserver/xseries/systems\\_management/ibm\\_director/](http://www.ibm.com/servers/eserver/xseries/systems_management/ibm_director/).

## ibmSystemTrapNetworkAdapterOnline

The `ibmSystemTrapNetworkAdapterOnline` event occurs when the state of a system network interface card (NIC) changes from offline to online.

## Resolution

The error has been resolved. This event is informative only.

## Details

Event type	Event text	Severity
ibmSystemTrapNetworkAdapterOnline	The network adapter is online.	Normal

This IBM Director SNMP event type uses the following set of variables:

- OID
- Identifier
- SourceObjectPath
- TargetObjectPath
- Severity
- Description
- TimeStamp
- Component

For the values that are bound to these variables for this event type, see the IBM-SYSTEM-TRAP-MIB.mib file in the *c:/Director/proddata/snmp* directory, where *c* is the hard disk drive and *Director* is the directory where you installed IBM Director. This MIB file also is contained in the IBM Director MIB file package that you can download from [www.ibm.com/servers/eserver/xseries/systems\\_management/ibm\\_director/](http://www.ibm.com/servers/eserver/xseries/systems_management/ibm_director/).

## ibmSystemTrapPFA

The `ibmSystemTrapPFA` event occurs when the Remote Supervisor Adapter detects that a component in a system is about to fail.

## Resolution

Identify and replace the component that is generating the Predictive Failure Analysis event.

**Note:** After correcting the hardware error, you must clear this event manually.

## Details

Event type	Event text	Severity
ibmSystemTrapPFA	Predictive Failure Detected. Please check the system management processor error log for more information. This event must be cleared manually.	Critical

## ibmSystemTrapPowerSupply

The `ibmSystemTrapPowerSupply` event occurs when the state of a system power supply changes with respect to its availability.

## Resolution

- If the severity is Critical or Warning: Check the power supply and line cord. Replace the power supply if required.
- If the severity is Normal: The error has been resolved. This event is informative only.

## Details

Event type	Event text	Severity
ibmSystemTrapPowerSupply	PowerSupply device identified as PowerSupply <i>number</i> reports critical state with possible loss of redundancy. where <i>number</i> is the affected power supply.	Critical
ibmSystemTrapPowerSupply	PowerSupply device identified as PowerSupply <i>number</i> has failed. This event must be cleared manually. where <i>number</i> is the affected power supply.	Critical

Event type	Event text	Severity
ibmSystemTrapPowerSupply	PowerSupply device identified as PowerSupply <i>number</i> has lost AC power and loss of standby power is imminent. where <i>number</i> is the affected power supply.	Warning
ibmSystemTrapPowerSupply	PowerSupply device identified as PowerSupply <i>number</i> reports normal. where <i>number</i> is the affected power supply.	Normal

## ibmSystemTrapProcessorPF

The ibmSystemTrapProcessorPF event occurs when the state of a system processor changes with respect to its availability.

### Resolution

- If the severity is Critical: Replace the specified processor that is failing or has failed.
- If the severity is Normal: The error has been resolved. This event is informative only.

### Details

Event type	Event text	Severity
ibmSystemTrapProcessorPF	Processor device identified as processor in slot <i>slot</i> is predicting an imminent failure. where <i>slot</i> is the affected processor slot.	Critical
ibmSystemTrapProcessorPF	Processor device identified as processor in slot <i>slot</i> is not predicting a failure. where <i>slot</i> is the affected processor slot.	Normal

## ibmSystemTrapRedundantNIC

The `ibmSystemTrapRedundantNIC` event occurs when the state of a system network interface card (NIC) changes with respect to its redundancy. There are certain limitations of the NIC that cannot be compensated for between a switchover and a switchback.

### Resolution

Check the network connection.

### Details

Event type	Event text	Severity
<code>ibmSystemTrapRedundantNIC</code>	A network interface card (NIC) failover has occurred. This requires a teamed configuration.	Warning

## ibmSystemTrapRedundantNICSwitchback

The `ibmSystemTrapRedundantNICSwitchback` event occurs when the primary network interface card (NIC) is restored in a teamed NIC configuration.

### Resolution

The error has been resolved. This event is informative only.

### Details

Event type	Event text	Severity
<code>ibmSystemTrapRedundantNICSwitchback</code>	Onboard NIC has Switched Back	Warning
<code>ibmSystemTrapRedundantNICSwitchback</code>	NIC in PCI Bus <i>bus</i> Slot <i>slot</i> has Switched Back where <i>bus</i> is the affected bus and <i>slot</i> is the affected slot.	Warning

Event type	Event text	Severity
ibmSystemTrapRedundantNICSwitchback	NIC in PCI Slot <i>slot</i> has Switched Back where <i>slot</i> is the affected slot.	Warning
ibmSystemTrapRedundantNICSwitchback	NIC has Switched Back	Warning

## ibmSystemTrapRedundantNICSwitchover

The ibmSystemTrapRedundantNICSwitchover event occurs when the primary network interface card (NIC) fails in a teamed NIC configuration and the standby NIC becomes the active NIC.

### Resolution

Check the network connection.

### Details

Event type	Event text	Severity
ibmSystemTrapRedundantNICSwitchover	Onboard NIC has Switched Over	Warning
ibmSystemTrapRedundantNICSwitchover	NIC in PCI Bus <i>bus</i> Slot <i>slot</i> has Switched Over where <i>bus</i> is the affected bus and <i>slot</i> is the affected slot.	Warning
ibmSystemTrapRedundantNICSwitchover	NIC in PCI Slot <i>slot</i> has Switched Over where <i>slot</i> is the affected slot.	Warning
ibmSystemTrapRedundantNICSwitchover	NIC has Switched Over	Warning

## ibmSystemTrapRemotelogin

The ibmSystemTrapRemotelogin event occurs when an end-user or application has logged in to the Web interface of the Remote Supervisor Adapter.

## Resolution

No resolution. This event is informative only.

**Note:** After correcting the hardware error, you must clear this event manually.

## Details

Event type	Event text	Severity
ibmSystemTrapRemotelogin	The system management processor has been accessed via a remote login. This event must be cleared manually.	Warning

## ibmSystemTrapsSMART

The `ibmSystemTrapsSMART` event occurs when the state of an IDE or SCSI hard disk drive that complies with the self-monitoring, analysis, and reporting technology (SMART) changes with respect to its availability.

## Resolution

- If the severity is Critical: Replace the specified hard disk drive that is failing or has failed.
- If the severity is Normal: The error has been resolved. This event is informative only.

## Details

Event type	Event text	Severity
ibmSystemTrapsSMART	<i>Device</i> device identified as physical drive <i>drive</i> is predicting an imminent failure. where <i>Device</i> is IDE, SCSI, or Unknown and <i>drive</i> is the affected SMART drive.	Critical
ibmSystemTrapsSMART	<i>Device</i> device identified as physical drive <i>drive</i> is not predicting a failure. where <i>Device</i> is IDE, SCSI, or Unknown and <i>drive</i> is the affected SMART drive.	Normal



## ibmSystemTrapSPPowerSupply

The `ibmSystemTrapSPPowerSupply` event occurs when the Advanced Systems Management processor (ASM processor) detects that the state of the system power supply changes with respect to its availability. This is sent from servers that do not have a power backplane and do not support a recovery severity or alert type.

### Resolution

- If the severity is Critical or Warning: Check the power supply and line cord. Replace the power supply if required.
- If the severity is Normal: The error has been resolved. This event is informative only.

**Note:** After correcting the hardware error, you must clear this event manually.

### Details

Event type	Event text	Severity
<code>ibmSystemTrapSPPowerSupply</code>	PowerSupply device identified as PowerSupply <i>number</i> reports critical state with possible loss of redundancy. where <i>number</i> is the affected power supply.	Critical
<code>ibmSystemTrapSPPowerSupply</code>	PowerSupply device identified as PowerSupply <i>number</i> has failed. This event must be cleared manually. where <i>number</i> is the affected power supply.	Critical
<code>ibmSystemTrapSPPowerSupply</code>	PowerSupply device identified as PowerSupply <i>number</i> has lost AC power and loss of standby power is imminent. where <i>number</i> is the affected power supply.	Warning
<code>ibmSystemTrapSPPowerSupply</code>	PowerSupply device identified as PowerSupply <i>number</i> reports normal. where <i>number</i> is the affected power supply.	Normal

## ibmSystemTrapStorage

The `ibmSystemTrapStorage` event occurs when the state of system hard disk drive space changes with respect to user-defined levels of hard disk drive space remaining. By default, the warning level is 5% remaining and critical level is 3% remaining.

### Resolution

- If the severity is Critical or Warning: Remove files from the specified hard disk or lower the minimum threshold.
- If the severity is Normal: The error has been resolved. This event is informative only.

### Details

Event type	Event text	Severity
<code>ibmSystemTrapStorage</code>	Logical drive <i>name</i> fell below threshold of <i>threshold</i> MB. The current value is <i>value</i> MB.  where: <ul style="list-style-type: none"><li>• <i>name</i> is the affected logical drive.</li><li>• <i>threshold</i> is the critical threshold value.</li><li>• <i>value</i> is the amount of current disk space available.</li></ul>	Critical
<code>ibmSystemTrapStorage</code>	Logical drive <i>name</i> fell below threshold of <i>threshold</i> MB. The current value is <i>value</i> MB.  where: <ul style="list-style-type: none"><li>• <i>name</i> is the affected logical drive.</li><li>• <i>threshold</i> is the warning threshold value.</li><li>• <i>value</i> is the amount of current disk space available.</li></ul>	Warning
<code>ibmSystemTrapStorage</code>	Logical drive <i>name</i> free space is normal. The current value is <i>value</i> MB.  where <i>name</i> is the affected logical drive and <i>value</i> is the amount of current disk space available.	Normal

Event type	Event text	Severity
ibmSystemTrapStorage	Logical drive <i>name</i> status could not be determined. where <i>name</i> is the affected logical drive.	Unknown

## ibmSystemTrapTemperature

The `ibmSystemTrapTemperature` event occurs when the state of a system temperature sensor changes with respect to a manufacturer-defined or user-defined threshold.

### Resolution

- If the severity is Critical or Warning: Identify the cause of the temperature increase. If necessary, increase the cooling capacity.
- If the severity is Normal: The error has been resolved. This event is informative only.

### Details

Event type	Event text	Severity
ibmSystemTrapTemperature	Temperature Sensor <i>number</i> exceeded the manufacturer defined threshold of <i>threshold</i> Celsius. The current value is <i>current</i> Celsius. where: <ul style="list-style-type: none"> <li>• <i>number</i> is the affected temperature sensor.</li> <li>• <i>threshold</i> is the manufacturer-defined threshold value.</li> <li>• <i>current</i> is the current temperature reading.</li> </ul>	Critical
ibmSystemTrapTemperature	Temperature Sensor <i>number</i> exceeded the user defined threshold of <i>threshold</i> Celsius. The current value is <i>current</i> Celsius. where: <ul style="list-style-type: none"> <li>• <i>number</i> is the affected temperature sensor.</li> <li>• <i>threshold</i> is the user-defined threshold value.</li> <li>• <i>current</i> is the current temperature reading.</li> </ul>	Critical

Event type	Event text	Severity
ibmSystemTrapTemperature	Temperature Sensor <i>number</i> exceeded the manufacturer defined threshold of <i>threshold</i> Celsius. The current value is <i>current</i> Celsius.  where: <ul style="list-style-type: none"> <li><i>number</i> is the affected temperature sensor.</li> <li><i>threshold</i> is the manufacturer-defined threshold value.</li> <li><i>current</i> is the current temperature reading.</li> </ul>	Warning
ibmSystemTrapTemperature	Temperature Sensor <i>number</i> exceeded the user defined threshold of <i>threshold</i> Celsius. The current value is <i>current</i> Celsius.  where: <ul style="list-style-type: none"> <li><i>number</i> is the affected temperature sensor.</li> <li><i>threshold</i> is the user-defined threshold value.</li> <li><i>current</i> is the current temperature reading.</li> </ul>	Warning
ibmSystemTrapTemperature	Temperature Sensor <i>number</i> reports normal. where <i>number</i> is the affected temperature sensor.	Normal

## ibmSystemTrapVoltage

The ibmSystemTrapVoltage event occurs when the state of a system voltage sensor changes with respect to a manufacturer-defined threshold.

### Resolution

- If the severity is Critical: Identify the cause of the voltage problem. Make sure that the power supply is working. If necessary, replace the power supply.
- If the severity is Normal: The error has been resolved. This event is informative only.

## Details

Event type	Event text	Severity
ibmSystemTrapVoltage	Voltage Sensor <i>number</i> fell below threshold of <i>threshold</i> Volts. The current value is <i>current</i> Volts.  where: <ul style="list-style-type: none"><li>• <i>number</i> is the affected voltage sensor.</li><li>• <i>threshold</i> is the threshold value.</li><li>• <i>current</i> is the current voltage reading.</li></ul>	Critical
ibmSystemTrapVoltage	Voltage Sensor <i>number</i> exceeded threshold of <i>threshold</i> Volts. The current value is <i>current</i> Volts.  where: <ul style="list-style-type: none"><li>• <i>number</i> is the affected voltage sensor.</li><li>• <i>threshold</i> is the threshold value.</li><li>• <i>current</i> is the current voltage reading.</li></ul>	Critical
ibmSystemTrapVoltage	Voltage Sensor <i>number</i> reports normal.  where <i>number</i> is the affected voltage sensor.	Normal

## ibmSystemTrapWarrantyExpiration

The ibmSystemTrapWarrantyExpiration event occurs when the system warranty expiration date has been reached with respect to the value configured for the date while using the Asset ID task.

### Resolution

- If the severity is Warning: The warranty has expired.
- If the severity is Normal: The error has been resolved. This event is informative only.

---

## ibmServerRAIDMIB

The ibmServerRAIDMIB events provide information about ServeRAID subcomponent failures and the status of ServeRAID operations such as synchronization, logical-drive migration, rebuild, compaction, compression, expansion, verify, and more. For detailed events, expand the **ibmServerRAIDMIB** node in the Event Filter Builder tree.

### Event source

ibmServerRAIDMIB events are generated by Level-2 managed systems that include ServeRAID controllers or integrated SCSI controllers with RAID capabilities. In addition to IBM Director Agent, these systems must have the managed-system agent for the ServeRAID Manager extension installed.

**Note:** These events are not generated by the ServeRAID Manager (Standalone Edition).

ibmServerRAIDMIB event types are generated by IBM Director Agent. IBM Director uses CIM indications to communicate hardware information. If you have configured your IBM Director environment to use SNMP traps, IBM Director converts the CIM indications into the ibmServerRAIDMIB SNMP traps. For information about configuring your IBM Director environment to use SNMP traps, see “Configuring SNMP trap forwarding.”

To support SNMP, the IBM Director Agent includes a CIM client that is called the IBM Director Agent SNMP agent. It translates the CIM-indication data into SNMP format and exports the SNMP data to SNMP clients, such as HP OpenView and Tivoli NetView Upward Integration Modules (UIMs). When you configure your IBM Director environment to use SNMP traps, the IBM Director Agent SNMP agent is registered with the operating system and any queries involving the IBM Director Agent enterprise OID are forwarded to the IBM Director Agent SNMP agent for processing.

When an SNMP client sends a Get request, the IBM Director Agent SNMP agent receives the request and queries the CIM server on the target managed system. Then, the CIM server performs the following steps:

1. Translates the SNMP request to a CIM client request
2. Converts the SNMP variable that is the subject of the request to a CIM instance and property
3. Translates the CIM response to an SNMP response

4. Returns the response to the SNMP client

While the IBM Director Agent SNMP agent is installed and registered, it creates and forwards SNMP traps to any configured alert destinations. and you cannot stop the forwarding of the SNMP traps. Unwanted SNMP traps must be filtered out by the listening event server.

### **Event Filter Builder tree path**

The full path for this event type in the Event Filter Builder tree is:

```
SNMP > iso > org > dod > internet > private > enterprises > ibm > ibmProd > ibmServerRAID > ibmServerRAIDMIB
```

### **Details**

If you select the **ibmServerRAIDMIB** check box in the Event Filter Builder tree, the event filter will process all of the events that are specified in the **ibmServerRAIDMib** subtree. You can choose to select specific event types that are displayed under the **ibmServerRAIDMIB** node in the Event Filter Builder tree. The event filter will process only the events that you select.

The MIB file for the **ibmServerRAIDMIB** event types, **IBM-SERVERRAID-MIB.mib**, is in the *c:/Director/proddata/snmp* directory, where *c* is the hard disk drive and *Director* is the directory where you installed IBM Director. This MIB file also is contained in the IBM Director MIB file package that you can download from [www.ibm.com/servers/eserver/xseries/systems\\_management/ibm\\_director/](http://www.ibm.com/servers/eserver/xseries/systems_management/ibm_director/).

### **ibmServerRAIDArrayFlashCopyComplete**

The **ibmServerRAIDArrayFlashCopyComplete** event occurs when a ServerRAID FlashCopy operation is completed on a specified array in a ServerRAID configuration.

### **Resolution**

No resolution. This event is informative only.

## Details

Event type	Event text	Severity
iBMServerRAIDArrayFlashCopyComplete	FlashCopy with backup complete: <i>array</i> . where <i>array</i> is the affected array.	Harmless

This event type uses the following variables:

- OID
- ArrayID
- AdapterID

### **iBMServerRAIDArrayFlashCopyDetected**

The iBMServerRAIDArrayFlashCopyDetected event occurs when a ServerRAID FlashCopy operation is in progress on a specified array in a ServerRAID configuration.

### **Resolution**

No resolution. This event is informative only.

### **Details**

Event type	Event text	Severity
iBMServerRAIDArrayFlashCopyDetected	FlashCopy in progress: <i>array</i> . where <i>array</i> is the affected array.	Harmless

This event type uses the following variables:

- OID
- ArrayID
- AdapterID



## iBMServeRAIDArrayFlashCopyFail

The iBMServeRAIDArrayFlashCopyFail event occurs when a ServeRAID FlashCopy operation fails on a specified array in a ServeRAID configuration.

### Resolution

The FlashCopy operation failed because a hardware error occurred. The specified logical drive might be offline.

If the source logical drive is offline, replace the failed hard disk drives and restore the data from tape backup. If the target logical drive is offline, replace the failed hard disk drives. FlashCopy operations will not work when the source or target logical drives are offline.

If the source or target logical drives are not offline, complete the following steps:

1. Verify that the controller, cables, and hard disk drives are installed correctly.
2. Verify that there is power to the hard disk drives.
3. Retry the command.
4. If the command still fails, restart the server and retry the command.
5. If the problem persists, contact your service representative.

### Details

Event type	Event text	Severity
iBMServeRAIDArrayFlashCopyFail	FlashCopy with backup failed: <i>array [error]</i> where <i>array</i> is the affected array and <i>error</i> is the error code.	Critical

This event type uses the following variables:

- OID
- ArrayID
- AdapterID
- ErrorCode

## iBMServerRAIDArrayRebuildComplete

The iBMServerRAIDArrayRebuildComplete event occurs when a ServerRAID rebuild operation is completed on a specified array in a ServerRAID configuration.

### Resolution

No resolution. This event is informative only.

### Details

Event type	Event text	Severity
iBMServerRAIDArrayRebuildComplete	Rebuild complete: <i>array</i> . where <i>array</i> is the affected array.	Harmless

This event type uses the following variables:

- OID
- ArrayID
- AdapterID

## iBMServerRAIDArrayRebuildDetected

The iBMServerRAIDArrayRebuildDetected event occurs when a ServerRAID rebuild operation is in progress on a specified array in a ServerRAID configuration.

### Resolution

No resolution. This event is informative only.

## Details

Event type	Event text	Severity
iBMServeRAIDArrayRebuildDetected	Rebuilding: <i>array</i> . where <i>array</i> is the affected array.	Harmless

This event type uses the following variables:

- OID
- ArrayID
- AdapterID

## iBMServeRAIDArrayRebuildFail

The iBMServeRAIDArrayRebuildFail event occurs when a ServeRAID rebuild operation fails on a specified array in a ServeRAID configuration.

### Resolution

A hardware error occurred. To correct the error, complete the following steps:

1. Verify that the controller, cables, and hard disk drives are installed correctly.
2. Verify that there is power to the hard disk drives.
3. Retry the command.
4. If the command still fails, restart the server and retry the command.
5. If the problem persists, contact your service representative.

### Details

Event type	Event text	Severity
iBMServeRAIDArrayRebuildFail	Rebuild failed: <i>array</i> [ <i>error</i> ] where <i>array</i> is the affected array and <i>error</i> is the error code.	Critical

This event type uses the following variables:

- OID
- ArrayID
- AdapterID
- ErrorCode

## ibmServerRAIDArraySyncComplete

The ibmServerRAIDArraySyncComplete event occurs when a ServeRAID synchronization operation is completed on a specified array in a ServeRAID configuration.

### Resolution

No resolution. This event is informative only.

### Details

Event type	Event text	Severity
ibmServerRAIDArraySyncComplete	Synchronize complete: <i>array</i> . where <i>array</i> is the affected array.	Harmless

This event type uses the following variables:

- OID
- ArrayID
- AdapterID

## ibmServerRAIDArraySyncDetected

The ibmServerRAIDArraySyncDetected event occurs when a ServeRAID synchronization operation is in progress on a specified array in a ServeRAID configuration.

## Resolution

No resolution. This event is informative only.

## Details

Event type	Event text	Severity
iBMServerRAIDArraySyncDetected	Synchronizing: <i>array</i> . where <i>array</i> is the affected array.	Harmless

This event type uses the following variables:

- OID
- ArrayID
- AdapterID

## iBMServerRAIDArraySyncFail

The iBMServerRAIDArraySyncFail event occurs when a ServeRAID synchronization operation fails on a specified array in a ServeRAID configuration.

## Resolution

A hardware error occurred. Verify that the specified logical drive is not offline or critical (that is, one hard disk drive that is offline in a RAID level-1, 1E, 5, 5E, 10, 1E0, or 50 logical drive). If the logical drive is critical, replace the failed hard disk drive. If the logical drive is offline, replace the failed hard disk drives and restore the data from tape backup.

If the source or target logical drives are *not* offline or critical, complete the following steps:

1. Verify that the controller, cables, and hard disk drives are installed correctly.
2. Verify that there is power to the hard disk drives.
3. Retry the command.
4. If the command still fails, restart the server and retry the command.

5. If the problem persists, contact your service representative.

## Details

Event type	Event text	Severity
ibmServerRAIDArraySyncFail	Synchronize failed: <i>array</i> [ <i>error</i> ] where <i>array</i> is the affected array and <i>error</i> is the error code.	Critical

This event type uses the following variables:

- OID
- ArrayID
- AdapterID
- ErrorCode

## ibmServerRAIDCompactionComplete

The `ibmServerRAIDCompactionComplete` event occurs when a ServeRAID compaction operation is completed on a specified logical drive in a ServeRAID configuration.

## Resolution

No resolution. This event is informative only.

## Details

Event type	Event text	Severity
ibmServerRAIDCompactionComplete	Compaction complete: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Harmless

This event type uses the following variables:

- OID

- ServerName
- LogicalDriveID
- AdapterID

## IBMServerRAIDCompactionDetected

The IBMServerRAIDCompactionDetected event occurs when a ServerRAID compaction operation is in progress on a specified logical drive in a ServerRAID configuration.

### Resolution

No resolution. This event is informative only.

### Details

Event type	Event text	Severity
IBMServerRAIDCompactionDetected	Compacting: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Harmless

This event type uses the following variables:

- OID
- ServerName
- LogicalDriveID
- AdapterID

## IBMServerRAIDCompactionFail

The IBMServerRAIDCompactionFail event occurs when a ServerRAID compaction operation fails on a specified logical drive in a ServerRAID configuration.

## Resolution

A hardware error occurred. Determine if one or more hard disk drives that are part of the specified logical drive have failed. If such a failure has occurred, restore the data from a tape backup. Otherwise, complete the following steps:

1. Verify that the controller, cables, and hard disk drives are installed correctly.
2. Verify that there is power to the hard disk drives.
3. Retry the command.
4. If the command still fails, restart the server and retry the command.

## Details

Event type	Event text	Severity
iBMServerRAIDCompactionFail	Compaction failed: <i>drive [error]</i> where <i>drive</i> is the affected logical drive and <i>error</i> is the error code.	Critical

This event type uses the following variables:

- OID
- ServerName
- LogicalDriveID
- AdapterID
- ErrorCode

## iBMServerRAIDCompressionComplete

The iBMServerRAIDCompressionComplete event occurs when a ServeRAID compression operation is completed on a specified logical drive in a ServeRAID configuration.



## Resolution

No resolution. This event is informative only.

## Details

Event type	Event text	Severity
iBMServerRAIDCompressionComplete	Compression complete: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Harmless

This event type uses the following variables:

- OID
- ServerName
- LogicalDriveID
- AdapterID

## iBMServerRAIDCompressionDetected

The iBMServerRAIDCompressionDetected event occurs when a ServerRAID compression operation is in progress on a specified logical drive in a ServerRAID configuration.

## Resolution

No resolution. This event is informative only.

## Details

Event type	Event text	Severity
iBMServerRAIDCompressionDetected	Compressing: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Harmless

This event type uses the following variables:

- OID
- ServerName
- LogicalDriveID
- AdapterID

## IBMServerRAIDCompressionFail

The IBMServerRAIDCompressionFail event occurs when a ServerRAID compression operation fails on a specified logical drive in a ServerRAID configuration.

### Resolution

A hardware error occurred. Determine if one or more hard disk drives that are part of the specified logical drive have failed. If such a failure has occurred, restore the data from a tape backup. Otherwise, complete the following steps:

1. Verify that the controller, cables, and hard disk drives are installed correctly.
2. Verify that there is power to the hard disk drives.
3. Retry the command.
4. If the command still fails, restart the server and retry the command.

### Details

Event type	Event text	Severity
IBMServerRAIDCompressionFail	Compression failed: <i>drive [error]</i> . where <i>drive</i> is the affected logical drive and <i>error</i> is the error code.	Critical

This event type uses the following variables:

- OID

- ServerName
- LogicalDriveID
- AdapterID
- ErrorCode

## IBMServerRAIDConfigFail

The IBMServerRAIDConfigFail event occurs when a ServeRAID controller configuration cannot be read.

### Resolution

A hardware error occurred. To correct the problem, complete the following steps:

1. Verify that the controller, cables, and hard disk drives are installed correctly.
2. Verify that there is power to the hard disk drives.
3. Retry the command.
4. If the command still fails, restart the server and retry the command.
5. If the problem persists, complete the following steps:
  - a. Restore to factory-default settings.
  - b. Recreate the configuration.

### Details

Event type	Event text	Severity
IBMServerRAIDConfigFail	Error getting controller configuration.	Critical

This event type uses the following variables:

- OID
- ServerName

## IBMServerRAIDControllerAdded

The IBMServerRAIDControllerAdded event occurs when a specified ServeRAID controller is added to a system.

## Resolution

No resolution. This event is informative only.

## Details

Event type	Event text	Severity
iBMServerRAIDControllerAdded	A controller has been added to the system: <i>controller</i> where <i>controller</i> is the added controller.	Harmless

This event type uses the following variables:

- `OID`
- `ServerName`
- `AdapterID`

## iBMServerRAIDControllerBadStripes

The iBMServerRAIDControllerBadStripes event occurs when one or more logical drives contain at least one bad stripe.

## Resolution

The Bad Stripe Table (BST) provides a means of recovering most data on a logical drive after multiple hardware errors prevent access to a logical drive stripe. An entry in the BST indicates that the data contained in a stripe has been lost.

While many conditions can produce a Bad Stripe Table entry, the most common cause is an error accessing one of the stripe units within a stripe of a critical logical drive. A single stripe unit failure is correctable and recoverable but two or more failures within the same redundant RAID stripe are not.

For example, in a critical RAID-5 array, in which one of the drives in the array is defunct, a stripe will be marked bad with an entry in the BST if a non-recoverable media error occurs when accessing one of the other drives of the array.

After an entry is logged in the BST, the controller will return an error code to the driver whenever the host system tries to access a Logical Block Address (LBA) within the affected stripe. This is one immediate indication that some part of the logical drive is unusable.

**Note:** It is not possible to correlate the bad stripe with a specific file in the operating system.

To resolve this error, complete the following steps:

- Check the ServeRAID Manager event logs to identify the affected logical drive(s).
- Because the data has been lost, the only way to recover from this condition is to complete the following steps:
  1. Delete the array.
  2. Recreate the array and its logical drives.
  3. Restore the data from backup media.

**Note:** The alternative is to take the entire logical drive offline, thus resulting in the loss of all data contained on that logical drive.

To minimize the risk of lost data, be sure to schedule frequent periodic backups.

## Details

**Note:** This event is new in IBM Director 4.20.

Event type	Event text	Severity
ibmServerRAIDControllerBadStripes	One or more logical drives contain a bad stripe: <i>controller</i> where <i>controller</i> is the controller for the affected logical drives.	Warning

This event type uses the following variables:

- OID
- ServerName
- AdapterID

## IBMServerRAIDControllerBatteryOvertemp

The IBMServerRAIDControllerBatteryOvertemp event occurs when the battery on a specified ServeRAID controller has exceeded its temperature threshold.

### Resolution

Battery temperature has exceeded 50 degrees Celsius. To resolve this error, complete the following steps:

1. Verify that the controller is installed properly.
2. Verify that the server has adequate ventilation.
3. If the problem persists, the battery might have failed or the server might require service. Contact your service representative.

### Details

Event type	Event text	Severity
IBMServerRAIDControllerBatteryOvertemp	The battery has exceeded normal operating temperature: <i>controller</i> where <i>controller</i> is the affected controller.	Warning

This event type uses the following variables:

- OID
- ServerName
- AdapterID

## IBMServerRAIDControllerBatteryTempNormal

The IBMServerRAIDControllerBatteryTempNormal event occurs when the battery on a specified ServeRAID controller has a normal temperature.

### Resolution

No resolution. This event is informative only.

## Details

**Note:** This event is new in IBM Director 4.20.

Event type	Event text	Severity
iBMServerRAIDControllerBatteryTempNormal	The battery operating temperature is normal: <i>controller</i> where <i>controller</i> is the affected controller.	Harmless

This event type uses the following variables:

- OID
- ServerName
- AdapterID

## iBMServerRAIDControllerFail

The iBMServerRAIDControllerFail event occurs when a specified ServeRAID controller fails.

### Resolution

A hardware error occurred. To correct the problem, complete the following steps:

1. Verify that the controller, cables, and hard disk drives are installed correctly.
2. Verify that there is power to the hard disk drives.
3. Retry the command.
4. If the command still fails, restart the server and retry the command.
5. If the problem persists, contact your service representative.

### Details

Event type	Event text	Severity
iBMServerRAIDControllerFail	Commands are not responding: <i>controller</i> where <i>controller</i> is the affected controller.	Critical

This event type uses the following variables:

- OID
- ServerName
- AdapterID

## **iBMServerRAIDControllerFailover**

The iBMServerRAIDControllerFailover event occurs when a specified ServerRAID controller fails over and the passive controller in the failover pairing is now active.

### **Resolution**

No resolution. This event is informative only.

### **Details**

Event type	Event text	Severity
iBMServerRAIDControllerFailover	A controller failover was detected: <i>controller</i> where <i>controller</i> is the controller that failed.	Critical

This event type uses the following variables:

- OID
- ServerName
- AdapterID

## **iBMServerRAIDControllerReplaced**

The iBMServerRAIDControllerReplaced event occurs when a specified controller is replaced in a ServerRAID configuration.



## Resolution

No resolution. This event is informative only.

## Details

Event type	Event text	Severity
iBMServerRAIDControllerReplaced	A controller has been replaced in the system: <i>controller</i> where <i>controller</i> is the affected controller.	Harmless

This event type uses the following variables:

- OID
- ServerName
- AdapterID

## iBMServerRAIDCopyBackComplete

The iBMServerRAIDCopyBackComplete event occurs when a copy-back operation is completed on a specified logical drive in a ServerRAID configuration.

## Resolution

No resolution. This event is informative only.

## Details

**Note:** This event is new in IBM Director 4.20.

Event type	Event text	Severity
iBMServerRAIDCopyBackComplete	Copy back complete: <i>location</i> . where <i>location</i> is the affected controller and array.	Harmless

This event type uses the following variables:

- OID
- ServerName
- AdapterID

## **iBMServerRAIDCopyBackDetected**

The iBMServerRAIDCopyBackDetected event occurs when a copy-back operation is in progress on a specified logical drive in a ServerRAID configuration.

### **Resolution**

No resolution. This event is informative only.

### **Details**

**Note:** This event is new in IBM Director 4.20.

<b>Event type</b>	<b>Event text</b>	<b>Severity</b>
iBMServerRAIDCopyBackDetected	Copy back in progress: <i>location</i> . Source: Channel <i>channel</i> , SCSI ID <i>id</i> . Target: Channel <i>channel</i> , SCSI ID <i>id</i> . where <ul style="list-style-type: none"><li>• <i>location</i> is the affected controller and array</li><li>• <i>channel</i> is the specified channel</li><li>• <i>id</i> is the specified SCSI ID</li></ul>	Harmless

This event type uses the following variables:

- OID
- ServerName
- AdapterID

## iBMSeverRAIDCopyBackFail

The iBMSeverRAIDCopyBackFail event occurs when a copy-back operation fails on a specified logical drive in a ServeRAID configuration.

### Resolution

A hardware error occurred. To resolve this error, complete the following steps:

1. Verify that the controller, cables, and hard disk drives are installed correctly.
2. Verify that there is power to the hard disk drives.
3. If the command still fails, restart the server and retry the command.
4. If the problem persists, replace the specified drive.

### Details

**Note:** This event is new in IBM Director 4.20.

Event type	Event text	Severity
iBMSeverRAIDCopyBackFail	Copy back failed: <i>location</i> [error] where <i>location</i> is the affected controller and array and <i>error</i> is the error code.	Critical

This event type uses the following variables:

- OID
- ServerName
- AdapterID
- ErrorCode

## iBMSeverRAIDDeadBattery

The iBMSeverRAIDDeadBattery event occurs when the battery fails on a specified controller.

## Resolution

To resolve this problem, complete the following steps:

1. Verify that the battery on the battery-backup cache device is installed properly.
2. If the problem persists, replace the battery.

## Details

Event type	Event text	Severity
iBMServerRAIDDeadBattery	The battery-backup cache device needs a new battery: <i>controller</i> where <i>controller</i> is the affected controller.	Critical

This event type uses the following variables:

- OID
- ServerName
- AdapterID

## iBMServerRAIDDeadBatteryCache

The iBMServerRAIDDeadBatteryCache event occurs when the battery-backup cache fails on a specified controller.

## Resolution

The battery-backup cache device is installed improperly or is defective. To resolve this error, complete the following steps:

1. Verify that the battery-backup cache device is installed properly.
2. If the battery-backup cache device is installed properly but is defective, contact your service representative.

## Details

Event type	Event text	Severity
iBMServerRAIDDeadBatteryCache	The battery-backup cache device is defective: <i>controller</i> . Error code: <i>error</i>	Critical
	where <i>controller</i> is the affected controller and <i>error</i> is the error code.	

This event type uses the following variables:

- OID
- ServerName
- AdapterID
- ErrorCode

## iBMServerRAIDDecompressionComplete

The iBMServerRAIDDecompressionComplete event occurs when a ServeRAID decompression operation is completed on a specified logical drive in a ServeRAID configuration.

### Resolution

No resolution. This event is informative only.

### Details

Event type	Event text	Severity
iBMServerRAIDDecompressionComplete	Decompression complete: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Harmless

This event type uses the following variables:

- OID
- ServerName

- AdapterID

## ibmServerRAIDDecompressionDetected

The IBMServerRAIDDecompressionComplete event occurs when a ServeRAID decompression operation is in progress on a specified logical drive in a ServeRAID configuration.

### Resolution

No resolution. This event is informative only.

### Details

Event type	Event text	Severity
ibmServerRAIDDecompressionDetected	Decompressing: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Harmless

This event type uses the following variables:

- OID
- ServerName
- LogicalDriveID
- AdapterID

## ibmServerRAIDDecompressionFail

The IBMServerRAIDDecompressionFail event occurs when a ServeRAID decompression operation fails on a specified logical drive in a ServeRAID configuration.

### Resolution

A hardware error occurred. Determine if one or more hard disk drives that are part of the specified logical drive have failed. If such a failure has occurred, restore the data from a tape backup. Otherwise, complete the following steps:

1. Verify that the controller, cables, and hard disk drives are installed correctly.
2. Verify that there is power to the hard disk drives.
3. Retry the command.
4. If the command still fails, restart the server and retry the command.

## Details

Event type	Event text	Severity
IBMSeverRAIDDecompressionFail	Decompression failed: <i>drive [error]</i> where <i>drive</i> is the affected logical drive and <i>error</i> is the error code.	Critical

This event type uses the following variables:

- OID
- LogicalDriveID
- AdapterID
- ErrorCode

## IBMSeverRAIDDefunctDrive

The IBMSeverRAIDDefunctDrive event occurs when a specified hard disk drive fails in a ServeRAID configuration.

### Resolution

A hardware error occurred. To resolve the error, complete one of the following steps:

- If the specified hard disk drive is part of an array, refer to the event pertaining to the logical drives in that array for additional information.
- If the specified hard disk drive is not part of an array, contact your service representative.

## Details

Event type	Event text	Severity
IBMServerRAIDDefunctDrive	Defunct drive: <i>location</i> . where <i>location</i> is the affected controller and port.	Critical

This event type uses the following variables:

- OID
- ServerName
- AdapterID
- ChannelID
- SCSIID

### IBMServerRAIDDefunctDriveFRU

The IBMServerRAIDDefunctDriveFRU event occurs when a specified hard disk drive with the provided field-replaceable unit (FRU) number fails in a ServerRAID configuration.

### Resolution

- A hardware error occurred. To resolve the error, complete one of the following steps:
- If the specified hard disk drive is part of an array, refer to the event pertaining to the logical drives in that array for additional information.
  - If the specified hard disk drive is not part of an array, contact your service representative.

### Details

Event type	Event text	Severity
IBMServerRAIDDefunctDriveFRU	Defunct drive: <i>location</i> (FRU Part # <i>FRU</i> ). where <i>location</i> is the affected controller and port and <i>FRU</i> is the FRU number of the hard disk drive.	Critical



This event type uses the following variables:

- OID
- ServerName
- FRU
- AdapterID
- ChannelID
- SCSIID

## ibmServerRAIDDefunctReplaced

The ibmServerRAIDDefunctReplaced event occurs when a specified defunct hard disk drive has been set to the hot-spare state in a ServeRAID configuration.

### Resolution

No resolution. This event is informative only.

### Details

Event type	Event text	Severity
ibmServerRAIDDefunctReplaced	Defunct drive: <i>location (error)</i> . where <i>location</i> is the affected controller and port and <i>error</i> is the error code.	Harmless

This event type uses the following variables:

- OID
- ServerName
- AdapterID
- ChannelID
- SCSIID

## IBMServerRAIDDriveAdded

The IBMServerRAIDDriveAdded event occurs when a specified hard disk drive is added to a ServerRAID configuration.

### Resolution

No resolution. This event is informative only.

### Details

**Note:** This event is new in IBM Director 4.20.

Event type	Event text	Severity
IBMServerRAIDDriveAdded	Physical drive added: <i>location</i> where <i>location</i> is the affected controller and port.	Harmless

This event type uses the following variables:

- OID
- ServerName
- AdapterID
- ChannelID
- SCSIID

## IBMServerRAIDDriveClearComplete

The IBMServerRAIDDriveClearComplete event occurs when a ServerRAID clear operation is completed on a specified hard disk drive in a ServerRAID configuration.

### Resolution

No resolution. This event is informative only.

## Details

**Note:** This event is new in IBM Director 4.20.

Event type	Event text	Severity
IBMServerRAIDDriveClearComplete	Clear complete: <i>drive</i> . where <i>drive</i> is the affected hard disk drive.	Harmless

This event type uses the following variables:

- OID
- ServerName
- AdapterID
- ChannelID
- SCSIID

## IBMServerRAIDDriveClearDetected

The IBMServerRAIDDriveClearDetected event occurs when a ServeRAID clear operation is in progress on a specified hard disk drive in a ServeRAID configuration.

### Resolution

No resolution. This event is informative only.

### Details

**Note:** This event is new in IBM Director 4.20.

Event type	Event text	Severity
IBMServerRAIDDriveClearDetected	Clearing: <i>drive</i> . where <i>drive</i> is the affected hard disk drive.	Harmless

This event type uses the following variables:

- OID
- ServerName
- AdapterID
- ChannelID
- SCSIID

## IBMServerRAIDDriveClearFail

The IBMServerRAIDDriveClearFail event occurs when a ServerRAID clear operation fails on a specified hard disk drive in a ServerRAID configuration.

### Resolution

A hardware error occurred. To resolve the error, complete the following steps:

1. Verify that the controller, cables, and hard disk drives are installed correctly.
2. Verify that there is power to the hard disk drives.
3. Retry the command.
4. If the command still fails, restart the server and retry the command.
5. If the command still fails, replace the specified drive.
6. If the problem persists, contact your service representative.

### Details

**Note:** This event is new in IBM Director 4.20.

Event type	Event text	Severity
IBMServerRAIDDriveClearFail	Clear failed: <i>drive [error]</i> where <i>drive</i> is the affected hard disk drive and <i>error</i> is the error code.	Critical

This event type uses the following variables:

- OID
- ServerName
- AdapterID
- ChannelID
- SCSIID
- ErrorCode

## IBMServerRAIDDriveRemoved

The IBMServerRAIDDriveRemoved event occurs when a specified hard disk drive is removed from a ServeRAID configuration.

### Resolution

No resolution. This event is informative only.

### Details

**Note:** This event is new in IBM Director 4.20.

Event type	Event text	Severity
IBMServerRAIDDriveRemoved	Physical drive removed: <i>location</i> . where <i>location</i> is the affected controller and port.	Harmless

This event type uses the following variables:

- OID
- ServerName
- AdapterID
- ChannelID
- SCSIID

## IBMServerRAIDDriveVerifyComplete

The IBMServerRAIDDriveVerifyComplete event occurs when a ServeRAID verify operation is completed on a specified hard disk drive in a ServeRAID configuration.

### Resolution

No resolution. This event is informative only.

### Details

**Note:** This event is new in IBM Director 4.20.

Event type	Event text	Severity
IBMServerRAIDDriveVerifyComplete	Verify complete: <i>drive</i> . where <i>drive</i> is the affected hard disk drive.	Harmless

This event type uses the following variables:

- OID
- ServerName
- AdapterID
- ChannelID
- SCSIID

## IBMServerRAIDDriveVerifyDetected

The IBMServerRAIDDriveVerifyDetected event occurs when a ServeRAID verify operation is in progress on a specified hard disk drive in a ServeRAID configuration.

### Resolution

No resolution. This event is informative only.

## Details

**Note:** This event is new in IBM Director 4.20.

Event type	Event text	Severity
IBMServerRAIDDriveVerifyDetected	Verifying: <i>drive</i> . where <i>drive</i> is the affected hard disk drive.	Harmless

This event type uses the following variables:

- OID
- ServerName
- AdapterID
- ChannelID
- SCSIID

### IBMServerRAIDDriveVerifyFail

The IBMServerRAIDDriveVerifyFail event occurs when a ServerRAID verify operation fails on a specified hard disk drive in a ServerRAID configuration.

### Resolution

A hardware error occurred. Verify that the specified logical drive is not offline or critical (that is, one hard disk drive that is offline in a RAID level-1, 1E, 5, 5E, 10, 1E0, or 50 logical drive). If the logical drive is critical, replace the failed hard disk drive. If the logical drive is offline, replace the failed hard disk drives and restore the data from tape backup.

If the source or target logical drives are *not* offline or critical, complete the following steps:

1. Verify that the controller, cables, and hard disk drives are installed correctly.
2. Verify that there is power to the hard disk drives.
3. Retry the command.

4. If the command still fails, restart the server and retry the command.
5. If the problem persists, contact your service representative.

## Details

**Note:** This event is new in IBM Director 4.20.

Event type	Event text	Severity
iBMServerRAIDDriveVerifyFail	Verify failed: <i>drive</i> . where <i>drive</i> is the affected hard disk drive.	Critical

This event type uses the following variables:

- OID
- ServerName
- AdapterID
- ChannelID
- SCSIID
- ErrorCode

## iBMServerRAIDEnclosureFail

The iBMServerRAIDEnclosureFail event occurs when an enclosure has failed on a specified controller and channel in a ServerRAID configuration.

## Resolution

A hardware error occurred. To resolve the error, complete the following steps:

1. Verify that the controller, cables, and hard disk drives are installed correctly.
2. Verify that there is power to the hard disk drives.
3. Retry the command.
4. If the command still fails, restart the server and retry the command.



5. If the problem persists, contact your service representative.

## Details

Event type	Event text	Severity
ibmServerRAIDEnclosureFail	Enclosure device is not responding: <i>location</i> where <i>location</i> is the controller and channel that the affected enclosure is attached to.	Critical

This event type uses the following variables:

- OID
- ServerName
- AdapterID
- ChannelID

## ibmServerRAIDEnclosureFanOK

The `ibmServerRAIDEnclosureFanOK` event occurs when a specified enclosure fan is functioning correctly on a specified controller and channel in a `ServerRAID` configuration.

## Resolution

No resolution. This event is informative only.

## Details

Event type	Event text	Severity
ibmServerRAIDEnclosureFanOK	Enclosure fan <i>fan</i> is now operational: <i>location</i> where <i>fan</i> is the affected fan and <i>location</i> is the controller and channel that the affected enclosure is attached to.	Harmless

This event type uses the following variables:

- OID
- ServerName
- FanID
- AdapterID
- ChannelID

## **iBMServerRAIDEnclosureOK**

The iBMServerRAIDEnclosureOK event occurs when an enclosure is functioning correctly on a specified controller and channel in a ServeRAID configuration.

### **Resolution**

No resolution. This event is informative only.

### **Details**

<b>Event type</b>	<b>Event text</b>	<b>Severity</b>
iBMServerRAIDEnclosureOK	Enclosure device is responding: <i>location</i> where <i>location</i> is the controller and channel that the affected enclosure is attached to.	Harmless

This event type uses the following variables:

- OID
- ServerName
- AdapterID
- ChannelID

## iBMServerRAIDExpansionComplete

The iBMServerRAIDExpansionComplete event occurs when a ServerRAID expansion operation is completed on a specified logical drive in a ServerRAID configuration.

### Resolution

No resolution. This event is informative only.

### Details

Event type	Event text	Severity
iBMServerRAIDExpansionComplete	Expansion complete: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Harmless

This event type uses the following variables:

- OID
- ServerName
- LogicalDriveID
- AdapterID

## iBMServerRAIDExpansionDetected

The iBMServerRAIDExpansionDetected event occurs when a ServerRAID expansion operation is in progress on a specified logical drive in a ServerRAID configuration.

### Resolution

No resolution. This event is informative only.

## Details

Event type	Event text	Severity
iBMServerRAIDExpansionDetected	Expanding: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Harmless

This event type uses the following variables:

- OID
- ServerName
- LogicalDriveID
- AdapterID

### **iBMServerRAIDExpansionFail**

The iBMServerRAIDExpansionFail event occurs when a ServerRAID expansion operation fails on a specified logical drive in a ServerRAID configuration.

### **Resolution**

A hardware error occurred. Determine if one or more hard disk drives that are part of the specified logical drive have failed. If such a failure has occurred, restore the data from a tape backup. Otherwise, complete the following steps:

1. Verify that the controller, cables, and hard disk drives are installed correctly.
2. Verify that there is power to the hard disk drives.
3. Retry the command.
4. If the command still fails, restart the server and retry the command.

## Details

Event type	Event text	Severity
iBMServerRAIDExpansionFail	Expansion failed: <i>drive [error]</i> . where <i>drive</i> is the affected logical drive and <i>error</i> is the error code.	Critical

This event type uses the following variables:

- OID
- ServerName
- LogicalDriveID
- AdapterID
- ErrorCode

### **iBMServerRAIDFanFail**

The iBMServerRAIDFanFail event occurs when a specified enclosure fan fails on a specified controller and channel in a ServerRAID configuration.

### **Resolution**

A hardware error occurred. Verify that the fan in the enclosure device is installed properly. If it is, complete the following steps:

1. Verify that the controller, cables, and hard disk drives are installed correctly.
2. Verify that there is power to the hard disk drives.
3. Retry the command.
4. If the command still fails, restart the server and retry the command.
5. If the problem persists, replace the specified fan.

## Details

Event type	Event text	Severity
iBMServeRAIDFanFail	Enclosure fan <i>fan</i> is malfunctioning: <i>location</i> where <i>fan</i> is the affected fan and <i>location</i> is the controller and channel that the affected enclosure is attached to.	Critical

This event type uses the following variables:

- OID
- ServerName
- FanID
- AdapterID
- ChannelID

### **iBMServeRAIDFanInstalled**

The iBMServeRAIDFanInstalled event occurs when a specified enclosure fan is installed on a specified controller and channel in a ServeRAID configuration.

### **Resolution**

No resolution. This event is informative only.

## Details

Event type	Event text	Severity
iBMServeRAIDFanInstalled	Enclosure fan <i>fan</i> has been installed: <i>location</i> where <i>fan</i> is the affected fan and <i>location</i> is the controller and channel that the affected enclosure is attached to.	Harmless

This event type uses the following variables:

- **OID**
- **ServerName**
- **FanID**
- **AdapterID**
- **ChannelID**

## **iBMServerRAIDFanRemoved**

The iBMServerRAIDFanInstalled event occurs when a specified enclosure fan is removed on a specified controller and channel in a ServeRAID configuration.

### **Resolution**

No resolution. This event is informative only.

### **Details**

<b>Event type</b>	<b>Event text</b>	<b>Severity</b>
iBMServerRAIDFanRemoved	Enclosure fan <i>fan</i> has been removed: <i>location</i> where <i>fan</i> is the affected fan and <i>location</i> is the controller and channel that the affected enclosure is attached to.	Warning

This event type uses the following variables:

- **OID**
- **ServerName**
- **FanID**
- **AdapterID**
- **ChannelID**

## iBMServerRAIDFlashCopyComplete

The iBMServerRAIDFlashCopyComplete event occurs when a ServerRAID FlashCopy operation is completed on a specified logical drive in a ServerRAID configuration.

### Resolution

No resolution. This event is informative only.

### Details

Event type	Event text	Severity
iBMServerRAIDFlashCopyComplete	FlashCopy with backup complete: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Harmless

This event type uses the following variables:

- OID
- LogicalDriveID
- AdapterID

## iBMServerRAIDFlashCopyDetected

The iBMServerRAIDFlashCopyDetected event occurs when a ServerRAID FlashCopy operation is in progress on a specified logical drive in a ServerRAID configuration.

### Resolution

No resolution. This event is informative only.



## Details

Event type	Event text	Severity
iBMServeRAIDFlashCopyDetected	FlashCopy in progress: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Harmless

This event type uses the following variables:

- OID
- LogicalDriveID
- AdapterID

### **iBMServeRAIDFlashCopyFail**

The iBMServeRAIDFlashCopyFail event occurs when a ServeRAID FlashCopy operation fails on a specified logical drive in a ServeRAID configuration.

### **Resolution**

The FlashCopy operation failed because a hardware error occurred. The specified logical drive might be offline. If the source logical drive is offline, replace the failed hard disk drives and restore the data from tape backup. If the target logical drive is offline, replace the failed hard disk drives. FlashCopy operations will not work when the source or target logical drives are offline.

If the source or target logical drives are not offline, complete the following steps:

1. Verify that the controller, cables, and hard disk drives are installed correctly.
2. Verify that there is power to the hard disk drives.
3. Retry the command.
4. If the command still fails, restart the server and retry the command.
5. If the problem persists, contact your service representative.

## Details

Event type	Event text	Severity
iBMServerRAIDFlashCopyFail	FlashCopy with backup failed: <i>drive [error]</i> . where <i>drive</i> is the affected logical drive and <i>error</i> is the error code.	Critical

This event type uses the following variables:

- OID
- LogicalDriveID
- AdapterID
- ErrorCode

### **iBMServerRAIDInitComplete**

The iBMServerRAIDInitComplete event occurs when a ServerRAID initialization operation is completed on a specified logical drive in a ServerRAID configuration.

### **Resolution**

No resolution. This event is informative only.

### **Details**

**Note:** This event is new in IBM Director 4.20.

Event type	Event text	Severity
iBMServerRAIDInitComplete	Clear complete: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Harmless

This event type uses the following variables:

- OID

- ServerName
- AdapterID

## **ibmServerRAIDInitDetected**

The ibmServerRAIDInitDetected event occurs when a ServeRAID initialization operation is in progress on a specified logical drive in a ServeRAID configuration.

### **Resolution**

No resolution. This event is informative only.

### **Details**

**Note:** This event is new in IBM Director 4.20.

<b>Event type</b>	<b>Event text</b>	<b>Severity</b>
ibmServerRAIDInitDetected	Clearing: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Harmless

This event type uses the following variables:

- OID
- ServerName
- AdapterID

## **ibmServerRAIDInitFail**

The ibmServerRAIDInitFail event occurs when a ServeRAID initialization operation fails on a specified logical drive in a ServeRAID configuration.

## Resolution

A hardware error occurred. Verify that the specified logical drive is not offline. If the logical drive is offline, replace the failed hard disk drives and restore the data from tape backup. If the specified logical drive is not offline, complete the following steps:

1. Verify that the controller, cables, and hard disk drives are installed correctly.
2. Verify that there is power to the hard disk drives.
3. Retry the command.
4. If the command still fails, restart the server and retry the command.
5. If the problem persists, contact your service representative.

## Details

**Note:** This event is new in IBM Director 4.20.

Event type	Event text	Severity
iBMSeverRAIDInitFail	Initialize failed: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Critical

This event type uses the following variables:

- OID
- ServerName
- AdapterID
- ErrorCode

## iBMSeverRAIDLogicalDriveAdded

The iBMSeverRAIDLogicalDriveAdded event occurs when a specified logical drive is added in a ServerRAID configuration.

## Resolution

No resolution. This event is informative only.

## Details

**Note:** This event is new in IBM Director 4.20.

Event type	Event text	Severity
IBMServerRAIDLogicalDriveAdded	Added logical drive: <i>drive</i> . Size <i>data</i> . where <i>drive</i> is the affected logical drive and <i>data</i> is the size and RAID level of that logical drive.	Harmless

This event type uses the following variables:

- OID
- ServerName
- AdapterID

## IBMServerRAIDLogicalDriveBlocked

The IBMServerRAIDLogicalDriveBlocked event occurs when a specified logical drive is in the blocked state.

## Resolution

When the ServerRAID controller performs a rebuild operation on an array, it reconstructs the data that was stored in RAID level-1 and RAID level-5 logical drives. However, the ServerRAID controller cannot reconstruct the data that was stored in any RAID level-0 logical drives in that array. The data in the RAID level-0 logical drives is blocked when the ServerRAID controller detects that the array is valid, but the data might be damaged.

To resolve this error, unblock the logical drive after the rebuild is complete. Restore the data from tape.

## Details

Event type	Event text	Severity
iBMServerRAIDLogicalDriveBlocked	Logical drive is blocked: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Critical

This event type uses the following variables:

- OID
- ServerName
- LogicalDriveID
- AdapterID

### **iBMServerRAIDLogicalDriveCritical**

The iBMServerRAIDLogicalDriveCritical event occurs when a specified logical drive is in the critical state.

### **Resolution**

A hard disk drive is defunct in the specified logical drive. The data on this logical drive is at risk. If another hard disk drive fails, the data might be lost.

Complete one of the following actions:

- If a rebuild operation is in progress, wait until the rebuild is complete.
- If a rebuild operation is not in progress, replace the failed hard disk drive with a new hard disk drive. After the hard disk drive is replaced, a rebuild operation will start automatically. See the troubleshooting chapter of the *IBM ServerRAID User's Reference*.

## Details

Event type	Event text	Severity
ibmServerRAIDLogicalDriveCritical	Logical drive is critical: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Warning

This event type uses the following variables:

- OID
- ServerName
- LogicalDriveID
- AdapterID

### **ibmServerRAIDLogicalDriveCriticalPeriodic**

The `ibmServerRAIDLogicalDriveCriticalPeriodic` event occurs when a periodic scan detects that one or more logical drives are in a critical state.

### **Resolution**

A hard disk drive is defunct in the specified logical drive. The data on this logical drive is at risk. If another hard disk drive fails, the data might be lost.

Complete one of the following actions:

- If a rebuild operation is in progress, wait until the rebuild is complete.
- If a rebuild operation is not in progress, replace the failed hard disk drive with a new hard disk drive. After the hard disk drive is replaced, a rebuild operation will start automatically. See the troubleshooting chapter of the *IBM ServerRAID User's Reference*.

## Details

Event type	Event text	Severity
iBMServerRAIDLogicalDriveCriticalPeriodic	Periodic scan found one or more critical logical drives: <i>drive</i> . Repair as soon as possible to avoid data loss.	Warning
	where <i>drive</i> is the affected logical drive.	

This event type uses the following variables:

- OID
- ServerName
- AdapterID

### **iBMServerRAIDLogicalDriveOffline**

The iBMServerRAIDLogicalDriveOffline event occurs when a specified logical drive is in the offline state.

### **Resolution**

A hardware error occurred. Contact your service representative.

### **Details**

Event type	Event text	Severity
iBMServerRAIDLogicalDriveOffline	Logical drive is offline: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Critical

This event type uses the following variables:

- OID
- ServerName
- LogicalDriveID
- AdapterID



## IBMServerRAIDLogicalDriveOK

The IBMServerRAIDLogicalDriveOK event occurs when a specified logical drive is functioning correctly.

### Resolution

No resolution. This event is informative only.

### Details

**Note:** This event is new in IBM Director 4.20.

Event type	Event text	Severity
IBMServerRAIDLogicalDriveOK	Logical drive is normal: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Harmless

This event type uses the following variables:

- OID
- ServerName
- AdapterID

## IBMServerRAIDLogicalDriveRemoved

The IBMServerRAIDLogicalDriveRemoved event occurs when a specified logical drive has been removed from a ServerRAID configuration.

### Resolution

No resolution. This event is informative only.

## Details

**Note:** This event is new in IBM Director 4.20.

Event type	Event text	Severity
iBMServerRAIDLogicalDriveRemoved	Deleted logical drive: <i>drive</i> .	Harmless
	where <i>drive</i> is the affected logical drive.	

This event type uses the following variables:

- OID
- ServerName
- AdapterID

## iBMServerRAIDLogicalDriveUnblocked

The iBMServerRAIDLogicalDriveUnblocked event occurs when a specified logical drive is in the unblocked state.

### Resolution

No resolution. This event is informative only.

### Details

Event type	Event text	Severity
iBMServerRAIDLogicalDriveUnblocked	Unblocked logical drive: <i>drive</i> .	Harmless
	where <i>drive</i> is the affected logical drive.	

This event type uses the following variables:

- OID
- LogicalDriveID
- AdapterID

## iBMServerRAIDMigrationComplete

The iBMServerRAIDMigrationComplete event occurs when a ServerRAID logical-drive migration is completed on a specified logical drive in a ServerRAID configuration.

### Resolution

No resolution. This event is informative only.

### Details

Event type	Event text	Severity
iBMServerRAIDMigrationComplete	Migration complete: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Harmless

This event type uses the following variables:

- OID
- ServerName
- LogicalDriveID
- AdapterID

## iBMServerRAIDMigrationDetected

The iBMServerRAIDMigrationDetected event occurs when a ServerRAID logical-drive migration is in progress on a specified logical drive in a ServerRAID configuration.

### Resolution

No resolution. This event is informative only.

## Details

Event type	Event text	Severity
iBMServeRAIDMigrationDetected	Migrating: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Harmless

This event type uses the following variables:

- OID
- ServerName
- LogicalDriveID
- AdapterID

### **iBMServeRAIDMigrationFail**

The iBMServeRAIDMigrationFail event occurs when a ServeRAID logical-drive migration fails on a specified logical drive in a ServeRAID configuration.

### **Resolution**

A hardware error occurred. Determine if one or more hard disk drives that are part of the specified logical drive have failed. If such a failure has occurred, restore the data from a tape backup. Otherwise, complete the following steps:

1. Verify that the controller, cables, and hard disk drives are installed correctly.
2. Verify that there is power to the hard disk drives.
3. Retry the command.
4. If the command still fails, restart the server and retry the command.

## Details

Event type	Event text	Severity
iBMServerRAIDMigrationFail	Migration failed: <i>drive [error]</i> where <i>drive</i> is the affected logical drive and <i>error</i> is the error code.	Critical

This event type uses the following variables:

- OID
- ServerName
- LogicalDriveID
- AdapterID
- ErrorCode

### iBMServerRAIDNoControllers

The iBMServerRAIDNoControllers event occurs when no ServerRAID controllers are detected.

### Resolution

No resolution. This event is informative only.

### Details

Event type	Event text	Severity
iBMServerRAIDNoControllers	No controllers were found in this system	Harmless

This event type uses the following variables:

- OID
- AdapterID

## IBMServerRAIDPFADrive

The IBMServerRAIDPFADrive event occurs when a Predictive Failure Analysis (PFA) is detected on a specified hard disk drive in a ServeRAID configuration.

### Resolution

The hard disk drive is going to fail. Contact your service representative.

### Details

Event type	Event text	Severity
IBMServerRAIDPFADrive	PFA detected for drive: <i>drive</i> . where <i>drive</i> is the affected hard disk drive.	Warning

This event type uses the following variables:

- OID
- ServerName
- AdapterID
- ChannelID
- SCSIID

## IBMServerRAIDPFADriveFRU

The IBMServerRAIDPFADriveFRU event occurs when a Predictive Failure Analysis (PFA) is detected on a specified hard disk drive with a specified field-replaceable unit (FRU) number in a ServeRAID configuration.

### Resolution

The hard disk drive is going to fail. Contact your service representative.

## Details

Event type	Event text	Severity
IBMServerRAIDPFADriveFRU	PFA detected for drive: <i>drive (FRU)</i> . where <i>drive</i> is the affected hard disk drive and <i>FRU</i> is the FRU number of that drive.	Warning

This event type uses the following variables:

- OID
- ServerName
- FRU
- AdapterID
- ChannelID
- SCSIID

### IBMServerRAIDPollingFail

The IBMServerRAIDPollingFail event occurs when a specified controller fails to respond to background polling commands.

### Resolution

A hardware error occurred. To resolve this error, complete the following steps:

1. Verify that the controller, cables, and hard disk drives are installed correctly.
2. Verify that there is power to the hard disk drives.
3. Retry the command.
4. If the problem persists, contact your service representative.

## Details

Event type	Event text	Severity
iBMServerRAIDPollingFail	Background polling commands are not responding: <i>controller</i> . Result codes: <i>error</i>	Warning
	where <i>controller</i> is the affected controller and <i>error</i> is the error code.	

This event type uses the following variables:

- OID
- ServerName
- AdapterID
- ErrorCode

### iBMServerRAIDPowerSupplyFail

The iBMServerRAIDPowerSupplyFail event occurs when the specified enclosure power supply fails in a ServerRAID configuration.

### Resolution

A hardware error occurred. Verify that the power supply in the enclosure device is installed properly. If it is, complete the following steps:

1. Verify that the controller, cables, and hard disk drives are installed correctly.
2. Verify that there is power to the hard disk drives.
3. Retry the command.
4. If the command still fails, restart the server and retry the command.
5. If the problem persists, replace the specified power supply.



## Details

Event type	Event text	Severity
iBMServerRAIDPowerSupplyFail	Enclosure power supply <i>supply</i> is malfunctioning: <i>location</i> where <i>supply</i> is the affected power supply and <i>location</i> is the controller and channel that the affected enclosure is attached to.	Critical

This event type uses the following variables:

- OID
- ServerName
- PowerSupplyID
- AdapterID
- ChannelID

### **iBMServerRAIDPowerSupplyInstalled**

The iBMServerRAIDPowerSupplyInstalled event occurs when a specified enclosure power supply is installed in a ServerRAID configuration.

### **Resolution**

No resolution. This event is informative only.

### **Details**

Event type	Event text	Severity
iBMServerRAIDPowerSupplyInstalled	Enclosure power supply <i>supply</i> has been installed: <i>location</i> where <i>supply</i> is the affected power supply and <i>location</i> is the controller and channel that the affected enclosure is attached to.	Harmless

This event type uses the following variables:

- **OID**
- **ServerName**
- **PowerSupplyID**
- **AdapterID**
- **ChannelID**

## **iBMServerRAIDPowerSupplyOK**

The iBMServerRAIDPowerSupplyOK event occurs when a specified enclosure power supply is functioning correctly in a ServerRAID configuration.

### **Resolution**

No resolution. This event is informative only.

### **Details**

<b>Event type</b>	<b>Event text</b>	<b>Severity</b>
iBMServerRAIDPowerSupplyOK	Enclosure power supply <i>supply</i> is now operational: <i>location</i> where <i>supply</i> is the affected power supply and <i>location</i> is the controller and channel that the affected enclosure is attached to.	Harmless

This event type uses the following variables:

- **OID**
- **ServerName**
- **PowerSupplyID**
- **AdapterID**
- **ChannelID**

## IBMServerRAIDPowerSupplyRemoved

The IBMServerRAIDPowerSupplyRemoved event occurs when a specified enclosure power supply is removed from a ServerRAID configuration.

### Resolution

No resolution. This event is informative only.

### Details

Event type	Event text	Severity
IBMServerRAIDPowerSupplyRemoved	Enclosure power supply <i>supply</i> has been removed: <i>location</i> where <i>supply</i> is the affected power supply and <i>location</i> is the controller and channel that the affected enclosure is attached to.	Warning

This event type uses the following variables:

- OID
- ServerName
- PowerSupplyID
- AdapterID
- ChannelID

## IBMServerRAIDRebuildComplete

The IBMServerRAIDRebuildComplete event occurs when a ServerRAID rebuild operation is completed on a specified logical drive in a ServerRAID configuration.

### Resolution

No resolution. This event is informative only.

## Details

Event type	Event text	Severity
iBMServerRAIDRebuildComplete	Rebuild complete: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Harmless

This event type uses the following variables:

- OID
- ServerName
- LogicalDriveID
- AdapterID

### **iBMServerRAIDRebuildDetected**

The iBMServerRAIDRebuildDetected event occurs when a ServerRAID rebuild operation is in progress on a specified logical drive in a ServerRAID configuration.

### **Resolution**

No resolution. This event is informative only.

## Details

Event type	Event text	Severity
iBMServerRAIDRebuildDetected	Rebuilding: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Harmless

This event type uses the following variables:

- OID
- ServerName
- LogicalDriveID

- AdapterID

## ibMServerRAIDRebuildFail

The ibMServerRAIDRebuildComplete event occurs when a ServerRAID rebuild operation fails on a specified logical drive in a ServerRAID configuration.

### Resolution

A hardware error occurred. To resolve this error, complete the following steps:

1. Verify that the controller, cables, and hard disk drives are installed correctly.
2. Verify that there is power to the hard disk drives.
3. If the command still fails, restart the server and retry the command.
4. If the problem persists, replace the specified drive.

### Details

Event type	Event text	Severity
ibMServerRAIDRebuildFail	Rebuild failed: <i>drive [error]</i> . where <i>drive</i> is the affected logical drive and <i>error</i> is the error code.	Critical

This event type uses the following variables:

- OID
- ServerName
- LogicalDriveID
- AdapterID
- ErrorCode

## ibMServerRAIDSyncComplete

The ibMServerRAIDSyncComplete event occurs when a ServerRAID synchronization operation is completed on a specified logical drive in a ServerRAID configuration.

## Resolution

No resolution. This event is informative only.

## Details

Event type	Event text	Severity
iBMServerRAIDSynccomplete	Synchronize complete: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Harmless

This event type uses the following variables:

- OID
- ServerName
- LogicalDriveID
- AdapterID

## iBMServerRAIDSynccomplete

The iBMServerRAIDSynccomplete event occurs when a ServerRAID synchronization operation is in progress on a specified logical drive in a ServerRAID configuration.

## Resolution

No resolution. This event is informative only.

## Details

Event type	Event text	Severity
iBMServerRAIDSynccomplete	Synchronizing: <i>drive</i> . where <i>drive</i> is the affected logical drive.	Harmless

This event type uses the following variables:

- OID
- ServerName
- LogicalDriveID
- AdapterID

## IBMServerRAIDSyncFail

The IBMServerRAIDSyncFail event occurs when a ServerRAID synchronization operation fails on a specified logical drive in a ServerRAID configuration.

### Resolution

A hardware error occurred. Verify that the specified logical drive is not offline or critical (that is, one hard disk drive that is offline in a RAID level-1, 1E, 5, 5E, 10, 1E0, or 50 logical drive). If the logical drive is critical, replace the failed hard disk drive. If the logical drive is offline, replace the failed hard disk drives and restore the data from tape backup.

If the specified logical drive is *not* offline or critical, complete the following steps:

1. Verify that the controller, cables, and hard disk drives are installed correctly.
2. Verify that there is power to the hard disk drives.
3. Retry the command.
4. If the command still fails, restart the server and retry the command.
5. If the problem persists, contact your service representative.

### Details

Event type	Event text	Severity
IBMServerRAIDSyncFail	Synchronize failed: <i>drive [error]</i> where <i>drive</i> is the affected logical drive and <i>error</i> is the error code.	Critical

This event type uses the following variables:

- OID
- ServerName
- LogicalDriveID
- AdapterID
- ErrorCode

## ibmServerRAIDTempFail

The ibmServerRAIDTempFail event occurs when an enclosure temperature exceeds a normal range on a specified controller in a ServeRAID configuration.

### Resolution

A hardware error occurred. Verify that the fans in the enclosure device are installed properly and working. If they are, complete the following steps:

1. Verify that the controller, cables, and hard disk drives are installed correctly.
2. Retry the command.
3. If the command still fails, restart the server and retry the command.
4. If the problem persists, contact your service representative.

### Details

Event type	Event text	Severity
ibmServerRAIDTempFail	Enclosure temperature is out of the normal range: <i>location</i> where <i>location</i> is the controller and channel that the affected enclosure is attached to.	Critical

This event type uses the following variables:

- OID



- ServerName
- AdapterID
- ChannelID

## **iBMServeRAIDTempOK**

The iBMServeRAIDTempOK event occurs when an enclosure temperature is within a normal range on a specified controller in a ServeRAID configuration.

### **Resolution**

No resolution. This event is informative only.

### **Details**

<b>Event type</b>	<b>Event text</b>	<b>Severity</b>
iBMServeRAIDTempOK	Enclosure temperature is in the normal range: <i>location</i> where <i>location</i> is the controller and channel that the affected enclosure is attached to.	Harmless

This event type uses the following variables:

- OID
- ServerName
- AdapterID
- ChannelID

## **iBMServeRAIDTestEvent**

The iBMServeRAIDTestEvent event occurs when a ServeRAID test event is generated.

### **Resolution**

No resolution. This event is informative only.

## Details

Event type	Event text	Severity
IBMServerRAIDTestEvent	This is a test event.	Harmless

This event type uses the following variables:

- OID
- ServerName

### **IBMServerRAIDUnsupportedDrive**

The IBMServerRAIDUnsupportedDrive event occurs when an unsupported hard disk drive is detected in a ServeRAID configuration.

### **Resolution**

Replace the specified hard disk drive with a hard disk drive model that is supported by IBM ServerRAID controllers.

### **Details**

Event type	Event text	Severity
IBMServerRAIDUnsupportedDrive	Possible non-warranted physical drive found: <i>drive</i> . where <i>drive</i> is the affected hard disk drive.	Warning

This event type uses the following variables:

- OID
- ServerName
- AdapterID
- ChannelID
- SCSIID

## IBMServerRAIDVersionMismatch

The IBMServerRAIDVersionMismatch event occurs when the versions of the BIOS, firmware, and driver for a specified ServeRAID controller do not match.

### Resolution

Upgrade to the latest version of the ServeRAID BIOS, firmware, and device driver.

### Details

**Note:** This event is new in IBM Director 4.20.

Event type	Event text	Severity
IBMServerRAIDVersionMismatch	Version mismatch detected: <i>controller</i> . The BIOS ( <i>version version</i> ), Firmware ( <i>version version</i> ), and Driver ( <i>version version</i> ) are not a matched set and are not compatible.  where <i>controller</i> is the affected controller and <i>version</i> is the version of the affected ServeRAID code.	Warning

This event type uses the following variables:

- OID
- ServerName
- AdapterID

---

## SNMP > Software

The Software events occur when specific software programs send SNMP traps in the IBM Director environment.

For more information about these SNMP traps, see the documentation for these programs.

## Event source

SNMP traps are generated by the following programs that are installed in the IBM Director environment:

- BrightStor Arcserve
- Veritas Backup Exec
- IBM Director

IBM Director receives the SNMP traps and converts them into the SNMP event types that are displayed in the Event Filter Builder tree.

## Details

If you select the **Software** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Software subtree. You can choose to select specific event types that are displayed under the **Software** node in the Event Filter Builder tree. The event filter will process only the event types that you select.

---

## Chapter 14. Storage events

The Storage events provide information about ServeRAID subcomponent failures and the status of ServeRAID operations such as synchronization, logical-drive migration, rebuild, compaction, compression, expansion, verify, and more. For detailed events, expand the **Storage** node in the Event Filter Builder tree.

### Event source

Storage events are generated by Level-2 managed systems that include ServeRAID controllers or integrated SCSI controllers with RAID capabilities. In addition to IBM Director Agent, these systems must have the managed-system agent for the ServeRAID Manager extension installed.

### Notes:

1. These events are generated *only* by managed systems running NetWare.
2. These events are not generated by the ServeRAID Manager (Standalone Edition).

### Details

If you select the **Storage** check box in the Event Filter Builder tree, the event filter will process all of the events that are specified in the Storage subtree. You can choose to select specific event types that are displayed under the **Storage** node in the Event Filter Builder tree. The event filter will process only the events that you select.

---

## Chapter 15. System Availability events

The System Availability events occur when System Availability identifies a managed system as problematic. A problematic system is one that has had too many unplanned outages over a specified period of time or a managed system that fails to report data to IBM Director Server or has availability data that is too old. When a system-availability report is generated, managed systems that meet the criteria that you specify as being problematic are flagged as such and an event is generated.

### Event source

This event is generated by the System Availability Agent that is installed on a Level-2 managed system. A prerequisite for the System Availability Agent is IBM Director Agent.

### Details

If you select the **System Availability** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the System Availability subtree.

Event type	Event text	Severity	Category	Extended attributes
System Availability	Not applicable	Not applicable	Not applicable	None

You can choose to select specific event types that are displayed under the System Availability node in the Event Filter Builder tree. The event filter will process only the event types that you select.

Event type	Event text	Severity	Category	Extended attributes
Problematic System	A problematic system has been detected.	Critical	Alert	None

---

## Chapter 16. Windows Event Log events

The Windows event log events are generated by the Windows operating system. If IBM Director Server does not discover any Level-2 managed systems (including the management server that IBM Director Server is installed on) running Microsoft Windows, these event types are not present in the Event Filter Builder tree.

In the Event Filter Builder tree, the Windows Event Log node expands to display three nodes:

- Application
- Security
- System

**Note:** Additional nodes might be displayed when you expand the Windows Event Log node. Whether these nodes are present depends on the managed systems discovered by IBM Director Server and their Windows registry settings.

These nodes map to the three folders displayed under the Event Log folder in the Windows Registry Editor.

**Note:** To view these folders in the Windows Registry Editor, complete the following steps:

1. Type `regedit` on a command line to start the Windows Registry Editor.
2. Click **My Computer** → **HKEY\_LOCAL\_MACHINE** → **System** → **CurrentControlSet** → **Services** → **Eventlog**.

Microsoft has requirements for how an application provides its events to the Windows event log. If an application fails to meet these requirements, IBM Director cannot map the application Windows events to the IBM Director Event Filter Builder tree. Application Windows events that can be mapped are displayed under the System node of the Event Filter Builder tree. Some of the requirements that must be met include providing a DLL that contains the event description. Windows event properties include an event ID. The event ID maps to the event description that is contained in the DLL.

**Note:** To view Windows event properties, including the event ID, complete the following steps:

1. From the Windows desktop, click **Start** → **Control Panel** → **Administrative Tools**.

2. In the Administrative Tools window, double-click **Event Viewer**
3. To open the Event Properties window, double-click an event. The event ID is displayed as well as the source of the event.

## **Details**

If you select the **Windows Event Log** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the Windows Event Log subtree. Expand this subtree to select specific event types or categories of event types.



---

## **Part 3. Events categorized by goal**

---

## Chapter 17. Events associated with BladeCenter products

The following events are associated with BladeCenter products, including management modules, network devices, blade servers, and chassis.

### Configuration Manager events

The following events are under the Configuration Manager node in the Event Filter Builder tree:

- Configuration Manager > Profile
- Configuration Manager > Profile > Execution

### MPA events

The following events are under the MPA > Component node in the Event Filter Builder tree:

- Blade Server > Capacity On Demand > Enabled
- Blade Server > Communication
- Blade Server > Inserted
- Blade Server > Insufficient Power
- Blade Server > Over Power Budget
- Blade Server > Removed
- Blade Server > Throttled
- Blade Server > VPD
- Chassis
- Chassis > Configuration
- Chassis > Failed
- Bus > Communication
- CPU > Failed
- CPU > Communication

- DASD > Failed
- DASD > Inserted
- DASD > Removed
- DIMM > Failed
- Fan > Failed
- Fan > Inserted
- Fan > PFA
- Fan > Removed
- I/O Module > Configuration
- I/O Module > Failed
- I/O Module > Inserted
- I/O Module > Insufficient Power
- I/O Module > POST
- I/O Module > Power > Off
- I/O Module > Power > On
- I/O Module > Redundancy
- I/O Module > Removed
- KVM > Owner
- PFA
- Power Subsystem > Low Fuel
- Power Subsystem > Mismatched Power Supplies
- Power Subsystem > Over Current
- Power Subsystem > Over Subscription
- Power Subsystem > Redundancy
- Power Supply > Failed
- Power Supply > Inserted

- Power Supply > Removed
- Server > Power > Off
- Server > Power > On
- Service Processor > Active
- Service Processor > Configuration
- Service Processor > Failover
- Service Processor > Inserted
- Service Processor > Log
- Service Processor > Network Stack
- Service Processor > OOB > Enabled
- Service Processor > OOB > Disabled
- Service Processor > Redundancy
- Service Processor > Removed
- Service Processor > Secure OOB > Enabled
- Service Processor > Secure OOB > Disabled
- Service Processor > Test
- USB > Inserted
- USB > Owner
- USB > Removed
- VRM > Failed

The following events are under the MPA > Environmental node in the Event Filter Builder tree:

- Temperature
- Voltage

The following events are under the MPA > Server Watchdog node in the Event Filter Builder tree:

- Boot

- OS
- POST

---

## Chapter 18. Events associated with system environments

The following events are associated with the condition of a system environment, such as voltage and temperature.

### **CIM events**

The following events are under the CIM > System node in the Event Filter Builder tree:

- Fan
- System Enclosure
- Temperature
- Voltage

### **MPA events**

The following events are under the MPA > Environmental node in the Event Filter Builder tree:

- Temperature
- Voltage

### **PET events**

The following events are under the PET > Environmental node in the Event Filter Builder tree:

- Sensor
- Hardware

The following events are under the PET > Hardware node in the Event Filter Builder tree:

- Sensor
- Hardware

---

## Chapter 19. Events associated with hardware component failures

The following events are associated with hardware components that are failing or have failed.

### **CIM events**

The following events are under the CIM > System node in the Event Filter Builder tree:

- DASD Backplane
- Disk Space Low
- Error Log
- Fan
- IPMI Log
- Lease Expiration
- Memory
- Memory PFA
- Network Adapter
- PFA
- SMART Drive
- System Enclosure
- Warranty Expiration

### **MPA events**

The following events are under the MPA > Component node in the Event Filter Builder tree:

- Chassis > Failed
- CPU > Failed
- DASD > Failed
- DIMM > Failed

- Fan > Failed
- Fan > PFA
- Hardware Information
- Hardware Information > Crash Dump
- I/O Module > Failed
- I/O Module > Redundancy
- PFA
- Power Subsystem > Redundancy
- Power Supply > Failed
- Service Processor > Failover
- Service Processor > Redundancy
- VRM > Failed

## **System Availability events**

- System Availability



---

## Chapter 20. Events associated with ServerRAID products

The following events are associated with ServerRAID controllers and storage solutions.

### **CIM > System events**

The following events are generated by the IBM Director ServerRAID Manager extension:

- ServerRAID Array FlashCopy Complete
- ServerRAID Array FlashCopy Detected
- ServerRAID Array FlashCopy Fail
- ServerRAID Array Rebuild Complete
- ServerRAID Array Rebuild Detected
- ServerRAID Array Rebuild Fail
- ServerRAID Array Sync Complete
- ServerRAID Array Sync Detected
- ServerRAID Array Sync Fail
- ServerRAID Compaction Complete
- ServerRAID Compaction Detected
- ServerRAID Compaction Fail
- ServerRAID Compression Complete
- ServerRAID Compression Detected
- ServerRAID Compression Fail
- ServerRAID Config Fail
- ServerRAID Controller Added
- ServerRAID Controller Bad Stripes
- ServerRAID Controller Battery Overtemp
- ServerRAID Controller Battery Temp Normal

- ServerRAID Controller Fail
- ServerRAID Controller Failover
- ServerRAID Controller Mismatched Versions
- ServerRAID Controller Replaced
- ServerRAID Copyback Complete
- ServerRAID Copyback Detected
- ServerRAID Copyback Fail
- ServerRAID Dead Battery
- ServerRAID Dead Battery Cache
- ServerRAID Decompression Complete
- ServerRAID Decompression Detected
- ServerRAID Decompression Fail
- ServerRAID Defunct Drive
- ServerRAID Defunct Drive FRU
- ServerRAID Defunct Replaced
- ServerRAID Drive Added
- ServerRAID Drive Clear Complete
- ServerRAID Drive Clear Detected
- ServerRAID Drive Clear Fail
- ServerRAID Drive Removed
- ServerRAID Drive Verify Complete
- ServerRAID Drive Verify Detected
- ServerRAID Drive Verify Fail
- ServerRAID Enclosure Fail
- ServerRAID Enclosure Fan Fail
- ServerRAID Enclosure Fan Installed

- ServerRAID Enclosure Fan OK
- ServerRAID Enclosure Fan Removed
- ServerRAID Enclosure OK
- ServerRAID Enclosure Power Supply Fail
- ServerRAID Enclosure Power Supply Installed
- ServerRAID Enclosure Power Supply OK
- ServerRAID Enclosure Power Supply Removed
- ServerRAID Enclosure Temp Fail
- ServerRAID Enclosure Temp OK
- ServerRAID Expansion Complete
- ServerRAID Expansion Detected
- ServerRAID Expansion Fail
- ServerRAID FlashCopy Complete
- ServerRAID FlashCopy Detected
- ServerRAID FlashCopy Fail
- ServerRAID Init Complete
- ServerRAID Init Detected
- ServerRAID Init Fail
- ServerRAID Logical Drive Added
- ServerRAID Logical Drive Blocked
- ServerRAID Logical Drive Critical
- ServerRAID Logical Drive Critical Periodic
- ServerRAID Logical Drive Off Line
- ServerRAID Logical Drive OK
- ServerRAID Logical Drive Removed
- ServerRAID Logical Drive Unblocked

- ServerRAID Migration Complete
- ServerRAID Migration Detected
- ServerRAID Migration Fail
- ServerRAID No Controllers
- ServerRAID PFA Drive
- ServerRAID PFA Drive FRU
- ServerRAID Polling Fail
- ServerRAID Rebuild Complete
- ServerRAID Rebuild Detected
- ServerRAID Rebuild Fail
- ServerRAID Sync Complete
- ServerRAID Sync Detected
- ServerRAID Sync Fail
- ServerRAID Test Event
- ServerRAID Unsupported Drive

## **SNMP > Hardware > Storage > RAID**

These events are generated by the ServerRAID Manager (Standalone Edition) in the IBM Director environment. For more information about these SNMP traps, see the ServerRAID hardware documentation.

## **SNMP > iso > org > dod > internet > private > enterprises > ibm > ibmProd > ibmServerRAID > ibmServerRAIDMIB events**

The following events are generated by the IBM Director ServerRAID Manager extension:

- IBMServerRAIDArrayFlashCopyComplete
- IBMServerRAIDArrayFlashCopyDetected
- IBMServerRAIDArrayFlashCopyFail
- IBMServerRAIDArrayRebuildComplete

- IBMServerRAIDArrayRebuildDetected
- IBMServerRAIDArrayRebuildFail
- IBMServerRAIDArraySyncComplete
- IBMServerRAIDArraySyncDetected
- IBMServerRAIDArraySyncFail
- IBMServerRAIDCompactionComplete
- IBMServerRAIDCompactionDetected
- IBMServerRAIDCompactionFail
- IBMServerRAIDCompressionComplete
- IBMServerRAIDCompressionDetected
- IBMServerRAIDCompressionFail
- IBMServerRAIDConfigFail
- IBMServerRAIDControllerAdded
- IBMServerRAIDControllerBadStripes
- IBMServerRAIDControllerBatteryOverTemp
- IBMServerRAIDBatteryTempNormal
- IBMServerRAIDControllerFail
- IBMServerRAIDControllerFailover
- IBMServerRAIDControllerReplaced
- IBMServerRAIDCopyBackComplete
- IBMServerRAIDCopyBackDetected
- IBMServerRAIDCopyBackFail
- IBMServerRAIDDeadBattery
- IBMServerRAIDDeadBatteryCache
- IBMServerRAIDDecompressionComplete
- IBMServerRAIDDecompressionDetected

- IBMServerRAIDDDecompressionFail
- IBMServerRAIDDDefunctDrive
- IBMServerRAIDDDefunctDriveFRU
- IBMServerRAIDDDefunctReplaced
- IBMServerRAIDDDriveAdded
- IBMServerRAIDDDriveClearComplete
- IBMServerRAIDDDriveClearDetected
- IBMServerRAIDDDriveClearFail
- IBMServerRAIDDDriveRemoved
- IBMServerRAIDDDriveVerifyComplete
- IBMServerRAIDDDriveVerifyDetected
- IBMServerRAIDDDriveVerifyFail
- IBMServerRAIDEnclosureFail
- IBMServerRAIDEnclosureFanOK
- IBMServerRAIDEnclosureOK
- IBMServerRAIDExpansionComplete
- IBMServerRAIDExpansionDetected
- IBMServerRAIDExpansionFail
- IBMServerRAIDFanFail
- IBMServerRAIDFanInstalled
- IBMServerRAIDFanRemoved
- IBMServerRAIDFlashCopyComplete
- IBMServerRAIDFlashCopyDetected
- IBMServerRAIDFlashCopyFail
- IBMServerRAIDInitComplete
- IBMServerRAIDInitDetected

- IBMServerRAIDInitFail
- IBMServerRAIDLlogicalDriveAdded
- IBMServerRAIDLlogicalDriveBlocked
- IBMServerRAIDLlogicalDriveCritical
- IBMServerRAIDLlogicalDriveCriticalPeriodic
- IBMServerRAIDLlogicalDriveOffline
- IBMServerRAIDLlogicalDriveOK
- IBMServerRAIDLlogicalDriveRemoved
- IBMServerRAIDLlogicalDriveUnblocked
- IBMServerRAIDMigrationComplete
- IBMServerRAIDMigrationDetected
- IBMServerRAIDMigrationFail
- IBMServerRAIDNoControllers
- IBMServerRAIDPFADDrive
- IBMServerRAIDPFADDriveFRU
- IBMServerRAIDPollingFail
- IBMServerRAIDPowerSupplyFail
- IBMServerRAIDPowerSupplyInstalled
- IBMServerRAIDPowerSupplyOK
- IBMServerRAIDPowerSupplyRemoved
- IBMServerRAIDRebuildComplete
- IBMServerRAIDRebuildDetected
- IBMServerRAIDRebuildFail
- IBMServerRAIDSyncComplete
- IBMServerRAIDSyncDetected
- IBMServerRAIDSyncFail

- IBMServerRAIDTempFail
- IBMServerRAIDTempOK
- IBMServerRAIDTestEvent
- IBMServerRAIDUnsupportedDrive
- IBMServerRAIDVersionMismatch

### **Storage > ServerRAID Controller**

These events are generated by the IBM Director ServerRAID Manager extension on managed systems running NetWare in the IBM Director environment.



---

## Chapter 21. Events associated with service processors

The following events are associated with IBM service processors. Use these events when constructing an event action plan that can capture information from IBM service processors.

### Director events

- MPA

### MPA events

- MPA
- Component
- Blade Server
- Bus
- Chassis
- Chassis Configuration
- Chassis Failed
- DASD
- DIMM
- Fan
- Hardware Information
- Crash Dump
- I/O Module
- KVM
- OS Image
- Crash Dump
- PFA
- Power Subsystem

- Power Supply
- Server
- Service Processor
- SMP Expansion
- USB
- VRM
- Environmental
- Platform
- Server Watchdog
- Unknown

## **Part 4. Supplementary information**

---

## Chapter 22. Extended attributes and variable-binding information

---

Some implementations of IBM Director event types use extended attributes to provide additional information about the occurrence that generated an event.

**Note:** PET and SNMP trap event types use variable bindings.

In this documentation, each event lists any extended attributes that they have. Some sets of events use the same extended attributes and they are defined in the following sections. If an event has additional extended attributes, they are documented with the affected event.

---

### Extended attributes for CIM events

The CIM event types use the following standard set of extended attributes.

- *AlertingManagedElement* is the system component that is affected by the alert.
- *Category* is one of the following hardware event categories defined by the Hardware Status task:
  - Communications
  - Device
  - Environmental
  - Security
- *EventID* provides the component node labels in the interface for the Hardware Status task.
- *EventTime* is a reserved extended attribute.
- *ProviderName* is a reserved extended attribute.

---

### Extended attributes for HMC CIM events

The CIM event types for HMC use the following standard set of extended attributes.

- *AlertingManagedElement* is the CIM object path of the system that generated the event
- *EventID* provides the component node labels in the interface for the Hardware Status task.

- *EventTime* provides the date and time that the event was generated. This value is based on the local date and time of the system that generated the event.
  - *SenderUUID* is the UUID of the HMC that sent the event.
- 

## **Extended attributes for the Director > Director Agent events**

The Director > Director Agent events use a standard set of extended attributes.

- *Duration* is the configured value that you assigned in the **Minimum Duration** field of the **Threshold Configuration** window.
- *Monitor Resource* is the type of monitor configured with a threshold.
- *Threshold Name* is the name that you assigned to the threshold.

## **Extended attributes for the Director > Scheduler events**

The Director > Scheduler events use a standard set of extended attributes.

The Director > Scheduler > System events use all of the following extended attributes. The Director > Scheduler > Job event types use only Job ID and Job Activation.

- *Client Category* indicates the status of the job on the system at the time the event was generated:
  - Complete
  - Failed
  - In progress
  - Pending
  - Skipped
  - Suspended
  - Unavailable
- *Job Activation Time* indicates the time that the job is scheduled to start.
- *Job Current Task ID* is the ID of the current task being performed by the job.
- *Job Current Subtask ID* is the ID of the current subtask being performed by the job.
- *Job Current Task Name* is the name of the current task being performed by the job.
- *Job ID* is the ID of the current job.

---

## Extended attributes for MPA events

The MPA events use extended attributes to provide information about a state change detected by a service processor or management module.

Most MPA events use some or all of the following extended attributes; however, the availability of certain extended attributes will vary depending on the system from which an event is generated. For example, events generated by an IPMI baseboard management controller does not provide the Sensor Label and Sensor Number extended attributes.

- *Firmware code* is a 32-bit code that the service processor sends IBM Director Server to indicate what has occurred. This attribute is useful when troubleshooting a problem with the assistance of IBM service representatives.
- *Sender UUID* is the universally unique identifier (UUID) of the physical system that sent the event, or the UUID of the management module if a management module sent the event. Typically, the Sender UUID and Source UUID are the same system. However, the sending physical system can be different from the source system of the event. For example, a BladeCenter chassis (sender) sends events for the blade servers (source) that it contains. Similarly, a server (sender) sends events for an attached RXE-100 expansion unit (source).
- *Sensor Label* identifies the purpose of the affected sensor. This extended attribute is provided only when the event is generated by an IPMI baseboard management controller.
- *Sensor Number* identifies the affected sensor. This extended attribute is provided only when the event is generated by an IPMI baseboard management controller.
- *Source UUID* is the universally unique identifier of the source physical system. The source system is the source of the event, but not necessarily the sender of the event. See Sender UUID for more information.

---

## Extended attributes for PET events

All PET events use the same standard set of extended attributes (variable bindings).

**Note:** For detailed information about these extended attributes (variable bindings), see the following documentation:

- *Intel Intelligent Platform Management Interface Specification Version 1.5*, dated June 1, 2004.

- *Intel IPMI Platform Event Trap Specification Version 1.0*, dated December 7, 1998.
  - *Entity* identifies the affected system component, such as a, microprocessor, system board, or power supply.
  - *Entity Instance* identifies the affected instance of the system component, such as power supply 1 and power supply 2.
  - *Event Data* provides additional event information as specified by a combination of the Event Type and Event Source extended attributes.
  - *Event Severity* identifies the severity of the event. See the IPMI Specification for defined values.
  - *Event Source Type* identifies the class of device or type of software that originated the event. This can be different than the device or type of software that sends the trap. See the IPMI Specification for defined values.
  - *Event Type* identifies what type of transition or state triggered the event.
  - *GUID* identifies the GUID for the system.
  - *Language Code* identifies, in combination with the OEM Custom Field extended attribute, the language that any strings are in.
- **Note:** Language is different than character set. Character sets are specified as ASCII or Unicode.
- *Local Timestamp* identifies the local time of the system, as a number of seconds.
- *Manufacturer ID* identifies the manufacturer ID using private enterprise IDs.
- *OEM Custom Field* provides customized information and can be used in combination with the Language Code extended attribute.
- *Offset* indicates which particular event occurred for a given Event Type.
- *Sensor Device* identifies the instance of the device that contains the sensor that generated the event.
- *Sensor Number* uniquely identifies this sensor among all the sensors monitored by this sensor device.
- *Sensor Type* identifies the types of events the event sensor is monitoring, such as temperature, voltage, current, BIOS, POST, processor, and fan. Sometimes referred to as the Event Sensor Type in the IPMI and PET Specifications.
- *Sequence ID* identifies whether the event trap is new or retransmitted. The function of this field is specific to the trap source type.

- *System ID* identifies the particular system, product model, in combination with the Manufacturer ID extended attribute.
- *Trap Source Type* identifies the class of the device or software that originated the trap on the network. See the IPMI Specification for defined values.
- *UTC Offset* identifies the coordinated universal time (UTC) offset in minutes.

---

## Variable-binding information for IBM Director SNMP events

The IBM Director SNMP events use the following variables in the variable-binding pairs.

For the values that are bound to these variables for each event type, see the IBM-SYSTEM-TRAP-MIB.mib file in the *c:/Director/proddata/snmp* directory, where *c* is the hard disk drive and *Director* is the directory where you installed IBM Director. This MIB file also is contained in the IBM Director MIB file package that you can download from [www.ibm.com/servers/eserver/xseries/systems\\_management/ibm\\_director/](http://www.ibm.com/servers/eserver/xseries/systems_management/ibm_director/).

*Table 1. IBM Director SNMP event variable-binding information*

Variable	Syntax	Definition (description)
OID	Not applicable	The SNMPv1-standard OID defined in enterprise 'director'.
Identifier	String	The internal ID for this event type.
SourceObjectPath	String	The CIM device ID value for the system whose intrusion state is being monitored. All IBM Director SNMP events are translated from CIM indicators.
TargetObjectPath	String	The CIM device ID value for the system whose intrusion state is being monitored. All IBM Director SNMP events are translated from CIM indicators.
Severity	Uint 16	The possible severities are critical, warning, or normal. Available severities vary depending on the event. See each event for its available severities.
Description	String	General information about what hardware scenario generates the event.
TimeStamp	Datetime	The date and time when the state change occurred for the component. A GMT-standard timestamp is used. For example: 20030416155614.000000-240.
Component	Uint 16	The physical PCI slot number or the onboard port number of the NIC.



---

## Variable-binding information for IBM Director SNMP ServeRAID events

The IBM Director SNMP ServeRAID events use the following variables in the variable-binding pairs.

For the values that are bound to these variables for each event type, see the IBM-SERVE RAID-MIB.mib file in the *c:/Director/proddata/snmp* directory, where *c* is the hard disk drive and *Director* is the directory where you installed IBM Director. This MIB file also is contained in the IBM Director MIB file package that you can download from [www.ibm.com/servers/eserver/xseries/systems/management/ibm\\_director/](http://www.ibm.com/servers/eserver/xseries/systems/management/ibm_director/).

Variable	Syntax	Definition (description)
OID	Not applicable	The SNMPv1-standard OID defined in enterprise 'director'.
Identifier	String	The internal ID for this event type.
SourceObjectPath	String	The CIM device ID value for the system whose intrusion state is being monitored. All IBM Director SNMP events are translated from CIM indicators.
TargetObjectPath	String	The CIM device ID value for the system whose intrusion state is being monitored. All IBM Director SNMP events are translated from CIM indicators.
Severity	Uint 16	The possible severities are critical, warning, or normal. Available severities vary depending on the event. See each event for its available severities.
Description	String	General information about what hardware scenario generates the event.
TimeStamp	Datetime	The date and time when the state change occurred for the component. A GMT-standard timestamp is used. For example: 20030416155614.000000-240.
Component	Uint 16	The physical PCI slot number or the onboard port number of the NIC.

---

## Chapter 23. CIM indications in IBM Director

IBM Director converts CIM indications for use by the following end consumers:

- IBM Director events
- IBM Director Console (Group Contents pane)
- Microsoft Operations Manager 2005 (alerts)
- Microsoft System Management Server (SMS) (native events)
- Microsoft Windows (event log event ID)
- SNMP
- Tivoli Enterprise Console (native events)
- Tivoli Enterprise Console (SNMP events)

### Notes:

1. The HP OpenView and Tivoli NetView Upward Integration Modules (UIMs) use SNMP traps.
2. (Microsoft Operations Manager 2005) All ServerRAID CIM indications are converted to the same value. However, each ServerRAID CIM indication provides a distinct event description.
3. (Microsoft SMS) All ServerRAID CIM indications use the same message ID of 50210. However, each ServerRAID CIM indication provides a distinct event description.
4. (Microsoft Windows event log) All ServerRAID CIM indications are converted to the same event ID. However, each ServerRAID CIM indication provides a distinct Windows event log description.

---

### IBMP5G\_ChassisEvent CIM indication

This CIM indication is generated when the state of a system chassis (enclosure) changes, such as when the cover is removed from the system.

End consumer	Critical severity	Warning severity	Normal severity
IBM Director event	CIM > System > System Enclosure	Not applicable	CIM > System > System Enclosure

<b>End consumer</b>	<b>Critical severity</b>	<b>Warning severity</b>	<b>Normal severity</b>
IBM Director Console (Group Contents pane)		Not applicable	No symbol displayed
Microsoft Operations Manager 2005 alert	Security Event	Security Event	Security Event
Microsoft SMS native events (Message ID 50040)	IBM_UMS_AGENT_CHASSIS_ERROR_	IBM_UMS_AGENT_CHASSIS_WARNING_	IBM_UMS_AGENT_CHASSIS_INFO_
Microsoft Windows event log event ID	4	Not applicable	4
SNMP	ibmSystemTrapChassis	Not applicable	ibmSystemTrapChassis
Tivoli Enterprise Console native event	IBMPSG_ChassisEvent	IBMPSG_ChassisEvent	IBMPSG_ChassisEvent
Tivoli Enterprise Console SNMP event	UMS_ChassisIntruded	Not applicable	UMS_ChassisInPlace

## **IBMPSG\_DASDBackplaneEvent CIM indication**

This CIM indication is generated when the Remote Supervisor Adapter detects that the state of the system hard disk drive changes with respect to its availability.

<b>End consumer</b>	<b>Critical severity</b>	<b>Warning severity</b>	<b>Normal severity</b>
IBM Director event	CIM > System > DASD Backplane	Not applicable	Not applicable
IBM Director Console (Group Contents pane)	Not applicable	Not applicable	Not applicable
Microsoft Operations Manager 2005 alert	Storage Event	Storage Event	Storage Event

<b>End consumer</b>	<b>Critical severity</b>	<b>Warning severity</b>	<b>Normal severity</b>
Microsoft SMS native events (Message ID 50300)	IBM_UMS_AGENT_DASDBACKPLANE_ERROR_	IBM_UMS_AGENT_DASDBACKPLANE_WARNING_	IBM_UMS_AGENT_DASDBACKPLANE_INFO_
Microsoft Windows event log event ID	30	Not applicable	Not applicable
SNMP	ibmSystemTrapDASDBackplane	Not applicable	Not applicable
Tivoli Enterprise Console native event	IBMPSG_DASDBackplaneEvent	Not applicable	Not applicable
Tivoli Enterprise Console SNMP event	UMS_DASDBackplaneEvent	Not applicable	Not applicable

## IBMPSG\_ErrorLogEvent CIM indication


This CIM indication is generated when the Remote Supervisor Adapter detects that its error log is at 75% or 100% of its capacity.

<b>End consumer</b>	<b>Critical severity</b>	<b>Warning severity</b>	<b>Normal severity</b>
IBM Director event	Not applicable	CIM > System > Error Log	Not applicable
IBM Director Console (Group Contents pane)	Not applicable	Not applicable	Not applicable
Microsoft Operations Manager 2005 alert	Other Event	Other Event	Other Event
Microsoft SMS native events (Message ID 50240)	IBM_UMS_AGENT_ERRORLOG_ERROR_	IBM_UMS_AGENT_ERRORLOG_WARNING_	IBM_UMS_AGENT_ERRORLOG_INFO_
Microsoft Windows event log event ID	24	24	Not applicable
SNMP	Not applicable	ibmSystemTrapErrorLog	Not applicable

<b>End consumer</b>	<b>Critical severity</b>	<b>Warning severity</b>	<b>Normal severity</b>
Tivoli Enterprise Console native event	IBMPSG_ErrorLogEvent	IBMPSG_ErrorLogEvent	Not applicable
Tivoli Enterprise Console SNMP event	UMS_ErrorLogEvent	UMS_ErrorLogEvent	Not applicable


## IBMPSG\_FanEvent CIM indication

This CIM indication is generated when the state of a system fan has changed with respect to the manufacturer-defined RPM values. If a Remote Supervisor Adapter is installed in a system, this event is sent when a fan stops, is removed, or is not performing optimally. If a Remote Supervisor Adapter is not installed, an event is sent when the fan stops or is removed.

<b>End consumer</b>	<b>Critical severity</b>	<b>Warning severity</b>	<b>Normal severity</b>
IBM Director event	CIM > System > Fan	Not applicable	CIM > System > Fan
IBM Director Console (Group Contents pane)	 Fan Event	Not applicable	No symbol displayed
Microsoft Operations Manager 2005 alert	Fan Event	Fan Event	Fan Event
Microsoft SMS native events (Message ID 50050)	IBM_UMS_AGENT_FAN_ERROR_	IBM_UMS_AGENT_FAN_WARNING_	IBM_UMS_AGENT_FAN_INFO_
Microsoft Windows event log event ID	5	5	5
SNMP	ibmSystemTrapFan	Not applicable	ibmSystemTrapFan
Tivoli Enterprise Console native event	IBMPSG_FanEvent	IBMPSG_FanEvent	IBMPSG_FanEvent
Tivoli Enterprise Console SNMP event	UMS_FanOutOfOrder	Not applicable	UMS_FanOperational


## IBMPSG\_GenericFanEvent CIM indication

This CIM indication is generated when the Remote Supervisor Adapter or ASM processor detects that the state of a system fan has changed with respect to its manufacturer-defined RPM thresholds but the precise fan instance cannot be determined.

End consumer	Critical severity	Warning severity	Normal severity
IBM Director event	CIM > System > Fan	Not applicable	Not applicable
IBM Director Console (Group Contents pane)		Not applicable	Not applicable
Microsoft Operations Manager 2005 alert	Fan Event	Fan Event	Fan Event
Microsoft SMS native events (Message ID 50310)	IBM_UMS_AGENT_GENERICFAN_ERROR_	IBM_UMS_AGENT_GENERICFAN_WARNING_	IBM_UMS_AGENT_GENERICFAN_INFO_
Microsoft Windows event log event ID	31	Not applicable	Not applicable
SNMP	ibmSystemTrapGenericFan	Not applicable	Not applicable
Tivoli Enterprise Console native event	IBMPSG_GenericFanEvent	Not applicable	Not applicable
Tivoli Enterprise Console SNMP event	UMS_GenericFanEvent	Not applicable	Not applicable


## IBMPSG\_GenericVoltageEvent CIM indication

This CIM indication is generated when the Remote Supervisor Adapter or the ASM processor detects that the state of a system voltage sensor has changed with respect to a manufacturer-defined threshold but the precise voltage sensor cannot be determined.

<b>End consumer</b>	<b>Critical severity</b>	<b>Warning severity</b>	<b>Normal severity</b>
IBM Director event	CIM > System > Voltage	Not applicable	Not applicable
IBM Director Console (Group Contents pane)	 Voltage Event	Not applicable	Not applicable
Microsoft Operations Manager 2005 alert	Voltage Event	Voltage Event	Voltage Event
Microsoft SMS native events (Message ID 50320)	IBM_UMS_AGENT_GENERICVOLTAGE_ERROR_	IBM_UMS_AGENT_GENERICVOLTAGE_WARNING_	IBM_UMS_AGENT_GENERICVOLTAGE_INFO_
Microsoft Windows event log event ID	32	Not applicable	Not applicable
SNMP	ibmSystemTrapGenericVoltage	Not applicable	Not applicable
Tivoli Enterprise Console native event	IBMPSG_GenericVoltageEvent	Not applicable	Not applicable
Tivoli Enterprise Console SNMP event	UMS_GenericVoltageEvent	Not applicable	Not applicable

## IBMPSG\_LeaseExpirationEvent CIM indication


This CIM indication is generated when the system lease expiration date has been reached with respect to the value configured for the date in the Asset ID task.

<b>End consumer</b>	<b>Critical severity</b>	<b>Warning severity</b>	<b>Normal severity</b>
IBM Director event	Not applicable	CIM > System > Lease Expiration	CIM > System > Lease Expiration
IBM Director Console (Group Contents pane)	Not applicable	 Not applicable	No symbol displayed

<b>End consumer</b>	<b>Critical severity</b>	<b>Warning severity</b>	<b>Normal severity</b>
Microsoft Operations Manager 2005 alert	Other Event	Other Event	Other Event
Microsoft SMS native events (Message ID 50130)	IBM_UMS_AGENT_LEASE_ERROR_	IBM_UMS_AGENT_LEASE_WARNING_	IBM_UMS_AGENT_LEASE_INFO_
Microsoft Windows event log event ID	Not applicable	13	13
SNMP	Not applicable	ibmSystemTrapLeaseExpiration	ibmSystemTrapLeaseExpiration
Tivoli Enterprise Console native event	IBMPSG_LeaseExpirationEvent	IBMPSG_LeaseExpirationEvent	IBMPSG_LeaseExpirationEvent
Tivoli Enterprise Console SNMP event	UMS_LeaseExpiredCritical	UMS_LeaseExpiredWarning	UMS_LeaseExpiredNormal

## IBMPSG\_MemoryPFEvent CIM indication

This CIM indication is generated when a dual inline memory module (DIMM) in a system changes with respect to its availability.


<b>End consumer</b>	<b>Critical severity</b>	<b>Warning severity</b>	<b>Normal severity</b>
IBM Director event	CIM > System > Memory PFA	Not applicable	CIM > System > Memory PFA
IBM Director Console (Group Contents pane)		Not applicable	No symbol displayed
Microsoft Operations Manager 2005 alert	Memory Event	Memory Event	Memory Event
Microsoft SMS native events (Message ID 50190)	IBM_UMS_AGENT_MEMORYPFA_ERROR_	IBM_UMS_AGENT_MEMORYPFA_WARNING_	IBM_UMS_AGENT_MEMORYPFA_INFO_
Microsoft Windows event log event ID	19	Not applicable	19



End consumer	Critical severity	Warning severity	Normal severity
SNMP	ibmSystemTrapMemoryPF	Not applicable	ibmSystemTrapMemoryPF
Tivoli Enterprise Console native event	IBMPSG_MemoryPFEEvent	IBMPSG_MemoryPFEEvent	IBMPSG_MemoryPFEEvent
Tivoli Enterprise Console SNMP event	UMS_MemoryPFCritical	UMS_MemoryPFWarning	UMS_MemoryPFNormal


## IBMPSG\_NetworkAdapterFailedEvent CIM indication

This CIM indication is generated when a network interface card (NIC) in a system has failed.

End consumer	Critical severity	Warning severity	Normal severity
IBM Director event	CIM > System > Network Adapter > Failed	Not applicable	Not applicable
IBM Director Console (Group Contents pane)	 Network Event	Not applicable	Not applicable
Microsoft Operations Manager 2005 alert	Network Event	Network Event	Network Event
Microsoft SMS native events (Message ID 50260)	IBM_UMS_AGENT_NETWORKADAPTER_FAILED_ERROR_	IBM_UMS_AGENT_NETWORKADAPTER_FAILED_WARNING_	IBM_UMS_AGENT_NETWORKADAPTER_FAILED_INFO_
Microsoft Windows event log event ID	Not applicable	26	Not applicable
SNMP	ibmSystemTrapNetworkAdapterFailed	Not applicable	Not applicable
Tivoli Enterprise Console native event	Not applicable	IBMPSG_NetworkAdapterFailedEvent	Not applicable
Tivoli Enterprise Console SNMP event	Not applicable	UMS_NetworkAdapterFailedEvent	Not applicable

## IBMPSG\_NetworkAdapterOfflineEvent CIM indication

This CIM indication is generated when a network interface card (NIC) in a system goes offline.

End consumer	Critical severity	Warning severity	Normal severity
IBM Director event	Not applicable	CIM > System > Network Adapter > Offline	Not applicable
IBM Director Console (Group Contents pane)	Not applicable	 Network Event	Not applicable
Microsoft Operations Manager 2005 alert	Network Event	Network Event	Network Event
Microsoft SMS native events (Message ID 50270)	IBM_UMS_AGENT_NETWORKADAPTER_OFFLINE_ERROR_	IBM_UMS_AGENT_NETWORKADAPTER_OFFLINE_WARNING_	IBM_UMS_AGENT_NETWORKADAPTER_OFFLINE_INFO_
Microsoft Windows event log event ID	Not applicable	27	Not applicable
SNMP	Not applicable	ibmSystemTrapNetworkAdapterOffline	Not applicable
Tivoli Enterprise Console native event	Not applicable	IBMPSG_NetworkAdapterOfflineEvent	Not applicable
Tivoli Enterprise Console SNMP event	Not applicable	UMS_NetworkAdapterOfflineEvent	Not applicable

## IBMPSG\_NetworkAdapterOnlineEvent CIM indication

This CIM indication is generated when the state of a system network interface card (NIC) changes from offline to online.

<b>End consumer</b>	<b>Critical severity</b>	<b>Warning severity</b>	<b>Normal severity</b>
IBM Director event	Not applicable	Not applicable	CIM > System > Network Adapter > Online
IBM Director Console (Group Contents pane)	Not applicable	Not applicable	Not applicable
Microsoft Operations Manager 2005 alert	Network Event	Network Event	Network Event
Microsoft SMS native events (Message ID 50280)	IBM_UMS_AGENT_NETWORKADAPTER_ONLINE_ERROR_	IBM_UMS_AGENT_NETWORKADAPTER_ONLINE_WARNING_	IBM_UMS_AGENT_NETWORKADAPTER_ONLINE_INFO_
Microsoft Windows event log event ID	Not applicable	Not applicable	28
SNMP	Not applicable	Not applicable	ibmSystemTrapNetworkAdapterOnline
Tivoli Enterprise Console native event	Not applicable	Not applicable	IBMPSG_NetworkAdapterOnlineEvent
Tivoli Enterprise Console SNMP event	Not applicable	Not applicable	UMS_NetworkAdapterOnlineEvent

## IBMPSG\_PFAEvent CIM indication


This CIM indication is generated when the Remote Supervisor Adapter detects that a component in a system is about to fail.

<b>End consumer</b>	<b>Critical severity</b>	<b>Warning severity</b>	<b>Normal severity</b>
IBM Director event	CIM > System > PFA	Not applicable	Not applicable
IBM Director Console (Group Contents pane)		Not applicable	Not applicable

<b>End consumer</b>	<b>Critical severity</b>	<b>Warning severity</b>	<b>Normal severity</b>
Microsoft Operations Manager 2005 alert	Other Event	Other Event	Other Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_PFA_ERROR_	IBM_UMS_AGENT_PFA_WARNING_	IBM_UMS_AGENT_PFA_INFO_
Microsoft Windows event log event ID	22	Not applicable	Not applicable
SNMP	ibmSystemTrappFA	Not applicable	Not applicable
Tivoli Enterprise Console native event	IBMPSG_PFAEvent	Not applicable	Not applicable
Tivoli Enterprise Console SNMP event	UMS_PFAEvent	Not applicable	Not applicable

## IBMPSG\_PowerSupplyEvent CIM indication


This CIM indication is generated when the state of a system power supply changes with respect to its availability.

<b>End consumer</b>	<b>Critical severity</b>	<b>Warning severity</b>	<b>Normal severity</b>
IBM Director event	CIM > System > Server Power Supply	Not applicable	CIM > System > Server Power Supply
IBM Director Console (Group Contents pane)		Not applicable	No symbol displayed
Microsoft Operations Manager 2005 alert	Power Supply Event	Power Supply Event	Power Supply Event
Microsoft SMS native events (Message ID 50230)	IBM_UMS_AGENT_POWERSUPPLY_ERROR_	IBM_UMS_AGENT_POWERSUPPLY_WARNING_	IBM_UMS_AGENT_POWERSUPPLY_INFO_
Microsoft Windows event log event ID	23	23	23

<b>End consumer</b>	<b>Critical severity</b>	<b>Warning severity</b>	<b>Normal severity</b>
SNMP	ibmSystemTrapPowerSupply	Not applicable	ibmSystemTrapPowerSupply
Tivoli Enterprise Console native event	IBMPSG_PowerSupplyEvent	IBMPSG_PowerSupplyEvent	IBMPSG_PowerSupplyEvent
Tivoli Enterprise Console SNMP event	UMS_PowerSupplyCritical	UMS_PowerSupplyWarning	UMS_PowerSupplyNormal


## IBMPSG\_ProcessorPFEvent CIM indication

This CIM indication is generated when the state of a system processor changes with respect to its availability.

<b>End consumer</b>	<b>Critical severity</b>	<b>Warning severity</b>	<b>Normal severity</b>
IBM Director event	CIM > System > Processor PFA	Not applicable	CIM > System > Processor PFA
IBM Director Console (Group Contents pane)	 Processor Event	Not applicable	No symbol displayed
Microsoft Operations Manager 2005 alert	Processor Event	Processor Event	Processor Event
Microsoft SMS native events (Message ID 50180)	IBM_UMS_AGENT_PROCESSORPF_ERROR_	IBM_UMS_AGENT_PROCESSORPF_WARNING_	IBM_UMS_AGENT_PROCESSORPF_INFO_
Microsoft Windows event log event ID	18	Not applicable	18
SNMP	ibmSystemTrapProcessorPF	Not applicable	ibmSystemTrapProcessorPF
Tivoli Enterprise Console native event	IBMPSG_ProcessorPFEvent	IBMPSG_ProcessorPFEvent	IBMPSG_ProcessorPFEvent
Tivoli Enterprise Console SNMP event	UMS_ProcessorPFCritical	UMS_ProcessorPFWarning	UMS_ProcessorPFNormal

## IBMPSG\_RedundantNetworkAdapterEvent CIM indication

This CIM indication is generated when the state of a system network interface card (NIC) changes with respect to its redundancy. There are certain limitations of the NIC that cannot be compensated for between a switchover and a switchback.

End consumer	Critical severity	Warning severity	Normal severity
IBM Director event	Not applicable	Not applicable	Not applicable
IBM Director Console (Group Contents pane)	Not applicable		No symbol displayed
Microsoft Operations Manager 2005 alert	Network Event	Network Event	Network Event
Microsoft SMS native events (Message ID 50150)	IBM_UMS_AGENT_REDUNDANTNETWORK_ADAPTER_ERROR_	IBM_UMS_AGENT_REDUNDANTNETWORK_ADAPTER_WARNING_	IBM_UMS_AGENT_REDUNDANTNETWORK_ADAPTER_INFO_
Microsoft Windows event log event ID	Not applicable	15	Not applicable
SNMP	Not applicable	ibmSystemTrapRedundantNIC	Not applicable
Tivoli Enterprise Console native event	Not applicable	IBMPSG_RedundantNetworkAdapterEvent	Not applicable
Tivoli Enterprise Console SNMP event	Not applicable	UMS_RedundantNetworkAdapterEvent	Not applicable

## IBMPSG\_RedundantNetworkAdapterSwitchbackEvent CIM indication


This CIM indication is generated when the primary network interface card (NIC) is restored in a teamed NIC configuration.

<b>End consumer</b>	<b>Critical severity</b>	<b>Warning severity</b>	<b>Normal severity</b>
IBM Director event	Not applicable	Not applicable	CIM > System > Redundant Network Adapter Switchback
IBM Director Console (Group Contents pane)	Not applicable	Not applicable	No symbol displayed
Microsoft Operations Manager 2005 alert	Network Event	Network Event	Network Event
Microsoft SMS native events (Message ID 50170)	IBM_UMS_AGENT_REDUNDANTNETWORK_ADAPTERSWITCHBACK_ERROR_	IBM_UMS_AGENT_REDUNDANTNETWORK_ADAPTERSWITCHBACK_WARNING_	IBM_UMS_AGENT_REDUNDANTNETWORK_ADAPTERSWITCHBACK_INFO_
Microsoft Windows event log event ID	Not applicable	Not applicable	17
SNMP	Not applicable	Not applicable	ibmSystemTrapRedundantNICSwitchback
Tivoli Enterprise Console native event	Not applicable	Not applicable	IBMPSG_RedundantNetworkAdapterSwitchbackEvent
Tivoli Enterprise Console SNMP event	Not applicable	Not applicable	UMS_RedundantNetworkAdapterSwitchback

## **IBMPSG\_RedundantNetworkAdaptersSwitchoverEvent CIM indication**

This CIM indication is generated when the primary network interface card (NIC) fails in a teamed NIC configuration and the standby NIC becomes the active NIC.

<b>End consumer</b>	<b>Critical severity</b>	<b>Warning severity</b>	<b>Normal severity</b>
IBM Director event	Not applicable	CIM > System > Redundant Network Adapter Switchover	Not applicable

<b>End consumer</b>	<b>Critical severity</b>	<b>Warning severity</b>	<b>Normal severity</b>
IBM Director Console (Group Contents pane)	Not applicable	 Network Event	Not applicable
Microsoft Operations Manager 2005 alert	Network Event	Network Event	Network Event
Microsoft SMS native events (Message ID 50160)	IBM_UMS_AGENT_REDUNDANTNETWORK ADAPTERSWITCHOVER_ERROR_	IBM_UMS_AGENT_REDUNDANTNETWORK ADAPTERSWITCHOVER_WARNING_	IBM_UMS_AGENT_REDUNDANTNETWORK ADAPTERSWITCHOVER_INFO_
Microsoft Windows event log event ID	Not applicable	16	Not applicable
SNMP	Not applicable	ibmSystemTrapRedundantNICSwitchover	Not applicable
Tivoli Enterprise Console native event	Not applicable	IBMPSG_RedundantNetworkAdapterSwitchoverEvent	Not applicable
Tivoli Enterprise Console SNMP event	Not applicable	UMS_RedundantNetworkAdapterSwitchover	Not applicable

## IBMPSG\_RemoteloginEvent CIM indication

This CIM indication is generated when an end-user or application has logged in to the Web interface of the Remote Supervisor Adapter.

<b>End consumer</b>	<b>Critical severity</b>	<b>Warning severity</b>	<b>Normal severity</b>
IBM Director event	Not applicable	CIM > System > Remote Login	Not applicable
IBM Director Console (Group Contents pane)	Not applicable	Not applicable	Not applicable
Microsoft Operations Manager 2005 alert	Security Event	Security Event	Security Event



<b>End consumer</b>	<b>Critical severity</b>	<b>Warning severity</b>	<b>Normal severity</b>
Microsoft SMS native events (Message ID 50250)	IBM_UMS_AGENT_REMOTELOGIN_ERROR_	IBM_UMS_AGENT_REMOTELOGIN_WARNING_	IBM_UMS_AGENT_REMOTELOGIN_INFO_
Microsoft Windows event log event ID	Not applicable	25	Not applicable
SNMP	Not applicable	ibmSystemTrapRemotelogin	Not applicable
Tivoli Enterprise Console native event	Not applicable	IBMPSSG_RemoteloginEvent	Not applicable
Tivoli Enterprise Console SNMP event	Not applicable	UMS_RemoteloginEvent	Not applicable

## **IBMPSSG\_ServerRAIDArrayFlashCopyComplete CIM indication**

This CIM indication is generated when a ServerRAID FlashCopy operation is completed on a specified array in a ServerRAID configuration.

<b>End consumer</b>	<b>Normal severity</b>
IBM Director event	CIM > System > ServerRAID Array FlashCopy Complete
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_INFO
Microsoft Windows event log event ID	20
SNMP	ibmServerRAIDArrayFlashCopyComplete
Tivoli Enterprise Console native event	IBMPSSG_ServerRAIDArrayFlashCopyComplete
Tivoli Enterprise Console SNMP event	ServerRAID_ArrayFlashCopyComplete

## IBMP5G\_ServerRAIDArrayFlashCopyDetected CIM indication

This CIM indication is generated when a ServeRAID FlashCopy operation is in progress on a specified array in a ServeRAID configuration.

End consumer	Normal severity
IBM Director event	CIM > System > ServeRAID Array FlashCopy Detected
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_INFO
Microsoft Windows event log event ID	20
SNMP	iBM ServeRAID Array FlashCopy Detected
Tivoli Enterprise Console native event	IBMP5G_ServerRAID Array FlashCopy Detected
Tivoli Enterprise Console SNMP event	ServeRAID_ArrayFlashCopyDetected

## IBMP5G\_ServerRAIDArrayFlashCopyFail CIM indication

This CIM indication is generated when a ServeRAID FlashCopy operation fails on a specified array in a ServeRAID configuration.

End consumer	Critical severity
IBM Director event	CIM > System > ServeRAID Array FlashCopy Fail
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_ERROR
Microsoft Windows event log event ID	20
SNMP	iBM ServeRAID Array FlashCopy Fail
Tivoli Enterprise Console native event	IBMP5G_ServerRAID Array FlashCopy Fail
Tivoli Enterprise Console SNMP event	ServeRAID_ArrayFlashCopyFail

---

## IBMP5G\_ServerRAIDArrayRebuildComplete CIM indication

This CIM indication is generated when a ServeRAID rebuild operation is completed on a specified array in a ServeRAID configuration.

End consumer	Normal severity
IBM Director event	CIM > System > ServeRAID Array Rebuild Complete
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGEERAIDHEALTH_INFO
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDArrayRebuildComplete
Tivoli Enterprise Console native event	IBMP5G_ServerRAIDArrayRebuildComplete
Tivoli Enterprise Console SNMP event	ServeRAID_ArrayRebuildComplete

---

## IBMP5G\_ServerRAIDArrayRebuildDetected CIM indication

This CIM indication is generated when a ServeRAID rebuild operation is in progress on a specified array in a ServeRAID configuration.

End consumer	Normal severity
IBM Director event	CIM > System > ServeRAID Array Rebuild Detected
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGEERAIDHEALTH_INFO
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDArrayRebuildDetected
Tivoli Enterprise Console native event	IBMP5G_ServerRAIDArrayRebuildDetected

<b>End consumer</b>	<b>Normal severity</b>
Tivoli Enterprise Console SNMP event	ServerRAID_ArrayRebuildDetected

## **IBMPSG\_ServerRAIDArrayRebuildFail CIM indication**

This CIM indication is generated when a ServerRAID rebuild operation fails on a specified array in a ServerRAID configuration.

<b>End consumer</b>	<b>Critical severity</b>
IBM Director event	CIM > System > ServerRAID Array Rebuild Fail
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_ERROR
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDArrayRebuildFail
Tivoli Enterprise Console native event	IBMPSG_ServerRAIDArrayRebuildFail
Tivoli Enterprise Console SNMP event	ServerRAID_ArrayRebuildFail

## **IBMPSG\_ServerRAIDArraySyncComplete CIM indication**

This CIM indication is generated when a ServerRAID synchronization operation is completed on a specified array in a ServerRAID configuration.

<b>End consumer</b>	<b>Normal severity</b>
IBM Director event	CIM > System > ServerRAID Array Sync Complete
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_INFO
Microsoft Windows event log event ID	20

<b>End consumer</b>	<b>Normal severity</b>
SNMP	iBMServerRAIDArraySyncnComplete
Tivoli Enterprise Console native event	IBMPMSG_ServerRAIDArraySyncnComplete
Tivoli Enterprise Console SNMP event	ServerRAID_ArraySyncnComplete

## **IBMPMSG\_ServerRAIDArraysyncDetected CIM indication**

This CIM indication is generated when a ServeRAID synchronization operation is in progress on a specified array in a ServeRAID configuration.

<b>End consumer</b>	<b>Normal severity</b>
IBM Director event	CIM > System > ServeRAID Array Sync Detected
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_INFO
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDArraySyncnDetected
Tivoli Enterprise Console native event	IBMPMSG_ServerRAIDArraySyncnDetected
Tivoli Enterprise Console SNMP event	ServerRAID_ArraySyncnDetected

## **IBMPMSG\_ServerRAIDArraysyncFail CIM indication**

This CIM indication is generated when a ServeRAID synchronization operation fails on a specified array in a ServeRAID configuration.

<b>End consumer</b>	<b>Critical severity</b>
IBM Director event	CIM > System > ServeRAID Array Sync Fail
Microsoft Operations Manager 2005 alert	Storage Event

<b>End consumer</b>	<b>Critical severity</b>
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_ERROR
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDArraySyncFail
Tivoli Enterprise Console native event	IBMPMSG_ServerRAIDArraySyncFail
Tivoli Enterprise Console SNMP event	ServerRAID_ArraySyncFail

## **IBMPMSG\_ServerRAIDCompactionComplete CIM indication**

This CIM indication is generated when a ServerRAID compaction operation is completed on a specified logical drive in a ServerRAID configuration.

<b>End consumer</b>	<b>Normal severity</b>
IBM Director event	CIM > System > ServerRAID Compaction Complete
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_INFO
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDCompactionComplete
Tivoli Enterprise Console native event	IBMPMSG_ServerRAIDCompactionComplete
Tivoli Enterprise Console SNMP event	ServerRAID_CompactionComplete

## **IBMPMSG\_ServerRAIDCompactionDetected CIM indication**

This CIM indication is generated when a ServerRAID compaction operation is in progress on a specified logical drive in a ServerRAID configuration.

<b>End consumer</b>	<b>Normal severity</b>
IBM Director event	CIM > System > ServerRAID Compaction Detected
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_INFO
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDCompactionDetected
Tivoli Enterprise Console native event	IBMPMSG_ServerRAIDCompactionDetected
Tivoli Enterprise Console SNMP event	ServerRAID_CompactionDetected

## **IBMPMSG\_ServerRAIDCompactionFail CIM indication**

This CIM indication is generated when a ServerRAID compaction operation fails on a specified logical drive in a ServerRAID configuration.

<b>End consumer</b>	<b>Critical severity</b>
IBM Director event	CIM > System > ServerRAID Compaction Fail
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_ERROR
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDCompactionFail
Tivoli Enterprise Console native event	IBMPMSG_ServerRAIDCompactionFail
Tivoli Enterprise Console SNMP event	ServerRAID_CompactionFail

## IBMPSG\_ServerRAIDCompressionComplete CIM indication

This CIM indication is generated when a ServeRAID compression operation is completed on a specified logical drive in a ServeRAID configuration.

End consumer	Normal severity
IBM Director event	CIM > System > ServeRAID Compression Complete
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGERAIDHEALTH_INFO
Microsoft Windows event log event ID	20
SNMP	iBMServeRAIDCompressionComplete
Tivoli Enterprise Console native event	IBMPSG_ServerRAIDCompressionComplete
Tivoli Enterprise Console SNMP event	ServeRAID_CompressionComplete

## IBMPSG\_ServerRAIDCompressionDetected CIM indication

This CIM indication is generated when a ServeRAID compression operation is in progress on a specified logical drive in a ServeRAID configuration.

End consumer	Normal severity
IBM Director event	CIM > System > ServeRAID Compression Detected
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGERAIDHEALTH_INFO
Microsoft Windows event log event ID	20
SNMP	iBMServeRAIDCompressionDetected
Tivoli Enterprise Console native event	IBMPSG_ServerRAIDCompressionDetected
Tivoli Enterprise Console SNMP event	ServeRAID_CompressionDetected



---

## IBMP5G\_ServerRAIDCompressionFail CIM indication

This CIM indication is generated when a ServeRAID compression operation fails on a specified logical drive in a ServeRAID configuration.

<b>End consumer</b>	<b>Critical severity</b>
IBM Director event	CIM > System > ServeRAID Compression Fail
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_ERROR
Microsoft Windows event log event ID	20
SNMP	iBM ServeRAIDCompressionFail
Tivoli Enterprise Console native event	IBMP5G_ServerRAIDCompressionFail
Tivoli Enterprise Console SNMP event	ServeRAID_CompressionFail

---

## IBMP5G\_ServerRAIDConfigFail CIM indication

This CIM indication is generated when a ServeRAID controller configuration cannot be read.

<b>End consumer</b>	<b>Critical severity</b>
IBM Director event	CIM > System > ServeRAID Config Fail
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_ERROR
Microsoft Windows event log event ID	20
SNMP	iBM ServeRAIDConfigFail
Tivoli Enterprise Console native event	IBMP5G_ServerRAIDConfigFail

<b>End consumer</b>	<b>Critical severity</b>
Tivoli Enterprise Console SNMP event	ServerRAID_ConfigFail

## IBMP5G\_ServerRAIDControllerAdded CIM indication

This CIM indication is generated when a specified ServerRAID controller is added to a system.

<b>End consumer</b>	<b>Normal severity</b>
IBM Director event	CIM > System > ServerRAID Controller Added
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_INFO
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDControllerAdded
Tivoli Enterprise Console native event	IBMP5G_ServerRAIDControllerAdded
Tivoli Enterprise Console SNMP event	ServerRAID_ControllerAdded

## IBMP5G\_ServerRAIDControllerBadStripes CIM indication

This CIM indication is generated when one or more logical drives contain at least one bad stripe.

<b>End consumer</b>	<b>Warning severity</b>
IBM Director event	CIM > System > ServerRAID Controller Bad Stripes
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_WARNING
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDControllerBadStripes

<b>End consumer</b>	<b>Warning severity</b>
Tivoli Enterprise Console native event	IBMPSG_ServerRAIDControllerBadStripes
Tivoli Enterprise Console SNMP event	ServerRAID_ControllerBadStripes

## **IBMPSG\_ServerRAIDControllerBatteryOvertemp CIM indication**

This CIM indication is generated when the battery on a specified ServerRAID controller has exceeded its temperature threshold.

<b>End consumer</b>	<b>Warning severity</b>
IBM Director event	CIM > System > ServerRAID Controller Battery Overtemp
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_WARNING
Microsoft Windows event log event ID SNMP	20 iBMServerRAIDControllerBatteryOvertemp
Tivoli Enterprise Console native event	IBMPSG_ServerRAIDControllerBatteryOvertemp
Tivoli Enterprise Console SNMP event	ServerRAID_ControllerBatteryOvertemp

## **IBMPSG\_ServerRAIDControllerBatteryTempNormal CIM indication**

This CIM indication is generated when the battery on a specified ServerRAID controller has a normal temperature.

<b>End consumer</b>	<b>Normal severity</b>
IBM Director event	CIM > System > ServerRAID Controller Battery Temp Normal
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_INFO
Microsoft Windows event log event ID	20

<b>End consumer</b>	<b>Normal severity</b>
SNMP	iBMServeRAIDControllerBatteryTempNormal
Tivoli Enterprise Console native event	IBMPMSG_ServerRAIDControllerBatteryTempNormal
Tivoli Enterprise Console SNMP event	ServeRAID_ControllerBatteryTempNormal

## IBMPMSG\_ServerRAIDControllerFail CIM indication

This CIM indication is generated when a specified ServeRAID controller fails.

<b>End consumer</b>	<b>Critical severity</b>
IBM Director event	CIM > System > ServeRAID Controller Fail
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGERAIDHEALTH_ERROR
Microsoft Windows event log event ID	20
SNMP	iBMServeRAIDControllerFail
Tivoli Enterprise Console native event	IBMPMSG_ServerRAIDControllerFail
Tivoli Enterprise Console SNMP event	ServeRAID_ControllerFail

## IBMPMSG\_ServerRAIDControllerFailover CIM indication

This CIM indication is generated when a specified ServeRAID controller fails over and the passive controller in the failover pairing is now active.

<b>End consumer</b>	<b>Normal severity</b>
IBM Director event	CIM > System > ServeRAID Controller Failover
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGERAIDHEALTH_INFO

<b>End consumer</b>	<b>Normal severity</b>
Microsoft Windows event log event ID	20
SNMP	iBMServeRAIDControllerFailover
Tivoli Enterprise Console native event	IBMPMSG_ServerRAIDControllerFailover
Tivoli Enterprise Console SNMP event	ServeRAID_ControllerFailover

## **IBMPMSG\_ServerRAIDControllerMismatchedVersions CIM indication**

This CIM indication is generated when the versions of the BIOS, firmware, and driver for a specified ServeRAID controller do not match.

<b>End consumer</b>	<b>Warning severity</b>
IBM Director event	CIM > System > ServeRAID Controller Mismatched Versions
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_WARNING
Microsoft Windows event log event ID	20
SNMP	iBMServeRAIDVersionMismatched
Tivoli Enterprise Console native event	IBMPMSG_ServerRAIDControllerMismatchedVersions
Tivoli Enterprise Console SNMP event	ServeRAID_ControllerMismatchedVersions

## **IBMPMSG\_ServerRAIDControllerReplaced CIM indication**

This CIM indication is generated when a specified controller is replaced in a ServeRAID configuration.

<b>End consumer</b>	<b>Normal severity</b>
IBM Director event	CIM > System > ServeRAID Controller Replaced
Microsoft Operations Manager 2005 alert	Storage Event

<b>End consumer</b>	<b>Normal severity</b>
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_INFO
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDControllerReplaced
Tivoli Enterprise Console native event	IBMPSG_ServerRAIDControllerReplaced
Tivoli Enterprise Console SNMP event	ServerRAID_ControllerReplaced

## **IBMPSG\_ServerRAIDCopyBackComplete CIM indication**

This CIM indication is generated when a copy-back operation is completed on a specified logical drive in a ServerRAID configuration.

<b>End consumer</b>	<b>Normal severity</b>
IBM Director event	CIM > System > ServerRAID CopyBack Complete
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_INFO
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDCopyBackComplete
Tivoli Enterprise Console native event	IBMPSG_ServerRAIDCopyBackComplete
Tivoli Enterprise Console SNMP event	ServerRAID_CopyBackComplete

## **IBMPSG\_ServerRAIDCopyBackDetected CIM indication**

This CIM indication is generated when a copy-back operation is in progress on a specified logical drive in a ServerRAID configuration.

<b>End consumer</b>	<b>Normal severity</b>
IBM Director event	CIM > System > ServerRAID CopyBack Detected
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_INFO
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDCopyBackDetected
Tivoli Enterprise Console native event	IBMPMSG_ServerRAIDCopyBackDetected
Tivoli Enterprise Console SNMP event	ServerRAID_CopyBackDetected

## **IBMPMSG\_ServerRAIDCopyBackFail CIM indication**

This CIM indication is generated when a copy-back operation fails on a specified logical drive in a ServerRAID configuration.

<b>End consumer</b>	<b>Critical severity</b>
IBM Director event	CIM > System > ServerRAID CopyBack Fail
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_ERROR
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDCopyBackFail
Tivoli Enterprise Console native event	IBMPMSG_ServerRAIDCopyBackFail
Tivoli Enterprise Console SNMP event	ServerRAID_CopyBackFail

## **IBMPMSG\_ServerRAIDDeadBattery CIM indication**

This CIM indication is generated when the battery fails on a specified controller.

<b>End consumer</b>	<b>Critical severity</b>
IBM Director event	CIM > System > ServerRAID Dead Battery
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGERAIDHEALTH_ERROR
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDDeadBattery
Tivoli Enterprise Console native event	IBMP5G_ServerRAIDDeadBattery
Tivoli Enterprise Console SNMP event	ServerRAID_DeadBattery

## **IBMP5G\_ServerRAIDDeadBatteryCache CIM indication**

This CIM indication is generated when the battery-backup cache fails on a specified controller.

<b>End consumer</b>	<b>Critical severity</b>
IBM Director event	CIM > System > ServerRAID Dead Battery Cache
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGERAIDHEALTH_ERROR
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDDeadBatteryCache
Tivoli Enterprise Console native event	IBMP5G_ServerRAIDDeadBatteryCache
Tivoli Enterprise Console SNMP event	ServerRAID_DeadBatteryCache

## **IBMP5G\_ServerRAIDDecompressionComplete CIM indication**

This CIM indication is generated when a ServerRAID decompression operation is completed on a specified logical drive in a ServeRAID configuration.



<b>End consumer</b>	<b>Normal severity</b>
IBM Director event	CIM > System > ServeRAID Decompression Complete
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_INFO
Microsoft Windows event log event ID	20
SNMP	iBM ServeRAID Decompression Complete
Tivoli Enterprise Console native event	IBMPMSG_ServeRAID Decompression Complete
Tivoli Enterprise Console SNMP event	ServeRAID_Decompression Complete

## **IBMPMSG\_ServerRAIDDecompressionDetected CIM indication**

This CIM indication is generated when a ServeRAID decompression operation is in progress on a specified logical drive in a ServeRAID configuration.

<b>End consumer</b>	<b>Normal severity</b>
IBM Director event	CIM > System > ServeRAID Decompression Detected
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_INFO
Microsoft Windows event log event ID	20
SNMP	iBM ServeRAID Decompression Detected
Tivoli Enterprise Console native event	IBMPMSG_ServeRAID Decompression Detected
Tivoli Enterprise Console SNMP event	ServeRAID_Decompression Detected

## IBMPSG\_ServerRAIDDecompressionFail CIM indication

This CIM indication is generated when a ServerRAID decompression operation fails on a specified logical drive in a ServerRAID configuration.

End consumer	Critical severity
IBM Director event	CIM > System > ServerRAID Decompression Fail
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_ERROR
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDDecompressionFail
Tivoli Enterprise Console native event	IBMPSG_ServerRAIDDecompressionFail
Tivoli Enterprise Console SNMP event	ServerRAID_DecompressionFail

## IBMPSG\_ServerRAIDDefunctDrive CIM indication

This CIM indication is generated when a specified hard disk drive fails in a ServerRAID configuration.

End consumer	Critical severity
IBM Director event	CIM > System > ServerRAID Defunct Drive
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_ERROR
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDDefunctDrive
Tivoli Enterprise Console native event	IBMPSG_ServerRAIDDefunctDrive
Tivoli Enterprise Console SNMP event	ServerRAID_DefunctDrive

## IBMPSG\_ServerRAIDDefunctDriveFRU CIM indication

This CIM indication is generated when a specified hard disk drive with the provided field-replaceable unit (FRU) number fails in a ServeRAID configuration.

End consumer	Critical severity
IBM Director event	CIM > System > ServeRAID Defunct Drive FRU
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_ERROR
Microsoft Windows event log event ID	20
SNMP	iBMServeRAIDDefunctDriveFRU
Tivoli Enterprise Console native event	IBMPSG_ServerRAIDDefunctDriveFRU
Tivoli Enterprise Console SNMP event	ServeRAID_DefunctDriveFRU

## IBMPSG\_ServerRAIDDefunctReplaced CIM indication

This CIM indication is generated when a specified defunct hard disk drive has been set to the hot-spare state in a ServeRAID configuration.

End consumer	Normal severity
IBM Director event	CIM > System > ServeRAID Defunct Replaced
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_INFO
Microsoft Windows event log event ID	20
SNMP	iBMServeRAIDDefunctReplaced
Tivoli Enterprise Console native event	IBMPSG_ServerRAIDDefunctReplaced
Tivoli Enterprise Console SNMP event	ServeRAID_DefunctReplaced

## IBMPSG\_ServerRAIDDriveAdded CIM indication

This CIM indication is generated when a specified hard disk drive is added to a ServerRAID configuration.

End consumer	Normal severity
IBM Director event	CIM > System > ServerRAID Drive Added
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_INFO
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDDriveAdded
Tivoli Enterprise Console native event	IBMPSG_ServerRAIDDriveAdded
Tivoli Enterprise Console SNMP event	ServerRAID_DriveAdded

## IBMPSG\_ServerRAIDDriveClearComplete CIM indication

This CIM indication is generated when a ServerRAID clear operation is completed on a specified hard disk drive in a ServerRAID configuration.

End consumer	Normal severity
IBM Director event	CIM > System > ServerRAID Drive Clear Complete
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_INFO
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDDriveClearComplete
Tivoli Enterprise Console native event	IBMPSG_ServerRAIDDriveClearComplete

<b>End consumer</b>	<b>Normal severity</b>
Tivoli Enterprise Console SNMP event	ServerRAID_DriveClearComplete

## IBMPSG\_ServerRAIDDriveClearDetected CIM indication

This CIM indication is generated when a ServerRAID clear operation is in progress on a specified hard disk drive in a ServerRAID configuration.

<b>End consumer</b>	<b>Normal severity</b>
IBM Director event	CIM > System > ServerRAID Drive Clear Detected
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_INFO
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDDriveClearDetected
Tivoli Enterprise Console native event	IBMPSG_ServerRAIDDriveClearDetected
Tivoli Enterprise Console SNMP event	ServerRAID_DriveClearDetected

## IBMPSG\_ServerRAIDDriveClearFail CIM indication

This CIM indication is generated when a ServerRAID clear operation fails on a specified hard disk drive in a ServerRAID configuration.

<b>End consumer</b>	<b>Critical severity</b>
IBM Director event	CIM > System > ServerRAID Drive Clear Fail
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_ERROR
Microsoft Windows event log event ID	20

<b>End consumer</b>	<b>Critical severity</b>
SNMP	iBMServeRAIDDriveClearFail
Tivoli Enterprise Console native event	IBMP5G_ServerRAIDDriveClearFail
Tivoli Enterprise Console SNMP event	ServerRAID_DriveClearFail

## **IBMP5G\_ServerRAIDDriveRemoved CIM indication**

This CIM indication is generated when a specified hard disk drive is removed from a ServeRAID configuration.

<b>End consumer</b>	<b>Normal severity</b>
IBM Director event	CIM > System > ServeRAID Drive Removed
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGERAIDHEALTH_INFO
Microsoft Windows event log event ID	20
SNMP	iBMServeRAIDDriveRemoved
Tivoli Enterprise Console native event	IBMP5G_ServerRAIDDriveRemoved
Tivoli Enterprise Console SNMP event	ServerRAID_DriveRemoved

## **IBMP5G\_ServerRAIDDriveVerifyComplete CIM indication**

This CIM indication is generated when a ServeRAID verify operation is completed on a specified hard disk drive in a ServeRAID configuration.

<b>End consumer</b>	<b>Normal severity</b>
IBM Director event	CIM > System > ServeRAID Drive Verify Complete
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGERAIDHEALTH_INFO

<b>End consumer</b>	<b>Normal severity</b>
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDDriveVerifyComplete
Tivoli Enterprise Console native event	IBMPMSG_ServerRAIDDriveVerifyComplete
Tivoli Enterprise Console SNMP event	ServerRAID_DriveVerifyComplete

## **IBMPMSG\_ServerRAIDDriveVerifyDetected CIM indication**

This CIM indication is generated when a ServerRAID verify operation is in progress on a specified hard disk drive in a ServerRAID configuration.

<b>End consumer</b>	<b>Normal severity</b>
IBM Director event	CIM > System > ServerRAID Drive Verify Detected
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_INFO
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDDriveVerifyDetected
Tivoli Enterprise Console native event	IBMPMSG_ServerRAIDDriveVerifyDetected
Tivoli Enterprise Console SNMP event	ServerRAID_DriveVerifyDetected

## **IBMPMSG\_ServerRAIDDriveVerifyFail CIM indication**

This CIM indication is generated when a ServerRAID verify operation fails on a specified hard disk drive in a ServerRAID configuration.

<b>End consumer</b>	<b>Critical severity</b>
IBM Director event	CIM > System > ServerRAID Drive Verify Fail

<b>End consumer</b>	<b>Critical severity</b>
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_ERROR
Microsoft Windows event log event ID	20
SNMP	IBM ServeRAID Drive Verify Fail
Tivoli Enterprise Console native event	IBMPSG_ServerRAID Drive Verify Fail
Tivoli Enterprise Console SNMP event	ServerRAID_Drive Verify Fail

## **IBMPSG\_ServerRAIDEnclosureFail CIM indication**

This CIM indication is generated when an enclosure has failed on a specified controller and channel in a ServeRAID configuration.

<b>End consumer</b>	<b>Critical severity</b>
IBM Director event	CIM > System > ServeRAID Enclosure Fail
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_ERROR
Microsoft Windows event log event ID	20
SNMP	IBM ServeRAID Enclosure Fail
Tivoli Enterprise Console native event	IBMPSG_ServerRAID Enclosure Fail
Tivoli Enterprise Console SNMP event	ServerRAID_Enclosure Fail

## **IBMPSG\_ServerRAIDEnclosureFanFail CIM indication**

This CIM indication is generated when a specified enclosure fan fails on a specified controller and channel in a ServeRAID configuration.



<b>End consumer</b>	<b>Critical severity</b>
IBM Director event	CIM > System > ServerRAID Enclosure Fan Fail
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_ERROR
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDFanFail
Tivoli Enterprise Console native event	IBMPMSG_ServerRAIDEnclosureFanFail
Tivoli Enterprise Console SNMP event	ServerRAID_FanFail

## **IBMPMSG\_ServerRAIDEnclosureFanInstalled CIM indication**

This CIM indication is generated when a specified enclosure fan is installed on a specified controller and channel in a ServerRAID configuration.

<b>End consumer</b>	<b>Normal severity</b>
IBM Director event	CIM > System > ServerRAID Enclosure Fan Installed
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_INFO
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDFanInstalled
Tivoli Enterprise Console native event	IBMPMSG_ServerRAIDEnclosureFanInstalled
Tivoli Enterprise Console SNMP event	ServerRAID_FanInstalled

## IBMPSG\_ServerRAIDEnclosureFanOK CIM indication

This CIM indication is generated when a specified enclosure fan is functioning correctly on a specified controller and channel in a ServeRAID configuration.

End consumer	Normal severity
IBM Director event	CIM > System > ServeRAID Enclosure Fan OK
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_INFO
Microsoft Windows event log event ID	20
SNMP	iBMServeRAIDEnclosureFanOK
Tivoli Enterprise Console native event	IBMPSG_ServerRAIDEnclosureFanOK
Tivoli Enterprise Console SNMP event	ServeRAID_EnclosureFanOK

## IBMPSG\_ServerRAIDEnclosureFanRemoved CIM indication

This CIM indication is generated when a specified enclosure fan is removed on a specified controller and channel in a ServeRAID configuration.

End consumer	Warning severity
IBM Director event	CIM > System > ServeRAID Enclosure Fan Removed
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_WARNING
Microsoft Windows event log event ID	20
SNMP	iBMServeRAIDFanRemoved
Tivoli Enterprise Console native event	IBMPSG_ServerRAIDEnclosureFanRemoved
Tivoli Enterprise Console SNMP event	ServeRAID_FanRemoved

---

## IBMP5G\_ServerRAIDEnclosureOK CIM indication

This CIM indication is generated when a specified enclosure fan is functioning correctly on a specified controller and channel in a ServeRAID configuration.

<b>End consumer</b>	<b>Normal severity</b>
IBM Director event	CIM > System > ServeRAID Enclosure OK
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_INFO
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDEnclosureOK
Tivoli Enterprise Console native event	IBMP5G_ServerRAIDEnclosureOK
Tivoli Enterprise Console SNMP event	ServeRAID_EnclosureOK

---

## IBMP5G\_ServerRAIDEnclosurePowerSupplyFail CIM indication

This CIM indication is generated when the specified enclosure power supply fails in a ServeRAID configuration.

<b>End consumer</b>	<b>Critical severity</b>
IBM Director event	CIM > System > ServeRAID Enclosure Power Supply Fail
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_ERROR
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDPowerSupplyFail
Tivoli Enterprise Console native event	IBMP5G_ServerRAIDEnclosurePowerSupplyFail

<b>End consumer</b>	<b>Critical severity</b>
Tivoli Enterprise Console SNMP event	ServerRAID_PowerSupplyFail

## IBMPSG\_ServerRAIDEnclosurePowerSupplyInstalled CIM indication

This CIM indication is generated when a specified enclosure power supply is installed in a ServerRAID configuration.

<b>End consumer</b>	<b>Normal severity</b>
IBM Director event	CIM > System > ServerRAID Enclosure Power Supply Installed
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_INFO
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDPowerSupplyInstalled
Tivoli Enterprise Console native event	IBMPSG_ServerRAIDEnclosurePowerSupplyInstalled
Tivoli Enterprise Console SNMP event	ServerRAID_PowerSupplyInstalled

## IBMPSG\_ServerRAIDEnclosurePowerSupplyOK CIM indication

This CIM indication is generated when a specified enclosure power supply is functioning correctly in a ServerRAID configuration.

<b>End consumer</b>	<b>Normal severity</b>
IBM Director event	CIM > System > ServerRAID Enclosure Power Supply OK
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_INFO
Microsoft Windows event log event ID	20

<b>End consumer</b>	<b>Normal severity</b>
SNMP	iBMServerRAIDPowerSupplyOK
Tivoli Enterprise Console native event	IBMPMSG_ServerRAIDEnclosurePowerSupplyOK
Tivoli Enterprise Console SNMP event	ServerRAID_PowerSupplyOK

## **IBMPMSG\_ServerRAIDEnclosurePowerSupplyRemoved CIM indication**

This CIM indication is generated when a specified enclosure power supply is removed from a ServerRAID configuration.

<b>End consumer</b>	<b>Warning severity</b>
IBM Director event	CIM > System > ServerRAID Enclosure Power Supply Removed
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_WARNING
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDPowerSupplyRemoved
Tivoli Enterprise Console native event	IBMPMSG_ServerRAIDEnclosurePowerSupplyRemoved
Tivoli Enterprise Console SNMP event	ServerRAID_PowerSupplyRemoved

## **IBMPMSG\_ServerRAIDEnclosureTempFail CIM indication**

This CIM indication is generated when an enclosure temperature exceeds a normal range on a specified controller in a ServerRAID configuration.

<b>End consumer</b>	<b>Critical severity</b>
IBM Director event	CIM > System > ServerRAID Enclosure Temp Fail
Microsoft Operations Manager 2005 alert	Storage Event

<b>End consumer</b>	<b>Critical severity</b>
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_ERROR
Microsoft Windows event log event ID	20
SNMP	iBMServeRAIDTempFail
Tivoli Enterprise Console native event	IBMPMSG_ServerRAIDEnclosureTempFail
Tivoli Enterprise Console SNMP event	ServerRAID_TempFail

## **IBMPMSG\_ServerRAIDEnclosureTempOK CIM indication**

This CIM indication is generated when an enclosure temperature is within a normal range on a specified controller in a ServeRAID configuration.

<b>End consumer</b>	<b>Normal severity</b>
IBM Director event	CIM > System > ServeRAID Enclosure Temp OK
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_INFO
Microsoft Windows event log event ID	20
SNMP	iBMServeRAIDTempOK
Tivoli Enterprise Console native event	IBMPMSG_ServerRAIDEnclosureTempOK
Tivoli Enterprise Console SNMP event	ServerRAID_TempOK

## **IBMPMSG\_ServerRAIDExpansionComplete CIM indication**

This CIM indication is generated when a ServeRAID expansion operation is completed on a specified logical drive in a ServeRAID configuration.

<b>End consumer</b>	<b>Normal severity</b>
IBM Director event	CIM > System > ServerRAID Expansion Complete
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_INFO
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDExpansionComplete
Tivoli Enterprise Console native event	IBMPMSG_ServerRAIDExpansionComplete
Tivoli Enterprise Console SNMP event	ServerRAID_ExpansionComplete

## **IBMPMSG\_ServerRAIDExpansionDetected CIM indication**

This CIM indication is generated when a ServerRAID expansion operation is in progress on a specified logical drive in a ServerRAID configuration.

<b>End consumer</b>	<b>Normal severity</b>
IBM Director event	CIM > System > ServerRAID Expansion Detected
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_INFO
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDExpansionDetected
Tivoli Enterprise Console native event	IBMPMSG_ServerRAIDExpansionDetected
Tivoli Enterprise Console SNMP event	ServerRAID_ExpansionDetected

## IBMPSG\_ServerRAIDExpansionFail CIM indication

This CIM indication is generated when a ServeRAID expansion operation fails on a specified logical drive in a ServeRAID configuration.

End consumer	Critical severity
IBM Director event	CIM > System > ServeRAID Expansion Fail
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_ERROR
Microsoft Windows event log event ID	20
SNMP	iBMServeRAIDExpansionFail
Tivoli Enterprise Console native event	IBMPSG_ServerRAIDExpansionFail
Tivoli Enterprise Console SNMP event	ServeRAID_ExpansionFail

## IBMPSG\_ServerRAIDFlashCopyComplete CIM indication

This CIM indication is generated when a ServeRAID FlashCopy operation is completed on a specified logical drive in a ServeRAID configuration.

End consumer	Normal severity
IBM Director event	CIM > System > ServeRAID FlashCopy Complete
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_INFO
Microsoft Windows event log event ID	20
SNMP	iBMServeRAIDFlashCopyComplete
Tivoli Enterprise Console native event	IBMPSG_ServerRAIDFlashCopyComplete
Tivoli Enterprise Console SNMP event	ServeRAID_FlashCopyComplete



---

## IBMP5G\_ServerRAIDFlashCopyDetected CIM indication

This CIM indication is generated when a ServerRAID FlashCopy operation is in progress on a specified logical drive in a ServerRAID configuration.

End consumer	Normal severity
IBM Director event	CIM > System > ServerRAID FlashCopy Detected
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGEERRAIDHEALTH_INFO
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDFlashCopyDetected
Tivoli Enterprise Console native event	IBMP5G_ServerRAIDFlashCopyDetected
Tivoli Enterprise Console SNMP event	ServerRAID_FlashCopyDetected

---

## IBMP5G\_ServerRAIDFlashCopyFail CIM indication

This CIM indication is generated when a ServerRAID FlashCopy operation fails on a specified logical drive in a ServerRAID configuration.

End consumer	Critical severity
IBM Director event	CIM > System > ServerRAID FlashCopy Fail
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGEERRAIDHEALTH_ERROR
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDFlashCopyFail
Tivoli Enterprise Console native event	IBMP5G_ServerRAIDFlashCopyFail

<b>End consumer</b>	<b>Critical severity</b>
Tivoli Enterprise Console SNMP event	ServerRAID_FlashCopyFail

## IBMPSG\_ServerRAIDInitComplete CIM indication

This CIM indication is generated when a ServerRAID initialization operation is completed on a specified logical drive in a ServerRAID configuration.

<b>End consumer</b>	<b>Normal severity</b>
IBM Director event	CIM > System > ServerRAID Init Complete
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_INFO
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDInitComplete
Tivoli Enterprise Console native event	IBMPSG_ServerRAIDInitComplete
Tivoli Enterprise Console SNMP event	ServerRAID_InitComplete

## IBMPSG\_ServerRAIDInitDetected CIM indication

This CIM indication is generated when a ServerRAID initialization operation is in progress on a specified logical drive in a ServerRAID configuration.

<b>End consumer</b>	<b>Normal severity</b>
IBM Director event	CIM > System > ServerRAID Init Detected
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_INFO
Microsoft Windows event log event ID	20

<b>End consumer</b>	<b>Normal severity</b>
SNMP	iBMServerRAIDInitDetected
Tivoli Enterprise Console native event	IBMPMSG_ServerRAIDInitDetected
Tivoli Enterprise Console SNMP event	ServerRAID_InitDetected

## **IBMPMSG\_ServerRAIDInitFail CIM indication**

This CIM indication is generated when a ServerRAID initialization operation fails on a specified logical drive in a ServerRAID configuration.

<b>End consumer</b>	<b>Critical severity</b>
IBM Director event	CIM > System > ServerRAID Init Fail
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_ERROR
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDInitFail
Tivoli Enterprise Console native event	IBMPMSG_ServerRAIDInitFail
Tivoli Enterprise Console SNMP event	ServerRAID_InitFail

## **IBMPMSG\_ServerRAIDLogicalDriveAdded CIM indication**

This CIM indication is generated when a specified logical drive is added in a ServerRAID configuration.

<b>End consumer</b>	<b>Normal severity</b>
IBM Director event	CIM > System > ServerRAID Logical Drive Added
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_INFO

<b>End consumer</b>	<b>Normal severity</b>
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDLogicalDriveAdded
Tivoli Enterprise Console native event	IBMPMSG_ServerRAIDLogicalDriveAdded
Tivoli Enterprise Console SNMP event	ServerRAID_DriveAdded

## **IBMPMSG\_ServerRAIDLogicalDriveBlocked CIM indication**

This CIM indication is generated when a specified logical drive is in the blocked state.

<b>End consumer</b>	<b>Critical severity</b>
IBM Director event	CIM > System > ServerRAID Logical Drive Blocked
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_ERROR
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDLogicalDriveBlocked
Tivoli Enterprise Console native event	IBMPMSG_ServerRAIDLogicalDriveBlocked
Tivoli Enterprise Console SNMP event	ServerRAID_DriveBlocked

## **IBMPMSG\_ServerRAIDLogicalDriveCritical CIM indication**

This CIM indication is generated when a specified logical drive is in the critical state.

<b>End consumer</b>	<b>Warning severity</b>
IBM Director event	CIM > System > ServerRAID Logical Drive Critical
Microsoft Operations Manager 2005 alert	Storage Event

<b>End consumer</b>	<b>Warning severity</b>
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_WARNING
Microsoft Windows event log event ID	20
SNMP	iBMServeRAIDLogicalDriveCritical
Tivoli Enterprise Console native event	IBMPMSG_ServerRAIDLogicalDriveCritical
Tivoli Enterprise Console SNMP event	ServeRAID_DriveCritical

## **IBMPMSG\_ServerRAIDLogicalDriveCriticalPeriodic CIM indication**

This CIM indication is generated when a periodic scan detects that one or more logical drives are in a critical state.

<b>End consumer</b>	<b>Warning severity</b>
IBM Director event	CIM > System > ServeRAID Logical Drive Critical Periodic
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_WARNING
Microsoft Windows event log event ID	20
SNMP	iBMServeRAIDLogicalDriveCriticalPeriodic
Tivoli Enterprise Console native event	IBMPMSG_ServerRAIDLogicalDriveCriticalPeriodic
Tivoli Enterprise Console SNMP event	ServeRAID_DriveCriticalPeriodic

## **IBMPMSG\_ServerRAIDLogicalDriveOffline CIM indication**

This CIM indication is generated when a specified logical drive is in the offline state.

<b>End consumer</b>	<b>Critical severity</b>
IBM Director event	CIM > System > ServeRAID Logical Drive Off Line

<b>End consumer</b>	<b>Critical severity</b>
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_ERROR
Microsoft Windows event log event ID	20
SNMP	IBM ServeRAID Logical Drive Offline
Tivoli Enterprise Console native event	IBMPSG_ServerRAID Logical Drive Offline
Tivoli Enterprise Console SNMP event	ServerRAID_DriveOffline

## **IBMPSG\_ServerRAID Logical Drive OK CIM indication**

This CIM indication is generated when a specified logical drive is functioning correctly.

<b>End consumer</b>	<b>Normal severity</b>
IBM Director event	CIM > System > ServerRAID Logical Drive OK
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_INFO
Microsoft Windows event log event ID	20
SNMP	IBM ServeRAID Logical Drive OK
Tivoli Enterprise Console native event	IBMPSG_ServerRAID Logical Drive OK
Tivoli Enterprise Console SNMP event	ServerRAID_DriveOK

## **IBMPSG\_ServerRAID Logical Drive Removed CIM indication**

This CIM indication is generated when a specified logical drive has been removed from a ServerRAID configuration.

<b>End consumer</b>	<b>Normal severity</b>
IBM Director event	CIM > System > ServerRAID Logical Drive Removed
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGERAIDHEALTH_INFO
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDLogicalDriveRemoved
Tivoli Enterprise Console native event	IBMPSG_ServerRAIDLogicalDriveRemoved
Tivoli Enterprise Console SNMP event	ServerRAID_DriveRemoved

## **IBMPSG\_ServerRAIDLogicalDriveUnblocked CIM indication**

This CIM indication is generated when a specified logical drive is in the unblocked state.

<b>End consumer</b>	<b>Normal severity</b>
IBM Director event	CIM > System > ServerRAID Logical Drive Unblocked
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGERAIDHEALTH_INFO
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDLogicalDriveUnblocked
Tivoli Enterprise Console native event	IBMPSG_ServerRAIDLogicalDriveUnblocked
Tivoli Enterprise Console SNMP event	ServerRAID_DriveUnblocked

## **IBMPSG\_ServerRAIDMigrationComplete CIM indication**

This CIM indication is generated when a ServerRAID logical-drive migration is completed on a specified logical drive in a ServeRAID configuration.

<b>End consumer</b>	<b>Normal severity</b>
IBM Director event	CIM > System > ServeRAID Migration Complete
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_INFO
Microsoft Windows event log event ID	20
SNMP	iBMServeRAIDMigrationComplete
Tivoli Enterprise Console native event	IBMPMSG_ServeRAIDMigrationComplete
Tivoli Enterprise Console SNMP event	ServeRAID_MigrationComplete

## **IBMPMSG\_ServerRAIDMigrationDetected CIM indication**

This CIM indication is generated when a ServeRAID logical-drive migration is in progress on a specified logical drive in a ServeRAID configuration.

<b>End consumer</b>	<b>Normal severity</b>
IBM Director event	CIM > System > ServeRAID Migration Detected
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_INFO
Microsoft Windows event log event ID	20
SNMP	iBMServeRAIDMigrationDetected
Tivoli Enterprise Console native event	IBMPMSG_ServeRAIDMigrationDetected
Tivoli Enterprise Console SNMP event	ServeRAID_MigrationDetected



## IBMPSG\_ServerRAIDMigrationFail CIM indication

This CIM indication is generated when a ServerRAID logical-drive migration fails on a specified logical drive in a ServerRAID configuration.

End consumer	Critical severity
IBM Director event	CIM > System > ServerRAID Migration Fail
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_ERROR
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDMigrationFail
Tivoli Enterprise Console native event	IBMPSG_ServerRAIDMigrationFail
Tivoli Enterprise Console SNMP event	ServerRAID_MigrationFail

## IBMPSG\_ServerRAIDNoControllers CIM indication

This CIM indication is generated when no ServerRAID controllers are detected.

End consumer	Normal severity
IBM Director event	CIM > System > ServerRAID No Controllers
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_INFO
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDNoControllers
Tivoli Enterprise Console native event	IBMPSG_ServerRAIDNoControllers
Tivoli Enterprise Console SNMP event	ServerRAID_NoControllers

## IBMPSG\_ServerRAIDPFADrive CIM indication

This CIM indication is generated when a Predictive Failure Analysis (PFA) is detected on a specified hard disk drive in a ServeRAID configuration.

End consumer	Warning severity
IBM Director event	CIM > System > ServeRAID PFA Drive
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGERAIDHEALTH_WARNING
Microsoft Windows event log event ID	20
SNMP	IBMServeRAIDPFADrive
Tivoli Enterprise Console native event	IBMPSG_ServerRAIDPFADrive
Tivoli Enterprise Console SNMP event	ServeRAID_PFADrive

## IBMPSG\_ServerRAIDPFADriveFRU CIM indication

This CIM indication is generated when a Predictive Failure Analysis (PFA) is detected on a specified hard disk drive with a specified field-replaceable unit (FRU) number in a ServeRAID configuration.

End consumer	Warning severity
IBM Director event	CIM > System > ServeRAID PFA Drive FRU
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGERAIDHEALTH_WARNING
Microsoft Windows event log event ID	20
SNMP	IBMServeRAIDPFADriveFRU
Tivoli Enterprise Console native event	IBMPSG_ServerRAIDPFADriveFRU
Tivoli Enterprise Console SNMP event	ServeRAID_PFADriveFRU

---

## IBMPSG\_ServerRAIDPollingFail CIM indication

This CIM indication is generated when a specified controller fails to respond to background polling commands.

End consumer	Warning severity
IBM Director event	CIM > System > ServerRAID Polling Fail
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_WARNING
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDPollingFail
Tivoli Enterprise Console native event	IBMPSG_ServerRAIDPollingFail
Tivoli Enterprise Console SNMP event	ServerRAID_PollingFail

---

## IBMPSG\_ServerRAIDRebuildComplete CIM indication

This CIM indication is generated when a ServerRAID rebuild operation is completed on a specified logical drive in a ServerRAID configuration.

End consumer	Normal severity
IBM Director event	CIM > System > ServerRAID Rebuild Complete
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_INFO
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDRebuildComplete
Tivoli Enterprise Console native event	IBMPSG_ServerRAIDRebuildComplete

<b>End consumer</b>	<b>Normal severity</b>
Tivoli Enterprise Console SNMP event	ServerRAID_RebuildComplete

## IBMP5G\_ServerRAIDRebuildDetected CIM indication

This CIM indication is generated when a ServerRAID rebuild operation is in progress on a specified logical drive in a ServerRAID configuration.

<b>End consumer</b>	<b>Normal severity</b>
IBM Director event	CIM > System > ServerRAID Rebuild Detected
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_INFO
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDRebuildDetected
Tivoli Enterprise Console native event	IBMP5G_ServerRAIDRebuildDetected
Tivoli Enterprise Console SNMP event	ServerRAID_RebuildDetected

## IBMP5G\_ServerRAIDRebuildFail CIM indication

This CIM indication is generated when a ServerRAID rebuild operation fails on a specified logical drive in a ServerRAID configuration.

<b>End consumer</b>	<b>Critical severity</b>
IBM Director event	CIM > System > ServerRAID Rebuild Fail
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_ERROR
Microsoft Windows event log event ID	20

<b>End consumer</b>	<b>Critical severity</b>
SNMP	iBMServerRAIDRebuildFail
Tivoli Enterprise Console native event	IBMPMSG_ServerRAIDRebuildFail
Tivoli Enterprise Console SNMP event	ServerRAID_RebuildFail

## **IBMPMSG\_ServerRAIDSynccComplete CIM indication**

This CIM indication is generated when a ServeRAID synchronization operation is completed on a specified logical drive in a ServeRAID configuration.

<b>End consumer</b>	<b>Normal severity</b>
IBM Director event	CIM > System > ServeRAID Sync Complete
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_INFO
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDSynccComplete
Tivoli Enterprise Console native event	IBMPMSG_ServerRAIDSynccComplete
Tivoli Enterprise Console SNMP event	ServerRAID_SynccComplete

## **IBMPMSG\_ServerRAIDSynccDetected CIM indication**

This CIM indication is generated when a ServeRAID synchronization operation is in progress on a specified logical drive in a ServeRAID configuration.

<b>End consumer</b>	<b>Normal severity</b>
IBM Director event	CIM > System > ServeRAID Sync Detected
Microsoft Operations Manager 2005 alert	Storage Event

<b>End consumer</b>	<b>Normal severity</b>
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_INFO
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDSyncdetected
Tivoli Enterprise Console native event	IBMPMSG_ServerRAIDSyncdetected
Tivoli Enterprise Console SNMP event	ServerRAID_Syncdetected

## IBMPMSG\_ServerRAIDSyncfail CIM indication

This CIM indication is generated when a ServerRAID synchronization operation fails on a specified logical drive in a ServerRAID configuration.

<b>End consumer</b>	<b>Critical severity</b>
IBM Director event	CIM > System > ServerRAID Sync Fail
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_ERROR
Microsoft Windows event log event ID	20
SNMP	iBMServerRAIDSyncfail
Tivoli Enterprise Console native event	IBMPMSG_ServerRAIDSyncfail
Tivoli Enterprise Console SNMP event	ServerRAID_Syncfail

## IBMPMSG\_ServerRAIDTestEvent CIM indication

This CIM indication is generated when a ServerRAID test event is generated.

<b>End consumer</b>	<b>Normal severity</b>
IBM Director event	CIM > System > ServerRAID Test Event

<b>End consumer</b>	<b>Normal severity</b>
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_INFO
Microsoft Windows event log event ID	20
SNMP	iBMServeRAIDTestEvent
Tivoli Enterprise Console native event	IBMPSG_ServerRAIDTestEvent
Tivoli Enterprise Console SNMP event	ServerRAID_TestTrap


## **IBMPSG\_ServerRAIDUnsupportedDrive CIM indication**

This CIM indication is generated when an unsupported hard disk drive is detected in a ServeRAID configuration.

<b>End consumer</b>	<b>Warning severity</b>
IBM Director event	CIM > System > ServeRAID Unsupported Drive
Microsoft Operations Manager 2005 alert	Storage Event
Microsoft SMS native events (Message ID 50210)	IBM_UMS_AGENT_STORAGE RAIDHEALTH_WARNING
Microsoft Windows event log event ID	20
SNMP	iBMServeRAIDUnsupportedDrive
Tivoli Enterprise Console native event	IBMPSG_ServerRAIDUnsupportedDrive
Tivoli Enterprise Console SNMP event	ServerRAID_UnsupportedDrive

## **IBMPSG\_SMARTEvent CIM indication**

This CIM indication is generated when the state of an IDE or SCSI hard disk drive that complies with the self-monitoring, analysis, and reporting technology (SMART) changes with respect to its availability.

<b>End consumer</b>	<b>Critical severity</b>	<b>Warning severity</b>	<b>Normal severity</b>
IBM Director event	CIM > System > SMART Drive	CIM > System > SMART Drive	CIM > System > SMART Drive
IBM Director Console (Group Contents pane)		Not applicable	No symbol displayed
Microsoft Operations Manager 2005 alert	Storage Event	Storage Event	Storage Event
Microsoft SMS native events (Message ID 50090)	IBM_UMS_AGENT_SMART_ERROR_	IBM_UMS_AGENT_SMART_WARNING_	IBM_UMS_AGENT_SMART_INFO_
Microsoft Windows event log event ID	9	9	9
SNMP	ibmSystemTrapSMART	Not applicable	Not applicable
Tivoli Enterprise Console native event	IBMPSG_SMARTEvent	IBMPSG_SMARTEvent	IBMPSG_SMARTEvent
Tivoli Enterprise Console SNMP event	UMS_SMARTCritical	UMS_SMARTWarning	UMS_SMARTNormal

## **IBMPSG\_SPPowersSupplyEvent CIM indication**

This CIM indication is generated when the Advanced Systems Management processor (ASM processor) detects that the state of the system power supply changes with respect to its availability. This is sent from servers that do not have a power backplane and do not support a recovery severity or alert type.



<b>End consumer</b>	<b>Critical severity</b>	<b>Warning severity</b>	<b>Normal severity</b>
IBM Director event	Not applicable	Not applicable	Not applicable
IBM Director Console (Group Contents pane)	Not applicable	Not applicable	Not applicable
Microsoft Operations Manager 2005 alert	Power Supply Event	Power Supply Event	Power Supply Event



End consumer	Critical severity	Warning severity	Normal severity
Microsoft SMS native events (Message ID 50130)	IBM_UMS_AGENT_SPPOWERSUPPLY_ERROR_	IBM_UMS_AGENT_SPPOWERSUPPLY_WARNING_	IBM_UMS_AGENT_SPPOWERSUPPLY_INFO_
Microsoft Windows event log event ID	29	Not applicable	Not applicable
SNMP	Not applicable	ibmSystemTrapsPower Supply	Not applicable
Tivoli Enterprise Console native event	IBMPSG_SP_PowerSupply Event	IBMPSG_SP_PowerSupply Event	IBMPSG_SP_PowerSupply Event
Tivoli Enterprise Console SNMP event	UMS_SPPowerSupplyEvent	UMS_SPPowerSupplyEvent	UMS_SPPowerSupplyEvent

## IBMPSG\_StorageEvent CIM indication



This CIM indication is generated when the state of system hard disk drive space changes with respect to user-defined levels of hard disk drive space remaining. By default, the warning level is 5% remaining and critical level is 3% remaining.

End consumer	Critical severity	Warning severity	Normal severity
IBM Director event	CIM > System > Disk Space Low	CIM > System > Disk Space Low	CIM > System > Disk Space Low
IBM Director Console (Group Contents pane)			No symbol displayed
Microsoft Operations Manager 2005 alert	Storage Event	Storage Event	Storage Event
Microsoft SMS native events (Message ID 50070)	IBM_UMS_AGENT_STORAGE_ERROR_	IBM_UMS_AGENT_STORAGE_WARNING_	IBM_UMS_AGENT_STORAGE_INFO_
Microsoft Windows event log event ID	20	20	Not applicable

<b>End consumer</b>	<b>Critical severity</b>	<b>Warning severity</b>	<b>Normal severity</b>
SNMP	ibmSystemTrapStorage	ibmSystemTrapStorage	ibmSystemTrapStorage
Tivoli Enterprise Console native event	IBMPSG_StorageEvent	IBMPSG_StorageEvent	IBMPSG_StorageEvent
Tivoli Enterprise Console SNMP event	UMS_StorageVeryLow	UMS_StorageLow	UMS_StorageNormal


## IBMPSG\_TemperatureEvent CIM indication

This CIM indication is generated when the state of a system temperature sensor changes with respect to a manufacturer-defined or user-defined threshold.

<b>End consumer</b>	<b>Critical severity</b>	<b>Warning severity</b>	<b>Normal severity</b>
IBM Director event	CIM > System > Temperature	CIM > System > Temperature	CIM > System > Temperature
IBM Director Console (Group Contents pane)	 Temperature Event	 Temperature Event	No symbol displayed
Microsoft Operations Manager 2005 alert	Temperature Event	Temperature Event	Temperature Event
Microsoft SMS native events (Message ID 50020)	IBM_UMS_AGENT_TEMPERATURE_ERROR_	IBM_UMS_AGENT_TEMPERATURE_WARNING_	IBM_UMS_AGENT_TEMPERATURE_INFO_
Microsoft Windows event log event ID	2	2	2
SNMP	ibmSystemTrapTemperature	ibmSystemTrapTemperature	ibmSystemTrapTemperature
Tivoli Enterprise Console native event	IBMPSG_TemperatureEvent	IBMPSG_TemperatureEvent	IBMPSG_TemperatureEvent
Tivoli Enterprise Console SNMP event	UMS_TemperatureCriticallyOutOfRange	UMS_TemperatureOutOfRange	UMS_TemperatureNormal

## IBMPSG\_VoltageEvent CIM indication


This CIM indication is generated when the state of a system voltage sensor changes with respect to a manufacturer-defined threshold.

End consumer	Critical severity	Warning severity	Normal severity
IBM Director event	CIM > System > Voltage	Not applicable	CIM > System > Voltage
IBM Director Console (Group Contents pane)	 Voltage Event	Not applicable	No symbol displayed
Microsoft Operations Manager 2005 alert	Voltage Event	Voltage Event	Voltage Event
Microsoft SMS native events (Message ID 50030)	IBM_UMS_AGENT_VOLTAGE_ERROR_	IBM_UMS_AGENT_VOLTAGE_WARNING_	IBM_UMS_AGENT_VOLTAGE_INFO_
Microsoft Windows event log event ID	3	Not applicable	3
SNMP	ibmSystemTrapVoltage	Not applicable	ibmSystemTrapVoltage
Tivoli Enterprise Console native event	IBMPSG_VoltageEvent	IBMPSG_VoltageEvent	IBMPSG_VoltageEvent
Tivoli Enterprise Console SNMP event	UMS_VoltageCriticallyOutOfRange	UMS_VoltageOutOfRange	UMS_VoltageNormal

## IBMPSG\_WarrantyExpirationEvent CIM indication

This CIM indication is generated when the system warranty expiration date has been reached with respect to the value configured for the date while using the Asset ID task.

End consumer	Critical severity	Warning severity	Normal severity
IBM Director event	Not applicable	CIM > System > Warranty Expiration	CIM > System > Warranty Expiration

<b>End consumer</b>	<b>Critical severity</b>	<b>Warning severity</b>	<b>Normal severity</b>
IBM Director Console (Group Contents pane)	Not applicable	 Other Event	No symbol displayed
Microsoft Operations Manager 2005 alert	Other Event	Other Event	Other Event
Microsoft SMS native events (Message ID 50140)	IBM_UMS_AGENT_LEASE_ERROR_	IBM_UMS_AGENT_LEASE_WARNING_	IBM_UMS_AGENT_LEASE_INFO_
Microsoft Windows event log event ID	Not applicable	14	14
SNMP	Not applicable	ibmSystemTrapWarrantyExpiration	ibmSystemTrapWarrantyExpiration
Tivoli Enterprise Console native event	IBMPSG_WarrantyExpirationEvent	IBMPSG_WarrantyExpirationEvent	IBMPSG_WarrantyExpirationEvent
Tivoli Enterprise Console SNMP event	UMS_WarrantyExpired Critical	UMS_WarrantyExpired Warning	UMS_WarrantyExpired Normal

---

## Appendix A. Configuring ASF

This topic describes how to configure ASF on a managed system. The available configuration options vary, depending on the type of network interface card (NIC) and the level of ASF that it supports.

To configure ASF:

- The managed system must contain an ASF-capable NIC, and the applicable device drivers must be installed.
- IBM Director must have performed an inventory collection on the managed system.

Complete the following steps:

1. In IBM Director Console, drag the **Configure ASF** task onto the managed system.
2. In the Alert Standard Format window, complete the following steps to enable ASF on the NIC:
  - a. Select the **Enable ASF Hardware** check box.
  - b. Select the **Enable all Platform Event Traps** check box if it is displayed. (This check box displays only for certain types of NICs.)
  - c. (ASF 2.0 systems only) To enable remote power management, select the **Enable Remote Management** check box.
3. Click the **Configuration** tab.
4. In the Configuration page, configure the ASF settings:
  - a. In the **Management Server (IP address)** field, type the IP address of the management server to which the PET alerts are sent.
  - b. To ensure that heartbeat alerts are sent, select the **Enabled** check box and type the number of seconds in the **Heartbeat frequency (seconds)** field.
  - c. In the **Minimum watchdog timer (seconds)** field, type the minimum number of seconds for the watchdog timer.
  - d. In the **Minimum ASF Sensor Inter Poll Wait Time (5 ms units)** field, type the minimum time to wait for the ASF Sensor Inter Poll.
5. (ASF 2.0 systems with remote management enabled only) Click the **Remote Management** tab.

6. In the Remote Management page, create or modify authentication keys:
  - a. If you have not created authentication keys previously, click **Generate Keys**. Three authentication keys are generated. If you want to copy the authentication keys, do so now. When you click **Apply**, the key values are replaced by asterisks.
  - b. If you want to create new authentication keys, select the **Overwrite the existing keys used by IBM Director Console for authentication** check box.
7. Click **Apply** . If you created or modified authentication keys, the keys are written to both IBM Director Server and the managed system.

---

## Appendix B. Preparing to install IBM Director on an xSeries server

This topic provides information about preparing an xSeries server for the installation of IBM Director.

Before you install IBM Director on an xSeries server, consider the following information:

- **All components**

- (Linux only) Make sure that the instance of IBM Director Agent running on the management server will be fully functional and able to send alerts to IBM Director Server. For the IBM Director Agent to be fully functional you might need to install service processor device drivers or the IBM LM78 and SMBus device drivers for Linux.
- (Linux only) Before you install IBM Director on Red Hat Enterprise Linux AS and ES, version 3.0, make sure that the following RPM file is installed:  
compat-libstdc++-7.3-2.96.122.i386.rpm
- (Linux only) Before you install IBM Director on Red Hat Enterprise Linux AS and ES, version 4.0, make sure that the following RPM files are installed:  
compat-libstdc++-296-2.96-132.7.2.i386.rpm
- (Intel Itanium systems; Linux only) Before you install IBM Director on an 64-bit Intel Itanium system running Red Hat Enterprise Linux AS, version 4.0, for Intel Itanium, make sure that the following RPM file is installed:  
compat-libstdc++-33-3.2.3-47.3.i664.rpm
- (Upgrades; Linux only) If you are upgrading from IBM Director, version 4.20 or later on SUSE LINUX Enterprise Server 9 for x86, ensure that the following RPM is installed:  
rpm-4.1.1-177.9.i586.rpm
- (Systems with IPMI Baseboard Management Controllers) The supporting IPMI device drivers and mapping layers must be installed. IBM Director cannot receive System Health Monitoring information if these drivers and mapping layers are not installed. The device drivers and mapping layers for Windows, Linux, and NetWare can be downloaded from the IBM Support Web site at [www.ibm.com/pc/support](http://www.ibm.com/pc/support).

For eServer 325 or eServer 326 models, download and install the following items (the exact names of the files to download are dependent upon your operating system):

- Microsoft Windows Installer (MSI) IPMI device drivers
- IBM IPMI Library (mapping layer)

For all other xSeries systems, download and install the following items (the exact names of the files to download are dependant upon your operating system):

- OSA IPMI device drivers
- IBM Mapping layer software source for OSA IPMI

**Important:** You must install the device driver first and then install the mapping layer.

- **(Linux only) IBM Director Server**

Before you install IBM Director on Red Hat Enterprise Linux AS and ES, version 4.0, make sure that the following RPM file is installed:

compat-libstdc++-33-3.2.3-47.3.i386.rpm

- **(Linux only)Level 1: IBM Director Core Services and Level 2: IBM Director Agent**

- If you want to use the Remote Session task on the managed system, make sure that the package that contains telnetd daemon is installed and configured. This is usually in the telnet\_server\_<version>.i386.RPM package, where <version> is the code level of your Linux distribution.



---

## Appendix C. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing  
IBM Corporation  
North Castle Drive  
Armonk, NY 10504-1785  
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation  
Licensing  
2-31 Roppongi 3-chome, Minato-ku  
Tokyo 106-0032, Japan

**The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR**

IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation  
MW9A/050  
5600 Cottle Road  
San Jose, CA 95193  
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

---

## **Trademarks**

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

AIX  
AIX 5L  
Alert on LAN  
Asset ID  
BladeCenter  
DB2  
DB2 Universal Database  
DirMaint

Electronic Service Agent  
Enterprise Storage Server  
eServer  
eServer logo  
FlashCopy  
HiperSockets  
i5/OS  
IBM  
IBM logo  
ibm.com  
IntelliStation  
iSeries  
Netfinity  
NetServer  
NetView  
OS/400  
POWER  
Predictive Failure Analysis  
pSeries  
RACF  
Redbooks  
ServeProven  
SurePOS  
System p5  
System z9  
Tivoli

Tivoli Enterprise  
Tivoli Enterprise Console  
Virtualization Engine  
Wake on LAN  
xSeries  
z/VM  
zSeries

Intel and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

Red Hat and all Red Hat-based trademarks and logos are trademarks or registered trademarks of Red Hat, Inc., in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

---

# Abbreviations, Acronyms, and Glossary

---

## Abbreviation and acronym list

This topic lists abbreviations and acronyms used in the IBM Director documentation.

*Table 2. Abbreviations and acronyms used in IBM Director documentation*

<b>Abbreviation or acronym</b>	<b>Definition</b>
AES	advanced encryption standard
APAR	authorized program analysis report
ASF	Alert Standard Format
ASM	Advanced System Management
ASM PCI Adapter	Advanced System Management PCI Adapter
BIOS	basic input/output system
CEC	Central Electronics Complex
CIM	Common Information Model
CIMOM	Common Information Model Object Manager
CP	control program
CRC	cyclic redundancy check
CSM	IBM Cluster Systems Management
CSV	comma-separated value
DASD	direct access storage device
DBCS	double-byte character set
DES	data encryption standard
DHCP	Dynamic Host Configuration Protocol

Table 2. Abbreviations and acronyms used in IBM Director documentation (continued)

Abbreviation or acronym	Definition
DIMM	dual inline memory module
DMI	Desktop Management Interface
DMTF	Distributed Management Task Force
DNS	Domain Name System
DSA	Digital Signature Algorithm
EEPROM	electrically erasable programmable read-only memory
FRU	field-replaceable unit
FTMI	fault tolerant management interface
FTP	file transfer protocol
GB	gigabyte
Gb	gigabit
GMT	Greenwich Mean Time
GUI	graphical user interface
GUID	globally unique identifier
HMC	Hardware Management Console
HTML	hypertext markup language
IIS	Microsoft Internet Information Server
I/O	input/output
IP	Internet protocol
IPC	interprocess communication
IPMI	Intelligent Platform Management Interface
IPX	internetwork packet exchange

Table 2. Abbreviations and acronyms used in IBM Director documentation (continued)

Abbreviation or acronym	Definition
ISDN	integrated services digital network
ISMP	integrated system management processor
JVM	Java™ Virtual Machine
JCE	Java Cryptography Extension
JDBC	Java Database Connectivity
JFC	Java Foundation Classes
JRE	Java Runtime Environment
KB	kilobyte
Kb	kilobit
kpbs	kilobits per second
KVM	keyboard/video/mouse
LAN	local area network
LED	light-emitting diode
LPAR	logical partition
MAC	media access control
MB	megabyte
Mb	megabit
Mbps	megabits per second
MD5	message digest 5
MDAC	Microsoft Data Access Control
MHz	megahertz
MIB	Management Information Base



Table 2. Abbreviations and acronyms used in IBM Director documentation (continued)

Abbreviation or acronym	Definition
MIF	Management Information Format
MMC	Microsoft Management Console
MPA	Management Processor Assistant
MPCLI	Management Processor Command-Line Interface
MSCS	Microsoft Cluster Server
MST	Microsoft software transformation
NIC	network interface card
NNTP	Network News Transfer Protocol
NTP	network time protocol
NVRAM	nonvolatile random access memory
ODBC	Open DataBase Connectivity
OID	object ID
PCI	peripheral component interconnect
OSA	Open Systems Adapter
PCI-X	peripheral component interconnect-extended
PDF	Portable Document Format
PFA	Predictive Failure Analysis
POST	power-on self-test
PTF	program temporary fix
RAM	random access memory
RDM	Remote Deployment Manager
RPM	(1) Red Hat Package Manager (2) revolutions per minute

Table 2. Abbreviations and acronyms used in IBM Director documentation (continued)

Abbreviation or acronym	Definition
RSA	Rivest-Shamir-Adleman
RXE	Remote Expansion Enclosure
SAS	Serial Attached SCSI
SATA	Serial ATA
SCSI	Small Computer System Interface
SFS	shared file system
SHA	Secure Hash Algorithm
SI	Solution Install
SID	(1) security identifier (2) Oracle system identifier
SLP	service location protocol
SLPD	service location protocol daemon
SMBIOS	System Management BIOS
SMI	System Management Information
SMP	symmetric multiprocessor
SMS	Systems Management Server
SMTP	Simple Mail Transfer Protocol
SMART	Self-Monitoring, Analysis, and Reporting Technology
SMI-S	Storage Management Initiative Specification
SNMP	Simple Network Management Protocol
SPB	software package block
SQL	Structured Query Language
SSH	Secure Shell

Table 2. Abbreviations and acronyms used in IBM Director documentation (continued)

Abbreviation or acronym	Definition
SSL	Secure Sockets Layer
TAP	Telocator Alphanumeric Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TTL	time to live
UDP	User Datagram Protocol
UID	unique ID
UIM	upward integration module
UNC	universal naming convention
USB	Universal Serial Bus
UUID	universal unique identifier
VPD	vital product data
VMRM	Virtual Machine Resource Manager
VRM	voltage regulator module
WAN	wide area network
WfM	Wired for Management
WINS	Windows Internet Naming Service
WMI	Windows Management Instrumentation
WQL	Windows Management Instrumentation Query Language
XML	extensible markup language

---

## Glossary

This glossary includes terms and definitions from:

- The *American National Dictionary for Information Systems*, ANSI X3.172-1990, copyright 1990 by the American National Standards Institute (ANSI). Copies may be purchased from the American National Standards Institute, 1430 Broadway, New York, New York 10018. Definitions are identified by the symbol (A) after the definition.
- The *Information Technology Vocabulary* developed by Subcommittee 1, Joint Technical Committee 1, of the International Organization for Standardization and the International Electrotechnical Committee (ISO/IEC JTC1/SC1). Definitions of published parts of this vocabulary are identified by the symbol (I) after the definition; definitions taken from draft international standards, committee drafts, and working papers being developed by ISO/IEC JTC1/SC1 are identified by the symbol (T) after the definition, indicating that final agreement has not yet been reached among the participating National Bodies of SC1.
- The *IBM Dictionary of Computing*, New York: McGraw-Hill, 1994.
- The *IBM Glossary of Computing Terms*, 1999.

To view other IBM glossary sources, see IBM Terminology at [www.ibm.com/ibm/terminology](http://www.ibm.com/ibm/terminology).

### A

#### **Advanced Encryption Setting (AES)**

A block cipher algorithm, also known as Rijndael, used to encrypt data transmitted between managed systems and the management server, which employs a key of 128, 192, or 256 bits. AES was developed as a replacement for DES.

#### **Advanced System Management (ASM) interconnect**

A feature of IBM service processors that enables users to connect up to 24 servers to one service processor, thus eliminating the need for multiple modems, telephones, and LAN ports. It provides such out-of-band management functions as system power control, service-processor event-log management, firmware updates, alert notification, and user profile configuration.

#### **Advanced System Management (ASM) interconnect network**

A network of IBM servers created by using the ASM interconnect feature. The servers are connected

through RS-485 ports. When servers containing integrated system management processors (ISMPs) and ASM processors are connected to an ASM interconnect network, IBM Director can manage them out-of-band.

### **Advanced System Management (ASM) PCI adapter**

An IBM service processor that is built into the Netfinity® 7000 M10 and 8500R servers. It also was available as an option that could be installed in a server that contained an ASM processor. When an ASM PCI adapter is used with an ASM processor, the ASM PCI adapter acts as an Ethernet gateway, while the ASM processor retains control of the server. When used as a gateway service processor, the ASM PCI adapter can communicate with other ASM PCI adapters and ASM processors only.

### **Advanced System Management (ASM) processor**

A service processor built into the mid-range Netfinity and early xSeries servers. IBM Director can connect out-of-band to an ASM processor located on an ASM interconnect; an ASM PCI adapter, a Remote Supervisor Adapter, or a Remote Supervisor II must serve as the gateway service processor.

### **alert**

A message or other indication that identifies a problem or an impending problem.

### **alert forwarding**

Alert forwarding can ensure that alerts are sent, even if a managed system experiences a catastrophic failure, such as an operating-system failure.

### **alert-forwarding profile**

A profile that specifies where remote alerts for the service processor should be sent.

### **alert standard format (ASF)**

A specification created by the Distributed Management Task Force (DMTF) that defines remote-control and alerting interfaces that can best serve a client system in an environment that does not have an operating system.

### **anonymous command execution**

Execution of commands on a target system as either *system account* (for managed systems running Windows) or *root* (for managed systems running Linux). To restrict anonymous command execution, disable this feature and always require a user ID and password.

**ASF** See *alert standard format*.

**ASM interconnect gateway**

See *gateway service processor*.

**association**

(1) A way of displaying the members of a group in a logical ordering. For example, the Object Type association displays the managed objects in a group in folders based on their type. (2) A way to display additional information about the members of the group. For example, the Event Action Plans association displays any event action plans applied to the managed objects in the group in an Event Action Plan folder.

**B**

**basic input/output system (BIOS)**

The code that controls basic hardware operations, such as interactions with diskette drives, hard disk drives, and the keyboard.

**BIOS**

See *Basic Input/Output System*.

**blade server**

An IBM  SERVER BladeCenter server. A high-throughput, two-way, Intel Xeon-based server on a card that supports symmetric multiprocessors {SMP}.

**BladeCenter chassis**

A BladeCenter unit that acts as an enclosure. This 7-U modular chassis can contain up to 14 blade servers. It enables the individual blade servers to share resources, such as the management, switch, power, and blower modules.

**bottleneck**

A place in the system where contention for a resource is affecting performance.

**C**

**chassis**

The metal frame in which various electronic components are mounted.

**chassis detect-and-deploy profile**

A profile that IBM Director automatically applies to all new BladeCenter chassis when they are discovered.

The profile settings include management module name, network protocols, and static IP addresses. If

Remote Deployment Manager (RDM) is installed on the management server, the chassis detect-and-deploy profile also can include deployment policies.

**CIM** See *Common Information Model*.

**Common Information Model (CIM)**

An implementation-neutral, object-oriented schema for describing network management information. The Distributed Management Task Force (DMTF) develops and maintains CIM specifications.

**component association**

In the IBM Director Rack Manager task, a function that can make a managed system or device rack-mountable when the inventory collection feature of IBM Director does not recognize the managed system or device. The function associates the system or device with a predefined component.

**D****Data Encryption Standard (DES)**

A cryptographic algorithm designed to encrypt and decrypt data using a private key.

**database server**

The server on which the database application and database used with IBM Director Server are installed.

**deployment policy**

A policy that associates a specific bay in a BladeCenter chassis with an RDM noninteractive task. When a blade server is added to or replaced in the bay, IBM Director automatically runs the RDM task.

**DES** See *Data Encryption Standard*.

**Desktop Management Interface (DMI)**

A protocol-independent set of application programming interfaces (APIs) that were defined by the Distributed Management Task Force (DMTF). These interfaces give management application programs standardized access to information about hardware and software in a system.

**Diffie-Hellman key exchange**

A public, key-exchange algorithm that is used for securely establishing a shared secret over an insecure channel. During Phase II negotiations, the Diffie-Hellman group prevents someone who intercepts your key from deducing future keys that are based on the one they have.

**digital signature algorithm (DSA)**

A security protocol that uses a pair of keys (one public and one private) and a one-way encryption algorithm to provide a robust way of authenticating users and systems. If a public key can successfully decrypt a digital signature, a user can be sure that the signature was encrypted using the private key.

**discovery**

The process of finding resources within an enterprise, including finding the new location of monitored resources that were moved.

**DMI** See *Desktop Management Interface*.

**E****enclosure**

A unit that houses the components of a storage subsystem, such as a control unit, disk drives, and power source.

**event**

An occurrence of significance to a task or system, such as the completion or failure of an operation. There are two types of events: alert and resolution.

**event action**

The action that IBM Director takes in response to a specific event or events.

**event-action plan**

A user-defined plan that determines how IBM Director will manage certain events. An event action plan comprises one or more event filters and one or more customized event actions.

**event-data substitution variable**

A variable that can be used to customize event-specific text messages for certain event actions.



**event filter**

A filter that specifies the event criteria for an event action plan. Events must meet the criteria specified in the event filter in order to be processed by the event action plan to which the filter is assigned.

**extension**

See *IBM Director extension*.

**F****field-replaceable unit (FRU)**

An assembly that is replaced in its entirety when any one of its components fails. In some cases, a FRU may contain other FRUs.

**file-distribution server**

In the Software Distribution task, an intermediate server that is used to distribute a software package when the redirected-distribution method is used.

**forecast**

A function that can provide a prediction of future performance of a managed system using past data collected on that managed system.

**FRU** See *field-replaceable unit*.

**G****gateway service processor**

A service processor that relays alerts from service processors on an Advanced System Management (ASM) interconnect network to IBM Director Server.

**group**

A logical set of managed objects. Groups can be dynamic, static, or task-based.

**GUID**

See *Universal Unique Identifier*.

## I

### **IBM Director Agent**

A component of IBM Director software. When IBM Director Agent is installed on a system, the system can be managed by IBM Director. IBM Director Agent transfers data to the management server using several network protocols, including TCP/IP, NetBIOS, and IPX.

### **IBM Director Console**

A component of IBM Director software. When installed on a system, it provides a graphical user interface (GUI) for accessing IBM Director Server. IBM Director Console transfers data to and from the management server using TCP/IP.

### **IBM Director database**

The database that contains the data stored by IBM Director Server.

### **IBM Director environment**

The complex, heterogeneous environment managed by IBM Director. It includes systems, BladeCenter chassis, software, SNMP devices.

### **IBM Director extension**

A tool that extends the functionality of IBM Director. Some of the IBM Director extensions are Capacity Manager, ServerRAID Manager, Remote Deployment Manager, Software Distribution.

### **IBM Director Server**

The main component of IBM Director software. When installed on the management server, it provides basic functions such as discovery of the managed systems, persistent storage of configuration and management data, an inventory database, event listening, security and authentication, management console support, and administrative tasks.

### **IBM Director Server service**

A service that runs automatically on the management server, and provides the server engine and application logic for IBM Director.

### **IBM Director service account**

The Windows operating-system account associated with the IBM Director Server service.

### **in-band communication**

Communication that occurs through the same channels as data transmissions. An example of in-band communication is the interprocess communication that occurs between IBM Director Server, IBM Director Agent, and IBM Director Console.

### **integrated system management processor (ISMP)**

A service processor built into the some xSeries servers. The successor to the Advanced System Management (ASM) processor, the ISMP does not support in-band communication in systems running NetWare. For IBM Director Server to connect out-of-band to an ISMP, the server containing the ISMP must be installed on an ASM interconnect network. A Remote Supervisor Adapter or a Remote Supervisor Adapter II must serve as the gateway service processor.

### **interprocess communication (IPC)**

- 1) The process by which programs communicate data to each other and synchronize their activities. Semaphores, signals, and internal message queues are common methods of interprocess communication.
- 2) A mechanism of an operating system that allows processes to communicate with each other within the same computer or over a network. It also is called in-band communication

### **inventory-software dictionary**

A file that tracks the software installed on managed systems in a network.

**IPC** See *interprocess communication*.

### **ISMP**

See *integrated system management processor*.

## **J**

**job** A separately executable unit of work defined by a user, and run by a computer.

## **L**

### **Level-0 managed system**

An IBM or non-IBM server, desktop computer, workstation, or mobile computer, that can be managed by IBM Director but does not have any IBM Director software installed on it.

**Level-1 managed system**

An IBM or non-IBM server, desktop computer, workstation, and mobile computer that has IBM Director Core Services installed. IBM Director uses IBM Director Core Services to communicate with and administer the Level-2 managed system. IBM Director Core Services includes the SLP instrumentation, the IBM Director Agent SLP service type, and Common Information Model (CIM).

**Level-2 managed system**

An IBM or non-IBM server, desktop computer, workstation, or mobile computer that has IBM Director Agent installed. IBM Director Agent provides managed systems with the full complement of IBM Director Agent function that is used to communicate with and administer the Level-2 managed system. The function of a Level-2 managed system varies depending on the operating system and platform.

**light path diagnostics**

A technology that provides a lighted path to failed or failing components to expedite hardware repairs.

**M****MAC address**

See media access control (MAC) address.

**managed group**

A group of systems or objects managed by IBM Director.

**managed object**

An item managed by IBM Director. In IBM Director Console, a managed object is represented by an icon that shows its type (such as chassis, cluster, system, or scalable system, for example).

**managed object ID**

A unique identifier for each managed object. It is the key value used by IBM Director database tables.

**managed system**

A system that is being controlled by a given system management application, for example, a system managed by IBM Director.

**management console**

A system (server, desktop computer, workstation, or mobile computer) on which IBM Director Console is installed.

**management module**

The BladeCenter component that handles system-management functions. It configures the chassis and switch modules, communicates with the blade servers and all I/O modules, multiplexes the keyboard/video/mouse (KVM), and monitors critical information about the chassis and blade servers.

**management server**

The server on which IBM Director Server is installed.

**media access control (MAC) address**

In a local area network, the protocol that determines which device has access to the transmission medium at a given time.

**N****nonvolatile random-access memory (NVRAM)**

Random access memory (storage) that retains its contents after the electrical power to the machine is shut off.

**notification**

See *alert*.

**NVRAM**

See *nonvolatile random-access memory*.

**O****out-of-band communication**

Communication that occurs through a modem or other asynchronous connection, for example, service processor alerts sent through a modem or over a LAN. In an IBM Director environment, such communication is independent of the operating system and interprocess communication (IPC).

## **P**

### **partition**

See *scalable partition*.

**PCI** See *Peripheral Component Interconnect*.

### **PCI-X**

See *Peripheral Component Interconnect-X*.

### **Peripheral Component Interconnect (PCI)**

A standard for connecting attached devices to a computer.

### **Peripheral Component Interconnect-X (PCI-X)**

An enhancement to the Peripheral Component Interconnect (PCI) architecture. PCI-X enhances the Peripheral Component Interconnect (PCI) standard by doubling the throughput capability and providing additional adapter-performance options while maintaining backward compatibility with PCI adapters.

**PFA** See *Predictive Failure Analysis*.

### **physical platform**

An IBM Director managed object that represents a single physical chassis or server that has been discovered through the use of the Service Location Protocol (SLP).

### **plug-in**

A software module, often written by a third party, that adds function to an existing program or application such as a Web browser. See *IBM Director extension*.

### **POST**

See *power-on self-test*.

### **power-on self-test**

A series of internal diagnostic tests activated each time the system power is turned on.

### **Predictive Failure Analysis (PFA)**

A scheduled evaluation of system data that detects and signals parametric degradation that might lead to functional failures.

**private key**

1) In secure communication, an algorithmic pattern used to encrypt messages that only the corresponding public key can decrypt. The private key is also used to decrypt messages that were encrypted by the corresponding public key. The private key is kept on the user's system and is protected by a password. 2) The secret half of a cryptographic key pair that is used with a public key algorithm. Private keys are typically used to digitally sign data and to decrypt data that has been encrypted with the corresponding public key.

**public key**

1) In secure communication, an algorithmic pattern used to decrypt messages that were encrypted by the corresponding private key. A public key is also used to encrypt messages that can be decrypted only by the corresponding private key. Users broadcast their public keys to everyone with whom they must exchange encrypted messages. 2) The non-secret half of a cryptographic key pair that is used with a public key algorithm. Public keys are typically used to verify digital signatures or decrypt data that has been encrypted with the corresponding private key.

**R****redirected distribution**

A method of software distribution that uses a file-distribution server.

**remote I/O enclosure**

An IBM Director managed object that represents an expansion enclosure of Peripheral Component Interconnect-X (PCI-X) slots, for example, an RXE-100 Remote Expansion Enclosure. The enclosure consists of one or two expansion kits.

**Remote Supervisor Adapter**

An IBM service processor. It is built into some xSeries servers and available as an optional adapter for use with others. When used as a gateway service processor, the Remote Supervisor Adapter can communicate with all service processors on the Advanced System Management (ASM) interconnect.

**resolution**

The occurrence of a correction or solution to a problem.

**resource-monitor threshold**

The point at which a resource monitor generates an event.

## **RXE Expansion Port**

The dedicated high-speed port used to connect a remote I/O expansion unit, such as the RXE-100 Remote Expansion Enclosure, to a server.

## **S**

### **scalable node**

A physical platform that has at least one SMP Expansion Module. Additional attributes are assigned to a physical platform when it is a scalable node. These additional attributes record the number of SMP Expansion Modules, SMP Expansion Ports, and RXE Expansion ports on the physical chassis.

### **scalable object**

An IBM Director managed object that is used with Scalable Systems Manager. Scalable objects include scalable nodes, scalable systems, scalable partitions, and remote I/O enclosures that are attached to scalable nodes.

### **scalable partition**

An IBM Director managed object that defines the scalable nodes that can run a single image of the operating system. A scalable partition has a single, continuous memory space and access to all associated adapters. A scalable partition is the logical equivalent of a physical platform. Scalable partitions are associated with scalable systems and comprise only the scalable nodes from their associated scalable systems.

### **scalable system**

An IBM Director managed object that consists of scalable nodes and the scalable partitions that are composed of the scalable nodes in the scalable system. When a scalable system contains two or more scalable nodes, the servers that they represent must be interconnected through their SMP Expansion Modules to make a multinode configuration, for example, a 16-way xSeries 455 server made from four scalable nodes.

### **Secure Sockets Layer (SSL)**

A security protocol that provides communication privacy. SSL enables client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery.



**Service Location Protocol (SLP)**

In the Internet suite of protocols, a protocol that identifies and uses network hosts without having to designate a specific network host name.

**service processor**

A generic term for Remote Supervisor Adapters, Advanced System Management processors, Advanced System Management PCI adapters, and integrated system management processors (ISMPs). These hardware-based management processors used in IBM Netfinity and xSeries servers work with IBM Director to provide hardware status and alert notification.

**SLP** See *Service Location Protocol*.

**SMBIOS**

See *systems management BIOS*.

**SMP Expansion Module**

An IBM xSeries hardware option. It is a single module that contains microprocessors, disk cache, random access memory, and three SMP Expansion Port connections. Two SMP Expansion Modules can fit in a chassis.

**SNMP Access and Trap Forwarding**

An IBM Director Agent feature that enables SNMP to access managed-system data. When installed on a managed system, this feature enables SNMP-based managers to poll the managed system and receive its alerts. If System Health Monitoring is installed on the managed system also, hardware alerts can be forwarded as SNMP traps.

**SNMP device**

A network device, printer, or computer that has an SNMP device installed or embedded.

**SQL** See *Structured Query Language*

**SSL** See *Secure Sockets Layer*.

**static partition**

A view-only scalable partition.

**sticky key**

An input method that enables the user to press and release a series of keys sequentially (for example, Ctrl+Alt+Del), yet have the keys behave as if they were pressed and released at the same time. This method can be used for those who require special-needs settings to make the keyboard easier to use.

**Structured Query Language (SQL)**

A standardized language for defining and manipulating data in a relational database.

**switch module**

The BladeCenter component that provides network connectivity for the BladeCenter chassis and blade servers. It also provides interconnectivity between the management module and blade servers.

**system**

The computer and its associated devices and programs.

**System Health Monitoring**

An IBM Director Agent feature that provides active monitoring of critical system functions, including system temperatures, voltages, and fan speeds. It also handles in-band alert notification for managed systems running Windows and some managed systems running Linux.

**system variable**

A user-defined keyword and value pair that can be used to test and track the status of network resources. System variables can be referred to wherever event-data substitution is allowed.

**systems management BIOS (SMBIOS)**

A key requirement of the Wired for Management (WfM) 2.0 specification. SMBIOS extends the system BIOS to support the retrieval of management data required by the WfM specification. To run IBM Director Agent, a system must support SMBIOS, version 2.2 or later.

**T****target system**

A managed system on which an IBM Director task is performed.

**time to live (TTL)**

A technique used by best-effort delivery protocols to inhibit endlessly looping packets. The packet is discarded if the TTL counter reaches 0.

**triple data encryption standard (DES)**

A block cipher algorithm that can be used to encrypt data transmitted between managed systems and the management server. Triple DES is a security enhancement of DES that employs three successive DES block operations.

**TTL** See *time to live*.

**U****universal unique identifier (UUID)**

A 128-bit character string guaranteed to be globally unique and used to identify components under management.

**uptime**

The time during which a system is working without failure.

**upward integration**

The methods, processes and procedures that enable lower-level systems-management software, such as IBM Director Agent, to work with higher-level systems-management software, such as Tivoli Enterprise™ or Microsoft SMS.

**upward integration module**

Software that enables higher-level systems-management software, such as Tivoli Enterprise or Microsoft Systems Manager Server (SMS), to interpret and display data provided by IBM Director Agent. This module also can provide enhancements that start IBM Director Agent from within the higher-level systems-management console, as well as collect IBM Director inventory data and view IBM Director alerts.

**UUID**

See *universal unique identifier*.

## V

### **vital product data (VPD)**

Information that uniquely defines the system, hardware, software, and microcode elements of a processing system.

**VPD** See *vital product data*.

## W

### **Wake on LAN®**

A technology that enables a user to remotely turn on systems for off-hours maintenance. A result of the Intel-IBM Advanced Manageability Alliance and part of the Wired for Management Baseline Specification, users of this technology can remotely turn on a server and control it across the network, thus saving time on automated software installations, upgrades, disk backups, and virus scans.

### **walk**

An SNMP operation that is used to discover all object instances of management information implemented in the SNMP agent that can be accessed by the SNMP manager.

### **Windows Management Instrumentation (WMI)**

An application programming interface (API) in the Windows operating system that enables devices and systems in a network to be configured and managed. WMI uses the Common Information Model (CIM) to enable network administrators to access and share management information.

**WMI** See *Windows Management Instrumentation*.

### **WMI Query Language (WQL)**

A subset of the Structured Query Language with minor semantic changes to support Windows Management Instrumentation.

### **WQL**

See *WMI Query Language*.

---

# Index

## A

- abbreviation list 454
- acronym list 454
- added events 24
- Alert on LAN events 256
- Alert Standard Format 241, 374
- all events filter 39
- array
  - FlashCopy 89, 90, 91, 279, 280, 281, 393, 394
  - rebuild 91, 92, 93, 282, 283, 395, 396
  - synchronization 93, 94, 95, 284, 285, 396, 397
- Asset ID task 75, 153, 185, 263, 277, 383, 443
- authentication keys 445

## B

- bad stripe 101, 292, 402
- battery 108, 300, 408
- battery-backup cache 108, 109, 300, 408
- BIOS 246
- BladeCenter
  - Assistant events 29
  - Deployment wizard events 29
  - documentation 20
  - events 193, 354
  - Fibre Channel switch events 256
  - products 155, 190
  - books 20
- bootstrap loader program 238
- bottleneck event 60
- BrightStor Arcserve 348

## C

- Capacity Manager events 60
- category
  - event filters 41
  - certmgr command 64
  - changed events 28
- chassis (See also enclosure) 259, 378
- CIM events
  - Array 66
  - Automatic Server Restart 69
  - Certificate 64
  - DASD Backplane 70
  - Disk Space Low 71
  - Error Log 72
  - extended attributes 372
  - Fan 73
  - IP Change 74
  - IPMI Log 75
  - Lease Expiration 75
  - Life Cycle 76
  - Memory 77
  - Memory PFA 78
  - Network Adapter 79
  - Network Adapter Failed 79
  - Network Adapter Offline 79
  - Network Adapter Online 79
  - overview 64
  - PFA 81
  - Power State 82
  - Processor 85
  - Processor PFA 85
  - Redundant Network Adapter Switchback 86

CIM events (*continued*)

Redundant Network Adapter Switchover	87
Remote Login	88
Server Power Supply	88
ServerRAID Array FlashCopy Complete	89
ServerRAID Array FlashCopy Detected	90
ServerRAID Array FlashCopy Fail	91
ServerRAID Array Rebuild Complete	91
ServerRAID Array Rebuild Detected	92
ServerRAID Array Rebuild Fail	93
ServerRAID Array Sync Complete	93
ServerRAID Array Sync Detected	94
ServerRAID Array Sync Fail	95
ServerRAID Compaction Complete	95
ServerRAID Compaction Detected	96
ServerRAID Compaction Fail	97
ServerRAID Compression Complete	97
ServerRAID Compression Detected	98
ServerRAID Compression Fail	99
ServerRAID Config Fail	99
ServerRAID Controller Added	100
ServerRAID Controller Bad Stripes	101
ServerRAID Controller Battery Overtemp	102
ServerRAID Controller Battery Temp Normal	103
ServerRAID Controller Fail	104
ServerRAID Controller Failover	104
ServerRAID Controller Mismatched Versions	105
ServerRAID Controller Replaced	106
ServerRAID Copyback Complete	106
ServerRAID Copyback Detected	107
ServerRAID Copyback Fail	108
ServerRAID Dead Battery	108
ServerRAID Dead Battery Cache	109
ServerRAID Decompression Complete	110
ServerRAID Decompression Detected	110
ServerRAID Decompression Fail	111

CIM events (*continued*)

ServerRAID Defunct Drive	112
ServerRAID Defunct Drive FRU	112
ServerRAID Defunct Replaced	113
ServerRAID Drive Added	114
ServerRAID Drive Clear Complete	114
ServerRAID Drive Clear Detected	115
ServerRAID Drive Clear Fail	115
ServerRAID Drive Removed	116
ServerRAID Drive Verify Complete	117
ServerRAID Drive Verify Detected	117
ServerRAID Drive Verify Fail	118
ServerRAID Enclosure Fail	119
ServerRAID Enclosure Fan Fail	119
ServerRAID Enclosure Fan Installed	120
ServerRAID Enclosure Fan OK	121
ServerRAID Enclosure Fan Removed	122
ServerRAID Enclosure OK	122
ServerRAID Enclosure Power Supply Fail	123
ServerRAID Enclosure Power Supply Installed	124
ServerRAID Enclosure Power Supply OK	124
ServerRAID Enclosure Power Supply Removed	125
ServerRAID Enclosure Temp Fail	126
ServerRAID Enclosure Temp OK	126
ServerRAID Expansion Complete	127
ServerRAID Expansion Detected	128
ServerRAID Expansion Fail	128
ServerRAID FlashCopy Complete	129
ServerRAID FlashCopy Detected	130
ServerRAID FlashCopy Fail	130
ServerRAID Health Event	131
ServerRAID Init Detected	132
ServerRAID Init Fail	133
ServerRAID Logical Drive Added	134
ServerRAID Logical Drive Blocked	134
ServerRAID Logical Drive Critical	135

CIM events (*continued*)

ServerRAID Logical Drive Critical Periodic	136
ServerRAID Logical Drive Off Line	136
ServerRAID Logical Drive OK	137
ServerRAID Logical Drive Removed	137
ServerRAID Logical Drive Unblocked	138
ServerRAID Migration Complete	138
ServerRAID Migration Detected	139
ServerRAID Migration Fail	140
ServerRAID No Controllers	140
ServerRAID PFA Drive	141
ServerRAID PFA Drive FRU	141
ServerRAID Polling Fail	142
ServerRAID Rebuild Complete	143
ServerRAID Rebuild Detected	143
ServerRAID Rebuild Fail	144
ServerRAID Sync Complete	145
ServerRAID Sync Detected	145
ServerRAID Sync Fail	146
ServerRAID Test Event	147
ServerRAID Unsupported Drive	147
SMART Drive	148
Storage	66
Storage events	66
System	69
System Enclosure	148
System Event	149
Temperature	150
Voltage	152
Warranty Expiration	153
Windows NT Event Log	154
Windows NT Service	154
Windows Registry	154

CIM indications

conversion	69, 257
IBMPSSG_ChassisEvent	378

CIM indications (*continued*)

IBMPSSG_DASDBackplaneEvent	379
IBMPSSG_ErrorLogEvent	380
IBMPSSG_FanEvent	381
IBMPSSG_GenericFanEvent	382
IBMPSSG_GenericVoltageEvent	383
IBMPSSG_LeaseExpirationEvent	383
IBMPSSG_MemoryPFEEvent	384
IBMPSSG_NetworkAdapterFailedEvent	385
IBMPSSG_NetworkAdapterOfflineEvent	386
IBMPSSG_NetworkAdapterOnlineEvent	387
IBMPSSG_PFAEvent	387
IBMPSSG_PowerSupplyEvent	388
IBMPSSG_ProcessorPFEEvent	389
IBMPSSG_RedundantNetworkAdapterEvent	390
IBMPSSG_RedundantNetworkAdapterSwitchbackEvent	391
IBMPSSG_RedundantNetworkAdapterSwitchoverEvent	391
IBMPSSG_RemoteLoginEvent	392
IBMPSSG_ServerRAIDArrayFlashCopyComplete	393
IBMPSSG_ServerRAIDArrayFlashCopyDetected	394
IBMPSSG_ServerRAIDArrayFlashCopyFail	394
IBMPSSG_ServerRAIDArrayRebuildComplete	395
IBMPSSG_ServerRAIDArrayRebuildDetected	395
IBMPSSG_ServerRAIDArrayRebuildFail	396
IBMPSSG_ServerRAIDArraySyncComplete	396
IBMPSSG_ServerRAIDArraySyncDetected	397
IBMPSSG_ServerRAIDArraySyncFail	397
IBMPSSG_ServerRAIDCompactionComplete	398
IBMPSSG_ServerRAIDCompactionDetected	399
IBMPSSG_ServerRAIDCompactionFail	399
IBMPSSG_ServerRAIDCompressionComplete	400
IBMPSSG_ServerRAIDCompressionDetected	400
IBMPSSG_ServerRAIDCompressionFail	401
IBMPSSG_ServerRAIDConfigFail	401
IBMPSSG_ServerRAIDControllerAdded	402
IBMPSSG_ServerRAIDControllerBadStripes	402

CIM indications (*continued*)

IBMPSSG_ServerRAIDControllerBatteryOvertemp	403
IBMPSSG_ServerRAIDControllerBatteryTempNormal	403
IBMPSSG_ServerRAIDControllerFail	404
IBMPSSG_ServerRAIDControllerFailover	404
IBMPSSG_ServerRAIDControllerMismatchedVersions	405
IBMPSSG_ServerRAIDControllerReplaced	405
IBMPSSG_ServerRAIDCopyBackComplete	406
IBMPSSG_ServerRAIDCopyBackDetected	407
IBMPSSG_ServerRAIDCopyBackFail	407
IBMPSSG_ServerRAIDDeadBattery	408
IBMPSSG_ServerRAIDDeadBatteryCache	408
IBMPSSG_ServerRAIDDecompressionComplete	409
IBMPSSG_ServerRAIDDecompressionDetected	409
IBMPSSG_ServerRAIDDecompressionFail	410
IBMPSSG_ServerRAIDFunctionDrive	410
IBMPSSG_ServerRAIDFunctionDriveFRU	411
IBMPSSG_ServerRAIDFunctionReplaced	411
IBMPSSG_ServerRAIDDriveAdded	412
IBMPSSG_ServerRAIDDriveClearComplete	412
IBMPSSG_ServerRAIDDriveClearDetected	413
IBMPSSG_ServerRAIDDriveClearFail	413
IBMPSSG_ServerRAIDDriveRemoved	414
IBMPSSG_ServerRAIDDriveVerifyComplete	414
IBMPSSG_ServerRAIDDriveVerifyDetected	415
IBMPSSG_ServerRAIDDriveVerifyFail	415
IBMPSSG_ServerRAIDEnclosureFail	416
IBMPSSG_ServerRAIDEnclosureFanFail	417
IBMPSSG_ServerRAIDEnclosureFanInstalled	417
IBMPSSG_ServerRAIDEnclosureFanOK	418
IBMPSSG_ServerRAIDEnclosureFanRemoved	418
IBMPSSG_ServerRAIDEnclosureOK	419
IBMPSSG_ServerRAIDEnclosurePowerSupplyFail	419
IBMPSSG_ServerRAIDEnclosurePowerSupplyInstalled	420
IBMPSSG_ServerRAIDEnclosurePowerSupplyOK	420
IBMPSSG_ServerRAIDEnclosurePowerSupplyRemoved	421

CIM indications (*continued*)

IBMPSSG_ServerRAIDEnclosureTempFail	421
IBMPSSG_ServerRAIDEnclosureTempOK	422
IBMPSSG_ServerRAIDExpansionComplete	423
IBMPSSG_ServerRAIDExpansionDetected	423
IBMPSSG_ServerRAIDExpansionFail	424
IBMPSSG_ServerRAIDFlashCopyComplete	424
IBMPSSG_ServerRAIDFlashCopyDetected	425
IBMPSSG_ServerRAIDFlashCopyFail	425
IBMPSSG_ServerRAIDInitComplete	426
IBMPSSG_ServerRAIDInitDetected	426
IBMPSSG_ServerRAIDInitFail	427
IBMPSSG_ServerRAIDLogicalDriveAdded	427
IBMPSSG_ServerRAIDLogicalDriveBlocked	428
IBMPSSG_ServerRAIDLogicalDriveCritical	428
IBMPSSG_ServerRAIDLogicalDriveCriticalPeriodic	429
IBMPSSG_ServerRAIDLogicalDriveOffline	429
IBMPSSG_ServerRAIDLogicalDriveOK	430
IBMPSSG_ServerRAIDLogicalDriveRemoved	431
IBMPSSG_ServerRAIDLogicalDriveUnlocked	431
IBMPSSG_ServerRAIDMigrationComplete	432
IBMPSSG_ServerRAIDMigrationDetected	432
IBMPSSG_ServerRAIDMigrationFail	433
IBMPSSG_ServerRAIDNoControllers	433
IBMPSSG_ServerRAIDPFADrive	434
IBMPSSG_ServerRAIDPFADriveFRU	434
IBMPSSG_ServerRAIDPollingFail	435
IBMPSSG_ServerRAIDRebuildComplete	435
IBMPSSG_ServerRAIDRebuildDetected	436
IBMPSSG_ServerRAIDRebuildFail	436
IBMPSSG_ServerRAIDSyncComplete	437
IBMPSSG_ServerRAIDSyncDetected	437
IBMPSSG_ServerRAIDSyncFail	438
IBMPSSG_ServerRAIDTestEvent	438
IBMPSSG_ServerRAIDUnsupportedDrive	439
IBMPSSG_SMARTEvent	440



CIM indications (*continued*)

- IBMPSG\_SPPowerSupplyEvent 440
- IBMPSG\_StorageEvent 441
- IBMPSG\_TemperatureEvent 442
- IBMPSG\_VoltageEvent 443
- IBMPSG\_WarrantyExpirationEvent 443
- overview 378
- clear 114, 115, 306, 307, 308, 412, 413
- compaction 95, 96, 97, 286, 287, 288, 398, 399
- compatibility documents 20
- compression 97, 98, 99, 289, 290, 400, 401
- Configuration Manager events 155
- Configure ASF task 185
- Configure SNMP Agent task 185
- controller
  - added 100, 292, 402
  - fail 104, 295, 404
  - failover 104, 296, 404
  - mismatched versions 105, 347, 405
  - none 140, 333, 433
  - polling 142, 335, 435
  - replaced 106, 297, 405
  - copyback 106, 107, 108, 297, 298, 299, 406, 407
  - crash dump 204
  - critical
    - events 39
  - events filter 39
  - customer support 20

**D**

- database events 163
- date and time
  - event filters 41
- decompression 110, 111, 301, 302, 409, 410
- deleted events 29

- deprecated events 29
- DIMM 77, 78, 200, 264, 384
- Director events
  - Action 183
- Authorization Failure 171
- Bad Password 159
- Bad User ID 159

- CIM indications 378
- Communication Failure 171
- Console 159
- Custom Collection 171
- Database 163
- Director Agent 165, 373
- Disabled User ID 159
- Downlevel Console 159
- Error 180, 182
- Expired Password 159
- extended attributes 373
- General Failure 171
- Hardware Failure 171
- Inventory 171
- Inventory Monitor 173
- Job 179
- Logon Failure 159
- MIB 174
- MPA 166
- No data found 171
- Offline 184
- Online 184
- overview 158
- Process Alert 168
- Process Failed to Start 168
- Process Monitors 167
- Process Started 168
- Process Terminated 168
- Resource Monitors 170, 174

Director events (*continued*)

- Row Added 173
- Row Changed 173
- Row Removed 173
- Scheduler 178, 373
- Server Connection Available 163
- Server Connection Not Available 163
- Software Failure 171
- Success 180, 182
- Successful 171
- System 181
- Test 183
- Timeout Failure 171
- Too Many Active IDs 159
- Too Many Active Logons 159
- Topology 184
- Uplevel Console 159
- User Logoff 162
- User Logon 163
- documentation 20
- downloading 20
- compatibility documents 20
- hardware compatibility information 20
- IBM Director code 20
- IBM Director publications 20
- systems-management software 20
- DS300 66
- DS400 66
- DS4000 66
- duplication event filter 39

**E**

- enclosure
  - BladeCenter chassis 193, 194, 196
  - fail 119, 312, 416

enclosure (*continued*)

- OK 122, 314, 419
- system 148, 259, 378
- temperature 126, 344, 345, 421, 422
- enclosure fan
  - fail 119, 317, 417
  - installed 120, 318, 417
  - OK 121, 313, 418
  - removed 122, 319, 418
- enclosure power supply
  - fail 123, 336, 419
  - installed 124, 337, 420
  - OK 124, 338, 420
  - removed 125, 339, 421
- environment (illustration) 31
- environmental
  - events 150, 152, 226, 242, 262, 275, 276, 358, 383, 442, 443
  - sensor events filter 39
  - error log 72, 75, 260, 380
- event
  - BladeCenter 354
  - Capacity Manager 60
  - changed in IBM Director 5.10 28
  - CIM 64
  - Configuration Manager 155
  - Director 158
  - environmental 358
  - hardware component failure 359
  - i5/OS-specific 39
  - Mass Configuration 185
  - MPA 187
  - new in IBM Director 5.10 24
  - PET 241
  - processing 35
  - removed from IBM Director 5.10 29

- event (*continued*)
  - ServerRAID 361
  - service processor 369
  - SNMP 255
  - System Availability 350
  - testing 183
  - viewing details 58
  - Windows Event Log 351
  - Windows-specific 39
- event action plans
  - builder 56
  - example 50, 52, 54
  - filtering 41
  - wizard 56
- event filters
  - category 41
  - date and time 41
  - duplication event filter 39
  - event text 41
  - event type 41
  - exclusion event filter 39
  - extended attributes 41
  - Hardware Predictive Failure events 39
  - managed objects 41
  - severity levels 41
  - simple event filter 39
  - system variables 41
  - threshold
    - event 39
  - event filter 39
  - event text
    - event filters 41
  - event type
    - event filters 41
  - exclusion event filter 39
  - expansion 127, 128, 315, 316, 423, 424

- extended attributes
  - CIM 372
  - Director 373
  - event filters 41
  - MPA 374
  - overview 372
  - PET 374
  - SNMP 376, 377

## F

- failover 104, 296, 404
- fan 73, 201, 260, 261, 381, 382
- fatal events filter 39
- file
  - IBM-SERVERAID-MIB.mib 278
  - IBM-SYSTEM-TRAP-MIB.mib 257
  - FlashCopy 89, 90, 91, 129, 130, 279, 280, 281, 320, 321, 393, 394, 424, 425
  - FRU 112, 141, 304, 334, 411, 434
- function
  - Event Action Plan 56
  - event log 58

## G

- glossary 460

## H

- hard disk drive
  - added 114, 306, 412
  - clear 114, 115, 306, 307, 308, 412, 413
  - defunct 112, 303, 410
  - defunct FRU 112, 304, 411
  - hot spare 113, 305, 411

- hard disk drive (*continued*)
  - nonwarranted 147, 346, 439
  - PFA 141, 334, 434
  - removed 116, 309, 414
  - SMART 148, 272, 440
  - state change 70, 198, 259, 379
  - storage low 71, 274, 441
  - unsupported 147, 346, 439
  - verify 117, 118, 310, 311, 414, 415
- hardware
  - failure events 81, 210, 248, 268, 350, 359, 387
  - predictive failure events 39
  - predictive failure events filter 39
  - status
    - CIM indications 378
    - icons 378
  - hardware compatibility 20
- Hardware Management Console 69, 74, 76, 82, 149, 372
- harmless events filter 39
- help, IBM Director resources 20
- HP OpenView 378

## I

- I/O module 205
- i5/OS
  - events 39
- IBM Director Agent
  - events 165
  - source of events 158
  - state change 184
- IBM Director Console hardware status icons 378
- IBM Director Hardware and Software Compatibility
  - document 20
- IBM Director Server
  - viewing event details 58

- IBM eServer Information Center 20
- IBM System Storage devices 66
- IBM systems-management software
  - downloading 20
  - overview 20

## IBM Web sites

- eServer Information Center 20
- Redbooks 20
- ServerProven 20
- Support 20
- Systems Management Software 20
- xSeries Systems Management 20
- IBM-SERVERAID-MIB.mib 278
- IBM-SYSTEM-TRAP-MIB.mib 257
- illustrations
  - IBM Director environment 31
- initialization 132, 133, 322, 323, 324, 426, 427
- interim fixes 20
- inventory events 171, 173

## J

- job 167, 168, 170, 179, 180, 181, 182

## K

- keys, authentication 445
- KVM 207

## L

- LAN Leash 29
- lease expiration 75, 263, 383
- legal notices 449
- Log All Events 56

- logical drive
  - added 134, 325, 427
  - blocked 134, 325, 428
  - critical 135, 136, 326, 327, 428, 429
  - expansion 127, 128, 315, 316, 423, 424
  - FlashCopy 129, 130, 320, 321, 424, 425
  - initialization 132, 133, 322, 323, 324, 426, 427
  - migration 138, 139, 140, 331, 332, 432, 433
  - offline 136, 328, 429
  - OK 137, 329, 430
  - rebuild 143, 144, 339, 340, 341, 435, 436
  - removed 137, 329, 431
  - unblocked 138, 330, 431
- logoff 162
- logon 163
- logon failure 159

## M

- managed objects
  - event filters 41
  - types 187
- managed systems
  - definition 31
  - Level 2 158
  - security 64
  - state change 69
- management module events 190, 192, 193, 194, 196, 198, 200, 201, 205, 207, 210, 211, 214, 216, 218, 224, 225, 226, 238
- Management Processor Assistant 166
- management server
  - definition 31
- Mass Configuration events 185
- memory 77, 78, 200, 264, 384

- Message Browser
  - description of 49
  - MIB file 255, 257, 278
  - microprocessor 85, 196, 269, 389
  - Microsoft Operations Manager 2005 378
  - Microsoft System Management Server 378
  - migration 138, 139, 140, 331, 332, 432, 433
  - minor events filter 39
  - mismatched versions 105, 347, 405
  - modified events 28
  - monitoring 167, 168, 170, 173, 174
- MPA events
  - Blade Server 190
  - Bus 192
  - Chassis 193
  - Component 189
  - Configuration 194
  - CPU 196
  - Crash Dump 204, 209
  - DASD 198
  - DIMM events 200
  - Environmental 226
  - extended attributes 374
  - Failed 196
  - Fan 201
  - Hardware Information 203
  - I/O module 205
  - KVM 207
  - Miscellaneous 237
  - OS Image 208
  - overview 187
  - PET events 241
  - PFA 210
  - Platform 238
  - Power Subsystem 211
  - Power Supply 214

MPA events (*continued*)

- Server 216
- Server WatchDog 238
- Service Processor 218
- SMP Expansion Module 223
- Unknown 240
- USB 224
- VRM 225

**N**

- network adapter 79, 86, 87, 265, 266, 267, 270, 271, 385, 386, 387, 390, 391
- Network Configuration task 185
- network device 205
- new events 24
- NIC 79, 86, 87, 265, 266, 267, 270, 271, 385, 386, 387, 390, 391
- nonwarranted hard disk drive 147, 346, 439

**O**

- operating system
  - compatibility 20
  - state change 208, 209, 252, 253

**P**

- PET events
  - BIOS 247
  - Boot 253
  - Cable/Interconnect 248
  - Case Intrusion 242
  - Current 242
  - Drivebay 248
  - Environmental 242

PET events (*continued*)

- extended attributes 374
- Fan 242
- Firmware 246
- Hardware 248
- Heartbeat 253
- Module/Board 248
- Monitor ASIC/IC 248
- Network 248
- Operation 253
- OS 253
- overview 241
- Power Supply 242
- Progress 247
- Sensor 242
- System 252
- Temperature 242
- Voltage 242
- Watchdog 248
- PFA 78, 81, 85, 141, 210, 264, 268, 269, 334, 384, 387, 389, 434
- Platform Event Trap 241
- polling 142, 335, 435
- POST failed 238
- power supply 88, 214, 268, 273, 388, 440
- Process Monitors events 167, 168
- processor 85
- pSeries events
  - IP Change 74
  - Life Cycle 76
  - Power State 82
  - System Event 149
  - publications 20

## R

- rebuild 91, 92, 93, 143, 144, 282, 283, 339, 340, 341, 395, 396, 435, 436
- Redbooks 20
- redundant NIC 86, 87, 270, 271, 390, 391
- related information 20
- remote login 29, 88, 272, 392
- Remote Supervisor Adapter
  - documentation 20
  - remote login 88, 272, 392
- removed events 29
- renamed events 28
- Resource Monitors events 170, 174
- revised events 28

## S

- scalable partition events 238
- Scalable Systems Manager 238
- scheduled job 167, 168, 170
- Scheduler events 178, 179, 180, 181, 182
- security
  - events filter 39
    - Level 1 64
- ServeRAID events
  - array
    - FlashCopy 89, 90, 91, 279, 280, 281, 393, 394
    - rebuild 91, 92, 93, 282, 283, 395, 396
    - synchronization 93, 94, 95, 284, 285, 396, 397
    - battery 102, 103, 108, 300, 403, 408
    - battery-backup cache 109, 300, 408
    - compaction 95, 96, 97, 286, 287, 288, 398, 399
    - compression 97, 98, 99, 289, 290, 400, 401
    - configuration 99, 291, 401

## ServeRAID events (*continued*)

- controller
  - added 100, 292, 402
  - bad stripe 101, 292, 402
  - battery 102, 103, 294, 403
  - fail 104, 295, 404
  - failover 104, 296, 404
  - mismatched versions 105, 347, 405
  - none 140, 333, 433
  - polling 142, 335, 435
  - replaced 106, 297, 405
- copyback 106, 107, 108, 297, 298, 299, 406, 407
- decompression 110, 111, 301, 302, 409, 410
- enclosure
  - fail 119, 312, 416
  - OK 122, 314, 419
  - temperature 126, 344, 345, 421, 422
- enclosure fan
  - fail 119, 317, 417
  - installed 120, 318, 417
  - OK 121, 313, 418
  - removed 122, 319, 418
- enclosure power supply
  - fail 123, 336, 419
  - installed 124, 337, 420
  - OK 124, 338, 420
  - removed 125, 339, 421
- event
  - Storage 349
  - expansion 127, 128, 315, 316, 423, 424
- hard disk drive
  - added 114, 306, 412
  - clear 114, 115, 306, 307, 308, 412, 413
  - defunct 112, 303, 410
  - defunct FRU 112, 304, 411
  - hot spare 113, 305, 411

## ServerRAID events (*continued*)

- hard disk drive (*continued*)
  - PFA 141, 334, 434
  - removed 116, 309, 414
  - unsupported 147, 346, 439
  - verify 117, 118, 310, 311, 414, 415
- initialization 132, 133, 322, 323, 324, 426, 427
- listing 361
- logical drive 106, 107, 108, 110, 111, 127, 128, 297, 298, 299, 301, 302, 315, 316, 406, 407, 409, 410, 423, 424
  - added 134, 325, 427
  - blocked 134, 325, 428
  - critical 135, 136, 326, 327, 428, 429
  - FlashCopy 129, 130, 320, 321, 424, 425
  - initialization 132, 133, 322, 323, 324, 426, 427
  - migration 138, 139, 140, 331, 332, 432, 433
  - offline 136, 328, 429
  - OK 137, 329, 430
  - rebuild 143, 144, 339, 340, 341, 435, 436
  - removed 137, 329, 431
  - synchronization 145, 146, 342, 343, 437, 438
  - unblocked 138, 330, 431
  - migration 138, 139, 140, 331, 332, 432, 433
- NetWare 349
- overview 278
- polling 142, 335, 435
- rebuild 143, 144, 339, 340, 341, 435, 436
- ServerRAID Health Event 131
- ServerRAID Manager (Standalone Edition) 256
- Storage 349
- synchronization 145, 146, 342, 343, 437, 438
- temperature 126, 344, 345, 421, 422
- test event 147, 345, 438
- variable binding 377
- ServerRAID Manager (Standalone Edition) 256
- service packs 20

## service processors

- documentation 20
- events 166, 192, 196, 198, 200, 201, 203, 204, 207, 208, 209, 210, 211, 214, 216, 218, 223, 224, 225, 226, 237, 238, 240, 369
- MPA events 187
- remote login 88, 272, 392
- severity levels
- event filters 41
- simple event filter
  - definition 39
  - predefined filters 39
- SMART drive 148, 272, 440
- SMI-S 66
- SMP Expansion Module 223
- SNMP devices
  - definition 31
- SNMP events
  - Alert on LAN 256
  - BladeCenter Fibre Channel switches 256
  - BrightStor Arcserve 348
  - CIM indications 378
  - hardware 256
  - iBMServeRAIDArrayFlashCopyComplete 279
  - iBMServeRAIDArrayFlashCopyDetected 280
  - iBMServeRAIDArrayFlashCopyFail 281
  - iBMServeRAIDArrayRebuildComplete 282
  - iBMServeRAIDArrayRebuildDetected 282
  - iBMServeRAIDArrayRebuildFail 283
  - iBMServeRAIDArraySyncComplete 284
  - iBMServeRAIDArraySyncDetected 285
  - iBMServeRAIDArraySyncFail 285
  - iBMServeRAIDCompactionComplete 286
  - iBMServeRAIDCompactionDetected 287
  - iBMServeRAIDCompactionFail 288
  - iBMServeRAIDCompressionComplete 289



SNMP events (*continued*)

iBMServerRAIDCompressionDetected 289  
 iBMServerRAIDCompressionFail 290  
 iBMServerRAIDConfigFail 291  
 iBMServerRAIDControllerAdded 292  
 iBMServerRAIDControllerBadStripes 292  
 iBMServerRAIDControllerBatteryOvertemp 294  
 iBMServerRAIDControllerBatteryTempNormal 294  
 iBMServerRAIDControllerFail 295  
 iBMServerRAIDControllerFailover 296  
 iBMServerRAIDControllerReplaced 297  
 iBMServerRAIDCopyBackComplete 297  
 iBMServerRAIDCopyBackDetected 298  
 iBMServerRAIDCopyBackFail 299  
 iBMServerRAIDDeadBattery 300  
 iBMServerRAIDDeadBatteryCache 300  
 iBMServerRAIDDecompressionComplete 301  
 iBMServerRAIDDecompressionDetected 302  
 iBMServerRAIDDecompressionFail 302  
 iBMServerRAIDDefunctDrive 303  
 iBMServerRAIDDefunctDriveFRU 304  
 iBMServerRAIDDefunctReplaced 305  
 iBMServerRAIDDriveAdded 306  
 iBMServerRAIDDriveClearComplete 306  
 iBMServerRAIDDriveClearDetected 307  
 iBMServerRAIDDriveClearFail 308  
 iBMServerRAIDDriveRemoved 309  
 iBMServerRAIDDriveVerifyComplete 310  
 iBMServerRAIDDriveVerifyDetected 310  
 iBMServerRAIDDriveVerifyFail 311  
 iBMServerRAIDEnclosureFail 312  
 iBMServerRAIDEnclosureFanOK 313  
 iBMServerRAIDEnclosureOK 314  
 iBMServerRAIDExpansionComplete 315  
 iBMServerRAIDExpansionDetected 315  
 iBMServerRAIDExpansionFail 316

SNMP events (*continued*)

iBMServerRAIDFanFail 317  
 iBMServerRAIDFanInstalled 318  
 iBMServerRAIDFanRemoved 319  
 iBMServerRAIDFlashCopyComplete 320  
 iBMServerRAIDFlashCopyDetected 320  
 iBMServerRAIDFlashCopyFail 321  
 iBMServerRAIDInitComplete 322  
 iBMServerRAIDInitDetected 323  
 iBMServerRAIDInitFail 324  
 iBMServerRAIDLogicalDriveAdded 325  
 iBMServerRAIDLogicalDriveBlocked 325  
 iBMServerRAIDLogicalDriveCritical 326  
 iBMServerRAIDLogicalDriveCriticalPeriodic 327  
 iBMServerRAIDLogicalDriveOffline 328  
 iBMServerRAIDLogicalDriveOK 329  
 iBMServerRAIDLogicalDriveRemoved 329  
 iBMServerRAIDLogicalDriveUnblocked 330  
 iBMServerRAIDMIB 278  
 iBMServerRAIDMigrationComplete 331  
 iBMServerRAIDMigrationDetected 331  
 iBMServerRAIDMigrationFail 332  
 iBMServerRAIDNoControllers 333  
 iBMServerRAIDPFADrive 334  
 iBMServerRAIDPFADriveFRU 334  
 iBMServerRAIDPollingFail 335  
 iBMServerRAIDPowerSupplyFail 336  
 iBMServerRAIDPowerSupplyInstalled 337  
 iBMServerRAIDPowerSupplyOK 338  
 iBMServerRAIDPowerSupplyRemoved 339  
 iBMServerRAIDRebuildComplete 339  
 iBMServerRAIDRebuildDetected 340  
 iBMServerRAIDRebuildFail 341  
 iBMServerRAIDSyncComplete 342  
 iBMServerRAIDSyncDetected 342  
 iBMServerRAIDSyncFail 343

SNMP events (*continued*)

- ibmServerRAIDTempFail 344
- ibmServerRAIDTempOK 345
- ibmServerRAIDTestEvent 345
- ibmServerRAIDUnsupportedDrive 346
- ibmServerRAIDVersionMismatch 347
- ibmSystemMIB 257
- ibmSystemTrapChassis 259
- ibmSystemTrapDASDBackplane 259
- ibmSystemTrapErrorLog 260
- ibmSystemTrapFan 260
- ibmSystemTrapGenericFan 261
- ibmSystemTrapGenericVoltage 262
- ibmSystemTrapLeaseExpiration 263
- ibmSystemTrapMemoryPF 264
- ibmSystemTrapNetworkAdapterFailed 265
- ibmSystemTrapNetworkAdapterOffline 266
- ibmSystemTrapNetworkAdapterOnline 267
- ibmSystemTrapPFA 268
- ibmSystemTrapPowerSupply 268
- ibmSystemTrapProcessorPF 269
- ibmSystemTrapRedundantNIC 270
- ibmSystemTrapRedundantNICSwitchback 270
- ibmSystemTrapRedundantNICSwitchover 271
- ibmSystemTrapRemotelogin 272
- ibmSystemTrapSMART 272
- ibmSystemTrapSPPowerSupply 273
- ibmSystemTrapStorage 274
- ibmSystemTrapTemperature 275
- ibmSystemTrapVoltage 276
- ibmSystemTrapWarrantyExpiration 277
- overview 255
- ServerRAID controllers 256
- Software 348
- Tape drives 256
- UPS devices 256

SNMP events (*continued*)

- variable binding 376, 377
- Veritas Backup Exec 348
- Storage events 349
- storage events filter 39
- switch 205
- synchronization 93, 94, 95, 145, 146, 284, 285, 342, 343, 396, 397, 437, 438
- System Availability events 350
- system capacity event 60
- system variables
- event filters 41

## T

- Tape drive events 256
- tasks
- Event Action Plan 56
- event log 58
- temperature 150, 275, 442
- terminology
- managed system 31
- management server 31
- SNMP device 31
- threshold event
- filter 39
- simple event filter 39
- timeout settings 238
- Tivoli Enterprise Console
- native events 378
- SNMP events 378
- Tivoli NetView 378
- trademarks 451

## U

- unknown events filter 39
- UPS device events 256
- Upward Integration Modules 257
- USB 224
- user
  - logoff 162
  - logon 163

## V

- variable binding 372, 374, 376, 377
- verify 117, 118, 310, 311, 414, 415
- Veritas Backup Exec 348
- voltage 152, 262, 276, 383, 443

## W

- warning events filter 39
- warranty expiration 153, 277, 443

## Web site

- IBM Director resources 20
- IBM Redbooks 20
- IBM ServerProven 20
- IBM Support 20
- IBM Systems Management Software 20
- IBM xSeries Systems Management 20

## Windows

- Event Log events 154, 351, 378
- Event Log ID 378
- events 39, 154, 351, 378

## wizards

- Event Action Plan 56