CDP Private Cloud Base 7.1.5

Cloudera Manager Health Tests

Date published: 2020-10-09
Date modified: 2020-11-25

Legal Notice

© Cloudera Inc. 2024. All rights reserved.

The documentation is and contains Cloudera proprietary information protected by copyright and other intellectual property rights. No license under copyright or any other intellectual property right is granted herein.

Unless otherwise noted, scripts and sample code are licensed under the Apache License, Version 2.0.

Copyright information for Cloudera software may be found within the documentation accompanying each component in a particular release.

Cloudera software includes software from various open source or other third party projects, and may be released under the Apache Software License 2.0 (“ASLv2”), the Affero General Public License version 3 (AGPLv3), or other license terms. Other software included may be released under the terms of alternative open source licenses. Please review the license and notice files accompanying the software for additional licensing information.

Please visit the Cloudera software product page for more information on Cloudera software. For more information on Cloudera support services, please visit either the Support or Sales page. Feel free to contact us directly to discuss your specific needs.

Cloudera reserves the right to change any products at any time, and without notice. Cloudera assumes no responsibility nor liability arising from the use of products, except as expressly agreed to in writing by Cloudera.

Cloudera, Cloudera Altus, HUE, Impala, Cloudera Impala, and other Cloudera marks are registered or unregistered trademarks in the United States and other countries. All other trademarks are the property of their respective owners.

Disclaimer: EXCEPT AS EXPRESSLY PROVIDED IN A WRITTEN AGREEMENT WITH CLOUDERA, CLOUDERA DOES NOT MAKE NOR GIVE ANY REPRESENTATION, WARRANTY, NOR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, IN CONNECTION WITH CLOUDERA TECHNOLOGY OR RELATED SUPPORT PROVIDED IN CONNECTION THEREWITH. CLOUDERA DOES NOT WARRANT THAT CLOUDERA PRODUCTS NOR SOFTWARE WILL OPERATE UNINTERRUPTED NOR THAT IT WILL BE FREE FROM DEFECTS NOR ERRORS, THAT IT WILL PROTECT YOUR DATA FROM LOSS, CORRUPTION NOR UNAVAILABILITY, NOR THAT IT WILL MEET ALL OF CUSTOMER’S BUSINESS REQUIREMENTS. WITHOUT LIMITING THE FOREGOING, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, CLOUDERA EXPRESSLY DISCLAIMS ANY AND ALL IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, QUALITY, NON-INFRINGEMENT, TITLE, AND FITNESS FOR A PARTICULAR PURPOSE AND ANY REPRESENTATION, WARRANTY, OR COVENANT BASED ON COURSE OF DEALING OR USAGE IN TRADE.

Contents

Cloudera Manager Health Tests....22
Active Database Health Tests....22
Active Database Audit Pipeline Test....22
Active Database File Descriptors....23
Active Database Host Health....23
Active Database Process Status....24
Active Database Swap Memory Usage....24
Active Database Unexpected Exits....25
Active Key Trustee Server Health Tests....25
Active Key Trustee Server Audit Pipeline Test....25
Active Key Trustee Server File Descriptors....26
Active Key Trustee Server Host Health....27
Active Key Trustee Server Log Directory Free Space....27
Active Key Trustee Server Process Status....28
Active Key Trustee Server Swap Memory Usage....28
Active Key Trustee Server Unexpected Exits....29
Activity Monitor Health Tests....29
Activity Monitor Activity Monitor Pipeline....29
Activity Monitor Activity Tree Pipeline....30
Activity Monitor Audit Pipeline Test....30
Activity Monitor Cloudera Manager Descriptor Age....31
Activity Monitor File Descriptors....32
Activity Monitor Heap Dump Directory Free Space....32
Activity Monitor Host Health....33
Activity Monitor Log Directory Free Space....33
Activity Monitor Pause Duration....34
Activity Monitor Process Status....35
Activity Monitor Swap Memory Usage....35
Activity Monitor Unexpected Exits....35
Activity Monitor Web Server Status....36
Alert Publisher Health Tests....37
Alert Publisher Audit Pipeline Test....37
Alert Publisher File Descriptors....38
Alert Publisher Heap Dump Directory Free Space....38
Alert Publisher Host Health....39
Alert Publisher Log Directory Free Space....39
Alert Publisher Process Status....40
Alert Publisher Swap Memory Usage....40
Alert Publisher Unexpected Exits....41
Atlas Health Tests....41
Atlas Server Health....41
Atlas Server Health Tests....42
Atlas Server Audit Pipeline Test....42
Atlas Server File Descriptors....43
Atlas Server Host Health....43
Atlas Server Log Directory Free Space....44
Atlas Server Process Status....44
Atlas Server Swap Memory Usage....45
Atlas Server Unexpected Exits....45

Authentication Server Health Tests....46
Authentication Server Audit Pipeline Test.... 46
Authentication Server File Descriptors....47
Authentication Server Heap Dump Directory Free Space....47
Authentication Server Host Health.... 48
Authentication Server Log Directory Free Space....48
Authentication Server Process Status....49
Authentication Server Swap Memory Usage....49
Authentication Server Unexpected Exits.... 50
Authentication Server Load Balancer Health Tests....50
Authentication Server Load Balancer Audit Pipeline Test....50
Authentication Server Load Balancer File Descriptors.... 51
Authentication Server Load Balancer Host Health....52
Authentication Server Load Balancer Log Directory Free Space....52
Authentication Server Load Balancer Process Status....53
Authentication Server Load Balancer Swap Memory Usage.... 53
Authentication Server Load Balancer Unexpected Exits....54
Authentication Service Health Tests....54
Authentication Service Authentication Server Health.... 54
Authentication Service Authentication Server Load Balancer Health....55
Authentication Service Canary....56
Cloudera Management Service Health Tests....56
Cloudera Management Service Activity Monitor Health.... 56
Cloudera Management Service Alert Publisher Health.... 56
Cloudera Management Service Certificate Expiration....57
Cloudera Management Service Cloudera Manager Server Clock Offset....57
Cloudera Management Service Command Storage Directory Free Space....57
Cloudera Management Service Embedded Database Free Space....58
Cloudera Management Service Event Server Health....58
Cloudera Management Service Host Monitor Health....59
Cloudera Management Service KDC Server Connection Health.... 59
Cloudera Management Service LDAP Server Connection Health.... 60
Cloudera Management Service Navigator Audit Server Health....60
Cloudera Management Service Navigator Metadata Server Health.... 60
Cloudera Management Service Reports Manager Health....61
Cloudera Management Service Service Monitor Health.... 61
Cloudera Management Service Telemetry Publisher Health.... 62
Cruise Control Health Tests....62
Cruise Control Server Health....62
Cruise Control Server Health Tests.... 62
Cruise Control Server Audit Pipeline Test.... 62
Cruise Control Server File Descriptors....63
Cruise Control Server Host Health.... 64
Cruise Control Server Log Directory Free Space....64
Cruise Control Server Process Status....65
Cruise Control Server Swap Memory Usage....65
Cruise Control Server Unexpected Exits.... 66
Data Analytics Studio Eventprocessor Health Tests....66
Data Analytics Studio Eventprocessor Audit Pipeline Test....66
Data Analytics Studio Eventprocessor File Descriptors.... 67
Data Analytics Studio Eventprocessor Host Health.... 68
Data Analytics Studio Eventprocessor Log Directory Free Space.... 68
Data Analytics Studio Eventprocessor Process Status....69
Data Analytics Studio Eventprocessor Swap Memory Usage.... 69
Data Analytics Studio Eventprocessor Unexpected Exits....70
Data Analytics Studio Webapp Server Health Tests.... 70

Data Analytics Studio Webapp Server Audit Pipeline Test....70
Data Analytics Studio Webapp Server File Descriptors....71
Data Analytics Studio Webapp Server Host Health....72
Data Analytics Studio Webapp Server Log Directory Free Space....72
Data Analytics Studio Webapp Server Process Status....73
Data Analytics Studio Webapp Server Swap Memory Usage....73
Data Analytics Studio Webapp Server Unexpected Exits....74
DataNode Health Tests....74
DataNode Audit Pipeline Test....74
DataNode Block Count....75
DataNode Data Directory Status....76
DataNode DataNode Data Directory Free Space....76
DataNode File Descriptors....77
DataNode Free Space....77
DataNode Heap Dump Directory Free Space....78
DataNode Host Health....78
DataNode Log Directory Free Space....79
DataNode NameNode Connectivity....79
DataNode Pause Duration....80
DataNode Process Status....81
DataNode Swap Memory Usage....81
DataNode Transceiver Usage....82
DataNode Unexpected Exits....82
DataNode Web Server Status....83
Event Server Health Tests....84
Event Server Audit Pipeline Test....84
Event Server Cloudera Manager Descriptor Age....85
Event Server Event Server Index Directory Free Space....85
Event Server Event Store Size....86
Event Server File Descriptors....86
Event Server GC Duration....87
Event Server Heap Dump Directory Free Space....87
Event Server Host Health....88
Event Server Log Directory Free Space....88
Event Server Process Status....89
Event Server Swap Memory Usage....89
Event Server Unexpected Exits....90
Event Server Web Server Status....90
Event Server Write Pipeline....91
Failover Controller Health Tests....92
Failover Controller Audit Pipeline Test....92
Failover Controller File Descriptors....93
Failover Controller Heap Dump Directory Free Space....93
Failover Controller Host Health....94
Failover Controller Log Directory Free Space....94
Failover Controller Process Status....95
Failover Controller Swap Memory Usage....95
Failover Controller Unexpected Exits....96
Flume Health Tests....96
Flume Agent Health....96
Flume Agent Health Tests....97
Flume Agent Audit Pipeline Test....97
Flume Agent File Descriptors....98
Flume Agent Heap Dump Directory Free Space....98
Flume Agent Host Health....99
Flume Agent Log Directory Free Space....99

Flume Agent Process Status....100
Flume Agent Swap Memory Usage....100
Flume Agent Unexpected Exits....101
Flume Agent Web Server Status....101
Garbage Collector Health Tests....102
Garbage Collector Audit Pipeline Test....102
Garbage Collector File Descriptors....103
Garbage Collector Host Health....103
Garbage Collector Log Directory Free Space....104
Garbage Collector Process Status....104
Garbage Collector Swap Memory Usage....105
Garbage Collector Unexpected Exits....105
HBase Health Tests....106
HBase Master Health....106
HBase RegionServer Health....107
HBase REST Server Health Tests....108
HBase REST Server Audit Pipeline Test....108
HBase REST Server File Descriptors....108
HBase REST Server Heap Dump Directory Free Space....109
HBase REST Server Host Health....110
HBase REST Server Log Directory Free Space....110
HBase REST Server Process Status....111
HBase REST Server Swap Memory Usage....111
HBase REST Server Unexpected Exits....111
HBase Thrift Server Health Tests....112
HBase Thrift Server Audit Pipeline Test....112
HBase Thrift Server File Descriptors....113
HBase Thrift Server Heap Dump Directory Free Space....113
HBase Thrift Server Host Health....114
HBase Thrift Server Log Directory Free Space....114
HBase Thrift Server Process Status....115
HBase Thrift Server Swap Memory Usage....116
HBase Thrift Server Unexpected Exits....116
HDFS Health Tests....117
HDFS Canary....117
HDFS Corrupt Blocks....117
HDFS DataNode Health....118
HDFS Erasure Coding Policy Verification Test....118
HDFS Failover Controllers Health....119
HDFS Free Space....119
HDFS Missing Blocks....120
HDFS NameNode Health....120
HDFS Under-Replicated Blocks....121
History Server Health Tests....122
History Server Audit Pipeline Test....122
History Server File Descriptors....123
History Server Host Health....123
History Server Log Directory Free Space....124
History Server Process Status....124
History Server Swap Memory Usage....125
History Server Unexpected Exits....125
Hive Health Tests....126
Hive Metastore Server Health....126
Hive WebHCat Server Health....126
HiveServer2 Health....127
Hive Execution Health Tests....128

Hive Execution HiveServer2 Health....128
Hive LLAP Health Tests....128
Hive LLAP HiveServer2 Health....128
Hive LLAP LLAP Proxy Health....129
Hive Metastore Server Health Tests....129
Hive Metastore Server Audit Pipeline Test....129
Hive Metastore Server File Descriptors....130
Hive Metastore Server Heap Dump Directory Free Space....130
Hive Metastore Server Hive Metastore Canary....131
Hive Metastore Server Host Health....132
Hive Metastore Server Log Directory Free Space....132
Hive Metastore Server Pause Duration....133
Hive Metastore Server Process Status....133
Hive Metastore Server Swap Memory Usage....134
Hive Metastore Server Unexpected Exits....134
Hive on Tez Health Tests....135
Hive on Tez HiveServer2 Health....135
HiveServer2 Health Tests....136
HiveServer2 Audit Pipeline Test....136
HiveServer2 File Descriptors....136
HiveServer2 Heap Dump Directory Free Space....137
HiveServer2 Hive Downloaded Resources Directory Free Space....138
HiveServer2 Hive Local Scratch Directory Free Space....138
HiveServer2 Host Health....139
HiveServer2 Log Directory Free Space....139
HiveServer2 Pause Duration....140
HiveServer2 Process Status....141
HiveServer2 Swap Memory Usage....141
HiveServer2 Unexpected Exits....141
Host Health Tests....142
Host Agent Log Directory....142
Host Agent Parcel Directory....143
Host Agent Process Directory....143
Host Agent Status....144
Host Certificate Expiration....145
Host Clock Offset....145
Host DNS Resolution....146
Host Entropy....146
Host Frame Errors....147
Host Network Interface Speed....147
Host Swapping....148
Host Monitor Health Tests....149
Host Monitor Audit Pipeline Test....149
Host Monitor Cloudera Manager Descriptor Age....150
Host Monitor Cloudera Manager Metric Schema Age....150
Host Monitor File Descriptors....151
Host Monitor Heap Dump Directory Free Space....151
Host Monitor Host Health....152
Host Monitor Host Monitor Storage Directory Free Space....152
Host Monitor Host Pipeline....153
Host Monitor Log Directory Free Space....154
Host Monitor Metrics Aggregation Run Duration Test....154
Host Monitor Pause Duration....155
Host Monitor Process Status....155
Host Monitor Swap Memory Usage....156
Host Monitor Unexpected Exits....156

Host Monitor Web Server Status.....157
HttpFS Health Tests.....158
HttpFS Audit Pipeline Test.....158
HttpFS File Descriptors.....158
HttpFS Heap Dump Directory Free Space.....159
HttpFS Host Health.....160
HttpFS Log Directory Free Space.....160
HttpFS Process Status.....161
HttpFS Swap Memory Usage.....161
HttpFS Unexpected Exits.....161
Hue Health Tests.....162
Hue Kerberos Ticket Renewer Health.....162
Hue Load Balancer Health.....163
Hue Server Health.....163
Hue Server Health Tests.....164
Hue Server Audit Pipeline Test.....164
Hue Server File Descriptors.....165
Hue Server Heap Dump Directory Free Space.....165
Hue Server Host Health.....166
Hue Server Log Directory Free Space.....166
Hue Server Process Status.....167
Hue Server Swap Memory Usage.....167
Hue Server Unexpected Exits.....167
Hue Server Web Server Status.....168
Impala Health Tests.....169
Impala Catalog Server Health.....169
Impala Daemon Health.....169
Impala Llama ApplicationMaster Health.....170
Impala StateStore Health.....170
Impala Catalog Server Health Tests.....171
Impala Catalog Server Audit Pipeline Test.....171
Impala Catalog Server File Descriptors.....172
Impala Catalog Server Heap Dump Directory Free Space.....172
Impala Catalog Server Host Health.....173
Impala Catalog Server Log Directory Free Space.....173
Impala Catalog Server Process Status.....174
Impala Catalog Server Resident Set Size.....174
Impala Catalog Server StateStore Connectivity.....175
Impala Catalog Server Swap Memory Usage.....176
Impala Catalog Server Unexpected Exits.....176
Impala Catalog Server Web Server Status.....177
Impala Daemon Health Tests.....177
Impala Daemon Audit Pipeline Test.....177
Impala Daemon File Descriptors.....178
Impala Daemon Heap Dump Directory Free Space.....179
Impala Daemon Host Health.....179
Impala Daemon Impala Concurrent Client Connections.....180
Impala Daemon Impala Daemon Ready Check.....180
Impala Daemon Impala Daemon Scratch Directories Free Space.....181
Impala Daemon Log Directory Free Space.....181
Impala Daemon Pause Duration.....182
Impala Daemon Process Status.....183
Impala Daemon Query Monitoring Status Check.....183
Impala Daemon Resident Set Size.....185
Impala Daemon StateStore Connectivity.....185
Impala Daemon Swap Memory Usage.....186

Impala Daemon Unexpected Exits....186
Impala Daemon Web Server Status....187
Impala Llama ApplicationMaster Health Tests....188
Impala Llama ApplicationMaster Audit Pipeline Test....188
Impala Llama ApplicationMaster File Descriptors....189
Impala Llama ApplicationMaster Heap Dump Directory Free Space....189
Impala Llama ApplicationMaster Host Health....190
Impala Llama ApplicationMaster Log Directory Free Space....190
Impala Llama ApplicationMaster Process Status....191
Impala Llama ApplicationMaster Swap Memory Usage....191
Impala Llama ApplicationMaster Unexpected Exits....192
Impala StateStore Health Tests....192
Impala StateStore Audit Pipeline Test....192
Impala StateStore File Descriptors....193
Impala StateStore Heap Dump Directory Free Space....194
Impala StateStore Host Health....194
Impala StateStore Log Directory Free Space....195
Impala StateStore Process Status....195
Impala StateStore Resident Set Size....196
Impala StateStore Swap Memory Usage....196
Impala StateStore Unexpected Exits....197
Impala StateStore Web Server Status....197
JobHistory Server Health Tests....198
JobHistory Server Audit Pipeline Test....198
JobHistory Server File Descriptors....199
JobHistory Server GC Duration....199
JobHistory Server Heap Dump Directory Free Space....200
JobHistory Server Host Health....201
JobHistory Server Log Directory Free Space....201
JobHistory Server Process Status....202
JobHistory Server Swap Memory Usage....202
JobHistory Server Unexpected Exits....203
JobHistory Server Web Server Status....203
JobTracker Health Tests....204
JobTracker Audit Pipeline Test....204
JobTracker File Descriptors....205
JobTracker GC Duration....205
JobTracker Heap Dump Directory Free Space....206
JobTracker Host Health....207
JobTracker Log Directory Free Space....207
JobTracker Process Status....208
JobTracker Swap Memory Usage....208
JobTracker Unexpected Exits....208
JobTracker Web Server Status....209
JournalNode Health Tests....210
JournalNode Audit Pipeline Test....210
JournalNode File Descriptors....211
JournalNode Fsync Latency....211
JournalNode GC Duration....211
JournalNode Heap Dump Directory Free Space....212
JournalNode Host Health....213
JournalNode JournalNode Edits Directory Free Space....213
JournalNode Log Directory Free Space....214
JournalNode Process Status....214
JournalNode Swap Memory Usage....215
JournalNode Sync Status....215

JournalNode Unexpected Exits.... 216
JournalNode Web Server Status....217
Kafka Health Tests.... 217
Kafka Broker Health....217
Kafka Connect Health.... 218
Kafka Broker Health Tests....218
Kafka Broker Audit Pipeline Test....218
Kafka Broker File Descriptors.... 219
Kafka Broker Host Health....220
Kafka Broker Lagging Replicas Test....220
Kafka Broker Log Directory Free Space.... 220
Kafka Broker Offline Directory Test.... 221
Kafka Broker Offline Partitions Test.... 221
Kafka Broker Process Status.... 221
Kafka Broker Swap Memory Usage.... 221
Kafka Broker Unexpected Exits....222
Kafka Connect Health Tests....222
Kafka Connect Audit Pipeline Test.... 222
Kafka Connect File Descriptors.... 223
Kafka Connect Host Health....224
Kafka Connect Log Directory Free Space....224
Kafka Connect Process Status....225
Kafka Connect Swap Memory Usage....225
Kafka Connect Unexpected Exits.... 226
Kafka MirrorMaker Health Tests....226
Kafka MirrorMaker Audit Pipeline Test....226
Kafka MirrorMaker File Descriptors.... 227
Kafka MirrorMaker Host Health....228
Kafka MirrorMaker Log Directory Free Space.... 228
Kafka MirrorMaker Process Status....229
Kafka MirrorMaker Swap Memory Usage.... 229
Kafka MirrorMaker Unexpected Exits....230
Kerberos Ticket Renewer Health Tests.... 230
Kerberos Ticket Renewer Audit Pipeline Test.... 230
Kerberos Ticket Renewer File Descriptors....231
Kerberos Ticket Renewer Heap Dump Directory Free Space....232
Kerberos Ticket Renewer Host Health.... 232
Kerberos Ticket Renewer Log Directory Free Space....233
Kerberos Ticket Renewer Process Status....233
Kerberos Ticket Renewer Swap Memory Usage....234
Kerberos Ticket Renewer Unexpected Exits.... 234
Key Management Server Health Tests....235
Key Management Server Audit Pipeline Test.... 235
Key Management Server File Descriptors....236
Key Management Server Host Health.... 236
Key Management Server Log Directory Free Space....237
Key Management Server Process Status....237
Key Management Server Swap Memory Usage....238
Key Management Server Unexpected Exits.... 238
Key Management Server Proxy Health Tests....239
Key Management Server Proxy Audit Pipeline Test....239
Key Management Server Proxy File Descriptors.... 240
Key Management Server Proxy Host Health....240
Key Management Server Proxy Log Directory Free Space....240
Key Management Server Proxy Process Status....241
Key Management Server Proxy Swap Memory Usage.... 242

Key Management Server Proxy Unexpected Exits....242
Key-Value Store Indexer Health Tests....243
Key-Value Store Indexer Lily HBase Indexer Health....243
Knox Health Tests....243
Knox Gateway Health....243
Knox IDBroker Health....244
Knox Gateway Health Tests....245
Knox Gateway Audit Pipeline Test....245
Knox Gateway File Descriptors....245
Knox Gateway Host Health....246
Knox Gateway Log Directory Free Space....246
Knox Gateway Process Status....247
Knox Gateway Swap Memory Usage....247
Knox Gateway Unexpected Exits....248
Knox IDBroker Health Tests....248
Knox IDBroker Audit Pipeline Test....248
Knox IDBroker File Descriptors....249
Knox IDBroker Host Health....250
Knox IDBroker Log Directory Free Space....250
Knox IDBroker Process Status....251
Knox IDBroker Swap Memory Usage....251
Knox IDBroker Unexpected Exits....252
Kudu Health Tests....252
Kudu Master Health....252
Kudu Tablet Server Health....253
LLAP Proxy Health Tests....253
LLAP Proxy Audit Pipeline Test....253
LLAP Proxy File Descriptors....254
LLAP Proxy Heap Dump Directory Free Space....255
LLAP Proxy Host Health....255
LLAP Proxy LLAP Daemons Ready Check....256
LLAP Proxy Log Directory Free Space....257
LLAP Proxy Pause Duration....257
LLAP Proxy Process Status....258
LLAP Proxy Swap Memory Usage....258
LLAP Proxy Unexpected Exits....259
Lily HBase Indexer Health Tests....259
Lily HBase Indexer Audit Pipeline Test....259
Lily HBase Indexer File Descriptors....260
Lily HBase Indexer Heap Dump Directory Free Space....261
Lily HBase Indexer Host Health....261
Lily HBase Indexer Log Directory Free Space....262
Lily HBase Indexer Process Status....262
Lily HBase Indexer Swap Memory Usage....263
Lily HBase Indexer Unexpected Exits....263
Livy Health Tests....264
Livy Server Health....264
Livy Server Health Tests....264
Livy Server Audit Pipeline Test....264
Livy Server File Descriptors....265
Livy Server Host Health....266
Livy Server Log Directory Free Space....266
Livy Server Process Status....267
Livy Server Swap Memory Usage....267
Livy Server Unexpected Exits....268
Load Balancer Health Tests....268

Load Balancer Audit Pipeline Test....268
Load Balancer File Descriptors....269
Load Balancer Heap Dump Directory Free Space....270
Load Balancer Host Health....270
Load Balancer Log Directory Free Space....271
Load Balancer Process Status....271
Load Balancer Swap Memory Usage....272
Load Balancer Unexpected Exits....272
MapReduce Health Tests....273
MapReduce Failover Controllers Health....273
MapReduce JobTracker Health....273
MapReduce TaskTracker Health....275
Master Health Tests....275
Master Audit Pipeline Test....275
Master Failed Data Directories....276
Master File Descriptors....276
Master Full Data Directories....276
Master GC Duration....277
Master HBase Master Canary....277
Master HBase Regions In Transition Over Threshold....278
Master Heap Dump Directory Free Space....278
Master Host Health....279
Master Log Directory Free Space....279
Master Process Status....280
Master Swap Memory Usage....280
Master Unexpected Exits....280
Master Web Server Status....281
Monitor Health Tests....282
Monitor Audit Pipeline Test....282
Monitor File Descriptors....283
Monitor Host Health....283
Monitor Log Directory Free Space....283
Monitor Process Status....284
Monitor Swap Memory Usage....285
Monitor Unexpected Exits....285
NFS Gateway Health Tests....286
NFS Gateway Audit Pipeline Test....286
NFS Gateway File Descriptors....287
NFS Gateway Heap Dump Directory Free Space....287
NFS Gateway Host Health....288
NFS Gateway Log Directory Free Space....288
NFS Gateway Process Status....289
NFS Gateway Swap Memory Usage....289
NFS Gateway Temporary Dump Directory Free Space....289
NFS Gateway Unexpected Exits....290
NameNode Health Tests....291
NameNode Audit Pipeline Test....291
NameNode Checkpoint Status....292
NameNode File Descriptors....292
NameNode Heap Dump Directory Free Space....293
NameNode Host Health....294
NameNode JournalNode Sync Status....294
NameNode Log Directory Free Space....294
NameNode Name Directory Status....295
NameNode NameNode Data Directories Free Space....295
NameNode Pause Duration....296

NameNode Process Status....297
NameNode RPC Latency....297
NameNode Rolling Upgrade Status....298
NameNode Safe Mode Status....298
NameNode Swap Memory Usage....299
NameNode Unexpected Exits....299
NameNode Upgrade Status....300
NameNode Web Server Status....300
Navigator Audit Server Health Tests....301
Navigator Audit Server Audit Pipeline Test....301
Navigator Audit Server File Descriptors....302
Navigator Audit Server GC Duration....302
Navigator Audit Server Heap Dump Directory Free Space....303
Navigator Audit Server Host Health....304
Navigator Audit Server Log Directory Free Space....304
Navigator Audit Server Process Status....305
Navigator Audit Server Swap Memory Usage....305
Navigator Audit Server Unexpected Exits....306
Navigator Audit Server Web Server Status....306
Navigator Luna KMS Metastore Health Tests....307
Navigator Luna KMS Metastore Audit Pipeline Test....307
Navigator Luna KMS Metastore File Descriptors....308
Navigator Luna KMS Metastore Host Health....308
Navigator Luna KMS Metastore Process Status....309
Navigator Luna KMS Metastore Swap Memory Usage....309
Navigator Luna KMS Metastore Unexpected Exits....310
Navigator Luna KMS Proxy Health Tests....310
Navigator Luna KMS Proxy Audit Pipeline Test....310
Navigator Luna KMS Proxy File Descriptors....311
Navigator Luna KMS Proxy Host Health....312
Navigator Luna KMS Proxy Log Directory Free Space....312
Navigator Luna KMS Proxy Process Status....313
Navigator Luna KMS Proxy Swap Memory Usage....313
Navigator Luna KMS Proxy Unexpected Exits....313
Navigator Metadata Server Health Tests....314
Navigator Metadata Server Audit Log Directory Free Space....314
Navigator Metadata Server Audit Pipeline Test....315
Navigator Metadata Server File Descriptors....316
Navigator Metadata Server Heap Dump Directory Free Space....316
Navigator Metadata Server Host Health....317
Navigator Metadata Server Log Directory Free Space....317
Navigator Metadata Server Navigator Metadata Server Storage Dir Free Space....318
Navigator Metadata Server Process Status....319
Navigator Metadata Server Solr Element Count Threshold Test....319
Navigator Metadata Server Solr Relation Count Threshold Test....319
Navigator Metadata Server Swap Memory Usage....320
Navigator Metadata Server Unexpected Exits....320
Navigator Thales KMS Metastore Health Tests....321
Navigator Thales KMS Metastore Audit Pipeline Test....321
Navigator Thales KMS Metastore File Descriptors....322
Navigator Thales KMS Metastore Host Health....322
Navigator Thales KMS Metastore Process Status....323
Navigator Thales KMS Metastore Swap Memory Usage....323
Navigator Thales KMS Metastore Unexpected Exits....324
Navigator Thales KMS Proxy Health Tests....324
Navigator Thales KMS Proxy Audit Pipeline Test....324

Navigator Thales KMS Proxy File Descriptors....325
Navigator Thales KMS Proxy Host Health....326
Navigator Thales KMS Proxy Log Directory Free Space....326
Navigator Thales KMS Proxy Process Status....327
Navigator Thales KMS Proxy Swap Memory Usage....327
Navigator Thales KMS Proxy Unexpected Exits....328
NodeManager Health Tests....328
NodeManager Audit Pipeline Test....328
NodeManager File Descriptors....329
NodeManager GC Duration....330
NodeManager Heap Dump Directory Free Space....330
NodeManager Host Health....331
NodeManager Log Directory Free Space....331
NodeManager NodeManager Container Log Directories Free Space....332
NodeManager NodeManager Health Checker....332
NodeManager NodeManager Local Directories Free Space....334
NodeManager NodeManager Recovery Directory Free Space....335
NodeManager Process Status....336
NodeManager ResourceManager Connectivity....336
NodeManager Swap Memory Usage....337
NodeManager Unexpected Exits....337
NodeManager Web Server Status....338
Oozie Health Tests....339
Oozie Server Health....339
Oozie Server Health Tests....339
Oozie Server Audit Pipeline Test....339
Oozie Server Callable Queue Size....340
Oozie Server File Descriptors....342
Oozie Server Heap Dump Directory Free Space....342
Oozie Server Host Health....343
Oozie Server Log Directory Free Space....343
Oozie Server Oozie Server Shared Library Check....344
Oozie Server Pause Duration....344
Oozie Server Process Status....345
Oozie Server Swap Memory Usage....345
Oozie Server Unexpected Exits....345
Oozie Server Web Server Status....346
Ozone DataNode Health Tests....347
Ozone DataNode Audit Pipeline Test....347
Ozone DataNode File Descriptors....348
Ozone DataNode Host Health....348
Ozone DataNode Log Directory Free Space....349
Ozone DataNode Process Status....349
Ozone DataNode Swap Memory Usage....350
Ozone DataNode Unexpected Exits....350
Ozone Manager Health Tests....351
Ozone Manager Audit Pipeline Test....351
Ozone Manager File Descriptors....352
Ozone Manager Host Health....352
Ozone Manager Log Directory Free Space....352
Ozone Manager Process Status....353
Ozone Manager Swap Memory Usage....354
Ozone Manager Unexpected Exits....354
Ozone Prometheus Health Tests....355
Ozone Prometheus Audit Pipeline Test....355
Ozone Prometheus File Descriptors....356

Ozone Prometheus Host Health.... 356
Ozone Prometheus Process Status....356
Ozone Prometheus Swap Memory Usage....357
Ozone Prometheus Unexpected Exits.... 357
Ozone Recon Health Tests....358
Ozone Recon Audit Pipeline Test....358
Ozone Recon File Descriptors....359
Ozone Recon Host Health....359
Ozone Recon Log Directory Free Space.... 360
Ozone Recon Process Status.... 360
Ozone Recon Swap Memory Usage.... 361
Ozone Recon Unexpected Exits....361
Passive Database Health Tests....362
Passive Database Audit Pipeline Test....362
Passive Database File Descriptors....363
Passive Database Host Health....363
Passive Database Process Status.... 363
Passive Database Swap Memory Usage.... 364
Passive Database Unexpected Exits....364
Passive Key Trustee Server Health Tests.... 365
Passive Key Trustee Server Audit Pipeline Test.... 365
Passive Key Trustee Server File Descriptors....366
Passive Key Trustee Server Host Health.... 366
Passive Key Trustee Server Log Directory Free Space....367
Passive Key Trustee Server Process Status.... 367
Passive Key Trustee Server Swap Memory Usage....368
Passive Key Trustee Server Unexpected Exits.... 368
Phoenix Health Tests....369
Phoenix Query Server Health....369
Query Server Health Tests.... 370
Query Server Audit Pipeline Test.... 370
Query Server File Descriptors....370
Query Server Host Health.... 371
Query Server Log Directory Free Space....371
Query Server Process Status.... 372
Query Server Swap Memory Usage....372
Query Server Unexpected Exits.... 373
Ranger Health Tests.... 373
Ranger Admin Health....373
Ranger Tagsync Health.... 374
Ranger Usersync Health....374
Ranger Admin Health Tests....375
Ranger Admin Audit Pipeline Test....375
Ranger Admin File Descriptors....376
Ranger Admin Host Health....376
Ranger Admin Log Directory Free Space.... 377
Ranger Admin Process Status.... 377
Ranger Admin Swap Memory Usage.... 378
Ranger Admin Unexpected Exits....378
Ranger KMS Health Tests.... 379
Ranger KMS Server Health....379
Ranger KMS Server Health Tests....379
Ranger KMS Server Audit Pipeline Test....379
Ranger KMS Server File Descriptors.... 380
Ranger KMS Server Host Health....381
Ranger KMS Server Log Directory Free Space.... 381

Ranger KMS Server Process Status....382
Ranger KMS Server Swap Memory Usage....382
Ranger KMS Server Unexpected Exits....383
Ranger KMS Server with KTS Health Tests....383
Ranger KMS Server with KTS Audit Pipeline Test....383
Ranger KMS Server with KTS File Descriptors....384
Ranger KMS Server with KTS Host Health....385
Ranger KMS Server with KTS Log Directory Free Space....385
Ranger KMS Server with KTS Process Status....386
Ranger KMS Server with KTS Swap Memory Usage....386
Ranger KMS Server with KTS Unexpected Exits....387
Ranger KMS with Key Trustee Server Health Tests....387
Ranger KMS with Key Trustee Server Ranger KMS Server with KTS Health....387
Ranger RMS Health Tests....388
Ranger RMS Server Health....388
Ranger RMS Server Health Tests....388
Ranger RMS Server Audit Pipeline Test....388
Ranger RMS Server File Descriptors....389
Ranger RMS Server Host Health....390
Ranger RMS Server Log Directory Free Space....390
Ranger RMS Server Process Status....391
Ranger RMS Server Swap Memory Usage....391
Ranger RMS Server Unexpected Exits....392
Ranger Raz Health Tests....392
Ranger Raz Server Health....392
Ranger Raz Server Health Tests....393
Ranger Raz Server Audit Pipeline Test....393
Ranger Raz Server File Descriptors....394
Ranger Raz Server Host Health....394
Ranger Raz Server Log Directory Free Space....395
Ranger Raz Server Process Status....395
Ranger Raz Server Swap Memory Usage....396
Ranger Raz Server Unexpected Exits....396
Ranger Tagsync Health Tests....397
Ranger Tagsync Audit Pipeline Test....397
Ranger Tagsync File Descriptors....398
Ranger Tagsync Host Health....398
Ranger Tagsync Log Directory Free Space....399
Ranger Tagsync Process Status....399
Ranger Tagsync Swap Memory Usage....400
Ranger Tagsync Unexpected Exits....400
Ranger Usersync Health Tests....401
Ranger Usersync Audit Pipeline Test....401
Ranger Usersync File Descriptors....402
Ranger Usersync Host Health....402
Ranger Usersync Log Directory Free Space....402
Ranger Usersync Process Status....403
Ranger Usersync Swap Memory Usage....404
Ranger Usersync Unexpected Exits....404
RegionServer Health Tests....405
RegionServer Audit Pipeline Test....405
RegionServer Cluster Connectivity....406
RegionServer Compaction Queue Size....406
RegionServer File Descriptors....407
RegionServer Flush Queue Size....408
RegionServer GC Duration....408

RegionServer Heap Dump Directory Free Space ... 409
RegionServer Host Health ... 409
RegionServer Log Directory Free Space ... 410
RegionServer Memstore Size ... 410
RegionServer Process Status ... 411
RegionServer Store File Index Size ... 411
RegionServer Swap Memory Usage ... 412
RegionServer Unexpected Exits ... 412
RegionServer Web Server Status ... 413
Reports Manager Health Tests ... 414
Reports Manager Audit Pipeline Test ... 414
Reports Manager Cloudera Manager Descriptor Age ... 414
Reports Manager File Descriptors ... 415
Reports Manager Heap Dump Directory Free Space ... 415
Reports Manager Host Health ... 416
Reports Manager Log Directory Free Space ... 416
Reports Manager Pause Duration ... 417
Reports Manager Process Status ... 418
Reports Manager Reports Manager Working Directory Free Space ... 418
Reports Manager Swap Memory Usage ... 419
Reports Manager Unexpected Exits ... 419
ResourceManager Health Tests ... 420
ResourceManager Audit Pipeline Test ... 420
ResourceManager File Descriptors ... 421
ResourceManager GC Duration ... 421
ResourceManager Heap Dump Directory Free Space ... 422
ResourceManager Host Health ... 423
ResourceManager Log Directory Free Space ... 423
ResourceManager Process Status ... 424
ResourceManager Swap Memory Usage ... 424
ResourceManager Unexpected Exits ... 424
ResourceManager Web Server Status ... 425
S3 Gateway Health Tests ... 426
S3 Gateway Audit Pipeline Test ... 426
S3 Gateway File Descriptors ... 427
S3 Gateway Host Health ... 427
S3 Gateway Log Directory Free Space ... 427
S3 Gateway Process Status ... 428
S3 Gateway Swap Memory Usage ... 429
S3 Gateway Unexpected Exits ... 429
SRM Driver Health Tests ... 430
SRM Driver Audit Pipeline Test ... 430
SRM Driver File Descriptors ... 431
SRM Driver Host Health ... 431
SRM Driver Log Directory Free Space ... 431
SRM Driver Process Status ... 432
SRM Driver Swap Memory Usage ... 432
SRM Driver Unexpected Exits ... 433
SRM Service Health Tests ... 434
SRM Service Audit Pipeline Test ... 434
SRM Service File Descriptors ... 434
SRM Service Host Health ... 435
SRM Service Log Directory Free Space ... 435
SRM Service Process Status ... 436
SRM Service Swap Memory Usage ... 436
SRM Service Unexpected Exits ... 437

Schema Registry Health Tests....437
Schema Registry Server Health....437
Schema Registry Server Health Tests....438
Schema Registry Server Audit Pipeline Test....438
Schema Registry Server File Descriptors....439
Schema Registry Server Host Health....439
Schema Registry Server Log Directory Free Space....440
Schema Registry Server Process Status....440
Schema Registry Server Swap Memory Usage....441
Schema Registry Server Unexpected Exits....441
SecondaryNameNode Health Tests....442
SecondaryNameNode Audit Pipeline Test....442
SecondaryNameNode File Descriptors....443
SecondaryNameNode GC Duration....443
SecondaryNameNode HDFS Checkpoint Directories Free Space....444
SecondaryNameNode Heap Dump Directory Free Space....445
SecondaryNameNode Host Health....445
SecondaryNameNode Log Directory Free Space....446
SecondaryNameNode Process Status....446
SecondaryNameNode Swap Memory Usage....447
SecondaryNameNode Unexpected Exits....447
SecondaryNameNode Web Server Status....448
Sentry Health Tests....449
Sentry Server Health....449
Sentry Server Health Tests....449
Sentry Server Audit Pipeline Test....449
Sentry Server File Descriptors....450
Sentry Server Heap Dump Directory Free Space....451
Sentry Server Host Health....451
Sentry Server Log Directory Free Space....452
Sentry Server Process Status....452
Sentry Server Swap Memory Usage....453
Sentry Server Unexpected Exits....453
Service Monitor Health Tests....454
Service Monitor Audit Pipeline Test....454
Service Monitor Cloudera Manager Descriptor Age....455
Service Monitor Cloudera Manager Metric Schema Age....455
Service Monitor File Descriptors....456
Service Monitor Heap Dump Directory Free Space....456
Service Monitor Heap Size....457
Service Monitor Host Health....457
Service Monitor Log Directory Free Space....457
Service Monitor Metrics Aggregation Run Duration Test....458
Service Monitor Pause Duration....458
Service Monitor Process Status....459
Service Monitor Role Pipeline....460
Service Monitor Service Monitor Storage Directory Free Space....460
Service Monitor Swap Memory Usage....461
Service Monitor Unexpected Exits....461
Service Monitor Web Server Status....462
Solr Health Tests....463
Solr Server Health....463
Solr Server Health Tests....463
Solr Server Audit Pipeline Test....463
Solr Server File Descriptors....464
Solr Server GC Duration....465

Solr Server Heap Dump Directory Free Space....465
Solr Server Host Health.... 466
Solr Server Log Directory Free Space....466
Solr Server Process Status....467
Solr Server Solr Server API Liveness.... 467
Solr Server Swap Memory Usage....468
Solr Server Unexpected Exits.... 468
Solr Server Web Server Status....469
Spark Health Tests....470
Spark History Server Health.... 470
Sqoop 2 Health Tests.... 470
Sqoop 2 Server Health.... 470
Sqoop 2 Server Health Tests....471
Sqoop 2 Server Audit Pipeline Test....471
Sqoop 2 Server File Descriptors.... 472
Sqoop 2 Server Heap Dump Directory Free Space.... 472
Sqoop 2 Server Host Health....473
Sqoop 2 Server Log Directory Free Space.... 473
Sqoop 2 Server Process Status....474
Sqoop 2 Server Swap Memory Usage.... 474
Sqoop 2 Server Unexpected Exits....475
Storage Container Manager Health Tests.... 475
Storage Container Manager Audit Pipeline Test.... 475
Storage Container Manager File Descriptors....476
Storage Container Manager Host Health.... 477
Storage Container Manager Log Directory Free Space....477
Storage Container Manager Process Status....478
Storage Container Manager Swap Memory Usage....478
Storage Container Manager Unexpected Exits.... 479
Streams Messaging Manager Health Tests.... 479
Streams Messaging Manager Rest Admin Server Health....479
Streams Messaging Manager UI Server Health....480
Streams Messaging Manager Rest Admin Server Health Tests.... 480
Streams Messaging Manager Rest Admin Server Audit Pipeline Test....480
Streams Messaging Manager Rest Admin Server File Descriptors....481
Streams Messaging Manager Rest Admin Server Host Health.... 482
Streams Messaging Manager Rest Admin Server Log Directory Free Space.... 482
Streams Messaging Manager Rest Admin Server Process Status....483
Streams Messaging Manager Rest Admin Server Swap Memory Usage.... 483
Streams Messaging Manager Rest Admin Server Unexpected Exits.... 484
Streams Messaging Manager UI Server Health Tests.... 484
Streams Messaging Manager UI Server Audit Pipeline Test.... 484
Streams Messaging Manager UI Server File Descriptors....485
Streams Messaging Manager UI Server Host Health.... 486
Streams Messaging Manager UI Server Log Directory Free Space.... 486
Streams Messaging Manager UI Server Process Status.... 487
Streams Messaging Manager UI Server Swap Memory Usage....487
Streams Messaging Manager UI Server Unexpected Exits.... 488
Streams Replication Manager Health Tests.... 488
Streams Replication Manager SRM Driver Health....488
Streams Replication Manager SRM Service Health.... 489
Tablet Server Health Tests....490
Tablet Server Audit Pipeline Test....490
Tablet Server Failed Data Directories....490
Tablet Server File Descriptors....491
Tablet Server Full Data Directories.... 491

Tablet Server Host Health....491
Tablet Server Log Directory Free Space....491
Tablet Server Process Status....492
Tablet Server Swap Memory Usage....492
Tablet Server Unexpected Exits....493
TaskTracker Health Tests....494
TaskTracker Audit Pipeline Test....494
TaskTracker Blacklisted Status....494
TaskTracker File Descriptors....495
TaskTracker GC Duration....495
TaskTracker Heap Dump Directory Free Space....496
TaskTracker Host Health....497
TaskTracker JobTracker Connectivity....497
TaskTracker Log Directory Free Space....498
TaskTracker Process Status....498
TaskTracker Swap Memory Usage....499
TaskTracker TaskTracker Local Data Directories Free Space....499
TaskTracker Unexpected Exits....500
TaskTracker Web Server Status....501
Telemetry Publisher Health Tests....501
Telemetry Publisher Audit Pipeline Test....501
Telemetry Publisher Data Export Test For Stream Hive-Query-Audits....502
Telemetry Publisher Data Export Test For Stream Hive-Tez-App....503
Telemetry Publisher Data Export Test For Stream Impala-Query-Profile....503
Telemetry Publisher Data Export Test For Stream Oozie-Workflows....504
Telemetry Publisher Data Export Test For Stream Spark2_on_yarn-Event-Log....505
Telemetry Publisher Data Export Test For Stream Yarn-Apps....505
Telemetry Publisher Data Export Test For Stream Yarn-Jhist....506
Telemetry Publisher Data Ingest Test For Stream Hive-Query-Audits....506
Telemetry Publisher Data Ingest Test For Stream Hive-Tez-App....507
Telemetry Publisher Data Ingest Test For Stream Impala-Query-Profile....507
Telemetry Publisher Data Ingest Test For Stream Oozie-Workflows....508
Telemetry Publisher Data Ingest Test For Stream Spark2_on_yarn-Event-Log....509
Telemetry Publisher Data Ingest Test For Stream Yarn-Apps....509
Telemetry Publisher Data Ingest Test For Stream Yarn-Jhist....510
Telemetry Publisher File Descriptors....510
Telemetry Publisher GC Duration....511
Telemetry Publisher Heap Dump Directory Free Space....511
Telemetry Publisher Host Health....512
Telemetry Publisher Log Directory Free Space....512
Telemetry Publisher Process Status....513
Telemetry Publisher Swap Memory Usage....514
Telemetry Publisher Telemetry Publisher Data Directory Free Space....514
Telemetry Publisher Unexpected Exits....515
Telemetry Publisher Web Server Status....515
Tracer Health Tests....516
Tracer Audit Pipeline Test....516
Tracer File Descriptors....517
Tracer Host Health....517
Tracer Log Directory Free Space....518
Tracer Process Status....518
Tracer Swap Memory Usage....519
Tracer Unexpected Exits....519
WebHCat Server Health Tests....520
WebHCat Server Audit Pipeline Test....520
WebHCat Server File Descriptors....521

WebHCat Server Heap Dump Directory Free Space....521
WebHCat Server Host Health....522
WebHCat Server Log Directory Free Space....522
WebHCat Server Process Status....523
WebHCat Server Swap Memory Usage....523
WebHCat Server Unexpected Exits....524
YARN Health Tests....524
YARN Container Usage Aggregation....524
YARN JobHistory Server Health....525
YARN NodeManager Health....525
YARN ResourceManager Health (HA)....526
YARN Queue Manager Store Health Tests....527
YARN Queue Manager Store Audit Pipeline Test....527
YARN Queue Manager Store File Descriptors....528
YARN Queue Manager Store Host Health....528
YARN Queue Manager Store Log Directory Free Space....529
YARN Queue Manager Store Process Status....530
YARN Queue Manager Store Swap Memory Usage....530
YARN Queue Manager Store Unexpected Exits....530
YARN Queue Manager Webapp Health Tests....531
YARN Queue Manager Webapp Audit Pipeline Test....531
YARN Queue Manager Webapp File Descriptors....532
YARN Queue Manager Webapp Host Health....532
YARN Queue Manager Webapp Log Directory Free Space....533
YARN Queue Manager Webapp Process Status....533
YARN Queue Manager Webapp Swap Memory Usage....534
YARN Queue Manager Webapp Unexpected Exits....534
Zeppelin Health Tests....535
Zeppelin Server Health....535
Zeppelin Server Health Tests....536
Zeppelin Server Audit Pipeline Test....536
Zeppelin Server File Descriptors....536
Zeppelin Server Host Health....537
Zeppelin Server Log Directory Free Space....537
Zeppelin Server Process Status....538
Zeppelin Server Swap Memory Usage....538
Zeppelin Server Unexpected Exits....539
ZooKeeper Health Tests....539
ZooKeeper Canary....539
ZooKeeper Server Health....541
ZooKeeper Server Health Tests....542
ZooKeeper Server Audit Pipeline Test....542
ZooKeeper Server Connection Count....542
ZooKeeper Server Data Directory Free Space....543
ZooKeeper Server File Descriptors....544
ZooKeeper Server GC Duration....544
ZooKeeper Server Heap Dump Directory Free Space....545
ZooKeeper Server Host Health....545
ZooKeeper Server Log Directory Free Space....546
ZooKeeper Server Maximum Request Latency....546
ZooKeeper Server Outstanding Requests....547
ZooKeeper Server Process Status....548
ZooKeeper Server Quorum Membership....548
ZooKeeper Server Swap Memory Usage....549
ZooKeeper Server Transaction Log Directory Free Space....549
ZooKeeper Server Unexpected Exits....550

Cloudera Manager Health Tests

This section provides information on health tests supported by Cloudera Manager.

There are two types of health tests:

- Pass-fail tests - there are two types:
  - Compare a property to a yes-no value. For example, whether a service or role started as expected, a DataNode is connected to its NameNode, or a TaskTracker is (or is not) blacklisted.
  - Exercise a service lightly to confirm it is working and responsive. HDFS (NameNode role), HBase, and ZooKeeper services perform these tests, which are referred to as "canary" tests.

  Both types of pass-fail tests result in the health reported as being either Good or Bad.
- Metric tests - compare a property to a numeric value. For example, the number of file descriptors in use, the amount of disk space used or free, how much time spent in garbage collection, or how many pages were swapped to disk in the previous 15 minutes. In these tests the property is compared to a threshold that determine whether everything is Good, (for example, plenty of disk space available), whether it is Concerning (disk space getting low), or is Bad (a critically low amount of disk space).

By default most health tests are enabled and (if appropriate) configured with reasonable thresholds. You can modify threshold values by editing the monitoring properties under the entity's Configuration tab. You can also enable or disable individual or summary health tests, and in some cases specify what should be included in the calculation of overall health for the service, role instance, or host.

Active Database Health Tests

Active Database Audit Pipeline Test

This Active Database health test checks that the Auditing for the Active Database role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Active Database process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Active Database host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Active Database monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Active Database File Descriptors

This Active Database health test checks that the number of file descriptors used does not rise above some percentage of the Active Database file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Active Database monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`db_active_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Active Database Host Health

This Active Database health test factors in the health of the host upon which the Active Database is running. A failure of this test means that the host running the Active Database is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Active Database Host Health Test Active Database monitoring setting.

Short Name: Host Health

Active Database Host Health Test

Description

When computing the overall Active Database health, consider the host's health.

Template Name

`db_active_host_health_enabled`

Default Value

true

Unit(s)

no unit

Active Database Process Status

This Active Database health test checks that the Cloudera Manager Agent on the Active Database host is heart beating correctly and that the process associated with the Active Database role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Active Database process, a lack of connectivity to the Cloudera Manager Agent on the Active Database host, or a problem with the Cloudera Manager Agent. This test can fail either because the Active Database has crashed or because the Active Database will not start or stop in a timely fashion. Check the Active Database logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Active Database host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Active Database host, or look in the Cloudera Manager Agent logs on the Active Database host for more details. This test can be enabled or disabled using the Active Database Process Health Test Active Database monitoring setting.

Short Name: Process Status

Active Database Process Health Test

Description

Enables the health test that the Active Database's process state is consistent with the role configuration

Template Name

`db_active_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Active Database Swap Memory Usage

This Active Database health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Active Database Unexpected Exits

This Active Database health test checks that the Active Database has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Active Database monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Active Key Trustee Server Health Tests

Active Key Trustee Server Audit Pipeline Test

This Active Key Trustee Server health test checks that the Auditing for the Active Key Trustee Server role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Active Key Trustee Server process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Active Key Trustee Server host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Active Key Trustee Server monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Active Key Trustee Server File Descriptors

This Active Key Trustee Server health test checks that the number of file descriptors used does not rise above some percentage of the Active Key Trustee Server file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Active Key Trustee Server monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`keytrustee_active_server_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Active Key Trustee Server Host Health

This Active Key Trustee Server health test factors in the health of the host upon which the Active Key Trustee Server is running. A failure of this test means that the host running the Active Key Trustee Server is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Active Key Trustee Server Host Health Test Active Key Trustee Server monitoring setting.

Short Name: Host Health

Active Key Trustee Server Host Health Test

Description

When computing the overall Active Key Trustee Server health, consider the host's health.

Template Name

`keytrustee_active_server_host_health_enabled`

Default Value

true

Unit(s)

no unit

Active Key Trustee Server Log Directory Free Space

This Active Key Trustee Server health test checks that the filesystem containing the log directory of this Active Key Trustee Server has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Active Key Trustee Server monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Active Key Trustee Server Process Status

This Active Key Trustee Server health test checks that the Cloudera Manager Agent on the Active Key Trustee Server host is heart beating correctly and that the process associated with the Active Key Trustee Server role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Active Key Trustee Server process, a lack of connectivity to the Cloudera Manager Agent on the Active Key Trustee Server host, or a problem with the Cloudera Manager Agent. This test can fail either because the Active Key Trustee Server has crashed or because the Active Key Trustee Server will not start or stop in a timely fashion. Check the Active Key Trustee Server logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Active Key Trustee Server host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Active Key Trustee Server host, or look in the Cloudera Manager Agent logs on the Active Key Trustee Server host for more details. This test can be enabled or disabled using the Active Key Trustee Server Process Health Test Active Key Trustee Server monitoring setting.

Short Name: Process Status

Active Key Trustee Server Process Health Test

Description

Enables the health test that the Active Key Trustee Server's process state is consistent with the role configuration

Template Name

`keytrustee_active_server_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Active Key Trustee Server Swap Memory Usage

This Active Key Trustee Server health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Active Key Trustee Server Unexpected Exits

This Active Key Trustee Server health test checks that the Active Key Trustee Server has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Active Key Trustee Server monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Activity Monitor Health Tests

Activity Monitor Activity Monitor Pipeline

This Activity Monitor health test checks that no messages are being dropped by the activity monitor stage of the Activity Monitor pipeline. A failure of this health test indicates a problem with the Activity Monitor. This may indicate a configuration problem or a bug in the Activity Monitor. This test can be configured using the Activity Monitor Activity Monitor Pipeline Monitoring Time Period monitoring setting.

Short Name: Activity Monitor Pipeline

Activity Monitor Activity Monitor Pipeline Monitoring Thresholds

Description

The health test thresholds for monitoring the Activity Monitor activity monitor pipeline. This specifies the number of dropped messages that will be tolerated over the monitoring time period.

Template Name

`activitymonitor_activity_monitor_pipeline_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Activity Monitor Activity Monitor Pipeline Monitoring Time Period

Description

The time period over which the Activity Monitor activity monitor pipeline will be monitored for dropped messages.

Template Name

`activitymonitor_activity_monitor_pipeline_window`

Default Value

5

Unit(s)

MINUTES

Activity Monitor Activity Tree Pipeline

This Activity Monitor health test checks that no messages are being dropped by the activity tree stage of the Activity Monitor pipeline. A failure of this health test indicates a problem with the Activity Monitor. This may indicate a configuration problem or a bug in the Activity Monitor. This test can be configured using the Activity Monitor Activity Tree Pipeline Monitoring Time Period monitoring setting.

Short Name: Activity Tree Pipeline

Activity Monitor Activity Tree Pipeline Monitoring Thresholds

Description

The health test thresholds for monitoring the Activity Monitor activity tree pipeline. This specifies the number of dropped messages that will be tolerated over the monitoring time period.

Template Name

`activitymonitor_activity_tree_pipeline_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Activity Monitor Activity Tree Pipeline Monitoring Time Period

Description

The time period over which the Activity Monitor activity tree pipeline will be monitored for dropped messages.

Template Name

`activitymonitor_activity_tree_pipeline_window`

Default Value

5

Unit(s)

MINUTES

Activity Monitor Audit Pipeline Test

This Activity Monitor health test checks that the Auditing for the Activity Monitor role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Activity Monitor process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Activity Monitor host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Activity Monitor monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Activity Monitor Cloudera Manager Descriptor Age

This is a Activity Monitor health test that checks if the Cloudera Manager descriptor has been refreshed recently. The Cloudera Manager descriptor is used to pass configuration information from the Cloudera Manager Server to the Activity Monitor. If the descriptor becomes stale, Activity Monitor operation may be impacted because the Activity Monitor will receive information about new hosts, roles, and services, or changes to existing hosts, roles, and services. A stale descriptor usually indicates problems communicating with the Cloudera Manager Server but can

also indicate performance problems or a bug. Consult the Activity Monitor log and the Cloudera Manager Server log for more information. This test can be configured using the Cloudera Manager Descriptor Age Thresholds Cloudera Manager Activity Monitor setting.

Short Name: Cloudera Manager Descriptor Age

Cloudera Manager Descriptor Age Thresholds

Description

The health test thresholds for monitoring the time since the Cloudera Manager descriptor was last refreshed.

Template Name

`scm_descriptor_age_thresholds`

Default Value

critical:120000.0, warning:60000.0

Unit(s)

no unit

Activity Monitor File Descriptors

This Activity Monitor health test checks that the number of file descriptors used does not rise above some percentage of the Activity Monitor file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Activity Monitor monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`activitymonitor_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Activity Monitor Heap Dump Directory Free Space

This Activity Monitor health test checks that the filesystem containing the heap dump directory of this Activity Monitor has sufficient free space. This test can be configured using the Heap Dump Directory Free Space Monitoring Absolute Thresholds and Heap Dump Directory Free Space Monitoring Percentage Thresholds Activity Monitor monitoring settings.

Short Name: Heap Dump Directory Free Space

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Template Name

`heap_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`heap_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Activity Monitor Host Health

This Activity Monitor health test factors in the health of the host upon which the Activity Monitor is running. A failure of this test means that the host running the Activity Monitor is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Activity Monitor Host Health Test Activity Monitor monitoring setting.

Short Name: Host Health

Activity Monitor Host Health Test

Description

When computing the overall Activity Monitor health, consider the host's health.

Template Name

`activitymonitor_host_health_enabled`

Default Value

true

Unit(s)

no unit

Activity Monitor Log Directory Free Space

This Activity Monitor health test checks that the filesystem containing the log directory of this Activity Monitor has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Activity Monitor monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Activity Monitor Pause Duration

This Activity Monitor health test checks that the Activity Monitor threads are not experiencing long scheduling pauses. The test uses a pause monitoring thread in the Activity Monitor that tracks scheduling delay by noting if it is run on its requested schedule. If the thread is not run on its requested schedule, the delay is noted and considered pause time. The health test checks that no more than some percentage of recent time is spent paused. A failure of this health test may indicate that the Activity Monitor is not getting enough CPU resources, or that it is spending too much time doing garbage collection. Inspect the Activity Monitor logs for any pause monitor output and check garbage collection metrics exposed by the Activity Monitor. This test can be configured using the Pause Duration Thresholds and Pause Duration Monitoring Period Activity Monitor monitoring settings.

Short Name: Pause Duration

Pause Duration Monitoring Period

Description

The period to review when computing the moving average of extra time the pause monitor spent paused.

Template Name

`activitymonitor_pause_duration_window`

Default Value

5

Unit(s)

MINUTES

Pause Duration Thresholds

Description

The health test thresholds for the weighted average extra time the pause monitor spent paused. Specified as a percentage of elapsed wall clock time.

Template Name

`activitymonitor_pause_duration_thresholds`

Default Value

critical:60.0, warning:30.0

Unit(s)

no unit

Activity Monitor Process Status

This Activity Monitor health test checks that the Cloudera Manager Agent on the Activity Monitor host is heart beating correctly and that the process associated with the Activity Monitor role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Activity Monitor process, a lack of connectivity to the Cloudera Manager Agent on the Activity Monitor host, or a problem with the Cloudera Manager Agent. This test can fail either because the Activity Monitor has crashed or because the Activity Monitor will not start or stop in a timely fashion. Check the Activity Monitor logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Activity Monitor host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Activity Monitor host, or look in the Cloudera Manager Agent logs on the Activity Monitor host for more details. This test can be enabled or disabled using the Activity Monitor Process Health Test Activity Monitor monitoring setting.

Short Name: Process Status

Activity Monitor Process Health Test

Description

Enables the health test that the Activity Monitor's process state is consistent with the role configuration

Template Name

`activitymonitor_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Activity Monitor Swap Memory Usage

This Activity Monitor health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Activity Monitor Unexpected Exits

This Activity Monitor health test checks that the Activity Monitor has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is

configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Activity Monitor monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Activity Monitor Web Server Status

This health test checks that the role's web server is responding quickly to requests by the Cloudera Manager Agent, and that the Cloudera Manager Agent can collect metrics from the web server. Failure of this health test may indicate a problem with the web server of the Activity Monitor, a misconfiguration of the Activity Monitor, or a problem with the Cloudera Manager Agent. Consult the Cloudera Manager Agent logs and the logs of the Activity Monitor for more detail. If the test failure message indicates a communication problem, the Cloudera Manager Agent's HTTP requests to the Activity Monitor's web server are failing or timing out. If the test's failure message indicates an unexpected response, the Activity Monitor's web server responded to the Cloudera Manager Agent's request, but the response could not be interpreted for some reason. This test can be configured using the Web Metric Collection Activity Monitor monitoring setting.

Short Name: Web Server Status

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Template Name

`activitymonitor_web_metric_collection_enabled`

Default Value

true

Unit(s)

no unit

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Template Name

`activitymonitor_web_metric_collection_thresholds`

Default Value

critical:never, warning:10000.0

Unit(s)

MILLISECONDS

Alert Publisher Health Tests

Alert Publisher Audit Pipeline Test

This Alert Publisher health test checks that the Auditing for the Alert Publisher role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Alert Publisher process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Alert Publisher host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Alert Publisher monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Alert Publisher File Descriptors

This Alert Publisher health test checks that the number of file descriptors used does not rise above some percentage of the Alert Publisher file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Alert Publisher monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`alertpublisher_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Alert Publisher Heap Dump Directory Free Space

This Alert Publisher health test checks that the filesystem containing the heap dump directory of this Alert Publisher has sufficient free space. This test can be configured using the Heap Dump Directory Free Space Monitoring Absolute Thresholds and Heap Dump Directory Free Space Monitoring Percentage Thresholds Alert Publisher monitoring settings.

Short Name: Heap Dump Directory Free Space

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Template Name

`heap_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`heap_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Alert Publisher Host Health

This Alert Publisher health test factors in the health of the host upon which the Alert Publisher is running. A failure of this test means that the host running the Alert Publisher is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Alert Publisher Host Health Test Alert Publisher monitoring setting.

Short Name: Host Health

Alert Publisher Host Health Test

Description

When computing the overall Alert Publisher health, consider the host's health.

Template Name

`alertpublisher_host_health_enabled`

Default Value

true

Unit(s)

no unit

Alert Publisher Log Directory Free Space

This Alert Publisher health test checks that the filesystem containing the log directory of this Alert Publisher has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Alert Publisher monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Alert Publisher Process Status

This Alert Publisher health test checks that the Cloudera Manager Agent on the Alert Publisher host is heart beating correctly and that the process associated with the Alert Publisher role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Alert Publisher process, a lack of connectivity to the Cloudera Manager Agent on the Alert Publisher host, or a problem with the Cloudera Manager Agent. This test can fail either because the Alert Publisher has crashed or because the Alert Publisher will not start or stop in a timely fashion. Check the Alert Publisher logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Alert Publisher host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Alert Publisher host, or look in the Cloudera Manager Agent logs on the Alert Publisher host for more details. This test can be enabled or disabled using the Alert Publisher Process Health Test Alert Publisher monitoring setting.

Short Name: Process Status

Alert Publisher Process Health Test

Description

Enables the health test that the Alert Publisher's process state is consistent with the role configuration

Template Name

`alertpublisher_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Alert Publisher Swap Memory Usage

This Alert Publisher health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Alert Publisher Unexpected Exits

This Alert Publisher health test checks that the Alert Publisher has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Alert Publisher monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Atlas Health Tests

Atlas Server Health

This is a Atlas service-level health test that checks that enough of the Atlas Servers in the cluster are healthy. The test returns "Concerning" health if the number of healthy Atlas Servers falls below a warning threshold, expressed

as a percentage of the total number of Atlas Servers. The test returns "Bad" health if the number of healthy and "Concerning" Atlas Servers falls below a critical threshold, expressed as a percentage of the total number of Atlas Servers. For example, if this test is configured with a warning threshold of 95% and a critical threshold of 90% for a cluster of 100 Atlas Servers, this test would return "Good" health if 95 or more Atlas Servers have good health. This test would return "Concerning" health if at least 90 Atlas Servers have either "Good" or "Concerning" health. If more than 10 Atlas Servers have bad health, this test would return "Bad" health. A failure of this health test indicates unhealthy Atlas Servers. Check the status of the individual Atlas Servers for more information. This test can be configured using the Atlas Atlas service-wide monitoring setting.

Short Name: Atlas Server Health

Healthy Atlas Server Monitoring Thresholds

Description

The health test thresholds of the overall Atlas Server health. The check returns "Concerning" health if the percentage of "Healthy" Atlas Servers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Atlas Servers falls below the critical threshold.

Template Name

`ATLAS_ATLAS_SERVER_healthy_thresholds`

Default Value

critical:90.0, warning:99.0

Unit(s)

PERCENT

Atlas Server Health Tests

Atlas Server Audit Pipeline Test

This Atlas Server health test checks that the Auditing for the Atlas Server role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Atlas Server process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Atlas Server host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Atlas Server monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Atlas Server File Descriptors

This Atlas Server health test checks that the number of file descriptors used does not rise above some percentage of the Atlas Server file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Atlas Server monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`atlas_server_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Atlas Server Host Health

This Atlas Server health test factors in the health of the host upon which the Atlas Server is running. A failure of this test means that the host running the Atlas Server is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Atlas Server Host Health Test Atlas Server monitoring setting.

Short Name: Host Health

Atlas Server Host Health Test

Description

When computing the overall Atlas Server health, consider the host's health.

Template Name

`atlas_server_host_health_enabled`

Default Value

true

Unit(s)

no unit

Atlas Server Log Directory Free Space

This Atlas Server health test checks that the filesystem containing the log directory of this Atlas Server has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Atlas Server monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Atlas Server Process Status

This Atlas Server health test checks that the Cloudera Manager Agent on the Atlas Server host is heart beating correctly and that the process associated with the Atlas Server role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Atlas Server process, a lack of connectivity to the Cloudera Manager Agent on the Atlas Server host, or a problem with the Cloudera Manager Agent. This test can fail either because the Atlas Server has crashed or because the Atlas Server will not start or stop in a timely fashion. Check the Atlas Server logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Atlas Server host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-

scm-agent status on the Atlas Server host, or look in the Cloudera Manager Agent logs on the Atlas Server host for more details. This test can be enabled or disabled using the Atlas Server Process Health Test Atlas Server monitoring setting.

Short Name: Process Status

Atlas Server Process Health Test

Description

Enables the health test that the Atlas Server's process state is consistent with the role configuration

Template Name

`atlas_server_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Atlas Server Swap Memory Usage

This Atlas Server health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Atlas Server Unexpected Exits

This Atlas Server health test checks that the Atlas Server has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Atlas Server monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Authentication Server Health Tests

Authentication Server Audit Pipeline Test

This Authentication Server health test checks that the Auditing for the Authentication Server role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Authentication Server process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Authentication Server host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Authentication Server monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Authentication Server File Descriptors

This Authentication Server health test checks that the number of file descriptors used does not rise above some percentage of the Authentication Server file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Authentication Server monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`authserver_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Authentication Server Heap Dump Directory Free Space

This Authentication Server health test checks that the filesystem containing the heap dump directory of this Authentication Server has sufficient free space. This test can be configured using the Heap Dump Directory Free Space Monitoring Absolute Thresholds and Heap Dump Directory Free Space Monitoring Percentage Thresholds Authentication Server monitoring settings.

Short Name: Heap Dump Directory Free Space

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Template Name

`heap_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`heap_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Authentication Server Host Health

This Authentication Server health test factors in the health of the host upon which the Authentication Server is running. A failure of this test means that the host running the Authentication Server is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Authentication Server Host Health Test Authentication Server monitoring setting.

Short Name: Host Health

Authentication Server Host Health Test

Description

When computing the overall Authentication Server health, consider the host's health.

Template Name

`authserver_host_health_enabled`

Default Value

true

Unit(s)

no unit

Authentication Server Log Directory Free Space

This Authentication Server health test checks that the filesystem containing the log directory of this Authentication Server has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Authentication Server monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Authentication Server Process Status

This Authentication Server health test checks that the Cloudera Manager Agent on the Authentication Server host is heart beating correctly and that the process associated with the Authentication Server role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Authentication Server process, a lack of connectivity to the Cloudera Manager Agent on the Authentication Server host, or a problem with the Cloudera Manager Agent. This test can fail either because the Authentication Server has crashed or because the Authentication Server will not start or stop in a timely fashion. Check the Authentication Server logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Authentication Server host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Authentication Server host, or look in the Cloudera Manager Agent logs on the Authentication Server host for more details. This test can be enabled or disabled using the Authentication Server Process Health Test Authentication Server monitoring setting.

Short Name: Process Status

Authentication Server Process Health Test

Description

Enables the health test that the Authentication Server's process state is consistent with the role configuration

Template Name

`authserver_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Authentication Server Swap Memory Usage

This Authentication Server health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Authentication Server Unexpected Exits

This Authentication Server health test checks that the Authentication Server has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Authentication Server monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Authentication Server Load Balancer Health Tests

Authentication Server Load Balancer Audit Pipeline Test

This Authentication Server Load Balancer health test checks that the Auditing for the Authentication Server Load Balancer role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Authentication Server Load Balancer process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Authentication Server Load Balancer host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Authentication Server Load Balancer monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Authentication Server Load Balancer File Descriptors

This Authentication Server Load Balancer health test checks that the number of file descriptors used does not rise above some percentage of the Authentication Server Load Balancer file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Authentication Server Load Balancer monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`auth_load_balancer_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Authentication Server Load Balancer Host Health

This Authentication Server Load Balancer health test factors in the health of the host upon which the Authentication Server Load Balancer is running. A failure of this test means that the host running the Authentication Server Load Balancer is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Authentication Server Load Balancer Host Health Test Authentication Server Load Balancer monitoring setting.

Short Name: Host Health

Authentication Server Load Balancer Host Health Test

Description

When computing the overall Authentication Server Load Balancer health, consider the host's health.

Template Name

`auth_load_balancer_host_health_enabled`

Default Value

true

Unit(s)

no unit

Authentication Server Load Balancer Log Directory Free Space

This Authentication Server Load Balancer health test checks that the filesystem containing the log directory of this Authentication Server Load Balancer has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Authentication Server Load Balancer monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Authentication Server Load Balancer Process Status

This Authentication Server Load Balancer health test checks that the Cloudera Manager Agent on the Authentication Server Load Balancer host is heart beating correctly and that the process associated with the Authentication Server Load Balancer role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Authentication Server Load Balancer process, a lack of connectivity to the Cloudera Manager Agent on the Authentication Server Load Balancer host, or a problem with the Cloudera Manager Agent. This test can fail either because the Authentication Server Load Balancer has crashed or because the Authentication Server Load Balancer will not start or stop in a timely fashion. Check the Authentication Server Load Balancer logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Authentication Server Load Balancer host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Authentication Server Load Balancer host, or look in the Cloudera Manager Agent logs on the Authentication Server Load Balancer host for more details. This test can be enabled or disabled using the Authentication Server Load Balancer Process Health Test Authentication Server Load Balancer monitoring setting.

Short Name: Process Status

Authentication Server Load Balancer Process Health Test

Description

Enables the health test that the Authentication Server Load Balancer's process state is consistent with the role configuration

Template Name

`auth_load_balancer_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Authentication Server Load Balancer Swap Memory Usage

This Authentication Server Load Balancer health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Authentication Server Load Balancer Unexpected Exits

This Authentication Server Load Balancer health test checks that the Authentication Server Load Balancer has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Authentication Server Load Balancer monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Authentication Service Health Tests

Authentication Service Authentication Server Health

This is a Authentication Service service-level health test that checks that enough of the Authentication Servers in the cluster are healthy. The test returns "Concerning" health if the number of healthy Authentication Servers falls below a warning threshold, expressed as a percentage of the total number of Authentication Servers. The test returns "Bad" health if the number of healthy and "Concerning" Authentication Servers falls below a critical threshold, expressed as a percentage of the total number of Authentication Servers. For example, if this test is configured with a warning threshold of 95% and a critical threshold of 90% for a cluster of 100 Authentication Servers, this test would return "Good" health if 95 or more Authentication Servers have good health. This test would return "Concerning" health if at least 90 Authentication Servers have either "Good" or "Concerning" health. If more than 10 Authentication Servers have bad health, this test would return "Bad" health. A failure of this health test indicates unhealthy Authentication Servers. Check the status of the individual Authentication Servers for more information. This test can be configured using the Authentication Service Authentication Service service-wide monitoring setting.

Short Name: Authentication Server Health

Healthy Authentication Server Monitoring Thresholds

Description

The health test thresholds of the overall Authentication Server health. The check returns "Concerning" health if the percentage of "Healthy" Authentication Servers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Authentication Servers falls below the critical threshold.

Template Name

`auth_authservers_healthy_thresholds`

Default Value

critical:51.0, warning:99.0

Unit(s)

PERCENT

Authentication Service Authentication Server Load Balancer Health

This is a Authentication Service service-level health test that checks that enough of the Authentication Server Load Balancers in the cluster are healthy. The test returns "Concerning" health if the number of healthy Authentication Server Load Balancers falls below a warning threshold, expressed as a percentage of the total number of Authentication Server Load Balancers. The test returns "Bad" health if the number of healthy and "Concerning" Authentication Server Load Balancers falls below a critical threshold, expressed as a percentage of the total number of Authentication Server Load Balancers. For example, if this test is configured with a warning threshold of 95% and a critical threshold of 90% for a cluster of 100 Authentication Server Load Balancers, this test would return "Good" health if 95 or more Authentication Server Load Balancers have good health. This test would return "Concerning" health if at least 90 Authentication Server Load Balancers have either "Good" or "Concerning" health. If more than 10 Authentication Server Load Balancers have bad health, this test would return "Bad" health. A failure of this health test indicates unhealthy Authentication Server Load Balancers. Check the status of the individual Authentication Server Load Balancers for more information. This test can be configured using the Authentication Service Authentication Service service-wide monitoring setting.

Short Name: Authentication Server Load Balancer Health

Healthy Authentication Server Load Balancer Monitoring Thresholds

Description

The health test thresholds of the overall Authentication Server Load Balancer health. The check returns "Concerning" health if the percentage of "Healthy" Authentication Server Load Balancers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Authentication Server Load Balancers falls below the critical threshold.

Template Name

`auth_auth_load_balancers_healthy_thresholds`

Default Value

critical:51.0, warning:99.0

Unit(s)

PERCENT

Authentication Service Canary

This canary checks whether it is possible to log in to the Authentication Service. A failure of this check indicates that it will not be possible to log in to anything that uses the Authentication Service for single-sign-on. Look in the Authentication Service logs for more information.

Short Name: Authentication Service Canary

Cloudera Management Service Health Tests

Cloudera Management Service Activity Monitor Health

This Cloudera Management Service service-level health test checks for the presence of a running, healthy Activity Monitor. The test returns "Bad" health if the service is running and the Activity Monitor is not running. In all other cases it returns the health of the Activity Monitor. A failure of this health test indicates a stopped or unhealthy Activity Monitor. Check the status of the Activity Monitor for more information. This test can be enabled or disabled using the Activity Monitor Role Health Test Activity Monitor service-wide monitoring setting.

Short Name: Activity Monitor Health

Activity Monitor Role Health Test

Description

When computing the overall MGMT health, consider Activity Monitor's health

Template Name

`mgmt_activitymonitor_health_enabled`

Default Value

true

Unit(s)

no unit

Cloudera Management Service Alert Publisher Health

This Cloudera Management Service service-level health test checks for the presence of a running, healthy Alert Publisher. The test returns "Bad" health if the service is running and the Alert Publisher is not running. In all other cases it returns the health of the Alert Publisher. A failure of this health test indicates a stopped or unhealthy Alert Publisher. Check the status of the Alert Publisher for more information. This test can be enabled or disabled using the Alert Publisher Role Health Test Alert Publisher service-wide monitoring setting.

Short Name: Alert Publisher Health

Alert Publisher Role Health Test

Description

When computing the overall MGMT health, consider Alert Publisher's health

Template Name

`mgmt_alertpublisher_health_enabled`

Default Value

true

Unit(s)

no unit

Cloudera Management Service Certificate Expiration

This health test checks the expiry time of the TLS certificate for the Cloudera Manager Server. This test can be configured using the Cloudera Manager TLS Certificate Expiry Thresholds Cloudera Manager Service monitoring setting. This test alerts when the certificate is close to expiry.

Short Name: Certificate Expiration

Cloudera Manager TLS Certificate Expiry Thresholds

Description

The health test thresholds for monitoring the certificate of Cloudera Manager Server.

Template Name

`mgmt_certificate_expiry_thresholds`

Default Value

critical:7.0, warning:60.0

Unit(s)

DAYS

Cloudera Management Service Cloudera Manager Server Clock Offset

This is a health test that checks if the clock offset between Cloudera Manager Server and Service Monitor is too large. This test can be configured using the Cloudera Manager Server Clock Offset Thresholds Cloudera Manager Service monitoring setting. This test calculates clock offset using the timestamp int messages that Cloudera Manager Server sends to Service Monitor and the timestamp when Service Monitor gets the messages. Check the NTP configuration on both Cloudera Manager Server and Service Monitor machines if this test fails.

Short Name: Cloudera Manager Server Clock Offset

Cloudera Manager Server Clock Offset Thresholds

Description

The health test thresholds for monitoring the clock offset between the Cloudera Manager Server and the Service Monitor.

Template Name

`mgmt_clock_offset_with_smon_thresholds`

Default Value

critical:60000.0, warning:30000.0

Unit(s)

MILLISECONDS

Cloudera Management Service Command Storage Directory Free Space

This Command Storage Directory Free Space Monitoring Thresholds health test checks that the filesystem containing the directory used to store the Cloudera Manager Server's command data has sufficient space. This test can be configured using the Command Storage Directory Free Space Monitoring Thresholds Management Services monitoring settings. This directory can be changed by setting the Cloudera Manager Server Local Data Storage Directory path in Cloudera Manager settings.

Short Name: Command Storage Directory Free Space

Cloudera Manager Server Local Data Storage Directory

Description

Local path used by Cloudera Manager for storing data, including command result files. Note that changes to this configuration will only apply to commands started after the change. It is highly recommended that existing data be migrated over to the new location for the data to be accessible via and managed by Cloudera Manager.

Template Name

`command_storage_path`

Default Value

/var/lib/cloudera-scm-server

Unit(s)

no unit

Command Storage Directory Free Space Monitoring Thresholds

Description

The health test thresholds for monitoring the free space on the filesystem that contains the Cloudera Manager Server command storage directory.

Template Name

`mgmt_command_storage_directory_free_space_absolute_thresholds`

Default Value

critical:1.073741824E9, warning:2.147483648E9

Unit(s)

BYTES

Cloudera Management Service Embedded Database Free Space

The embedded PostgreSQL database running on the Cloudera Manager Server host is using a partition with a small amount of free space. Typically, the data for this embedded postgreSQL server is in /var/lib/cloudera-scm-server-db. Increase the available disk space or adjust the retention period of activity monitoring or auditing data. This test can be configured using the Embedded Database Free Space Monitoring Thresholds Management Services monitoring settings.

Short Name: Embedded Database Free Space

Embedded Database Free Space Monitoring Thresholds

Description

The health test thresholds for monitoring the free space on the volume for the embedded PostgreSQL database optionally running on the Cloudera Manager Server. If the embedded database is not in use, this has no effect.

Template Name

`mgmt_embedded_database_free_space_absolute_thresholds`

Default Value

critical:1.073741824E9, warning:2.147483648E9

Unit(s)

BYTES

Cloudera Management Service Event Server Health

This Cloudera Management Service service-level health test checks for the presence of a running, healthy Event Server. The test returns "Bad" health if the service is running and the Event Server is not running. In all other cases

it returns the health of the Event Server. A failure of this health test indicates a stopped or unhealthy Event Server. Check the status of the Event Server for more information. This test can be enabled or disabled using the Event Server Role Health Test Event Server service-wide monitoring setting.

Short Name: Event Server Health

Event Server Role Health Test

Description

When computing the overall MGMT health, consider Event Server's health

Template Name

`mgmt_eventserver_health_enabled`

Default Value

true

Unit(s)

no unit

Cloudera Management Service Host Monitor Health

This Cloudera Management Service service-level health test checks for the presence of a running, healthy Host Monitor. The test returns "Bad" health if the service is running and the Host Monitor is not running. In all other cases it returns the health of the Host Monitor. A failure of this health test indicates a stopped or unhealthy Host Monitor. Check the status of the Host Monitor for more information. This test can be enabled or disabled using the Host Monitor Role Health Test Host Monitor service-wide monitoring setting.

Short Name: Host Monitor Health

Host Monitor Role Health Test

Description

When computing the overall MGMT health, consider Host Monitor's health

Template Name

`mgmt_hostmonitor_health_enabled`

Default Value

true

Unit(s)

no unit

Cloudera Management Service KDC Server Connection Health

This health test checks the KDC Service Connection's Health. This test can be configured using the Cloudera Manager KDC Server Connection Health Thresholds Cloudera Manager Service monitoring setting. This test alerts when connection to the KDC Server is slow or not available.

Short Name: KDC Server Connection Health

Cloudera Manager KDC Server Connection Health Thresholds

Description

The health test thresholds for monitoring the KDC Server connection health by login time.

Template Name

`kdc_availability_thresholds`

Default Value

critical:1000.0, warning:500.0

Unit(s)

MILLISECONDS

Cloudera Management Service LDAP Server Connection Health

This health test checks the LDAP Service Connection's Health. This test can be configured using the Cloudera Manager LDAP Server Connection Health Thresholds Cloudera Manager Service monitoring setting. This test alerts when connection to the LDAP Server is slow or not available.

Short Name: LDAP Server Connection Health

Cloudera Manager LDAP Server Connection Health Thresholds

Description

The health test thresholds for monitoring the LDAP Server connection health by login time.

Template Name

`ldap_availability_thresholds`

Default Value

critical:1000.0, warning:500.0

Unit(s)

MILLISECONDS

Cloudera Management Service Navigator Audit Server Health

This Cloudera Management Service service-level health test checks for the presence of a running, healthy Navigator Audit Server. The test returns "Bad" health if the service is running and the Navigator Audit Server is not running. In all other cases it returns the health of the Navigator Audit Server. A failure of this health test indicates a stopped or unhealthy Navigator Audit Server. Check the status of the Navigator Audit Server for more information. This test can be enabled or disabled using the Navigator Audit Server Role Health Test Navigator Audit Server service-wide monitoring setting.

Short Name: Navigator Audit Server Health

Navigator Audit Server Role Health Test

Description

When computing the overall MGMT health, consider Navigator Audit Server's health

Template Name

`mgmt_navigator_health_enabled`

Default Value

true

Unit(s)

no unit

Cloudera Management Service Navigator Metadata Server Health

This Cloudera Management Service service-level health test checks for the presence of a running, healthy Navigator Metadata Server. The test returns "Bad" health if the service is running and the Navigator Metadata Server is not running. In all other cases it returns the health of the Navigator Metadata Server. A failure of this health test indicates a stopped or unhealthy Navigator Metadata Server. Check the status of the Navigator Metadata Server for more information. This test can be enabled or disabled using the Navigator Metadata Server Role Health Test Navigator Metadata Server service-wide monitoring setting.

Short Name: Navigator Metadata Server Health

Navigator Metadata Server Role Health Test

Description

When computing the overall MGMT health, consider Navigator Metadata Server's health

Template Name

`mgmt_navigatormetaserver_health_enabled`

Default Value

true

Unit(s)

no unit

Cloudera Management Service Reports Manager Health

This Cloudera Management Service service-level health test checks for the presence of a running, healthy Reports Manager. The test returns "Bad" health if the service is running and the Reports Manager is not running. In all other cases it returns the health of the Reports Manager. A failure of this health test indicates a stopped or unhealthy Reports Manager. Check the status of the Reports Manager for more information. This test can be enabled or disabled using the Reports Manager Role Health Test Reports Manager service-wide monitoring setting.

Short Name: Reports Manager Health

Reports Manager Role Health Test

Description

When computing the overall MGMT health, consider Reports Manager's health

Template Name

`mgmt_reportsmanager_health_enabled`

Default Value

true

Unit(s)

no unit

Cloudera Management Service Service Monitor Health

This Cloudera Management Service service-level health test checks for the presence of a running, healthy Service Monitor. The test returns "Bad" health if the service is running and the Service Monitor is not running. In all other cases it returns the health of the Service Monitor. A failure of this health test indicates a stopped or unhealthy Service Monitor. Check the status of the Service Monitor for more information. This test can be enabled or disabled using the Service Monitor Role Health Test Service Monitor service-wide monitoring setting.

Short Name: Service Monitor Health

Service Monitor Role Health Test

Description

When computing the overall MGMT health, consider Service Monitor's health

Template Name

`mgmt_servicemonitor_health_enabled`

Default Value

true

Unit(s)

no unit

Cloudera Management Service Telemetry Publisher Health

This Cloudera Management Service service-level health test checks for the presence of a running, healthy Telemetry Publisher. The test returns "Bad" health if the service is running and the Telemetry Publisher is not running. In all other cases it returns the health of the Telemetry Publisher. A failure of this health test indicates a stopped or unhealthy Telemetry Publisher. Check the status of the Telemetry Publisher for more information. This test can be enabled or disabled using the Telemetry Publisher Role Health Test Telemetry Publisher service-wide monitoring setting.

Short Name: Telemetry Publisher Health

Telemetry Publisher Role Health Test

Description

When computing the overall MGMT health, consider Telemetry Publisher's health

Template Name

`mgmt_telemetrypublisher_health_enabled`

Default Value

true

Unit(s)

no unit

Cruise Control Health Tests

Cruise Control Server Health

This Cruise Control service-level health test checks for the presence of a running, healthy Cruise Control Server. The test returns "Bad" health if the service is running and the Cruise Control Server is not running. In all other cases it returns the health of the Cruise Control Server. A failure of this health test indicates a stopped or unhealthy Cruise Control Server. Check the status of the Cruise Control Server for more information. This test can be enabled or disabled using the Cruise Control Server Role Health Test Cruise Control Server service-wide monitoring setting.

Short Name: Cruise Control Server Health

Cruise Control Server Role Health Test

Description

When computing the overall CRUISE_CONTROL health, consider Cruise Control Server's health

Template Name

`CRUISE_CONTROL_CRUISE_CONTROL_SERVER_health_enabled`

Default Value

true

Unit(s)

no unit

Cruise Control Server Health Tests

Cruise Control Server Audit Pipeline Test

This Cruise Control Server health test checks that the Auditing for the Cruise Control Server role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Cruise Control Server process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the

Cloudera Manager Agent on the Cruise Control Server host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Cruise Control Server monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Cruise Control Server File Descriptors

This Cruise Control Server health test checks that the number of file descriptors used does not rise above some percentage of the Cruise Control Server file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Cruise Control Server monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`cruise_control_server_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Cruise Control Server Host Health

This Cruise Control Server health test factors in the health of the host upon which the Cruise Control Server is running. A failure of this test means that the host running the Cruise Control Server is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Cruise Control Server Host Health Test Cruise Control Server monitoring setting.

Short Name: Host Health

Cruise Control Server Host Health Test

Description

When computing the overall Cruise Control Server health, consider the host's health.

Template Name

`cruise_control_server_host_health_enabled`

Default Value

true

Unit(s)

no unit

Cruise Control Server Log Directory Free Space

This Cruise Control Server health test checks that the filesystem containing the log directory of this Cruise Control Server has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Cruise Control Server monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Cruise Control Server Process Status

This Cruise Control Server health test checks that the Cloudera Manager Agent on the Cruise Control Server host is heart beating correctly and that the process associated with the Cruise Control Server role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Cruise Control Server process, a lack of connectivity to the Cloudera Manager Agent on the Cruise Control Server host, or a problem with the Cloudera Manager Agent. This test can fail either because the Cruise Control Server has crashed or because the Cruise Control Server will not start or stop in a timely fashion. Check the Cruise Control Server logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Cruise Control Server host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Cruise Control Server host, or look in the Cloudera Manager Agent logs on the Cruise Control Server host for more details. This test can be enabled or disabled using the Cruise Control Server Process Health Test Cruise Control Server monitoring setting.

Short Name: Process Status

Cruise Control Server Process Health Test

Description

Enables the health test that the Cruise Control Server's process state is consistent with the role configuration

Template Name

`cruise_control_server_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Cruise Control Server Swap Memory Usage

This Cruise Control Server health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Cruise Control Server Unexpected Exits

This Cruise Control Server health test checks that the Cruise Control Server has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Cruise Control Server monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Data Analytics Studio Eventprocessor Health Tests

Data Analytics Studio Eventprocessor Audit Pipeline Test

This Data Analytics Studio Eventprocessor health test checks that the Auditing for the Data Analytics Studio Eventprocessor role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Data Analytics Studio Eventprocessor process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Data Analytics Studio Eventprocessor host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent

logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Data Analytics Studio Eventprocessor monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Data Analytics Studio Eventprocessor File Descriptors

This Data Analytics Studio Eventprocessor health test checks that the number of file descriptors used does not rise above some percentage of the Data Analytics Studio Eventprocessor file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Data Analytics Studio Eventprocessor monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`das_event_processor_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Data Analytics Studio Eventprocessor Host Health

This Data Analytics Studio Eventprocessor health test factors in the health of the host upon which the Data Analytics Studio Eventprocessor is running. A failure of this test means that the host running the Data Analytics Studio Eventprocessor is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Data Analytics Studio Eventprocessor Host Health Test Data Analytics Studio Eventprocessor monitoring setting.

Short Name: Host Health

Data Analytics Studio Eventprocessor Host Health Test

Description

When computing the overall Data Analytics Studio Eventprocessor health, consider the host's health.

Template Name

`das_event_processor_host_health_enabled`

Default Value

true

Unit(s)

no unit

Data Analytics Studio Eventprocessor Log Directory Free Space

This Data Analytics Studio Eventprocessor health test checks that the filesystem containing the log directory of this Data Analytics Studio Eventprocessor has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Data Analytics Studio Eventprocessor monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Data Analytics Studio Eventprocessor Process Status

This Data Analytics Studio Eventprocessor health test checks that the Cloudera Manager Agent on the Data Analytics Studio Eventprocessor host is heart beating correctly and that the process associated with the Data Analytics Studio Eventprocessor role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Data Analytics Studio Eventprocessor process, a lack of connectivity to the Cloudera Manager Agent on the Data Analytics Studio Eventprocessor host, or a problem with the Cloudera Manager Agent. This test can fail either because the Data Analytics Studio Eventprocessor has crashed or because the Data Analytics Studio Eventprocessor will not start or stop in a timely fashion. Check the Data Analytics Studio Eventprocessor logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Data Analytics Studio Eventprocessor host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Data Analytics Studio Eventprocessor host, or look in the Cloudera Manager Agent logs on the Data Analytics Studio Eventprocessor host for more details. This test can be enabled or disabled using the Data Analytics Studio Eventprocessor Process Health Test Data Analytics Studio Eventprocessor monitoring setting.

Short Name: Process Status

Data Analytics Studio Eventprocessor Process Health Test

Description

Enables the health test that the Data Analytics Studio Eventprocessor's process state is consistent with the role configuration

Template Name

`das_event_processor_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Data Analytics Studio Eventprocessor Swap Memory Usage

This Data Analytics Studio Eventprocessor health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Data Analytics Studio Eventprocessor Unexpected Exits

This Data Analytics Studio Eventprocessor health test checks that the Data Analytics Studio Eventprocessor has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Data Analytics Studio Eventprocessor monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Data Analytics Studio Webapp Server Health Tests

Data Analytics Studio Webapp Server Audit Pipeline Test

This Data Analytics Studio Webapp Server health test checks that the Auditing for the Data Analytics Studio Webapp Server role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Data Analytics Studio Webapp Server process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Data Analytics Studio Webapp Server host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera

Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Data Analytics Studio Webapp Server monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Data Analytics Studio Webapp Server File Descriptors

This Data Analytics Studio Webapp Server health test checks that the number of file descriptors used does not rise above some percentage of the Data Analytics Studio Webapp Server file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Data Analytics Studio Webapp Server monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`das_webapp_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Data Analytics Studio Webapp Server Host Health

This Data Analytics Studio Webapp Server health test factors in the health of the host upon which the Data Analytics Studio Webapp Server is running. A failure of this test means that the host running the Data Analytics Studio Webapp Server is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Data Analytics Studio Webapp Server Host Health Test Data Analytics Studio Webapp Server monitoring setting.

Short Name: Host Health

Data Analytics Studio Webapp Server Host Health Test

Description

When computing the overall Data Analytics Studio Webapp Server health, consider the host's health.

Template Name

`das_webapp_host_health_enabled`

Default Value

true

Unit(s)

no unit

Data Analytics Studio Webapp Server Log Directory Free Space

This Data Analytics Studio Webapp Server health test checks that the filesystem containing the log directory of this Data Analytics Studio Webapp Server has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Data Analytics Studio Webapp Server monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Data Analytics Studio Webapp Server Process Status

This Data Analytics Studio Webapp Server health test checks that the Cloudera Manager Agent on the Data Analytics Studio Webapp Server host is heart beating correctly and that the process associated with the Data Analytics Studio Webapp Server role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Data Analytics Studio Webapp Server process, a lack of connectivity to the Cloudera Manager Agent on the Data Analytics Studio Webapp Server host, or a problem with the Cloudera Manager Agent. This test can fail either because the Data Analytics Studio Webapp Server has crashed or because the Data Analytics Studio Webapp Server will not start or stop in a timely fashion. Check the Data Analytics Studio Webapp Server logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Data Analytics Studio Webapp Server host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Data Analytics Studio Webapp Server host, or look in the Cloudera Manager Agent logs on the Data Analytics Studio Webapp Server host for more details. This test can be enabled or disabled using the Data Analytics Studio Webapp Server Process Health Test Data Analytics Studio Webapp Server monitoring setting.

Short Name: Process Status

Data Analytics Studio Webapp Server Process Health Test

Description

Enables the health test that the Data Analytics Studio Webapp Server's process state is consistent with the role configuration

Template Name

`das_webapp_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Data Analytics Studio Webapp Server Swap Memory Usage

This Data Analytics Studio Webapp Server health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Data Analytics Studio Webapp Server Unexpected Exits

This Data Analytics Studio Webapp Server health test checks that the Data Analytics Studio Webapp Server has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Data Analytics Studio Webapp Server monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

DataNode Health Tests

DataNode Audit Pipeline Test

This DataNode health test checks that the Auditing for the DataNode role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of DataNode process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the DataNode host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and

Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check DataNode monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

DataNode Block Count

This is a DataNode health test that checks for whether the DataNode has too many blocks. Having too many blocks on a DataNode may affect the DataNode's performance. A DataNode with a large number of blocks will require a larger java heap and may experience longer garbage collection pauses. Additionally, a large number of blocks may be an indicator of the presence of many small files. HDFS is not optimized for dealing with many small files, and processing times may suffer when operating across many small files. If only some DataNodes have a high number of blocks, running the HDFS Rebalance command may address this issue by moving data between DataNodes. If the HDFS Rebalance command reports the cluster as balanced without fixing the block imbalance then the problem is related to the presence of many small files. Consult the HDFS documentation for best-practices on addressing this issue. If many small files is not a concern for your use case, consider disabling this health test. If all DataNodes have

a high number of blocks and the issue is not related to small files, additional DataNodes should be added. This test can be configured using the DataNode Block Count Thresholds DataNode monitoring setting.

Short Name: Block Count

DataNode Block Count Thresholds

Description

The health test thresholds of the number of blocks on a DataNode

Template Name

`datanode_block_count_thresholds`

Default Value

CDH=[[CDH 4.0.0..CDH 4.5.0)=critical:never, warning:200000.0, [CDH 4.5.0..CDH 6.0.0)=critical:never, warning:500000.0, [CDH 6.0.0..CDH 8.0.0)=critical:never, warning:1000000.0]

Unit(s)

no unit

DataNode Data Directory Status

This is a DataNode health test that checks for whether the DataNode has reported any failed volumes. A failure of this health test indicates that there is a problem with one or more volumes on the DataNode. See the DataNode system for more information. This test can be configured using the DataNode Volume Failures Thresholds DataNode monitoring setting.

Short Name: Data Directory Status

DataNode Volume Failures Thresholds

Description

The health test thresholds of failed volumes in a DataNode.

Template Name

`datanode_volume_failures_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

DataNode DataNode Data Directory Free Space

This is a DataNode health test that checks that the filesystem containing the DataNode Data Directory of this DataNode has sufficient free space. See the DataNode Data Directory description on the DataNode configuration page for more information on this directory type. This test can be configured using the DataNode Data Directory Free Space Monitoring Absolute Thresholds and DataNode Data Directory Free Space Monitoring Percentage Thresholds DataNode monitoring settings.

Short Name: DataNode Data Directory Free Space

DataNode Data Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's DataNode Data Directory.

Template Name

`datanode_data_directories_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

DataNode Data Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's DataNode Data Directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a DataNode Data Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`datanode_data_directories_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

DataNode File Descriptors

This DataNode health test checks that the number of file descriptors used does not rise above some percentage of the DataNode file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds DataNode monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`datanode_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

DataNode Free Space

This is a DataNode health test that checks that the amount of free space available for HDFS block data on the DataNode does not fall below some percentage of total configured capacity of the DataNode. A failure of this health test may indicate a capacity planning problem. Try adding more disk capacity and additional data directories to the DataNode, or add additional DataNodes and take steps to rebalance your HDFS cluster. This test can be configured using the DataNode Free Space Monitoring Thresholds DataNode monitoring setting.

Short Name: Free Space

DataNode Free Space Monitoring Thresholds

Description

The health test thresholds of free space in a DataNode. Specified as a percentage of the capacity on the DataNode.

Template Name

`datanode_free_space_thresholds`

Default Value

critical:10.0, warning:20.0

Unit(s)

PERCENT

DataNode Heap Dump Directory Free Space

This DataNode health test checks that the filesystem containing the heap dump directory of this DataNode has sufficient free space. This test can be configured using the Heap Dump Directory Free Space Monitoring Absolute Thresholds and Heap Dump Directory Free Space Monitoring Percentage Thresholds DataNode monitoring settings.

Short Name: Heap Dump Directory Free Space

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Template Name

`heap_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`heap_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

DataNode Host Health

This DataNode health test factors in the health of the host upon which the DataNode is running. A failure of this test means that the host running the DataNode is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the DataNode Host Health Test DataNode monitoring setting.

Short Name: Host Health

DataNode Host Health Test

Description

When computing the overall DataNode health, consider the host's health.

Template Name

`datanode_host_health_enabled`

Default Value

true

Unit(s)

no unit

DataNode Log Directory Free Space

This DataNode health test checks that the filesystem containing the log directory of this DataNode has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds DataNode monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

DataNode NameNode Connectivity

This is a DataNode health test that checks that all the running NameNodes in the HDFS service consider the DataNode alive. A failure of this health test may indicate that the DataNode is having trouble communicating with some or all NameNodes in the service. Look in the DataNode logs for more details. This test can be enabled or disabled using the DataNode Connectivity Health Test DataNode monitoring setting. The DataNode Connectivity Tolerance at Startup DataNode monitoring setting and the Health Test Startup Tolerance NameNode monitoring setting can be used to control the test's tolerance windows around DataNode and NameNode restarts respectively.

Short Name: NameNode Connectivity

DataNode Connectivity Health Test

Description

Enables the health test that verifies the DataNode is connected to the NameNode

Template Name

`datanode_connectivity_health_enabled`

Default Value

true

Unit(s)

no unit

DataNode Connectivity Tolerance at Startup

Description

The amount of time to wait for the DataNode to fully start up and connect to the NameNode before enforcing the connectivity check.

Template Name

`datanode_connectivity_tolerance`

Default Value

180

Unit(s)

SECONDS

Health Test Startup Tolerance

Description

The amount of time allowed after this role is started that failures of health tests that rely on communication with this role will be tolerated.

Template Name

`namenode_startup_tolerance`

Default Value

5

Unit(s)

MINUTES

DataNode Pause Duration

This DataNode health test checks that the DataNode threads are not experiencing long scheduling pauses. The test uses a pause monitoring thread in the DataNode that tracks scheduling delay by noting if it is run on its requested schedule. If the thread is not run on its requested schedule, the delay is noted and considered pause time. The health test checks that no more than some percentage of recent time is spent paused. A failure of this health test may indicate that the DataNode is not getting enough CPU resources, or that it is spending too much time doing garbage collection. Inspect the DataNode logs for any pause monitor output and check garbage collection metrics exposed by the DataNode. This test can be configured using the Pause Duration Thresholds and Pause Duration Monitoring Period DataNode monitoring settings.

Short Name: Pause Duration

Pause Duration Monitoring Period

Description

The period to review when computing the moving average of extra time the pause monitor spent paused.

Template Name

`datanode_pause_duration_window`

Default Value

5

Unit(s)

MINUTES

Pause Duration Thresholds

Description

The health test thresholds for the weighted average extra time the pause monitor spent paused. Specified as a percentage of elapsed wall clock time.

Template Name

`datanode_pause_duration_thresholds`

Default Value

critical:60.0, warning:30.0

Unit(s)

no unit

DataNode Process Status

This DataNode health test checks that the Cloudera Manager Agent on the DataNode host is heart beating correctly and that the process associated with the DataNode role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the DataNode process, a lack of connectivity to the Cloudera Manager Agent on the DataNode host, or a problem with the Cloudera Manager Agent. This test can fail either because the DataNode has crashed or because the DataNode will not start or stop in a timely fashion. Check the DataNode logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the DataNode host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the DataNode host, or look in the Cloudera Manager Agent logs on the DataNode host for more details. This test can be enabled or disabled using the DataNode Process Health Test DataNode monitoring setting.

Short Name: Process Status

DataNode Process Health Test

Description

Enables the health test that the DataNode's process state is consistent with the role configuration

Template Name

`datanode_scm_health_enabled`

Default Value

true

Unit(s)

no unit

DataNode Swap Memory Usage

This DataNode health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

DataNode Transceiver Usage

This is a DataNode health test that checks for whether the DataNode transceivers usage is nearing the configured transceivers limit. A transceiver is a thread used to transfer data into or out of the DataNode. If a DataNode hits its transceivers limit, HDFS reads and writes begin to fail. This test can be configured using the DataNode Transceivers Usage Thresholds DataNode monitoring setting. The Maximum Number of Transfer Threads DataNode setting controls the DataNode transceivers limit.

Short Name: Transceiver Usage

DataNode Transceivers Usage Thresholds

Description

The health test thresholds of transceivers usage in a DataNode. Specified as a percentage of the total configured number of transceivers.

Template Name

`datanode_transceivers_usage_thresholds`

Default Value

critical:95.0, warning:75.0

Unit(s)

PERCENT

Maximum Number of Transfer Threads

Description

Specifies the maximum number of threads to use for transferring data in and out of the DataNode.

Template Name

`dfs_datanode_max_xcievers`

Default Value

4096

Unit(s)

no unit

DataNode Unexpected Exits

This DataNode health test checks that the DataNode has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is

enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period DataNode monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

DataNode Web Server Status

This health test checks that the role's web server is responding quickly to requests by the Cloudera Manager Agent, and that the Cloudera Manager Agent can collect metrics from the web server. Failure of this health test may indicate a problem with the web server of the DataNode, a misconfiguration of the DataNode, or a problem with the Cloudera Manager Agent. Consult the Cloudera Manager Agent logs and the logs of the DataNode for more detail. If the test failure message indicates a communication problem, the Cloudera Manager Agent's HTTP requests to the DataNode's web server are failing or timing out. If the test's failure message indicates an unexpected response, the DataNode's web server responded to the Cloudera Manager Agent's request, but the response could not be interpreted for some reason. This test can be configured using the Web Metric Collection DataNode monitoring setting.

Short Name: Web Server Status

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Template Name

`datanode_web_metric_collection_enabled`

Default Value

true

Unit(s)

no unit

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Template Name

`datanode_web_metric_collection_thresholds`

Default Value

critical:never, warning:10000.0

Unit(s)

MILLISECONDS

Event Server Health Tests

Event Server Audit Pipeline Test

This Event Server health test checks that the Auditing for the Event Server role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Event Server process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Event Server host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Event Server monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Event Server Cloudera Manager Descriptor Age

This is a Event Server health test that checks if the Cloudera Manager descriptor has been refreshed recently. The Cloudera Manager descriptor is used to pass configuration information from the Cloudera Manager Server to the Event Server. If the descriptor becomes stale, Event Server operation may be impacted because the Event Server will receive information about new hosts, roles, and services, or changes to existing hosts, roles, and services. A stale descriptor usually indicates problems communicating with the Cloudera Manager Server but can also indicate performance problems or a bug. Consult the Event Server log and the Cloudera Manager Server log for more information. This test can be configured using the Cloudera Manager Descriptor Age Thresholds Cloudera Manager Event Server setting.

Short Name: Cloudera Manager Descriptor Age

Cloudera Manager Descriptor Age Thresholds

Description

The health test thresholds for monitoring the time since the Cloudera Manager descriptor was last refreshed.

Template Name

`scm_descriptor_age_thresholds`

Default Value

critical:120000.0, warning:60000.0

Unit(s)

no unit

Event Server Event Server Index Directory Free Space

This is a Event Server health test that checks that the filesystem containing the Event Server Index Directory of this Event Server has sufficient free space. See the Event Server Index Directory description on the Event Server configuration page for more information on this directory type. This test can be configured using the Event Server Index Directory Free Space Monitoring Absolute Thresholds and Event Server Index Directory Free Space Monitoring Percentage Thresholds Event Server monitoring settings.

Short Name: Event Server Index Directory Free Space

Event Server Index Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Event Server Index Directory.

Template Name

`eventserver_index_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Event Server Index Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Event Server Index Directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Event Server Index Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`eventserver_index_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Event Server Event Store Size

This is an Event Server health test that checks that the event store size has not grown too far above the configured event store capacity. A failure of this health test indicates that the Event Server is having a problem performing cleanup. This may indicate a configuration problem or bug in the Event Server. This test can be configured using the Event Store Capacity Monitoring Thresholds Event Server monitoring setting.

Short Name: Event Store Size

Event Store Capacity Monitoring Thresholds

Description

The health test thresholds on the number of events in the event store. Specified as a percentage of the maximum number of events in Event Server store.

Template Name

`eventserver_capacity_thresholds`

Default Value

critical:130.0, warning:115.0

Unit(s)

PERCENT

Event Server File Descriptors

This Event Server health test checks that the number of file descriptors used does not rise above some percentage of the Event Server file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Event Server monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`eventserver_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Event Server GC Duration

This Event Server health test checks that the Event Server is not spending too much time performing Java garbage collection. It checks that no more than some percentage of recent time is spent performing Java garbage collection. A failure of this health test may indicate a capacity planning problem or misconfiguration of the Event Server. This test can be configured using the Garbage Collection Duration Thresholds and Garbage Collection Duration Monitoring Period Event Server monitoring settings.

Short Name: GC Duration

Garbage Collection Duration Monitoring Period

Description

The period to review when computing the moving average of garbage collection time.

Template Name

`eventserver_gc_duration_window`

Default Value

5

Unit(s)

MINUTES

Garbage Collection Duration Thresholds

Description

The health test thresholds for the weighted average time spent in Java garbage collection. Specified as a percentage of elapsed wall clock time.

Template Name

`eventserver_gc_duration_thresholds`

Default Value

critical:60.0, warning:30.0

Unit(s)

no unit

Event Server Heap Dump Directory Free Space

This Event Server health test checks that the filesystem containing the heap dump directory of this Event Server has sufficient free space. This test can be configured using the Heap Dump Directory Free Space Monitoring Absolute Thresholds and Heap Dump Directory Free Space Monitoring Percentage Thresholds Event Server monitoring settings.

Short Name: Heap Dump Directory Free Space

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Template Name

`heap_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`heap_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Event Server Host Health

This Event Server health test factors in the health of the host upon which the Event Server is running. A failure of this test means that the host running the Event Server is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Event Server Host Health Test Event Server monitoring setting.

Short Name: Host Health

Event Server Host Health Test

Description

When computing the overall Event Server health, consider the host's health.

Template Name

`eventserver_host_health_enabled`

Default Value

true

Unit(s)

no unit

Event Server Log Directory Free Space

This Event Server health test checks that the filesystem containing the log directory of this Event Server has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Event Server monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Event Server Process Status

This Event Server health test checks that the Cloudera Manager Agent on the Event Server host is heart beating correctly and that the process associated with the Event Server role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Event Server process, a lack of connectivity to the Cloudera Manager Agent on the Event Server host, or a problem with the Cloudera Manager Agent. This test can fail either because the Event Server has crashed or because the Event Server will not start or stop in a timely fashion. Check the Event Server logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Event Server host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Event Server host, or look in the Cloudera Manager Agent logs on the Event Server host for more details. This test can be enabled or disabled using the Event Server Process Health Test Event Server monitoring setting.

Short Name: Process Status

Event Server Process Health Test

Description

Enables the health test that the Event Server's process state is consistent with the role configuration

Template Name

`eventserver_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Event Server Swap Memory Usage

This Event Server health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Event Server Unexpected Exits

This Event Server health test checks that the Event Server has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Event Server monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Event Server Web Server Status

This health test checks that the role's web server is responding quickly to requests by the Cloudera Manager Agent, and that the Cloudera Manager Agent can collect metrics from the web server. Failure of this health test may indicate a problem with the web server of the Event Server, a misconfiguration of the Event Server, or a problem with the Cloudera Manager Agent. Consult the Cloudera Manager Agent logs and the logs of the Event Server for more detail.

If the test failure message indicates a communication problem, the Cloudera Manager Agent's HTTP requests to the Event Server's web server are failing or timing out. If the test's failure message indicates an unexpected response, the Event Server's web server responded to the Cloudera Manager Agent's request, but the response could not be interpreted for some reason. This test can be configured using the Web Metric Collection Event Server monitoring setting.

Short Name: Web Server Status

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Template Name

`eventserver_web_metric_collection_enabled`

Default Value

true

Unit(s)

no unit

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Template Name

`eventserver_web_metric_collection_thresholds`

Default Value

critical:never, warning:10000.0

Unit(s)

MILLISECONDS

Event Server Write Pipeline

This Event Server health test checks that no messages are being dropped by the writer stage of the Event Server pipeline. A failure of this health test indicates a problem with the Event Server. This may indicate a configuration problem or a bug in the Event Server. This test can be configured using the Event Server Write Pipeline Monitoring Time Period monitoring setting.

Short Name: Write Pipeline

Event Server Write Pipeline Monitoring Thresholds

Description

The health test thresholds for monitoring the Event Server write pipeline. This specifies the number of dropped messages that will be tolerated over the monitoring time period.

Template Name

`eventserver_write_pipeline_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Event Server Write Pipeline Monitoring Time Period

Description

The time period over which the Event Server write pipeline will be monitored for dropped messages.

Template Name

`eventserver_write_pipeline_window`

Default Value

5

Unit(s)

MINUTES

Failover Controller Health Tests

Failover Controller Audit Pipeline Test

This Failover Controller health test checks that the Auditing for the Failover Controller role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Failover Controller process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Failover Controller host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Failover Controller monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Failover Controller File Descriptors

This Failover Controller health test checks that the number of file descriptors used does not rise above some percentage of the Failover Controller file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Failover Controller monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`failovercontroller_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Failover Controller Heap Dump Directory Free Space

This Failover Controller health test checks that the filesystem containing the heap dump directory of this Failover Controller has sufficient free space. This test can be configured using the Heap Dump Directory Free Space Monitoring Absolute Thresholds and Heap Dump Directory Free Space Monitoring Percentage Thresholds Failover Controller monitoring settings.

Short Name: Heap Dump Directory Free Space

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Template Name

`heap_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`heap_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Failover Controller Host Health

This Failover Controller health test factors in the health of the host upon which the Failover Controller is running. A failure of this test means that the host running the Failover Controller is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Failover Controller Host Health Test Failover Controller monitoring setting.

Short Name: Host Health

Failover Controller Host Health Test

Description

When computing the overall Failover Controller health, consider the host's health.

Template Name

`failovercontroller_host_health_enabled`

Default Value

true

Unit(s)

no unit

Failover Controller Log Directory Free Space

This Failover Controller health test checks that the filesystem containing the log directory of this Failover Controller has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Failover Controller monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Failover Controller Process Status

This Failover Controller health test checks that the Cloudera Manager Agent on the Failover Controller host is heart beating correctly and that the process associated with the Failover Controller role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Failover Controller process, a lack of connectivity to the Cloudera Manager Agent on the Failover Controller host, or a problem with the Cloudera Manager Agent. This test can fail either because the Failover Controller has crashed or because the Failover Controller will not start or stop in a timely fashion. Check the Failover Controller logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Failover Controller host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Failover Controller host, or look in the Cloudera Manager Agent logs on the Failover Controller host for more details. This test can be enabled or disabled using the Failover Controller Process Health Test Failover Controller monitoring setting.

Short Name: Process Status

Failover Controller Process Health Test

Description

Enables the health test that the Failover Controller's process state is consistent with the role configuration

Template Name

`failovercontroller_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Failover Controller Swap Memory Usage

This Failover Controller health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Failover Controller Unexpected Exits

This Failover Controller health test checks that the Failover Controller has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Failover Controller monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Flume Health Tests

Flume Agent Health

This is a Flume service-level health test that checks that enough of the Agents in the cluster are healthy. The test returns "Concerning" health if the number of healthy Agents falls below a warning threshold, expressed as a percentage of the total number of Agents. The test returns "Bad" health if the number of healthy and "Concerning" Agents falls below a critical threshold, expressed as a percentage of the total number of Agents. For example, if this test is configured with a warning threshold of 95% and a critical threshold of 90% for a cluster of 100 Agents, this test would return "Good" health if 95 or more Agents have good health. This test would return "Concerning" health if at

least 90 Agents have either "Good" or "Concerning" health. If more than 10 Agents have bad health, this test would return "Bad" health. A failure of this health test indicates unhealthy Agents. Check the status of the individual Agents for more information. This test can be configured using the Flume Flume service-wide monitoring setting.

Short Name: Agent Health

Healthy Agent Monitoring Thresholds

Description

The health test thresholds of the overall Agent health. The check returns "Concerning" health if the percentage of "Healthy" Agents falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Agents falls below the critical threshold.

Template Name

`flume_agents_healthy_thresholds`

Default Value

critical:never, warning:95.0

Unit(s)

PERCENT

Flume Agent Health Tests

Flume Agent Audit Pipeline Test

This Agent health test checks that the Auditing for the Agent role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Agent process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Agent host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Agent monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Flume Agent File Descriptors

This Agent health test checks that the number of file descriptors used does not rise above some percentage of the Agent file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Agent monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`flume_agent_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Flume Agent Heap Dump Directory Free Space

This Agent health test checks that the filesystem containing the heap dump directory of this Agent has sufficient free space. This test can be configured using the Heap Dump Directory Free Space Monitoring Absolute Thresholds and Heap Dump Directory Free Space Monitoring Percentage Thresholds Agent monitoring settings.

Short Name: Heap Dump Directory Free Space

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Template Name

`heap_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`heap_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Flume Agent Host Health

This Agent health test factors in the health of the host upon which the Agent is running. A failure of this test means that the host running the Agent is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Agent Host Health Test Agent monitoring setting.

Short Name: Host Health

Agent Host Health Test

Description

When computing the overall Agent health, consider the host's health.

Template Name

`flume_agent_host_health_enabled`

Default Value

true

Unit(s)

no unit

Flume Agent Log Directory Free Space

This Agent health test checks that the filesystem containing the log directory of this Agent has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Agent monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Flume Agent Process Status

This Agent health test checks that the Cloudera Manager Agent on the Agent host is heart beating correctly and that the process associated with the Agent role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Agent process, a lack of connectivity to the Cloudera Manager Agent on the Agent host, or a problem with the Cloudera Manager Agent. This test can fail either because the Agent has crashed or because the Agent will not start or stop in a timely fashion. Check the Agent logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Agent host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Agent host, or look in the Cloudera Manager Agent logs on the Agent host for more details. This test can be enabled or disabled using the Agent Process Health Test Agent monitoring setting.

Short Name: Process Status

Agent Process Health Test

Description

Enables the health test that the Agent's process state is consistent with the role configuration

Template Name

`flume_agent_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Flume Agent Swap Memory Usage

This Agent health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Flume Agent Unexpected Exits

This Agent health test checks that the Agent has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Agent monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Flume Agent Web Server Status

This health test checks that the role's web server is responding quickly to requests by the Cloudera Manager Agent, and that the Cloudera Manager Agent can collect metrics from the web server. Failure of this health test may indicate a problem with the web server of the Agent, a misconfiguration of the Agent, or a problem with the Cloudera Manager Agent. Consult the Cloudera Manager Agent logs and the logs of the Agent for more detail. If the test failure message indicates a communication problem, the Cloudera Manager Agent's HTTP requests to the Agent's web server are failing or timing out. If the test's failure message indicates an unexpected response, the Agent's web server responded to the Cloudera Manager Agent's request, but the response could not be interpreted for some reason. This test can be configured using the Web Metric Collection Agent monitoring setting.

Short Name: Web Server Status

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Template Name

`agent_web_metric_collection_enabled`

Default Value

true

Unit(s)

no unit

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Template Name

`agent_web_metric_collection_thresholds`

Default Value

critical:never, warning:10000.0

Unit(s)

MILLISECONDS

Garbage Collector Health Tests

Garbage Collector Audit Pipeline Test

This Garbage Collector health test checks that the Auditing for the Garbage Collector role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Garbage Collector process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Garbage Collector host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Garbage Collector monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Garbage Collector File Descriptors

This Garbage Collector health test checks that the number of file descriptors used does not rise above some percentage of the Garbage Collector file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Garbage Collector monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`accumulo16_gc_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Garbage Collector Host Health

This Garbage Collector health test factors in the health of the host upon which the Garbage Collector is running. A failure of this test means that the host running the Garbage Collector is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Garbage Collector Host Health Test Garbage Collector monitoring setting.

Short Name: Host Health

Garbage Collector Host Health Test

Description

When computing the overall Garbage Collector health, consider the host's health.

Template Name

`accumulo16_gc_host_health_enabled`

Default Value

true

Unit(s)

no unit

Garbage Collector Log Directory Free Space

This Garbage Collector health test checks that the filesystem containing the log directory of this Garbage Collector has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Garbage Collector monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Garbage Collector Process Status

This Garbage Collector health test checks that the Cloudera Manager Agent on the Garbage Collector host is heart beating correctly and that the process associated with the Garbage Collector role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Garbage Collector process, a lack of connectivity to the Cloudera Manager Agent on the Garbage Collector host, or a problem with the Cloudera Manager Agent. This test can fail either because the Garbage Collector has crashed or because the Garbage Collector will not start or stop in a timely fashion. Check the Garbage Collector logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Garbage Collector host, check the status of the

Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Garbage Collector host, or look in the Cloudera Manager Agent logs on the Garbage Collector host for more details. This test can be enabled or disabled using the Garbage Collector Process Health Test Garbage Collector monitoring setting.

Short Name: Process Status

Garbage Collector Process Health Test

Description

Enables the health test that the Garbage Collector's process state is consistent with the role configuration

Template Name

`accumulo16_gc_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Garbage Collector Swap Memory Usage

This Garbage Collector health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Garbage Collector Unexpected Exits

This Garbage Collector health test checks that the Garbage Collector has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Garbage Collector monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

HBase Health Tests

HBase Master Health

This is an HBase service-level health test that checks for an active, healthy HBase Master. The test returns "Bad" health if the service is running and an active Master cannot be found. If an active Master is found, then the test checks the health of that Master as well as the health of any standby Masters configured. A "Good" health result will only be returned if the active Master is healthy and all running standby Masters are healthy. A failure of this health test may indicate stopped or unhealthy Master roles, or it may indicate a problem with communication between the Cloudera Manager Service Monitor and the HBase service. Check the status of the HBase service's Master roles and look in the Cloudera Manager Service Monitor's log files for more information when this test fails. This test can be enabled or disabled using the Active Master Health Test HBase service-wide monitoring setting. The check for a healthy standby Master can be enabled or disabled with Backup Masters Health Test. In addition, the HBase Active Master Detection Window can be used to adjust the amount of time that the Cloudera Manager Service Monitor has to detect the active HBase Master before this health test fails.

Short Name: HBase Master Health

Active Master Health Test

Description

When computing the overall HBase cluster health, consider the active HBase Master's health.

Template Name

`hbase_master_health_enabled`

Default Value

true

Unit(s)

no unit

Backup Masters Health Test

Description

When computing the overall HBase cluster health, consider the health of the backup HBase Masters.

Template Name

`hbase_backup_masters_health_enabled`

Default Value

true

Unit(s)

no unit

HBase Active Master Detection Window

Description

The tolerance window that will be used in HBase service tests that depend on detection of the active HBase Master.

Template Name

`hbase_active_master_detection_window`

Default Value

3

Unit(s)

MINUTES

HBase RegionServer Health

This is a HBase service-level health test that checks that enough of the RegionServers in the cluster are healthy. The test returns "Concerning" health if the number of healthy RegionServers falls below a warning threshold, expressed as a percentage of the total number of RegionServers. The test returns "Bad" health if the number of healthy and "Concerning" RegionServers falls below a critical threshold, expressed as a percentage of the total number of RegionServers. For example, if this test is configured with a warning threshold of 95% and a critical threshold of 90% for a cluster of 100 RegionServers, this test would return "Good" health if 95 or more RegionServers have good health. This test would return "Concerning" health if at least 90 RegionServers have either "Good" or "Concerning" health. If more than 10 RegionServers have bad health, this test would return "Bad" health. A failure of this health test indicates unhealthy RegionServers. Check the status of the individual RegionServers for more information. This test can be configured using the HBase HBase service-wide monitoring setting.

Short Name: RegionServer Health

Healthy RegionServer Monitoring Thresholds

Description

The health test thresholds of the overall RegionServer health. The check returns "Concerning" health if the percentage of "Healthy" RegionServers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" RegionServers falls below the critical threshold.

Template Name

`hbase_regionservers_healthy_thresholds`

Default Value

critical:90.0, warning:95.0

Unit(s)

PERCENT

HBase REST Server Health Tests

HBase REST Server Audit Pipeline Test

This HBase REST Server health test checks that the Auditing for the HBase REST Server role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of HBase REST Server process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the HBase REST Server host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check HBase REST Server monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

HBase REST Server File Descriptors

This HBase REST Server health test checks that the number of file descriptors used does not rise above some percentage of the HBase REST Server file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds HBase REST Server monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`hbaserestserver_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

HBase REST Server Heap Dump Directory Free Space

This HBase REST Server health test checks that the filesystem containing the heap dump directory of this HBase REST Server has sufficient free space. This test can be configured using the Heap Dump Directory Free Space Monitoring Absolute Thresholds and Heap Dump Directory Free Space Monitoring Percentage Thresholds HBase REST Server monitoring settings.

Short Name: Heap Dump Directory Free Space

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Template Name

`heap_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`heap_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

HBase REST Server Host Health

This HBase REST Server health test factors in the health of the host upon which the HBase REST Server is running. A failure of this test means that the host running the HBase REST Server is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the HBase REST Server Host Health Test HBase REST Server monitoring setting.

Short Name: Host Health

HBase REST Server Host Health Test

Description

When computing the overall HBase REST Server health, consider the host's health.

Template Name

`hbaserestserver_host_health_enabled`

Default Value

true

Unit(s)

no unit

HBase REST Server Log Directory Free Space

This HBase REST Server health test checks that the filesystem containing the log directory of this HBase REST Server has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds HBase REST Server monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

HBase REST Server Process Status

This HBase REST Server health test checks that the Cloudera Manager Agent on the HBase REST Server host is heart beating correctly and that the process associated with the HBase REST Server role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the HBase REST Server process, a lack of connectivity to the Cloudera Manager Agent on the HBase REST Server host, or a problem with the Cloudera Manager Agent. This test can fail either because the HBase REST Server has crashed or because the HBase REST Server will not start or stop in a timely fashion. Check the HBase REST Server logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the HBase REST Server host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the HBase REST Server host, or look in the Cloudera Manager Agent logs on the HBase REST Server host for more details. This test can be enabled or disabled using the HBase REST Server Process Health Test HBase REST Server monitoring setting.

Short Name: Process Status

HBase REST Server Process Health Test

Description

Enables the health test that the HBase REST Server's process state is consistent with the role configuration

Template Name

`hbaserestserver_scm_health_enabled`

Default Value

true

Unit(s)

no unit

HBase REST Server Swap Memory Usage

This HBase REST Server health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

HBase REST Server Unexpected Exits

This HBase REST Server health test checks that the HBase REST Server has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory

monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period HBase REST Server monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

HBase Thrift Server Health Tests

HBase Thrift Server Audit Pipeline Test

This HBase Thrift Server health test checks that the Auditing for the HBase Thrift Server role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of HBase Thrift Server process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the HBase Thrift Server host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check HBase Thrift Server monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

HBase Thrift Server File Descriptors

This HBase Thrift Server health test checks that the number of file descriptors used does not rise above some percentage of the HBase Thrift Server file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds HBase Thrift Server monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`hbasethriftserver_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

HBase Thrift Server Heap Dump Directory Free Space

This HBase Thrift Server health test checks that the filesystem containing the heap dump directory of this HBase Thrift Server has sufficient free space. This test can be configured using the Heap Dump Directory Free Space Monitoring Absolute Thresholds and Heap Dump Directory Free Space Monitoring Percentage Thresholds HBase Thrift Server monitoring settings.

Short Name: Heap Dump Directory Free Space

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Template Name

`heap_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`heap_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

HBase Thrift Server Host Health

This HBase Thrift Server health test factors in the health of the host upon which the HBase Thrift Server is running. A failure of this test means that the host running the HBase Thrift Server is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the HBase Thrift Server Host Health Test HBase Thrift Server monitoring setting.

Short Name: Host Health

HBase Thrift Server Host Health Test

Description

When computing the overall HBase Thrift Server health, consider the host's health.

Template Name

`hbasethriftserver_host_health_enabled`

Default Value

true

Unit(s)

no unit

HBase Thrift Server Log Directory Free Space

This HBase Thrift Server health test checks that the filesystem containing the log directory of this HBase Thrift Server has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute

Thresholds and Log Directory Free Space Monitoring Percentage Thresholds HBase Thrift Server monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

HBase Thrift Server Process Status

This HBase Thrift Server health test checks that the Cloudera Manager Agent on the HBase Thrift Server host is heart beating correctly and that the process associated with the HBase Thrift Server role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the HBase Thrift Server process, a lack of connectivity to the Cloudera Manager Agent on the HBase Thrift Server host, or a problem with the Cloudera Manager Agent. This test can fail either because the HBase Thrift Server has crashed or because the HBase Thrift Server will not start or stop in a timely fashion. Check the HBase Thrift Server logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the HBase Thrift Server host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the HBase Thrift Server host, or look in the Cloudera Manager Agent logs on the HBase Thrift Server host for more details. This test can be enabled or disabled using the HBase Thrift Server Process Health Test HBase Thrift Server monitoring setting.

Short Name: Process Status

HBase Thrift Server Process Health Test

Description

Enables the health test that the HBase Thrift Server's process state is consistent with the role configuration

Template Name

`hbasethriftserver_scm_health_enabled`

Default Value

true

Unit(s)

no unit

HBase Thrift Server Swap Memory Usage

This HBase Thrift Server health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

HBase Thrift Server Unexpected Exits

This HBase Thrift Server health test checks that the HBase Thrift Server has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period HBase Thrift Server monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

HDFS Health Tests

HDFS Canary

This is an HDFS service-level health test that checks that basic client operations are working and are completing in a reasonable amount of time. This test reports the results of a periodic "canary" test that performs the following sequence of operations. First, it creates a file. By default, the path is /tmp/.cloudera_health_monitoring_canary_timestamp. The canary test then writes a small amount of data to that file, reads that data back, and verifies that the data is correct. Lastly, the canary test removes the created file. The test returns "Bad" health if any of the basic operations fail. The test returns "Concerning" health if the canary test runs too slowly. A failure of this health test may indicate that the cluster is failing to satisfy basic client requests correctly or in a timely fashion. Check the status of the NameNode and other service-level health tests. Look in the Service Monitor logs for log messages from the canary test. Look in the NameNode logs for more details about the processing of the canary test requests. This test can be enabled or disabled using the HDFS Canary Health Check HDFS service-wide monitoring setting.

Short Name: HDFS Canary

HDFS Canary Health Check

Description

Enables the health check that a client can create, read, write, and delete files

Template Name

`hdfs_canary_health_enabled`

Default Value

true

Unit(s)

no unit

HDFS Corrupt Blocks

This is an HDFS service-level health test that checks that the number of corrupt blocks does not rise above some percentage of the cluster's total blocks. A block is called corrupt by HDFS if it has at least one corrupt replica along with at least one live replica. As such, a corrupt block does not indicate unavailable data, but they do indicate an increased chance that data may become unavailable. If none of a block's replicas are live, the block is called a missing block by HDFS, not a corrupt block. HDFS automatically fixes corrupt blocks in the background. A failure of this health test may indicate a problem with the underlying storage or filesystem of a DataNode. Use the HDFS fsck command to identify which files contain corrupt blocks. This test can be configured using the Blocks With Corrupt Replicas Monitoring Thresholds HDFS service-wide monitoring setting.

Short Name: Corrupt Blocks

Blocks With Corrupt Replicas Monitoring Thresholds

Description

The health check thresholds of the number of blocks that have at least one corrupt replica. Specified as a percentage of the total number of blocks.

Template Name

`hdfs_blocks_with_corrupt_replicas_thresholds`

Default Value

critical:1.0, warning:0.5

Unit(s)

PERCENT

HDFS DataNode Health

This is a HDFS service-level health test that checks that enough of the DataNodes in the cluster are healthy. The test returns "Concerning" health if the number of healthy DataNodes falls below a warning threshold, expressed as a percentage of the total number of DataNodes. The test returns "Bad" health if the number of healthy and "Concerning" DataNodes falls below a critical threshold, expressed as a percentage of the total number of DataNodes. For example, if this test is configured with a warning threshold of 95% and a critical threshold of 90% for a cluster of 100 DataNodes, this test would return "Good" health if 95 or more DataNodes have good health. This test would return "Concerning" health if at least 90 DataNodes have either "Good" or "Concerning" health. If more than 10 DataNodes have bad health, this test would return "Bad" health. A failure of this health test indicates unhealthy DataNodes. Check the status of the individual DataNodes for more information. This test can be configured using the HDFS HDFS service-wide monitoring setting.

Short Name: DataNode Health

Healthy DataNode Monitoring Thresholds

Description

The health test thresholds of the overall DataNode health. The check returns "Concerning" health if the percentage of "Healthy" DataNodes falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" DataNodes falls below the critical threshold.

Template Name

`hdfs_datanodes_healthy_thresholds`

Default Value

critical:90.0, warning:95.0

Unit(s)

PERCENT

HDFS Erasure Coding Policy Verification Test

There is a high risk of losing data if the offending erasure coding policy is used. For more information, see *Best Practices for Rack and Node Setup for EC*. Do one of the following to clear this health issue: Add more DataNodes or Racks to your Cluster, if you want to use all the enabled erasure coding policies. Disable the offending erasure coding policy:

- Change the default erasure coding policy, if the offending policy is set as the default policy: Go to the HDFS configuration page, search for 'Fallback Erasure Coding Policy', and select one that is compliant with your existing cluster setup.
- Disable the offending erasure coding policy: Use the 'hdfs ec -disablePolicy -policy <policyName>' command.

Disable the health test: Go to the HDFS configuration page, search for 'Erasure Coding Policy Verification Health Check', and unselect it. This is not recommended, because there is a high risk of losing data if the offending erasure coding policy is used.

Short Name: Erasure Coding Policy Verification Test

Erasure Coding Policy Verification Health Check

Description

Enables the health test for verifying if the cluster topology supports all the enabled erasure coding policies.

Template Name

`hdfs_verify_ec_with_topology_enabled`

Default Value

false

Unit(s)

no unit

Fallback Erasure Coding Policy

Description

The fallback Erasure Coding policy that HDFS uses if no policy is specified when you run the -setPolicy command.

Template Name

`erasure_coding_default_policy`

Default Value

CDH=[[CDH 6.0.0..CDH 8.0.0)=RS_6_3_1024K]

Unit(s)

no unit

HDFS Failover Controllers Health

This is a HDFS service-level health test that checks that all the Failover Controllers associated with this service are healthy and running. The test returns "Bad" health if any of Failover Controllers that the service depends on is unhealthy or not running. Check the Failover Controllers logs for more details This test can be enabled or disabled using the Failover Controllers Healthy service-wide monitoring setting.

Short Name: Failover Controllers Health

Failover Controllers Healthy

Description

Enables the health check that verifies that the failover controllers associated with this service are healthy and running.

Template Name

`failover_controllers_healthy_enabled`

Default Value

true

Unit(s)

no unit

HDFS Free Space

This is an HDFS service-level health test that checks that the amount of free space in the HDFS cluster does not fall below some percentage of total configured capacity. A failure of this health test may indicate a capacity planning problem, or a loss of DataNodes. An unfinalized HDFS metadata upgrade can also significantly decrease free space. This test can be configured using the HDFS Free Space Monitoring Thresholds HDFS service-wide monitoring setting.

Short Name: Free Space

HDFS Free Space Monitoring Thresholds

Description

The health check thresholds of free space in HDFS. Specified as a percentage of total HDFS capacity.

Template Name

`hdfs_free_space_thresholds`

Default Value

critical:10.0, warning:20.0

Unit(s)

PERCENT

HDFS Missing Blocks

This is an HDFS service-level health test that checks the number of missing blocks does not rise above some percentage of the cluster's total blocks. A missing block is a block with no live replicas. All replicas are either missing or corrupt. This may happen because of corruption or because DataNodes are offline or being decommissioned. A failure of this health test may indicate the loss of several DataNodes at once. If there are files stored in the cluster with a replication factor value of 1, you may see missing blocks with the loss or malfunction of a single DataNode. Use the HDFS fsck command to identify which files contain missing blocks. This test can be configured using the Missing Block Monitoring Thresholds HDFS service-wide monitoring setting.

Short Name: Missing Blocks

Missing Block Monitoring Thresholds

Description

The health check thresholds of the number of missing blocks. Specified as a percentage of the total number of blocks.

Template Name

`hdfs_missing_blocks_thresholds`

Default Value

critical:any, warning:never

Unit(s)

PERCENT

HDFS NameNode Health

This is an HDFS service-level health test that checks for and active, healthy NameNode. The test returns "Bad" health if the service is running and an active NameNode cannot be found. If an active NameNode is found, then the test checks the health of that NameNode as well as the health of any standby NameNode configured. A "Good" health result will only be returned if both the active and Standby NameNodes are healthy. A failure of this health test may indicate stopped or unhealthy NameNode roles, or it may indicate a problem with communication between the Cloudera Manager Service Monitor and the NameNodes. Check the status of the HDFS service's NameNode roles and look in the Cloudera Manager Service Monitor's log files for more information when this test fails. This test can be enabled or disabled using the Active NameNode Role Health Check HDFS service-wide monitoring setting. The check for a healthy standby NameNode can be enabled or disabled with Standby NameNode Health Check. In addition, the Active NameNode Detection Window can be used to adjust the amount of time that the Cloudera Manager Service Monitor has to detect the active NameNode before this health test fails, and the NameNode Activation Startup Tolerance can be used to adjust the amount of time around NameNode startup that the test allows for a NameNode to be made active.

Short Name: NameNode Health

Active NameNode Detection Window

Description

The tolerance window that will be used in HDFS service tests that depend on detection of the active NameNode.

Template Name

`hdfs_active_namenode_detection_window`

Default Value

3

Unit(s)

MINUTES

Active NameNode Role Health Check

Description

When computing the overall HDFS cluster health, consider the active NameNode's health

Template Name

`hdfs_namenode_health_enabled`

Default Value

true

Unit(s)

no unit

NameNode Activation Startup Tolerance

Description

The amount of time after NameNode(s) start that the lack of an active NameNode will be tolerated. This is intended to allow either the auto-failover daemon to make a NameNode active, or a specifically issued failover command to take effect. This is an advanced option that does not often need to be changed.

Template Name

`hdfs_namenode_activation_startup_tolerance`

Default Value

180

Unit(s)

SECONDS

Standby NameNode Health Check

Description

When computing the overall HDFS cluster health, consider the health of the standby NameNode.

Template Name

`hdfs_standby_namenodes_health_enabled`

Default Value

true

Unit(s)

no unit

HDFS Under-Replicated Blocks

This is an HDFS service-level health test that checks that the number of under-replicated blocks does not rise above some percentage of the cluster's total blocks. A failure of this health test may indicate a loss of DataNodes. Use the HDFS fsck command to identify which files contain under-replicated blocks. This test can be configured using the Under-replicated Block Monitoring Thresholds HDFS service-wide monitoring setting.

Short Name: Under-Replicated Blocks

Under-replicated Block Monitoring Thresholds

Description

The health check thresholds of the number of under-replicated blocks. Specified as a percentage of the total number of blocks.

Template Name

`hdfs_under_replicated_blocks_thresholds`

Default Value

critical:40.0, warning:10.0

Unit(s)

PERCENT

History Server Health Tests

History Server Audit Pipeline Test

This History Server health test checks that the Auditing for the History Server role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of History Server process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the History Server host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check History Server monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

History Server File Descriptors

This History Server health test checks that the number of file descriptors used does not rise above some percentage of the History Server file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds History Server monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`spark_yarn_history_server_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

History Server Host Health

This History Server health test factors in the health of the host upon which the History Server is running. A failure of this test means that the host running the History Server is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the History Server Host Health Test History Server monitoring setting.

Short Name: Host Health

History Server Host Health Test

Description

When computing the overall History Server health, consider the host's health.

Template Name

`spark_yarn_history_server_host_health_enabled`

Default Value

true

Unit(s)

no unit

History Server Log Directory Free Space

This History Server health test checks that the filesystem containing the log directory of this History Server has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds History Server monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

History Server Process Status

This History Server health test checks that the Cloudera Manager Agent on the History Server host is heart beating correctly and that the process associated with the History Server role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the History Server process, a lack of connectivity to the Cloudera Manager Agent on the History Server host, or a problem with the Cloudera Manager Agent. This test can fail either because the History Server has crashed or because the History Server will not start or stop in a timely fashion. Check the History Server logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the History Server host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the History Server host, or look in the Cloudera Manager Agent logs on the History Server host for more details. This test can be enabled or disabled using the History Server Process Health Test History Server monitoring setting.

Short Name: Process Status

History Server Process Health Test

Description

Enables the health test that the History Server's process state is consistent with the role configuration

Template Name

`spark_yarn_history_server_scm_health_enabled`

Default Value

true

Unit(s)

no unit

History Server Swap Memory Usage

This History Server health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

History Server Unexpected Exits

This History Server health test checks that the History Server has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period History Server monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Hive Health Tests

Hive Metastore Server Health

This is a Hive service-level health test that checks that enough of the Hive Metastore Servers in the cluster are healthy. The test returns "Concerning" health if the number of healthy Hive Metastore Servers falls below a warning threshold, expressed as a percentage of the total number of Hive Metastore Servers. The test returns "Bad" health if the number of healthy and "Concerning" Hive Metastore Servers falls below a critical threshold, expressed as a percentage of the total number of Hive Metastore Servers. For example, if this test is configured with a warning threshold of 95% and a critical threshold of 90% for a cluster of 100 Hive Metastore Servers, this test would return "Good" health if 95 or more Hive Metastore Servers have good health. This test would return "Concerning" health if at least 90 Hive Metastore Servers have either "Good" or "Concerning" health. If more than 10 Hive Metastore Servers have bad health, this test would return "Bad" health. A failure of this health test indicates unhealthy Hive Metastore Servers. Check the status of the individual Hive Metastore Servers for more information. This test can be configured using the Hive Hive service-wide monitoring setting.

Short Name: Hive Metastore Server Health

Healthy Hive Metastore Server Monitoring Thresholds

Description

The health test thresholds of the overall Hive Metastore Server health. The check returns "Concerning" health if the percentage of "Healthy" Hive Metastore Servers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Hive Metastore Servers falls below the critical threshold.

Template Name

`hive_hivemetastores_healthy_thresholds`

Default Value

critical:51.0, warning:99.0

Unit(s)

PERCENT

Hive WebHCat Server Health

This is a Hive service-level health test that checks that enough of the WebHCat Servers in the cluster are healthy. The test returns "Concerning" health if the number of healthy WebHCat Servers falls below a warning threshold, expressed as a percentage of the total number of WebHCat Servers. The test returns "Bad" health if the number of healthy and "Concerning" WebHCat Servers falls below a critical threshold, expressed as a percentage of the total

number of WebHCat Servers. For example, if this test is configured with a warning threshold of 95% and a critical threshold of 90% for a cluster of 100 WebHCat Servers, this test would return "Good" health if 95 or more WebHCat Servers have good health. This test would return "Concerning" health if at least 90 WebHCat Servers have either "Good" or "Concerning" health. If more than 10 WebHCat Servers have bad health, this test would return "Bad" health. A failure of this health test indicates unhealthy WebHCat Servers. Check the status of the individual WebHCat Servers for more information. This test can be configured using the Hive Hive service-wide monitoring setting.

Short Name: WebHCat Server Health

Healthy WebHCat Server Monitoring Thresholds

Description

The health test thresholds of the overall WebHCat Server health. The check returns "Concerning" health if the percentage of "Healthy" WebHCat Servers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" WebHCat Servers falls below the critical threshold.

Template Name

`hive_webhcats_healthy_thresholds`

Default Value

critical:51.0, warning:99.0

Unit(s)

PERCENT

HiveServer2 Health

This is a Hive service-level health test that checks that enough of the HiveServer2s in the cluster are healthy. The test returns "Concerning" health if the number of healthy HiveServer2s falls below a warning threshold, expressed as a percentage of the total number of HiveServer2s. The test returns "Bad" health if the number of healthy and "Concerning" HiveServer2s falls below a critical threshold, expressed as a percentage of the total number of HiveServer2s. For example, if this test is configured with a warning threshold of 95% and a critical threshold of 90% for a cluster of 100 HiveServer2s, this test would return "Good" health if 95 or more HiveServer2s have good health. This test would return "Concerning" health if at least 90 HiveServer2s have either "Good" or "Concerning" health. If more than 10 HiveServer2s have bad health, this test would return "Bad" health. A failure of this health test indicates unhealthy HiveServer2s. Check the status of the individual HiveServer2s for more information. This test can be configured using the Hive Hive service-wide monitoring setting.

Short Name: HiveServer2 Health

Healthy HiveServer2 Monitoring Thresholds

Description

The health test thresholds of the overall HiveServer2 health. The check returns "Concerning" health if the percentage of "Healthy" HiveServer2s falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" HiveServer2s falls below the critical threshold.

Template Name

`hive_hiveserver2s_healthy_thresholds`

Default Value

critical:51.0, warning:99.0

Unit(s)

PERCENT

Hive Execution Health Tests

Hive Execution HiveServer2 Health

This is a Hive Execution service-level health test that checks that enough of the HiveServer2s in the cluster are healthy. The test returns "Concerning" health if the number of healthy HiveServer2s falls below a warning threshold, expressed as a percentage of the total number of HiveServer2s. The test returns "Bad" health if the number of healthy and "Concerning" HiveServer2s falls below a critical threshold, expressed as a percentage of the total number of HiveServer2s. For example, if this test is configured with a warning threshold of 95% and a critical threshold of 90% for a cluster of 100 HiveServer2s, this test would return "Good" health if 95 or more HiveServer2s have good health. This test would return "Concerning" health if at least 90 HiveServer2s have either "Good" or "Concerning" health. If more than 10 HiveServer2s have bad health, this test would return "Bad" health. A failure of this health test indicates unhealthy HiveServer2s. Check the status of the individual HiveServer2s for more information. This test can be configured using the Hive Execution Hive Execution service-wide monitoring setting.

Short Name: HiveServer2 Health

Healthy HiveServer2 Monitoring Thresholds

Description

The health test thresholds of the overall HiveServer2 health. The check returns "Concerning" health if the percentage of "Healthy" HiveServer2s falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" HiveServer2s falls below the critical threshold.

Template Name

`hive_exec_hiveserver2s_healthy_thresholds`

Default Value

critical:51.0, warning:99.0

Unit(s)

PERCENT

Hive LLAP Health Tests

Hive LLAP HiveServer2 Health

This is a Hive LLAP service-level health test that checks that enough of the HiveServer2s in the cluster are healthy. The test returns "Concerning" health if the number of healthy HiveServer2s falls below a warning threshold, expressed as a percentage of the total number of HiveServer2s. The test returns "Bad" health if the number of healthy and "Concerning" HiveServer2s falls below a critical threshold, expressed as a percentage of the total number of HiveServer2s. For example, if this test is configured with a warning threshold of 95% and a critical threshold of 90% for a cluster of 100 HiveServer2s, this test would return "Good" health if 95 or more HiveServer2s have good health. This test would return "Concerning" health if at least 90 HiveServer2s have either "Good" or "Concerning" health. If more than 10 HiveServer2s have bad health, this test would return "Bad" health. A failure of this health test indicates unhealthy HiveServer2s. Check the status of the individual HiveServer2s for more information. This test can be configured using the Hive LLAP Hive LLAP service-wide monitoring setting.

Short Name: HiveServer2 Health

Healthy HiveServer2 Monitoring Thresholds

Description

The health test thresholds of the overall HiveServer2 health. The check returns "Concerning" health if the percentage of "Healthy" HiveServer2s falls below the warning threshold. The check

is unhealthy if the total percentage of "Healthy" and "Concerning" HiveServer2s falls below the critical threshold.

Template Name

`hive_llap_hiveserver2s_healthy_thresholds`

Default Value

critical:51.0, warning:99.0

Unit(s)

PERCENT

Hive LLAP LLAP Proxy Health

This Hive LLAP service-level health test checks for the presence of a running, healthy LLAP Proxy. The test returns "Bad" health if the service is running and the LLAP Proxy is not running. In all other cases it returns the health of the LLAP Proxy. A failure of this health test indicates a stopped or unhealthy LLAP Proxy. Check the status of the LLAP Proxy for more information. This test can be enabled or disabled using the LLAP Proxy Role Health Test LLAP Proxy service-wide monitoring setting.

Short Name: LLAP Proxy Health

LLAP Proxy Role Health Test

Description

When computing the overall HIVE_LLAP health, consider LLAP Proxy's health

Template Name

`hive_llap_llapproxy_health_enabled`

Default Value

true

Unit(s)

no unit

Hive Metastore Server Health Tests

Hive Metastore Server Audit Pipeline Test

This Hive Metastore Server health test checks that the Auditing for the Hive Metastore Server role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Hive Metastore Server process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Hive Metastore Server host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Hive Metastore Server monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Hive Metastore Server File Descriptors

This Hive Metastore Server health test checks that the number of file descriptors used does not rise above some percentage of the Hive Metastore Server file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Hive Metastore Server monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`hivemetastore_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Hive Metastore Server Heap Dump Directory Free Space

This Hive Metastore Server health test checks that the filesystem containing the heap dump directory of this Hive Metastore Server has sufficient free space. This test can be configured using the Heap Dump Directory Free Space Monitoring Absolute Thresholds and Heap Dump Directory Free Space Monitoring Percentage Thresholds Hive Metastore Server monitoring settings.

Short Name: Heap Dump Directory Free Space

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Template Name

`heap_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`heap_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Hive Metastore Server Hive Metastore Canary

This is a Hive Metastore health test that checks that a client can connect and perform basic operations. The operations include: (1) creating a database, (2) creating a table within that database with several types of columns and two partition keys, (3) creating a number of partitions, and (4) dropping both the table and the database. The database is created under the /user/hue/.cloudera_manager_hive_metastore_canary/<Hive Metastore role name>/ and is named "cloudera_manager_metastore_canary_test_db". The test returns "Bad" health if any of these operations fail. The test returns "Concerning" health if an unknown failure happens. The canary publishes a metric 'canary_duration' for the time it took for the canary to complete. Here is an example of a trigger, defined for the Hive Metastore role configuration group, that changes the health to "Bad" when the duration of the canary is longer than 5 sec: "IF (SELECT canary_duration WHERE entityName=$ROLENAME AND category = ROLE and last(canary_duration) > 5s) DO health:bad" A failure of this health test may indicate that the Hive Metastore is failing basic operations. Check the logs of the Hive Metastore and the Cloudera Manager Service Monitor for more details. This test can be enabled or disabled using the Hive Metastore Canary Health Test Hive Metastore monitoring setting.

Short Name: Hive Metastore Canary

Hive Metastore Canary Health Test

Description

Enables the health test that checks that basic Hive Metastore operations succeed

Template Name

`metastore_canary_health_enabled`

Default Value

true

Unit(s)

no unit

Hive Metastore Server Host Health

This Hive Metastore Server health test factors in the health of the host upon which the Hive Metastore Server is running. A failure of this test means that the host running the Hive Metastore Server is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Hive Metastore Server Host Health Test Hive Metastore Server monitoring setting.

Short Name: Host Health

Hive Metastore Server Host Health Test

Description

When computing the overall Hive Metastore Server health, consider the host's health.

Template Name

`hivemetastore_host_health_enabled`

Default Value

true

Unit(s)

no unit

Hive Metastore Server Log Directory Free Space

This Hive Metastore Server health test checks that the filesystem containing the log directory of this Hive Metastore Server has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Hive Metastore Server monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Hive Metastore Server Pause Duration

This Hive Metastore Server health test checks that the Hive Metastore Server threads are not experiencing long scheduling pauses. The test uses a pause monitoring thread in the Hive Metastore Server that tracks scheduling delay by noting if it is run on its requested schedule. If the thread is not run on its requested schedule, the delay is noted and considered pause time. The health test checks that no more than some percentage of recent time is spent paused. A failure of this health test may indicate that the Hive Metastore Server is not getting enough CPU resources, or that it is spending too much time doing garbage collection. Inspect the Hive Metastore Server logs for any pause monitor output and check garbage collection metrics exposed by the Hive Metastore Server. This test can be configured using the Pause Duration Thresholds and Pause Duration Monitoring Period Hive Metastore Server monitoring settings.

Short Name: Pause Duration

Pause Duration Monitoring Period

Description

The period to review when computing the moving average of extra time the pause monitor spent paused.

Template Name

`hivemetastore_pause_duration_window`

Default Value

5

Unit(s)

MINUTES

Pause Duration Thresholds

Description

The health test thresholds for the weighted average extra time the pause monitor spent paused. Specified as a percentage of elapsed wall clock time.

Template Name

`hivemetastore_pause_duration_thresholds`

Default Value

critical:60.0, warning:30.0

Unit(s)

no unit

Hive Metastore Server Process Status

This Hive Metastore Server health test checks that the Cloudera Manager Agent on the Hive Metastore Server host is heart beating correctly and that the process associated with the Hive Metastore Server role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Hive Metastore Server process, a lack of connectivity to the Cloudera Manager Agent on the Hive Metastore Server host, or a problem with the Cloudera Manager Agent. This test can fail either because the Hive Metastore Server has crashed or because the Hive Metastore Server will not start or stop in a timely fashion. Check the Hive Metastore Server logs for more details. If

the test fails because of problems communicating with the Cloudera Manager Agent on the Hive Metastore Server host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Hive Metastore Server host, or look in the Cloudera Manager Agent logs on the Hive Metastore Server host for more details. This test can be enabled or disabled using the Hive Metastore Server Process Health Test Hive Metastore Server monitoring setting.

Short Name: Process Status

Hive Metastore Server Process Health Test

Description

Enables the health test that the Hive Metastore Server's process state is consistent with the role configuration

Template Name

`hivemetastore_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Hive Metastore Server Swap Memory Usage

This Hive Metastore Server health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Hive Metastore Server Unexpected Exits

This Hive Metastore Server health test checks that the Hive Metastore Server has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Hive Metastore Server monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Hive on Tez Health Tests

Hive on Tez HiveServer2 Health

This is a Hive on Tez service-level health test that checks that enough of the HiveServer2s in the cluster are healthy. The test returns "Concerning" health if the number of healthy HiveServer2s falls below a warning threshold, expressed as a percentage of the total number of HiveServer2s. The test returns "Bad" health if the number of healthy and "Concerning" HiveServer2s falls below a critical threshold, expressed as a percentage of the total number of HiveServer2s. For example, if this test is configured with a warning threshold of 95% and a critical threshold of 90% for a cluster of 100 HiveServer2s, this test would return "Good" health if 95 or more HiveServer2s have good health. This test would return "Concerning" health if at least 90 HiveServer2s have either "Good" or "Concerning" health. If more than 10 HiveServer2s have bad health, this test would return "Bad" health. A failure of this health test indicates unhealthy HiveServer2s. Check the status of the individual HiveServer2s for more information. This test can be configured using the Hive on Tez Hive on Tez service-wide monitoring setting.

Short Name: HiveServer2 Health

Healthy HiveServer2 Monitoring Thresholds

Description

The health test thresholds of the overall HiveServer2 health. The check returns "Concerning" health if the percentage of "Healthy" HiveServer2s falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" HiveServer2s falls below the critical threshold.

Template Name

`hive_on_tez_hiveserver2s_healthy_thresholds`

Default Value

critical:51.0, warning:99.0

Unit(s)

PERCENT

HiveServer2 Health Tests

HiveServer2 Audit Pipeline Test

This HiveServer2 health test checks that the Auditing for the HiveServer2 role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of HiveServer2 process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the HiveServer2 host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check HiveServer2 monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

HiveServer2 File Descriptors

This HiveServer2 health test checks that the number of file descriptors used does not rise above some percentage of the HiveServer2 file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds HiveServer2 monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`hiveserver2_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

HiveServer2 Heap Dump Directory Free Space

This HiveServer2 health test checks that the filesystem containing the heap dump directory of this HiveServer2 has sufficient free space. This test can be configured using the Heap Dump Directory Free Space Monitoring Absolute Thresholds and Heap Dump Directory Free Space Monitoring Percentage Thresholds HiveServer2 monitoring settings.

Short Name: Heap Dump Directory Free Space

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Template Name

`heap_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`heap_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

HiveServer2 Hive Downloaded Resources Directory Free Space

This is a HiveServer2 health test that checks that the filesystem containing the Hive Downloaded Resources Directory of this HiveServer2 has sufficient free space. See the Hive Downloaded Resources Directory description on the HiveServer2 configuration page for more information on this directory type. This test can be configured using the Hive Downloaded Resources Directory Free Space Monitoring Absolute Thresholds and Hive Downloaded Resources Directory Free Space Monitoring Percentage Thresholds HiveServer2 monitoring settings.

Short Name: Hive Downloaded Resources Directory Free Space

Hive Downloaded Resources Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Hive Downloaded Resources Directory.

Template Name

`hiveserver2_downloaded_resources_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Hive Downloaded Resources Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Hive Downloaded Resources Directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Hive Downloaded Resources Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`hiveserver2_downloaded_resources_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

HiveServer2 Hive Local Scratch Directory Free Space

This is a HiveServer2 health test that checks that the filesystem containing the Hive Local Scratch Directory of this HiveServer2 has sufficient free space. See the Hive Local Scratch Directory description on the HiveServer2 configuration page for more information on this directory type. This test can be configured using the Hive Local Scratch Directory Free Space Monitoring Absolute Thresholds and Hive Local Scratch Directory Free Space Monitoring Percentage Thresholds HiveServer2 monitoring settings.

Short Name: Hive Local Scratch Directory Free Space

Hive Local Scratch Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Hive Local Scratch Directory.

Template Name

`hiveserver2_exec_local_scratch_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Hive Local Scratch Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Hive Local Scratch Directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Hive Local Scratch Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`hiveserver2_exec_local_scratch_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

HiveServer2 Host Health

This HiveServer2 health test factors in the health of the host upon which the HiveServer2 is running. A failure of this test means that the host running the HiveServer2 is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the HiveServer2 Host Health Test HiveServer2 monitoring setting.

Short Name: Host Health

HiveServer2 Host Health Test

Description

When computing the overall HiveServer2 health, consider the host's health.

Template Name

`hiveserver2_host_health_enabled`

Default Value

true

Unit(s)

no unit

HiveServer2 Log Directory Free Space

This HiveServer2 health test checks that the filesystem containing the log directory of this HiveServer2 has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds HiveServer2 monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

HiveServer2 Pause Duration

This HiveServer2 health test checks that the HiveServer2 threads are not experiencing long scheduling pauses. The test uses a pause monitoring thread in the HiveServer2 that tracks scheduling delay by noting if it is run on its requested schedule. If the thread is not run on its requested schedule, the delay is noted and considered pause time. The health test checks that no more than some percentage of recent time is spent paused. A failure of this health test may indicate that the HiveServer2 is not getting enough CPU resources, or that it is spending too much time doing garbage collection. Inspect the HiveServer2 logs for any pause monitor output and check garbage collection metrics exposed by the HiveServer2. This test can be configured using the Pause Duration Thresholds and Pause Duration Monitoring Period HiveServer2 monitoring settings.

Short Name: Pause Duration

Pause Duration Monitoring Period

Description

The period to review when computing the moving average of extra time the pause monitor spent paused.

Template Name

`hiveserver2_pause_duration_window`

Default Value

5

Unit(s)

MINUTES

Pause Duration Thresholds

Description

The health test thresholds for the weighted average extra time the pause monitor spent paused. Specified as a percentage of elapsed wall clock time.

Template Name

`hiveserver2_pause_duration_thresholds`

Default Value

critical:60.0, warning:30.0

Unit(s)

no unit

HiveServer2 Process Status

This HiveServer2 health test checks that the Cloudera Manager Agent on the HiveServer2 host is heart beating correctly and that the process associated with the HiveServer2 role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the HiveServer2 process, a lack of connectivity to the Cloudera Manager Agent on the HiveServer2 host, or a problem with the Cloudera Manager Agent. This test can fail either because the HiveServer2 has crashed or because the HiveServer2 will not start or stop in a timely fashion. Check the HiveServer2 logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the HiveServer2 host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the HiveServer2 host, or look in the Cloudera Manager Agent logs on the HiveServer2 host for more details. This test can be enabled or disabled using the HiveServer2 Process Health Test HiveServer2 monitoring setting.

Short Name: Process Status

HiveServer2 Process Health Test

Description

Enables the health test that the HiveServer2's process state is consistent with the role configuration

Template Name

`hiveserver2_scm_health_enabled`

Default Value

true

Unit(s)

no unit

HiveServer2 Swap Memory Usage

This HiveServer2 health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

HiveServer2 Unexpected Exits

This HiveServer2 health test checks that the HiveServer2 has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits

were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period HiveServer2 monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Host Health Tests

Host Agent Log Directory

This is a host health test that checks that the filesystem containing the Cloudera Manager Agent's log directory has sufficient free space. This test can be configured using the Cloudera Manager Agent Log Directory Free Space Monitoring Absolute Thresholds and Cloudera Manager Agent Log Directory Free Space Monitoring Percentage Thresholds host monitoring settings.

Short Name: Agent Log Directory

Cloudera Manager Agent Log Directory Free Space Monitoring Absolute Thresholds

Description

The health check thresholds for monitoring of free space on the filesystem that contains the Cloudera Manager Agent's log directory.

Template Name

`host_agent_log_directory_free_space_absolute_thresholds`

Default Value

critical:1.073741824E9, warning:2.147483648E9

Unit(s)

BYTES

Cloudera Manager Agent Log Directory Free Space Monitoring Percentage Thresholds

Description

The health check thresholds for monitoring of free space on the filesystem that contains the Cloudera Manager Agent's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Cloudera Manager Agent Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`host_agent_log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Host Agent Parcel Directory

This is a host health test that checks whether the filesystem containing the Cloudera Manager Agent's parcel directory has sufficient free space. This test can be configured using the Cloudera Manager Agent Parcel Directory Free Space Monitoring Absolute Thresholds and Cloudera Manager Agent Parcel Directory Free Space Monitoring Percentage Thresholds host monitoring settings.

Short Name: Agent Parcel Directory

Cloudera Manager Agent Parcel Directory Free Space Monitoring Absolute Thresholds

Description

The health check thresholds for monitoring of free space on the filesystem that contains the Cloudera Manager Agent's parcel directory.

Template Name

`host_agent_parcel_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Cloudera Manager Agent Parcel Directory Free Space Monitoring Percentage Thresholds

Description

The health check thresholds for monitoring of free space on the filesystem that contains the Cloudera Manager Agent's parcel directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Cloudera Manager Agent Parcel Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`host_agent_parcel_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Host Agent Process Directory

This is a host health test that checks that the filesystem containing the Cloudera Manager Agent's process directory has sufficient free space. The process directory contains the configuration files for the processes which the Cloudera

Manager Agent starts. This test can be configured using the Cloudera Manager Agent Process Directory Free Space Monitoring Absolute Thresholds and Cloudera Manager Agent Process Directory Free Space Monitoring Percentage Thresholds host monitoring settings.

Short Name: Agent Process Directory

Cloudera Manager Agent Process Directory Free Space Monitoring Absolute Thresholds

Description

The health check thresholds for monitoring of free space on the filesystem that contains the Cloudera Manager Agent's process directory.

Template Name

`host_agent_process_directory_free_space_absolute_thresholds`

Default Value

critical:1.048576E8, warning:2.097152E8

Unit(s)

BYTES

Cloudera Manager Agent Process Directory Free Space Monitoring Percentage Thresholds

Description

The health check thresholds for monitoring of free space on the filesystem that contains the Cloudera Manager Agent's process directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Cloudera Manager Agent Process Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`host_agent_process_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Host Agent Status

This is a host health test that checks that the host's Cloudera Manager Agent is heartbeating correctly to the Cloudera Manager Server, is in contact with the Host Monitor, and has the correct software version. A failure of this health test may indicate a lack of connectivity between the host's Cloudera Manager Agent and the Cloudera Manager Server, a lack of connectivity betwen the host's Cloudera Manager Agent and the Host Monitor, or that the Cloudera Manager Agent or Host Monitor software is out of date. Check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the host, or look in the host's Cloudera Manager Agent logs for more details. If this test reports a software version mismatch between the Cloudera Manager Agent and the Host Monitor, check the version of each component by consulting the appropriate logs or the appropriate status web pages. This test can be enabled or disabled using the Host Process Health Test host configuration setting.

Short Name: Agent Status

Host Process Health Test

Description

Enables the health test that the host's process state is consistent with the role configuration

Template Name

`host_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Host Certificate Expiration

This health test checks the expiry time of the TLS certificate for the Cloudera Manager Agent on the given host. This test can be configured using the Cloudera Manager Agent TLS Certificate Expiry Thresholds host monitoring setting. This test alerts when the certificate is close to expiry.

Short Name: Certificate Expiration

Cloudera Manager Agent TLS Certificate Expiry Thresholds

Description

The health test thresholds for monitoring the certificate of Cloudera Manager Agent.

Template Name

`host_agent_certificate_expiry_thresholds`

Default Value

critical:7.0, warning:60.0

Unit(s)

DAYS

Host Clock Offset

This is a host health test that checks whether the host's system clock appears to be out-of-sync with its NTP server(s). The test uses either the 'ntpq -np' (if ntpd is running) or 'chronyc sources' (if chronyd is running) command to check that whether the host is synchronized to an NTP peer and that the absolute value of the host's clock offset from that peer is not too large. The test returns "Bad" health If the command fails to find a synchronized NTP peer or an offset between the peer and the host time is too large. To troubleshoot, run 'ntpq -np' or 'chronyc sources' on the host. The output should contain a row for each of the host's NTP servers. The row starting with a '*' (if ntpdc) or '^*' (if chronyc) contains the peer to which the host is currently synchronized. If no row starts with a '*' or '^*', this indicates that the host is not currently synchronized. Make sure you have a pool of valid ntp servers in your ntp.conf (if ntpdc) or chrony.conf (if chronyc). Make sure that UDP port 123 is open on any firewall that is in use. Check the system log for ntpd or chronyd messages related to configuration errors. If the issue persists or the offset between the peer and the host time is too large, please seek assistance from your system administrator. If NTP is not in use on the host, disable this check by setting both 'Warning' and 'Critical' thresholds to 'NEVER' using the configuration options shown below for the host. Cloudera recommends using NTP for time synchronization of Hadoop clusters. This test can be configured using the Host Clock Offset Thresholds host configuration setting.

Short Name: Clock Offset

Host Clock Offset Thresholds

Description

The thresholds for the host clock offset health test. The test compares this threshold against the absolute value of the clock offset reported by the host's NTP service from the 'ntpdc -np' or 'chronyc sources' command. Setting both the warning and critical threshold values to never turns off collection of the clock offset by the Cloudera Manager Agent. If no time synchronization is in use, both threshold values should be set to never. Cloudera recommends using NTP for time synchronization of Hadoop clusters.

Template Name

`host_clock_offset_thresholds`

Default Value

critical:10000.0, warning:3000.0

Unit(s)

MILLISECONDS

Host DNS Resolution

This is a host health test that checks that the host's hostname and canonical name are consistent when checked from a Java process, and that the DNS resolution completes in a timely manner. The DNS resolution duration is calculated by measuring the time taken to call getLocalHost in a Java process on this host. Note that DNS information may be cached on the host, and this caching can affect the reported resolution duration. A failure of this health test may indicate that the host's DNS configuration is not correct or the host's DNS server is responding slowly. Check the Cloudera Manager Agent log for the names that were detected by this test or for errors running the Java process. The hostname and canonical name are considered to be consistent if the hostname or the hostname plus a domain name is the same as the canonical name. This health test uses domain names from the domain and search lines in /etc/resolv.conf. This health test does not consult /etc/nsswitch.conf and may give incorrect results if /etc/resolv.conf is not used by the host. There may be a delay of up to 5 minutes before this health test picks up changes to /etc/resolv.conf. This test can be configured using the Hostname and Canonical Name Health Check host configuration setting.

Short Name: DNS Resolution

Hostname and Canonical Name Health Check

Description

Whether the hostname and canonical names for this host are consistent when checked from a Java process.

Template Name

`host_dns_resolution_enabled`

Default Value

true

Unit(s)

no unit

Host Entropy

This is a health test that checks that the host in a cluster has sufficient entropy. A failure of this health may indicate that entropy pool is depleted, which might cause applications waiting for the randomness to pause until more entropy is available. Random connection timeout issues usually happen when the available entropy count reaches zero. Increase the entropy using rng-tools for the host. This test can be configured using the Host Entropy Thresholds host configuration settings.

Short Name: Entropy

Host Entropy Thresholds

Description

The health check thresholds for the available entropy on the host.

Template Name

`host_available_entropy_thresholds`

Default Value

critical:50.0, warning:100.0

Unit(s)

no unit

Host Frame Errors

This is a host health test that checks for network frame errors across all network interfaces. A failure of this health test may indicate a problem with network hardware (e.g. switches) and can potentially cause other service or role-level performance problems. Check the host and network hardware logs for more details. This test can be configured using the Host Network Frame Error Percentage Thresholds, Host Network Frame Error Check Window, Host Network Frame Error Test Minimum Required Packets host configuration settings.

Short Name: Frame Errors

Host Network Frame Error Check Window

Description

The amount of time over which the host frame error checks for frame errors.

Template Name

`host_network_frame_errors_window`

Default Value

15

Unit(s)

MINUTES

Host Network Frame Error Percentage Thresholds

Description

The health check thresholds for the percentage of received packets that are frame errors.

Template Name

`host_network_frame_errors_thresholds`

Default Value

critical:0.5, warning:any

Unit(s)

PERCENT

Host Network Frame Error Test Minimum Required Packets

Description

The minimum number of received packets that must be received within the test window for this test to return "Bad" health. If less that this number of packets is received during the test window, the health check will never return "Bad" health.

Template Name

`host_network_frame_errors_floor`

Default Value

0

Unit(s)

no unit

Host Network Interface Speed

This is a host health test that checks for network interfaces that appear to be operating at less than full speed. The Cloudera Manager Agent uses ethtool ioctl to determine the network interface speed and duplex mode. A failure of this health test may indicate that network interface(s) may be configured incorrectly and may be causing performance problems. Use the ethtool command to check and configure the host's network interfaces to use the fastest available link speed and duplex mode. For inactive interfaces or for interfaces that do not support ethtool ioctl, the Cloudera

Manager Agent cannot collect speed metrics. If the Cloudera Manager Agent fails to collect speed metrics for all network interfaces on the host, the test is disabled. This test can be configured using the Host's Network Interfaces Slow Link Modes Thresholds, Network Interface Expected Link Speed and Network Interface Expected Duplex Mode host configuration settings.

Short Name: Network Interface Speed

Host's Network Interfaces Slow Link Modes Thresholds

Description

The thresholds for the health check of the number of network interfaces that appear to be operating at less than full speed.

Template Name

`host_network_interfaces_slow_mode_thresholds`

Default Value

critical:never, warning:any

Unit(s)

no unit

Network Interface Expected Duplex Mode

Description

The expected duplex mode for network interfaces.

Template Name

`host_nic_expected_duplex_mode`

Default Value

Full

Unit(s)

no unit

Network Interface Expected Link Speed

Description

The expected network interface link speed.

Template Name

`host_nic_expected_speed`

Default Value

1000

Unit(s)

no unit

Host Swapping

This is a health test that checks that the host has not swapped out more than a certain number of pages over the last fifteen minutes. A failure of this health test may indicate misconfiguration of the host operating system, or too many processes running on the host. Try reducing vm.swappiness, or add more memory to the host. This test can be configured using the Host Memory Swapping Thresholds, Host Memory Swapping Check Window host configuration settings.

Short Name: Swapping

Host Memory Swapping Check Window

Description

The amount of time over which the memory swapping test checks for pages swapped.

Template Name

`host_memswap_window`

Default Value

15

Unit(s)

MINUTES

Host Memory Swapping Thresholds

Description

The health test thresholds of the number of pages swapped out on the host in the last 15 minutes

Template Name

`host_memswap_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

PAGES

Host Monitor Health Tests

Host Monitor Audit Pipeline Test

This Host Monitor health test checks that the Auditing for the Host Monitor role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Host Monitor process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Host Monitor host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Host Monitor monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Host Monitor Cloudera Manager Descriptor Age

This is a Host Monitor health test that checks if the Cloudera Manager descriptor has been refreshed recently. The Cloudera Manager descriptor is used to pass configuration information from the Cloudera Manager Server to the Host Monitor. If the descriptor becomes stale, Host Monitor operation may be impacted because the Host Monitor will receive information about new hosts, roles, and services, or changes to existing hosts, roles, and services. A stale descriptor usually indicates problems communicating with the Cloudera Manager Server but can also indicate performance problems or a bug. Consult the Host Monitor log and the Cloudera Manager Server log for more information. This test can be configured using the Cloudera Manager Descriptor Age Thresholds Cloudera Manager Host Monitor setting.

Short Name: Cloudera Manager Descriptor Age

Cloudera Manager Descriptor Age Thresholds

Description

The health test thresholds for monitoring the time since the Cloudera Manager descriptor was last refreshed.

Template Name

`scm_descriptor_age_thresholds`

Default Value

critical:120000.0, warning:60000.0

Unit(s)

no unit

Host Monitor Cloudera Manager Metric Schema Age

This is a Host Monitor health test that checks if the Cloudera Manager metric schema has been refreshed recently. If the metric schema becomes stale, Host Monitor operation may be impacted because the Host Monitor will not receive information about new metrics and changes to existing metrics. A stale metric schema usually indicates problems communicating with the Cloudera Manager Server but can also indicate performance problems or a bug. Consult the Host Monitor log and the Cloudera Manager Server log for more information. This test can be configured using the Cloudera Manager Metric Schema Age Thresholds Cloudera Manager Host Monitor setting.

Short Name: Cloudera Manager Metric Schema Age

Cloudera Manager Metric Schema Age Thresholds

Description

The health test thresholds for monitoring the time since the Cloudera Manager metric schema was last refreshed.

Template Name

`metric_schema_age_thresholds_name`

Default Value

critical:120000.0, warning:60000.0

Unit(s)

no unit

Host Monitor File Descriptors

This Host Monitor health test checks that the number of file descriptors used does not rise above some percentage of the Host Monitor file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Host Monitor monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`hostmonitor_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Host Monitor Heap Dump Directory Free Space

This Host Monitor health test checks that the filesystem containing the heap dump directory of this Host Monitor has sufficient free space. This test can be configured using the Heap Dump Directory Free Space Monitoring Absolute Thresholds and Heap Dump Directory Free Space Monitoring Percentage Thresholds Host Monitor monitoring settings.

Short Name: Heap Dump Directory Free Space

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Template Name

`heap_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`heap_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Host Monitor Host Health

This Host Monitor health test factors in the health of the host upon which the Host Monitor is running. A failure of this test means that the host running the Host Monitor is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Host Monitor Host Health Test Host Monitor monitoring setting.

Short Name: Host Health

Host Monitor Host Health Test

Description

When computing the overall Host Monitor health, consider the host's health.

Template Name

`hostmonitor_host_health_enabled`

Default Value

true

Unit(s)

no unit

Host Monitor Host Monitor Storage Directory Free Space

This is a Host Monitor health test that checks that the filesystem containing the Host Monitor Storage Directory of this Host Monitor has sufficient free space. See the Host Monitor Storage Directory description on the Host Monitor configuration page for more information on this directory type. This test can be configured using the Host Monitor Storage Directory Free Space Monitoring Absolute Thresholds and Host Monitor Storage Directory Free Space Monitoring Percentage Thresholds Host Monitor monitoring settings.

Short Name: Host Monitor Storage Directory Free Space

Host Monitor Storage Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Host Monitor Storage Directory.

Template Name

`firehose_storage_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Host Monitor Storage Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Host Monitor Storage Directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Host Monitor Storage Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`firehose_storage_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Host Monitor Host Pipeline

This Host Monitor health test checks that no messages are being dropped by the host stage of the Host Monitor pipeline. A failure of this health test indicates a problem with the Host Monitor. This may indicate a configuration problem or a bug in the Host Monitor. This test can be configured using the Host Monitor Host Pipeline Monitoring Time Period monitoring setting.

Short Name: Host Pipeline

Host Monitor Host Pipeline Monitoring Thresholds

Description

The health test thresholds for monitoring the Host Monitor host pipeline. This specifies the number of dropped messages that will be tolerated over the monitoring time period.

Template Name

`hostmonitor_host_pipeline_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Host Monitor Host Pipeline Monitoring Time Period

Description

The time period over which the Host Monitor host pipeline will be monitored for dropped messages.

Template Name

`hostmonitor_host_pipeline_window`

Default Value

5

Unit(s)

MINUTES

Host Monitor Log Directory Free Space

This Host Monitor health test checks that the filesystem containing the log directory of this Host Monitor has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Host Monitor monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Host Monitor Metrics Aggregation Run Duration Test

This is a Host Monitor health test that checks whether Cloudera Manager's aggregation run durations are within the thresholds. If the test fails, Host Monitor operation may be impacted because the Host Monitor is not able to process the metrics fast enough. This test can be configured using the Metrics Aggregation Run Duration Thresholds Cloudera Manager Host Monitor setting.

Short Name: Metrics Aggregation Run Duration Test

Metrics Aggregation Run Duration Thresholds

Description

The health test thresholds for monitoring the metrics aggregation run duration.

Template Name

`aggregation_run_duration_thresholds`

Default Value

critical:30000.0, warning:10000.0

Unit(s)

MILLISECONDS

Host Monitor Pause Duration

This Host Monitor health test checks that the Host Monitor threads are not experiencing long scheduling pauses. The test uses a pause monitoring thread in the Host Monitor that tracks scheduling delay by noting if it is run on its requested schedule. If the thread is not run on its requested schedule, the delay is noted and considered pause time. The health test checks that no more than some percentage of recent time is spent paused. A failure of this health test may indicate that the Host Monitor is not getting enough CPU resources, or that it is spending too much time doing garbage collection. Inspect the Host Monitor logs for any pause monitor output and check garbage collection metrics exposed by the Host Monitor. This test can be configured using the Pause Duration Thresholds and Pause Duration Monitoring Period Host Monitor monitoring settings.

Short Name: Pause Duration

Pause Duration Monitoring Period

Description

The period to review when computing the moving average of extra time the pause monitor spent paused.

Template Name

`hostmonitor_pause_duration_window`

Default Value

5

Unit(s)

MINUTES

Pause Duration Thresholds

Description

The health test thresholds for the weighted average extra time the pause monitor spent paused. Specified as a percentage of elapsed wall clock time.

Template Name

`hostmonitor_pause_duration_thresholds`

Default Value

critical:60.0, warning:30.0

Unit(s)

no unit

Host Monitor Process Status

This Host Monitor health test checks that the Cloudera Manager Agent on the Host Monitor host is heart beating correctly and that the process associated with the Host Monitor role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Host Monitor process, a lack of connectivity to the Cloudera Manager Agent on the Host Monitor host, or a problem with the Cloudera Manager Agent. This test can fail either because the Host Monitor has crashed or because the Host Monitor will not start or stop in a timely fashion. Check the Host Monitor logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Host Monitor host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Host Monitor host, or look in the Cloudera Manager Agent logs on the Host Monitor host for more details. This test can be enabled or disabled using the Host Monitor Process Health Test Host Monitor monitoring setting.

Short Name: Process Status

Host Monitor Process Health Test

Description

Enables the health test that the Host Monitor's process state is consistent with the role configuration

Template Name

`hostmonitor_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Host Monitor Swap Memory Usage

This Host Monitor health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Host Monitor Unexpected Exits

This Host Monitor health test checks that the Host Monitor has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Host Monitor monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Host Monitor Web Server Status

This health test checks that the role's web server is responding quickly to requests by the Cloudera Manager Agent, and that the Cloudera Manager Agent can collect metrics from the web server. Failure of this health test may indicate a problem with the web server of the Host Monitor, a misconfiguration of the Host Monitor, or a problem with the Cloudera Manager Agent. Consult the Cloudera Manager Agent logs and the logs of the Host Monitor for more detail. If the test failure message indicates a communication problem, the Cloudera Manager Agent's HTTP requests to the Host Monitor's web server are failing or timing out. If the test's failure message indicates an unexpected response, the Host Monitor's web server responded to the Cloudera Manager Agent's request, but the response could not be interpreted for some reason. This test can be configured using the Web Metric Collection Host Monitor monitoring setting.

Short Name: Web Server Status

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Template Name

`hostmonitor_web_metric_collection_enabled`

Default Value

true

Unit(s)

no unit

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Template Name

`hostmonitor_web_metric_collection_thresholds`

Default Value

critical:never, warning:10000.0

Unit(s)

MILLISECONDS

HttpFS Health Tests

HttpFS Audit Pipeline Test

This HttpFS health test checks that the Auditing for the HttpFS role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of HttpFS process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the HttpFS host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check HttpFS monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

HttpFS File Descriptors

This HttpFS health test checks that the number of file descriptors used does not rise above some percentage of the HttpFS file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds HttpFS monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`httpfs_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

HttpFS Heap Dump Directory Free Space

This HttpFS health test checks that the filesystem containing the heap dump directory of this HttpFS has sufficient free space. This test can be configured using the Heap Dump Directory Free Space Monitoring Absolute Thresholds and Heap Dump Directory Free Space Monitoring Percentage Thresholds HttpFS monitoring settings.

Short Name: Heap Dump Directory Free Space

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Template Name

`heap_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`heap_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

HttpFS Host Health

This HttpFS health test factors in the health of the host upon which the HttpFS is running. A failure of this test means that the host running the HttpFS is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the HttpFS Host Health Test HttpFS monitoring setting.

Short Name: Host Health

HttpFS Host Health Test

Description

When computing the overall HttpFS health, consider the host's health.

Template Name

`httpfs_host_health_enabled`

Default Value

true

Unit(s)

no unit

HttpFS Log Directory Free Space

This HttpFS health test checks that the filesystem containing the log directory of this HttpFS has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds HttpFS monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

HttpFS Process Status

This HttpFS health test checks that the Cloudera Manager Agent on the HttpFS host is heart beating correctly and that the process associated with the HttpFS role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the HttpFS process, a lack of connectivity to the Cloudera Manager Agent on the HttpFS host, or a problem with the Cloudera Manager Agent. This test can fail either because the HttpFS has crashed or because the HttpFS will not start or stop in a timely fashion. Check the HttpFS logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the HttpFS host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the HttpFS host, or look in the Cloudera Manager Agent logs on the HttpFS host for more details. This test can be enabled or disabled using the HttpFS Process Health Test HttpFS monitoring setting.

Short Name: Process Status

HttpFS Process Health Test

Description

Enables the health test that the HttpFS's process state is consistent with the role configuration

Template Name

`httpfs_scm_health_enabled`

Default Value

true

Unit(s)

no unit

HttpFS Swap Memory Usage

This HttpFS health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

HttpFS Unexpected Exits

This HttpFS health test checks that the HttpFS has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period HttpFS monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Hue Health Tests

Hue Kerberos Ticket Renewer Health

This is a Hue service-level health test that checks that enough of the Kerberos Ticket Renewers in the cluster are healthy. The test returns "Concerning" health if the number of healthy Kerberos Ticket Renewers falls below a warning threshold, expressed as a percentage of the total number of Kerberos Ticket Renewers. The test returns "Bad" health if the number of healthy and "Concerning" Kerberos Ticket Renewers falls below a critical threshold, expressed as a percentage of the total number of Kerberos Ticket Renewers. For example, if this test is configured with a warning threshold of 95% and a critical threshold of 90% for a cluster of 100 Kerberos Ticket Renewers, this test would return "Good" health if 95 or more Kerberos Ticket Renewers have good health. This test would return "Concerning" health if at least 90 Kerberos Ticket Renewers have either "Good" or "Concerning" health. If more than 10 Kerberos Ticket Renewers have bad health, this test would return "Bad" health. A failure of this health test indicates unhealthy Kerberos Ticket Renewers. Check the status of the individual Kerberos Ticket Renewers for more information. This test can be configured using the Hue Hue service-wide monitoring setting.

Short Name: Kerberos Ticket Renewer Health

Healthy Kerberos Ticket Renewer Monitoring Thresholds

Description

The health test thresholds of the overall Kerberos Ticket Renewer health. The check returns "Concerning" health if the percentage of "Healthy" Kerberos Ticket Renewers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Kerberos Ticket Renewers falls below the critical threshold.

Template Name

`hue_kt_renewers_healthy_thresholds`

Default Value

critical:51.0, warning:99.0

Unit(s)

PERCENT

Hue Load Balancer Health

This is a Hue service-level health test that checks that enough of the Load Balancers in the cluster are healthy. The test returns "Concerning" health if the number of healthy Load Balancers falls below a warning threshold, expressed as a percentage of the total number of Load Balancers. The test returns "Bad" health if the number of healthy and "Concerning" Load Balancers falls below a critical threshold, expressed as a percentage of the total number of Load Balancers. For example, if this test is configured with a warning threshold of 95% and a critical threshold of 90% for a cluster of 100 Load Balancers, this test would return "Good" health if 95 or more Load Balancers have good health. This test would return "Concerning" health if at least 90 Load Balancers have either "Good" or "Concerning" health. If more than 10 Load Balancers have bad health, this test would return "Bad" health. A failure of this health test indicates unhealthy Load Balancers. Check the status of the individual Load Balancers for more information. This test can be configured using the Hue Hue service-wide monitoring setting.

Short Name: Load Balancer Health

Healthy Load Balancer Monitoring Thresholds

Description

The health test thresholds of the overall Load Balancer health. The check returns "Concerning" health if the percentage of "Healthy" Load Balancers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Load Balancers falls below the critical threshold.

Template Name

`hue_load_balancer_healthy_thresholds`

Default Value

critical:51.0, warning:99.0

Unit(s)

PERCENT

Hue Server Health

This is a Hue service-level health test that checks that enough of the Hue Servers in the cluster are healthy. The test returns "Concerning" health if the number of healthy Hue Servers falls below a warning threshold, expressed as a percentage of the total number of Hue Servers. The test returns "Bad" health if the number of healthy and "Concerning" Hue Servers falls below a critical threshold, expressed as a percentage of the total number of Hue Servers. For example, if this test is configured with a warning threshold of 95% and a critical threshold of 90% for a cluster of 100 Hue Servers, this test would return "Good" health if 95 or more Hue Servers have good health. This test would return "Concerning" health if at least 90 Hue Servers have either "Good" or "Concerning" health. If more than 10 Hue Servers have bad health, this test would return "Bad" health. A failure of this health test indicates unhealthy Hue Servers. Check the status of the individual Hue Servers for more information. This test can be configured using the Hue Hue service-wide monitoring setting.

Short Name: Hue Server Health

Healthy Hue Server Monitoring Thresholds

Description

The health test thresholds of the overall Hue Server health. The check returns "Concerning" health if the percentage of "Healthy" Hue Servers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Hue Servers falls below the critical threshold.

Template Name

`hue_hue_servers_healthy_thresholds`

Default Value

critical:51.0, warning:99.0

Unit(s)

PERCENT

Hue Server Health Tests

Hue Server Audit Pipeline Test

This Hue Server health test checks that the Auditing for the Hue Server role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Hue Server process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Hue Server host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Hue Server monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Hue Server File Descriptors

This Hue Server health test checks that the number of file descriptors used does not rise above some percentage of the Hue Server file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Hue Server monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`hue_server_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Hue Server Heap Dump Directory Free Space

This Hue Server health test checks that the filesystem containing the heap dump directory of this Hue Server has sufficient free space. This test can be configured using the Heap Dump Directory Free Space Monitoring Absolute Thresholds and Heap Dump Directory Free Space Monitoring Percentage Thresholds Hue Server monitoring settings.

Short Name: Heap Dump Directory Free Space

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Template Name

`heap_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`heap_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Hue Server Host Health

This Hue Server health test factors in the health of the host upon which the Hue Server is running. A failure of this test means that the host running the Hue Server is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Hue Server Host Health Test Hue Server monitoring setting.

Short Name: Host Health

Hue Server Host Health Test

Description

When computing the overall Hue Server health, consider the host's health.

Template Name

`hue_server_host_health_enabled`

Default Value

true

Unit(s)

no unit

Hue Server Log Directory Free Space

This Hue Server health test checks that the filesystem containing the log directory of this Hue Server has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Hue Server monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Hue Server Process Status

This Hue Server health test checks that the Cloudera Manager Agent on the Hue Server host is heart beating correctly and that the process associated with the Hue Server role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Hue Server process, a lack of connectivity to the Cloudera Manager Agent on the Hue Server host, or a problem with the Cloudera Manager Agent. This test can fail either because the Hue Server has crashed or because the Hue Server will not start or stop in a timely fashion. Check the Hue Server logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Hue Server host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Hue Server host, or look in the Cloudera Manager Agent logs on the Hue Server host for more details. This test can be enabled or disabled using the Hue Server Process Health Test Hue Server monitoring setting.

Short Name: Process Status

Hue Server Process Health Test

Description

Enables the health test that the Hue Server's process state is consistent with the role configuration

Template Name

`hue_server_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Hue Server Swap Memory Usage

This Hue Server health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Hue Server Unexpected Exits

This Hue Server health test checks that the Hue Server has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a

critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Hue Server monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Hue Server Web Server Status

This health test checks that the role's web server is responding quickly to requests by the Cloudera Manager Agent, and that the Cloudera Manager Agent can collect metrics from the web server. Failure of this health test may indicate a problem with the web server of the Hue Server, a misconfiguration of the Hue Server, or a problem with the Cloudera Manager Agent. Consult the Cloudera Manager Agent logs and the logs of the Hue Server for more detail. If the test failure message indicates a communication problem, the Cloudera Manager Agent's HTTP requests to the Hue Server's web server are failing or timing out. If the test's failure message indicates an unexpected response, the Hue Server's web server responded to the Cloudera Manager Agent's request, but the response could not be interpreted for some reason. This test can be configured using the Web Metric Collection Hue Server monitoring setting.

Short Name: Web Server Status

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Template Name

`hue_server_web_metric_collection_enabled`

Default Value

true

Unit(s)

no unit

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Template Name

`hue_server_web_metric_collection_thresholds`

Default Value

critical:never, warning:10000.0

Unit(s)

MILLISECONDS

Impala Health Tests

Impala Catalog Server Health

This Impala service-level health test checks for the presence of a running, healthy Impala Catalog Server. The test returns "Bad" health if the service is running and the Impala Catalog Server is not running. In all other cases it returns the health of the Impala Catalog Server. A failure of this health test indicates a stopped or unhealthy Impala Catalog Server. Check the status of the Impala Catalog Server for more information. This test can be enabled or disabled using the Impala Catalog Server Role Health Test Impala Catalog Server service-wide monitoring setting.

Short Name: Impala Catalog Server Health

Impala Catalog Server Role Health Test

Description

When computing the overall IMPALA health, consider Impala Catalog Server's health

Template Name

`impala_catalogserver_health_enabled`

Default Value

true

Unit(s)

no unit

Impala Daemon Health

This is a Impala service-level health test that checks that enough of the Impala Daemons in the cluster are healthy. The test returns "Concerning" health if the number of healthy Impala Daemons falls below a warning threshold, expressed as a percentage of the total number of Impala Daemons. The test returns "Bad" health if the number of healthy and "Concerning" Impala Daemons falls below a critical threshold, expressed as a percentage of the total number of Impala Daemons. For example, if this test is configured with a warning threshold of 95% and a critical threshold of 90% for a cluster of 100 Impala Daemons, this test would return "Good" health if 95 or more Impala Daemons have good health. This test would return "Concerning" health if at least 90 Impala Daemons have either "Good" or "Concerning" health. If more than 10 Impala Daemons have bad health, this test would return "Bad" health. A failure of this health test indicates unhealthy Impala Daemons. Check the status of the individual Impala Daemons for more information. This test can be configured using the Impala Impala service-wide monitoring setting.

Short Name: Impala Daemon Health

Healthy Impala Daemon Monitoring Thresholds

Description

The health test thresholds of the overall Impala Daemon health. The check returns "Concerning" health if the percentage of "Healthy" Impala Daemons falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Impala Daemons falls below the critical threshold.

Template Name

`impala_impalads_healthy_thresholds`

Default Value

critical:90.0, warning:95.0

Unit(s)

PERCENT

Impala Llama ApplicationMaster Health

This is a Impala service-level health test that checks that enough of the Impala Llama ApplicationMasters in the cluster are healthy. The test returns "Concerning" health if the number of healthy Impala Llama ApplicationMasters falls below a warning threshold, expressed as a percentage of the total number of Impala Llama ApplicationMasters. The test returns "Bad" health if the number of healthy and "Concerning" Impala Llama ApplicationMasters falls below a critical threshold, expressed as a percentage of the total number of Impala Llama ApplicationMasters. For example, if this test is configured with a warning threshold of 95% and a critical threshold of 90% for a cluster of 100 Impala Llama ApplicationMasters, this test would return "Good" health if 95 or more Impala Llama ApplicationMasters have good health. This test would return "Concerning" health if at least 90 Impala Llama ApplicationMasters have either "Good" or "Concerning" health. If more than 10 Impala Llama ApplicationMasters have bad health, this test would return "Bad" health. A failure of this health test indicates unhealthy Impala Llama ApplicationMasters. Check the status of the individual Impala Llama ApplicationMasters for more information. This test can be configured using the Impala Impala service-wide monitoring setting.

Short Name: Impala Llama ApplicationMaster Health

Healthy Impala Llama ApplicationMaster Monitoring Thresholds

Description

The health test thresholds of the overall Impala Llama ApplicationMaster health. The check returns "Concerning" health if the percentage of "Healthy" Impala Llama ApplicationMasters falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Impala Llama ApplicationMasters falls below the critical threshold.

Template Name

`impala_llamas_healthy_thresholds`

Default Value

critical:51.0, warning:99.0

Unit(s)

PERCENT

Impala StateStore Health

This Impala service-level health test checks for the presence of a running, healthy Impala StateStore. The test returns "Bad" health if the service is running and the Impala StateStore is not running. In all other cases it returns the health of the Impala StateStore. A failure of this health test indicates a stopped or unhealthy Impala StateStore. Check the status of the Impala StateStore for more information. This test can be enabled or disabled using the Impala StateStore Role Health Test Impala StateStore service-wide monitoring setting.

Short Name: Impala StateStore Health

Impala StateStore Role Health Test

Description

When computing the overall IMPALA health, consider Impala StateStore's health

Template Name

`impala_statestore_health_enabled`

Default Value

true

Unit(s)

no unit

Impala Catalog Server Health Tests

Impala Catalog Server Audit Pipeline Test

This Impala Catalog Server health test checks that the Auditing for the Impala Catalog Server role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Impala Catalog Server process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Impala Catalog Server host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Impala Catalog Server monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Impala Catalog Server File Descriptors

This Impala Catalog Server health test checks that the number of file descriptors used does not rise above some percentage of the Impala Catalog Server file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Impala Catalog Server monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`catalogserver_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Impala Catalog Server Heap Dump Directory Free Space

This Impala Catalog Server health test checks that the filesystem containing the heap dump directory of this Impala Catalog Server has sufficient free space. This test can be configured using the Heap Dump Directory Free Space Monitoring Absolute Thresholds and Heap Dump Directory Free Space Monitoring Percentage Thresholds Impala Catalog Server monitoring settings.

Short Name: Heap Dump Directory Free Space

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Template Name

`heap_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`heap_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Impala Catalog Server Host Health

This Impala Catalog Server health test factors in the health of the host upon which the Impala Catalog Server is running. A failure of this test means that the host running the Impala Catalog Server is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Impala Catalog Server Host Health Test Impala Catalog Server monitoring setting.

Short Name: Host Health

Impala Catalog Server Host Health Test

Description

When computing the overall Impala Catalog Server health, consider the host's health.

Template Name

`catalogserver_host_health_enabled`

Default Value

true

Unit(s)

no unit

Impala Catalog Server Log Directory Free Space

This Impala Catalog Server health test checks that the filesystem containing the log directory of this Impala Catalog Server has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Impala Catalog Server monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Impala Catalog Server Process Status

This Impala Catalog Server health test checks that the Cloudera Manager Agent on the Impala Catalog Server host is heart beating correctly and that the process associated with the Impala Catalog Server role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Impala Catalog Server process, a lack of connectivity to the Cloudera Manager Agent on the Impala Catalog Server host, or a problem with the Cloudera Manager Agent. This test can fail either because the Impala Catalog Server has crashed or because the Impala Catalog Server will not start or stop in a timely fashion. Check the Impala Catalog Server logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Impala Catalog Server host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Impala Catalog Server host, or look in the Cloudera Manager Agent logs on the Impala Catalog Server host for more details. This test can be enabled or disabled using the Impala Catalog Server Process Health Test Impala Catalog Server monitoring setting.

Short Name: Process Status

Impala Catalog Server Process Health Test

Description

Enables the health test that the Impala Catalog Server's process state is consistent with the role configuration

Template Name

`catalogserver_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Impala Catalog Server Resident Set Size

This Impala Catalog Server health test checks that the size of the resident set does not rise above a configured threshold value. A failure of this health test may indicates that the Impala Catalog Server process is consuming more memory than expected. It is possible that that unexpected memory consumption may lead to swapping and decreased performance for processes running on the same host as this Impala Catalog Server. Increased Impala Catalog Server memory consumption may be caused by an increased workload on the Impala service, or by a bug in the Impala Catalog Server software. To avoid failures of this health test, free up additional memory for this Impala Catalog Server process and increase the Resident Set Size Thresholds monitoring setting. This test can be configured using the Resident Set Size Thresholds Impala Catalog Server monitoring setting.

Short Name: Resident Set Size

Resident Set Size Thresholds

Description

The health test thresholds on the resident size of the process.

Template Name

`process_resident_set_size_thresholds`

Default Value

critical:never, warning:never

Unit(s)

BYTES

Impala Catalog Server StateStore Connectivity

This is a Catalog Server health test that checks whether the StateStore considers the Catalog Server alive. A failure of this health test may indicate that the Catalog Server is having trouble communicating with the StateStore. Look in the Catalog Server logs for more details. This test may return an unknown result if the Service Monitor is not able to communicate with the StateStore web server. Check the status of the StateStore web server and the Service Monitor logs if this test is returning an unknown result. This test can be enabled or disabled using the Catalog Server Connectivity Health Test Catalog Server monitoring setting. The Catalog Server Connectivity Tolerance at Startup Catalog Server monitoring setting and the Health Test Startup Tolerance StateStore monitoring setting can be used to control the test's tolerance windows around Catalog Server and StateStore restarts respectively.

Short Name: StateStore Connectivity

Catalog Server Connectivity Health Test

Description

Enables the health test that verifies the Catalog Server is connected to the StateStore

Template Name

`catalogserver_connectivity_health_enabled`

Default Value

true

Unit(s)

no unit

Catalog Server Connectivity Tolerance at Startup

Description

The amount of time to wait for the Catalog Server to fully start up and connect to the StateStore before enforcing the connectivity check.

Template Name

`catalogserver_connectivity_tolerance`

Default Value

180

Unit(s)

SECONDS

Health Test Startup Tolerance

Description

The amount of time allowed after this role is started that failures of health tests that rely on communication with this role will be tolerated.

Template Name

`statestore_startup_tolerance`

Default Value

5

Unit(s)

MINUTES

Impala Catalog Server Swap Memory Usage

This Impala Catalog Server health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Impala Catalog Server Unexpected Exits

This Impala Catalog Server health test checks that the Impala Catalog Server has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Impala Catalog Server monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Impala Catalog Server Web Server Status

This health test checks that the role's web server is responding quickly to requests by the Cloudera Manager Agent, and that the Cloudera Manager Agent can collect metrics from the web server. Failure of this health test may indicate a problem with the web server of the Impala Catalog Server, a misconfiguration of the Impala Catalog Server, or a problem with the Cloudera Manager Agent. Consult the Cloudera Manager Agent logs and the logs of the Impala Catalog Server for more detail. If the test failure message indicates a communication problem, the Cloudera Manager Agent's HTTP requests to the Impala Catalog Server's web server are failing or timing out. If the test's failure message indicates an unexpected response, the Impala Catalog Server's web server responded to the Cloudera Manager Agent's request, but the response could not be interpreted for some reason. This test can be configured using the Web Metric Collection Impala Catalog Server monitoring setting.

Short Name: Web Server Status

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Template Name

`catalogserver_web_metric_collection_enabled`

Default Value

true

Unit(s)

no unit

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Template Name

`catalogserver_web_metric_collection_thresholds`

Default Value

critical:never, warning:10000.0

Unit(s)

MILLISECONDS

Impala Daemon Health Tests

Impala Daemon Audit Pipeline Test

This Impala Daemon health test checks that the Auditing for the Impala Daemon role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Impala Daemon process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Impala Daemon host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Impala Daemon monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Impala Daemon File Descriptors

This Impala Daemon health test checks that the number of file descriptors used does not rise above some percentage of the Impala Daemon file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Impala Daemon monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`impalad_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Impala Daemon Heap Dump Directory Free Space

This Impala Daemon health test checks that the filesystem containing the heap dump directory of this Impala Daemon has sufficient free space. This test can be configured using the Heap Dump Directory Free Space Monitoring Absolute Thresholds and Heap Dump Directory Free Space Monitoring Percentage Thresholds Impala Daemon monitoring settings.

Short Name: Heap Dump Directory Free Space

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Template Name

`heap_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`heap_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Impala Daemon Host Health

This Impala Daemon health test factors in the health of the host upon which the Impala Daemon is running. A failure of this test means that the host running the Impala Daemon is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Impala Daemon Host Health Test Impala Daemon monitoring setting.

Short Name: Host Health

Impala Daemon Host Health Test

Description

When computing the overall Impala Daemon health, consider the host's health.

Template Name

`impalad_host_health_enabled`

Default Value

true

Unit(s)

no unit

Impala Daemon Impala Concurrent Client Connections

This is an Impala Daemon health test that checks the number of active client connections. This check will warn or fail when the number of active connections reaches the user-defined thresholds. This test can be configured using the Impala Daemon Concurrent Client Connections Monitoring Percentage Thresholds Impala Daemon monitoring setting.

Short Name: Impala Concurrent Client Connections

Impala Daemon Concurrent Client Connections Monitoring Percentage Thresholds

Description

The health check thresholds for monitoring of the number of concurrent client connections to Impala Daemon. Specified as a percentage of the maximum client connections parameter.

Template Name

`impalad_frontend_connections_thresholds`

Default Value

critical:95.0, warning:80.0

Unit(s)

PERCENT

Impala Daemon Impala Daemon Ready Check

This is an Impala Daemon health test that checks if the Impala Daemon is ready to process queries. This test can be configured using the Impala Daemon Ready Status Health Check and Impala Daemon Ready Status Startup Tolerance impalad monitoring settings.

Short Name: Impala Daemon Ready Check

Impala Daemon Ready Status Health Check

Description

Enables the health check that determines if the Impala daemon is ready to process queries.

Template Name

`impalad_ready_status_check_enabled`

Default Value

true

Unit(s)

no unit

Impala Daemon Ready Status Startup Tolerance

Description

The amount of time at Impala Daemon startup allowed for the Impala Daemon to start accepting new queries for processing.

Template Name

`impalad_ready_status_check_startup_tolerance`

Default Value

180

Unit(s)

SECONDS

Impala Daemon Impala Daemon Scratch Directories Free Space

This is a Impala Daemon health test that checks that the filesystem containing the Impala Daemon Scratch Directories of this Impala Daemon has sufficient free space. See the Impala Daemon Scratch Directories description on the Impala Daemon configuration page for more information on this directory type. This test can be configured using the Impala Daemon Scratch Directories Free Space Monitoring Absolute Thresholds and Impala Daemon Scratch Directories Free Space Monitoring Percentage Thresholds Impala Daemon monitoring settings.

Short Name: Impala Daemon Scratch Directories Free Space

Impala Daemon Scratch Directories Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Impala Daemon Scratch Directories.

Template Name

`impalad_scratch_directories_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Impala Daemon Scratch Directories Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Impala Daemon Scratch Directories. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Impala Daemon Scratch Directories Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`impalad_scratch_directories_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Impala Daemon Log Directory Free Space

This Impala Daemon health test checks that the filesystem containing the log directory of this Impala Daemon has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Impala Daemon monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Impala Daemon Pause Duration

This Impala Daemon health test checks that the Impala Daemon threads are not experiencing long scheduling pauses. The test uses a pause monitoring thread in the Impala Daemon that tracks scheduling delay by noting if it is run on its requested schedule. If the thread is not run on its requested schedule, the delay is noted and considered pause time. The health test checks that no more than some percentage of recent time is spent paused. A failure of this health test may indicate that the Impala Daemon is not getting enough CPU resources, or that it is spending too much time doing garbage collection. Inspect the Impala Daemon logs for any pause monitor output and check garbage collection metrics exposed by the Impala Daemon. This test can be configured using the Pause Duration Thresholds and Pause Duration Monitoring Period Impala Daemon monitoring settings.

Short Name: Pause Duration

Pause Duration Monitoring Period

Description

The period to review when computing the moving average of extra time the pause monitor spent paused.

Template Name

`impalad_pause_duration_window`

Default Value

5

Unit(s)

MINUTES

Pause Duration Thresholds

Description

The health test thresholds for the weighted average extra time the pause monitor spent paused. Specified as a percentage of elapsed wall clock time.

Template Name

`impalad_pause_duration_thresholds`

Default Value

critical:60.0, warning:30.0

Unit(s)

no unit

Impala Daemon Process Status

This Impala Daemon health test checks that the Cloudera Manager Agent on the Impala Daemon host is heart beating correctly and that the process associated with the Impala Daemon role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Impala Daemon process, a lack of connectivity to the Cloudera Manager Agent on the Impala Daemon host, or a problem with the Cloudera Manager Agent. This test can fail either because the Impala Daemon has crashed or because the Impala Daemon will not start or stop in a timely fashion. Check the Impala Daemon logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Impala Daemon host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Impala Daemon host, or look in the Cloudera Manager Agent logs on the Impala Daemon host for more details. This test can be enabled or disabled using the Impala Daemon Process Health Test Impala Daemon monitoring setting.

Short Name: Process Status

Impala Daemon Process Health Test

Description

Enables the health test that the Impala Daemon's process state is consistent with the role configuration

Template Name

`impalad_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Impala Daemon Query Monitoring Status Check

This is an Impala Daemon health test that checks if query monitoring for the Impala Daemon is successful. This check fails if the Impala Daemon web server is not available, or error is encountered when processing Impala query profiles. If the Impala Daemon web server is not available, no Impala queries that are currently running can be collected. If there is error processing Impala query profiles, collection of completed queries will be impacted. Check Cloudera Manager Agent log for more details. This test can be configured using the Impala Daemon Query Collection Status Health Check Impala Daemon monitoring setting.

Short Name: Query Monitoring Status Check

Impala Daemon Query Collection Status Health Check

Description

Enables the health check that determines if query collection for the Impala Daemon is successful.

Template Name

`impala_query_monitoring_status_check_enabled`

Default Value

true

Unit(s)

no unit

Monitoring Period For Query Monitoring Failures

Description

The period to review when computing query monitoring failures.

Template Name

`impala_query_monitoring_failure_window`

Default Value

5

Unit(s)

MINUTES

Query Monitoring Failures Thresholds

Description

The health test thresholds for failures encountered when monitoring queries within a recent period specified by the impala_query_monitoring_failure_window configuration for the role.

Template Name

`impala_query_monitoring_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Query Monitoring Full Sync Period

Description

The full sync period of the Impala query monitor in the Cloudera Manager Agent, specified in minutes. When a full sync is happening, all query profiles are sent over regardless of having been updated or not. If set to zero, a full sync is performed at each polling period.

Template Name

`query_monitoring_full_sync_period_minutes`

Default Value

2.0

Unit(s)

MINUTES

Query Monitoring Period

Description

The polling period of the Impala query monitor in the Cloudera Manager Agent, specified in seconds. If set to zero, query monitoring is disabled.

Template Name

`query_monitoring_period_seconds`

Default Value

1.0

Unit(s)

SECONDS

Impala Daemon Resident Set Size

This Impala Daemon health test checks that the size of the resident set does not rise above a configured threshold value. A failure of this health test may indicates that the Impala Daemon process is consuming more memory than expected. It is possible that that unexpected memory consumption may lead to swapping and decreased performance for processes running on the same host as this Impala Daemon. Increased Impala Daemon memory consumption may be caused by an increased workload on the Impala service, or by a bug in the Impala Daemon software. To avoid failures of this health test, free up additional memory for this Impala Daemon process and increase the Resident Set Size Thresholds monitoring setting. This test can be configured using the Resident Set Size Thresholds Impala Daemon monitoring setting.

Short Name: Resident Set Size

Resident Set Size Thresholds

Description

The health test thresholds on the resident size of the process.

Template Name

`process_resident_set_size_thresholds`

Default Value

critical:never, warning:never

Unit(s)

BYTES

Impala Daemon StateStore Connectivity

This is an Impala Daemon health test that checks whether the StateStore considers the Impala Daemon alive. A failure of this health test may indicate that the Impala Daemon is having trouble communicating with the StateStore. Look in the Impala Daemon logs for more details. This test may return an unknown result if the Service Monitor is not able to communicate with the StateStore web server. Check the status of the StateStore web server and the Service Monitor logs if this test is returning an unknown result. This test can be enabled or disabled using the Impala Daemon Connectivity Health Test Impala Daemon monitoring setting. The Impala Daemon Connectivity Tolerance at Startup Impala Daemon monitoring setting and the Health Test Startup Tolerance StateStore monitoring setting can be used to control the test's tolerance windows around Impala Daemon and StateStore restarts respectively.

Short Name: StateStore Connectivity

Health Test Startup Tolerance

Description

The amount of time allowed after this role is started that failures of health tests that rely on communication with this role will be tolerated.

Template Name

`statestore_startup_tolerance`

Default Value

5

Unit(s)

MINUTES

Impala Daemon Connectivity Health Test

Description

Enables the health test that verifies the Impala Daemon is connected to the StateStore.

Template Name

`impalad_connectivity_health_enabled`

Default Value

true

Unit(s)

no unit

Impala Daemon Connectivity Tolerance at Startup

Description

The amount of time to wait for the Impala Daemon to fully start up and connect to the StateStore before enforcing the connectivity check.

Template Name

`impalad_connectivity_tolerance`

Default Value

180

Unit(s)

SECONDS

Impala Daemon Swap Memory Usage

This Impala Daemon health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:any, warning:any

Unit(s)

BYTES

Impala Daemon Unexpected Exits

This Impala Daemon health test checks that the Impala Daemon has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Impala Daemon monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Impala Daemon Web Server Status

This health test checks that the role's web server is responding quickly to requests by the Cloudera Manager Agent, and that the Cloudera Manager Agent can collect metrics from the web server. Failure of this health test may indicate a problem with the web server of the Impala Daemon, a misconfiguration of the Impala Daemon, or a problem with the Cloudera Manager Agent. Consult the Cloudera Manager Agent logs and the logs of the Impala Daemon for more detail. If the test failure message indicates a communication problem, the Cloudera Manager Agent's HTTP requests to the Impala Daemon's web server are failing or timing out. If the test's failure message indicates an unexpected response, the Impala Daemon's web server responded to the Cloudera Manager Agent's request, but the response could not be interpreted for some reason. This test can be configured using the Web Metric Collection Impala Daemon monitoring setting.

Short Name: Web Server Status

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Template Name

`impalad_web_metric_collection_enabled`

Default Value

true

Unit(s)

no unit

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Template Name

`impalad_web_metric_collection_thresholds`

Default Value

critical:never, warning:10000.0

Unit(s)

MILLISECONDS

Impala Llama ApplicationMaster Health Tests

Impala Llama ApplicationMaster Audit Pipeline Test

This Impala Llama ApplicationMaster health test checks that the Auditing for the Impala Llama ApplicationMaster role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Impala Llama ApplicationMaster process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Impala Llama ApplicationMaster host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Impala Llama ApplicationMaster monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Impala Llama ApplicationMaster File Descriptors

This Impala Llama ApplicationMaster health test checks that the number of file descriptors used does not rise above some percentage of the Impala Llama ApplicationMaster file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Impala Llama ApplicationMaster monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`llama_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Impala Llama ApplicationMaster Heap Dump Directory Free Space

This Impala Llama ApplicationMaster health test checks that the filesystem containing the heap dump directory of this Impala Llama ApplicationMaster has sufficient free space. This test can be configured using the Heap Dump Directory Free Space Monitoring Absolute Thresholds and Heap Dump Directory Free Space Monitoring Percentage Thresholds Impala Llama ApplicationMaster monitoring settings.

Short Name: Heap Dump Directory Free Space

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Template Name

`heap_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`heap_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Impala Llama ApplicationMaster Host Health

This Impala Llama ApplicationMaster health test factors in the health of the host upon which the Impala Llama ApplicationMaster is running. A failure of this test means that the host running the Impala Llama ApplicationMaster is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Impala Llama ApplicationMaster Host Health Test Impala Llama ApplicationMaster monitoring setting.

Short Name: Host Health

Impala Llama ApplicationMaster Host Health Test

Description

When computing the overall Impala Llama ApplicationMaster health, consider the host's health.

Template Name

`llama_host_health_enabled`

Default Value

true

Unit(s)

no unit

Impala Llama ApplicationMaster Log Directory Free Space

This Impala Llama ApplicationMaster health test checks that the filesystem containing the log directory of this Impala Llama ApplicationMaster has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Impala Llama ApplicationMaster monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Impala Llama ApplicationMaster Process Status

This Impala Llama ApplicationMaster health test checks that the Cloudera Manager Agent on the Impala Llama ApplicationMaster host is heart beating correctly and that the process associated with the Impala Llama ApplicationMaster role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Impala Llama ApplicationMaster process, a lack of connectivity to the Cloudera Manager Agent on the Impala Llama ApplicationMaster host, or a problem with the Cloudera Manager Agent. This test can fail either because the Impala Llama ApplicationMaster has crashed or because the Impala Llama ApplicationMaster will not start or stop in a timely fashion. Check the Impala Llama ApplicationMaster logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Impala Llama ApplicationMaster host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Impala Llama ApplicationMaster host, or look in the Cloudera Manager Agent logs on the Impala Llama ApplicationMaster host for more details. This test can be enabled or disabled using the Impala Llama ApplicationMaster Process Health Test Impala Llama ApplicationMaster monitoring setting.

Short Name: Process Status

Impala Llama ApplicationMaster Process Health Test

Description

Enables the health test that the Impala Llama ApplicationMaster's process state is consistent with the role configuration

Template Name

`llama_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Impala Llama ApplicationMaster Swap Memory Usage

This Impala Llama ApplicationMaster health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Impala Llama ApplicationMaster Unexpected Exits

This Impala Llama ApplicationMaster health test checks that the Impala Llama ApplicationMaster has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Impala Llama ApplicationMaster monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Impala StateStore Health Tests

Impala StateStore Audit Pipeline Test

This Impala StateStore health test checks that the Auditing for the Impala StateStore role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Impala StateStore process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Impala StateStore host isn't able to send audits because of some network issue. Check the

Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Impala StateStore monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Impala StateStore File Descriptors

This Impala StateStore health test checks that the number of file descriptors used does not rise above some percentage of the Impala StateStore file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Impala StateStore monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`statestore_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Impala StateStore Heap Dump Directory Free Space

This Impala StateStore health test checks that the filesystem containing the heap dump directory of this Impala StateStore has sufficient free space. This test can be configured using the Heap Dump Directory Free Space Monitoring Absolute Thresholds and Heap Dump Directory Free Space Monitoring Percentage Thresholds Impala StateStore monitoring settings.

Short Name: Heap Dump Directory Free Space

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Template Name

`heap_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`heap_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Impala StateStore Host Health

This Impala StateStore health test factors in the health of the host upon which the Impala StateStore is running. A failure of this test means that the host running the Impala StateStore is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Impala StateStore Host Health Test Impala StateStore monitoring setting.

Short Name: Host Health

Impala StateStore Host Health Test

Description

When computing the overall Impala StateStore health, consider the host's health.

Template Name

`statestore_host_health_enabled`

Default Value

true

Unit(s)

no unit

Impala StateStore Log Directory Free Space

This Impala StateStore health test checks that the filesystem containing the log directory of this Impala StateStore has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Impala StateStore monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Impala StateStore Process Status

This Impala StateStore health test checks that the Cloudera Manager Agent on the Impala StateStore host is heart beating correctly and that the process associated with the Impala StateStore role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Impala StateStore process, a lack of connectivity to the Cloudera Manager Agent on the Impala StateStore host, or a problem with the Cloudera Manager Agent. This test can fail either because the Impala StateStore has crashed or because the Impala StateStore will not start or stop in a timely fashion. Check the Impala StateStore logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Impala StateStore host, check the status of the

Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Impala StateStore host, or look in the Cloudera Manager Agent logs on the Impala StateStore host for more details. This test can be enabled or disabled using the Impala StateStore Process Health Test Impala StateStore monitoring setting.

Short Name: Process Status

Impala StateStore Process Health Test

Description

Enables the health test that the Impala StateStore's process state is consistent with the role configuration

Template Name

`statestore_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Impala StateStore Resident Set Size

This Impala StateStore health test checks that the size of the resident set does not rise above a configured threshold value. A failure of this health test may indicates that the Impala StateStore process is consuming more memory than expected. It is possible that that unexpected memory consumption may lead to swapping and decreased performance for processes running on the same host as this Impala StateStore. Increased Impala StateStore memory consumption may be caused by an increased workload on the Impala service, or by a bug in the Impala StateStore software. To avoid failures of this health test, free up additional memory for this Impala StateStore process and increase the Resident Set Size Thresholds monitoring setting. This test can be configured using the Resident Set Size Thresholds Impala StateStore monitoring setting.

Short Name: Resident Set Size

Resident Set Size Thresholds

Description

The health test thresholds on the resident size of the process.

Template Name

`process_resident_set_size_thresholds`

Default Value

critical:never, warning:never

Unit(s)

BYTES

Impala StateStore Swap Memory Usage

This Impala StateStore health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Impala StateStore Unexpected Exits

This Impala StateStore health test checks that the Impala StateStore has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Impala StateStore monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Impala StateStore Web Server Status

This health test checks that the role's web server is responding quickly to requests by the Cloudera Manager Agent, and that the Cloudera Manager Agent can collect metrics from the web server. Failure of this health test may indicate a problem with the web server of the Impala StateStore, a misconfiguration of the Impala StateStore, or a problem with the Cloudera Manager Agent. Consult the Cloudera Manager Agent logs and the logs of the Impala StateStore for more detail. If the test failure message indicates a communication problem, the Cloudera Manager Agent's HTTP requests to the Impala StateStore's web server are failing or timing out. If the test's failure message indicates an unexpected response, the Impala StateStore's web server responded to the Cloudera Manager Agent's request, but

the response could not be interpreted for some reason. This test can be configured using the Web Metric Collection Impala StateStore monitoring setting.

Short Name: Web Server Status

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Template Name

`statestore_web_metric_collection_enabled`

Default Value

true

Unit(s)

no unit

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Template Name

`statestore_web_metric_collection_thresholds`

Default Value

critical:never, warning:10000.0

Unit(s)

MILLISECONDS

JobHistory Server Health Tests

JobHistory Server Audit Pipeline Test

This JobHistory Server health test checks that the Auditing for the JobHistory Server role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of JobHistory Server process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the JobHistory Server host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check JobHistory Server monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

JobHistory Server File Descriptors

This JobHistory Server health test checks that the number of file descriptors used does not rise above some percentage of the JobHistory Server file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds JobHistory Server monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`jobhistory_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

JobHistory Server GC Duration

This JobHistory Server health test checks that the JobHistory Server is not spending too much time performing Java garbage collection. It checks that no more than some percentage of recent time is spent performing Java garbage collection. A failure of this health test may indicate a capacity planning problem or misconfiguration of the JobHistory Server. This test can be configured using the Garbage Collection Duration Thresholds and Garbage Collection Duration Monitoring Period JobHistory Server monitoring settings.

Short Name: GC Duration

Garbage Collection Duration Monitoring Period

Description

The period to review when computing the moving average of garbage collection time.

Template Name

`jobhistory_gc_duration_window`

Default Value

5

Unit(s)

MINUTES

Garbage Collection Duration Thresholds

Description

The health test thresholds for the weighted average time spent in Java garbage collection. Specified as a percentage of elapsed wall clock time.

Template Name

`jobhistory_gc_duration_thresholds`

Default Value

critical:60.0, warning:30.0

Unit(s)

no unit

JobHistory Server Heap Dump Directory Free Space

This JobHistory Server health test checks that the filesystem containing the heap dump directory of this JobHistory Server has sufficient free space. This test can be configured using the Heap Dump Directory Free Space Monitoring Absolute Thresholds and Heap Dump Directory Free Space Monitoring Percentage Thresholds JobHistory Server monitoring settings.

Short Name: Heap Dump Directory Free Space

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Template Name

`heap_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`heap_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

JobHistory Server Host Health

This JobHistory Server health test factors in the health of the host upon which the JobHistory Server is running. A failure of this test means that the host running the JobHistory Server is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the JobHistory Server Host Health Test JobHistory Server monitoring setting.

Short Name: Host Health

JobHistory Server Host Health Test

Description

When computing the overall JobHistory Server health, consider the host's health.

Template Name

`jobhistory_host_health_enabled`

Default Value

true

Unit(s)

no unit

JobHistory Server Log Directory Free Space

This JobHistory Server health test checks that the filesystem containing the log directory of this JobHistory Server has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds JobHistory Server monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

JobHistory Server Process Status

This JobHistory Server health test checks that the Cloudera Manager Agent on the JobHistory Server host is heart beating correctly and that the process associated with the JobHistory Server role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the JobHistory Server process, a lack of connectivity to the Cloudera Manager Agent on the JobHistory Server host, or a problem with the Cloudera Manager Agent. This test can fail either because the JobHistory Server has crashed or because the JobHistory Server will not start or stop in a timely fashion. Check the JobHistory Server logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the JobHistory Server host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the JobHistory Server host, or look in the Cloudera Manager Agent logs on the JobHistory Server host for more details. This test can be enabled or disabled using the JobHistory Server Process Health Test JobHistory Server monitoring setting.

Short Name: Process Status

JobHistory Server Process Health Test

Description

Enables the health test that the JobHistory Server's process state is consistent with the role configuration

Template Name

`jobhistory_scm_health_enabled`

Default Value

true

Unit(s)

no unit

JobHistory Server Swap Memory Usage

This JobHistory Server health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

JobHistory Server Unexpected Exits

This JobHistory Server health test checks that the JobHistory Server has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period JobHistory Server monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

JobHistory Server Web Server Status

This health test checks that the role's web server is responding quickly to requests by the Cloudera Manager Agent, and that the Cloudera Manager Agent can collect metrics from the web server. Failure of this health test may indicate a problem with the web server of the JobHistory Server, a misconfiguration of the JobHistory Server, or a problem with the Cloudera Manager Agent. Consult the Cloudera Manager Agent logs and the logs of the JobHistory Server for more detail. If the test failure message indicates a communication problem, the Cloudera Manager Agent's HTTP requests to the JobHistory Server's web server are failing or timing out. If the test's failure message indicates an unexpected response, the JobHistory Server's web server responded to the Cloudera Manager Agent's request, but the response could not be interpreted for some reason. This test can be configured using the Web Metric Collection JobHistory Server monitoring setting.

Short Name: Web Server Status

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Template Name

`jobhistory_web_metric_collection_enabled`

Default Value

true

Unit(s)

no unit

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Template Name

`jobhistory_web_metric_collection_thresholds`

Default Value

critical:never, warning:10000.0

Unit(s)

MILLISECONDS

JobTracker Health Tests

JobTracker Audit Pipeline Test

This JobTracker health test checks that the Auditing for the JobTracker role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of JobTracker process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the JobTracker host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check JobTracker monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

JobTracker File Descriptors

This JobTracker health test checks that the number of file descriptors used does not rise above some percentage of the JobTracker file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds JobTracker monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`jobtracker_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

JobTracker GC Duration

This JobTracker health test checks that the JobTracker is not spending too much time performing Java garbage collection. It checks that no more than some percentage of recent time is spent performing Java garbage collection. A failure of this health test may indicate a capacity planning problem or misconfiguration of the JobTracker. This test can be configured using the Garbage Collection Duration Thresholds and Garbage Collection Duration Monitoring Period JobTracker monitoring settings.

Short Name: GC Duration

Garbage Collection Duration Monitoring Period

Description

The period to review when computing the moving average of garbage collection time.

Template Name

`jobtracker_gc_duration_window`

Default Value

5

Unit(s)

MINUTES

Garbage Collection Duration Thresholds

Description

The health test thresholds for the weighted average time spent in Java garbage collection. Specified as a percentage of elapsed wall clock time.

Template Name

`jobtracker_gc_duration_thresholds`

Default Value

critical:60.0, warning:30.0

Unit(s)

no unit

JobTracker Heap Dump Directory Free Space

This JobTracker health test checks that the filesystem containing the heap dump directory of this JobTracker has sufficient free space. This test can be configured using the Heap Dump Directory Free Space Monitoring Absolute Thresholds and Heap Dump Directory Free Space Monitoring Percentage Thresholds JobTracker monitoring settings.

Short Name: Heap Dump Directory Free Space

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Template Name

`heap_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`heap_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

JobTracker Host Health

This JobTracker health test factors in the health of the host upon which the JobTracker is running. A failure of this test means that the host running the JobTracker is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the JobTracker Host Health Test JobTracker monitoring setting.

Short Name: Host Health

JobTracker Host Health Test

Description

When computing the overall JobTracker health, consider the host's health.

Template Name

`jobtracker_host_health_enabled`

Default Value

true

Unit(s)

no unit

JobTracker Log Directory Free Space

This JobTracker health test checks that the filesystem containing the log directory of this JobTracker has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds JobTracker monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

JobTracker Process Status

This JobTracker health test checks that the Cloudera Manager Agent on the JobTracker host is heart beating correctly and that the process associated with the JobTracker role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the JobTracker process, a lack of connectivity to the Cloudera Manager Agent on the JobTracker host, or a problem with the Cloudera Manager Agent. This test can fail either because the JobTracker has crashed or because the JobTracker will not start or stop in a timely fashion. Check the JobTracker logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the JobTracker host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the JobTracker host, or look in the Cloudera Manager Agent logs on the JobTracker host for more details. This test can be enabled or disabled using the JobTracker Process Health Test JobTracker monitoring setting.

Short Name: Process Status

JobTracker Process Health Test

Description

Enables the health test that the JobTracker's process state is consistent with the role configuration

Template Name

`jobtracker_scm_health_enabled`

Default Value

true

Unit(s)

no unit

JobTracker Swap Memory Usage

This JobTracker health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

JobTracker Unexpected Exits

This JobTracker health test checks that the JobTracker has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period JobTracker monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

JobTracker Web Server Status

This health test checks that the role's web server is responding quickly to requests by the Cloudera Manager Agent, and that the Cloudera Manager Agent can collect metrics from the web server. Failure of this health test may indicate a problem with the web server of the JobTracker, a misconfiguration of the JobTracker, or a problem with the Cloudera Manager Agent. Consult the Cloudera Manager Agent logs and the logs of the JobTracker for more detail. If the test failure message indicates a communication problem, the Cloudera Manager Agent's HTTP requests to the JobTracker's web server are failing or timing out. If the test's failure message indicates an unexpected response, the JobTracker's web server responded to the Cloudera Manager Agent's request, but the response could not be interpreted for some reason. This test can be configured using the Web Metric Collection JobTracker monitoring setting.

Short Name: Web Server Status

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Template Name

`jobtracker_web_metric_collection_enabled`

Default Value

true

Unit(s)

no unit

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Template Name

`jobtracker_web_metric_collection_thresholds`

Default Value

critical:never, warning:10000.0

Unit(s)

MILLISECONDS

JournalNode Health Tests

JournalNode Audit Pipeline Test

This JournalNode health test checks that the Auditing for the JournalNode role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of JournalNode process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the JournalNode host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check JournalNode monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

JournalNode File Descriptors

This JournalNode health test checks that the number of file descriptors used does not rise above some percentage of the JournalNode file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds JournalNode monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`journalnode_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

JournalNode Fsync Latency

This is a JournalNode health test that checks the JournalNode's fsync latency. This test returns "Bad" health if the 99th percentile fsync latency over the previous minute is above a configured threshold value. Poor fsync performance may indicate a bad or overloaded disk and will negatively impact the performance of HDFS metadata operations performed by the NameNode. This test can be configured using the JournalNode Fsync Latency Thresholds JournalNode monitoring settings.

Short Name: Fsync Latency

JournalNode Fsync Latency Thresholds

Description

The health test thresholds for JournalNode fsync latency.

Template Name

`journalnode_fsync_latency_thresholds`

Default Value

critical:3000.0, warning:1000.0

Unit(s)

MILLISECONDS

JournalNode GC Duration

This JournalNode health test checks that the JournalNode is not spending too much time performing Java garbage collection. It checks that no more than some percentage of recent time is spent performing Java garbage collection. A failure of this health test may indicate a capacity planning problem or misconfiguration of the JournalNode. This test can be configured using the Garbage Collection Duration Thresholds and Garbage Collection Duration Monitoring Period JournalNode monitoring settings.

Short Name: GC Duration

Garbage Collection Duration Monitoring Period

Description

The period to review when computing the moving average of garbage collection time.

Template Name

`journalnode_gc_duration_window`

Default Value

5

Unit(s)

MINUTES

Garbage Collection Duration Thresholds

Description

The health test thresholds for the weighted average time spent in Java garbage collection. Specified as a percentage of elapsed wall clock time.

Template Name

`journalnode_gc_duration_thresholds`

Default Value

critical:60.0, warning:30.0

Unit(s)

no unit

JournalNode Heap Dump Directory Free Space

This JournalNode health test checks that the filesystem containing the heap dump directory of this JournalNode has sufficient free space. This test can be configured using the Heap Dump Directory Free Space Monitoring Absolute Thresholds and Heap Dump Directory Free Space Monitoring Percentage Thresholds JournalNode monitoring settings.

Short Name: Heap Dump Directory Free Space

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Template Name

`heap_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`heap_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

JournalNode Host Health

This JournalNode health test factors in the health of the host upon which the JournalNode is running. A failure of this test means that the host running the JournalNode is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the JournalNode Host Health Test JournalNode monitoring setting.

Short Name: Host Health

JournalNode Host Health Test

Description

When computing the overall JournalNode health, consider the host's health.

Template Name

`journalnode_host_health_enabled`

Default Value

true

Unit(s)

no unit

JournalNode JournalNode Edits Directory Free Space

This is a JournalNode health test that checks that the filesystem containing the JournalNode Edits Directory of this JournalNode has sufficient free space. See the JournalNode Edits Directory description on the JournalNode configuration page for more information on this directory type. This test can be configured using the JournalNode Edits Directory Free Space Monitoring Absolute Thresholds and JournalNode Edits Directory Free Space Monitoring Percentage Thresholds JournalNode monitoring settings.

Short Name: JournalNode Edits Directory Free Space

JournalNode Edits Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's JournalNode Edits Directory.

Template Name

`journalnode_edits_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

JournalNode Edits Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's JournalNode Edits Directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a JournalNode Edits Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`journalnode_edits_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

JournalNode Log Directory Free Space

This JournalNode health test checks that the filesystem containing the log directory of this JournalNode has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds JournalNode monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

JournalNode Process Status

This JournalNode health test checks that the Cloudera Manager Agent on the JournalNode host is heart beating correctly and that the process associated with the JournalNode role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the JournalNode process, a lack of connectivity to the Cloudera Manager Agent on the JournalNode host, or a problem with the Cloudera Manager Agent. This test can fail either

because the JournalNode has crashed or because the JournalNode will not start or stop in a timely fashion. Check the JournalNode logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the JournalNode host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the JournalNode host, or look in the Cloudera Manager Agent logs on the JournalNode host for more details. This test can be enabled or disabled using the JournalNode Process Health Test JournalNode monitoring setting.

Short Name: Process Status

JournalNode Process Health Test

Description

Enables the health test that the JournalNode's process state is consistent with the role configuration

Template Name

`journalnode_scm_health_enabled`

Default Value

true

Unit(s)

no unit

JournalNode Swap Memory Usage

This JournalNode health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

JournalNode Sync Status

This is a JournalNode health test that checks that the active NameNode is in sync with this JournalNode. This test returns "Bad" health if the active NameNode is out-of-sync with the JournalNode. This test is disabled when there is no active NameNode. This test can be configured using the Active NameNode Sync Status Health Check and Active NameNode Sync Status Startup Tolerance JournalNode monitoring settings.

Short Name: Sync Status

Active NameNode Sync Status Health Check

Description

Enables the health check that verifies the active NameNode's sync status to the JournalNode

Template Name

`journalnode_sync_status_enabled`

Default Value

true

Unit(s)

no unit

Active NameNode Sync Status Startup Tolerance

Description

The amount of time at JournalNode startup allowed for the active NameNode to get in sync with the JournalNode.

Template Name

`journalnode_sync_status_startup_tolerance`

Default Value

180

Unit(s)

SECONDS

JournalNode Unexpected Exits

This JournalNode health test checks that the JournalNode has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period JournalNode monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

JournalNode Web Server Status

This health test checks that the role's web server is responding quickly to requests by the Cloudera Manager Agent, and that the Cloudera Manager Agent can collect metrics from the web server. Failure of this health test may indicate a problem with the web server of the JournalNode, a misconfiguration of the JournalNode, or a problem with the Cloudera Manager Agent. Consult the Cloudera Manager Agent logs and the logs of the JournalNode for more detail. If the test failure message indicates a communication problem, the Cloudera Manager Agent's HTTP requests to the JournalNode's web server are failing or timing out. If the test's failure message indicates an unexpected response, the JournalNode's web server responded to the Cloudera Manager Agent's request, but the response could not be interpreted for some reason. This test can be configured using the Web Metric Collection JournalNode monitoring setting.

Short Name: Web Server Status

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Template Name

`journalnode_web_metric_collection_enabled`

Default Value

true

Unit(s)

no unit

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Template Name

`journalnode_web_metric_collection_thresholds`

Default Value

critical:never, warning:10000.0

Unit(s)

MILLISECONDS

Kafka Health Tests

Kafka Broker Health

This is a Kafka service-level health test that checks that enough of the Kafka Brokers in the cluster are healthy. The test returns "Concerning" health if the number of healthy Kafka Brokers falls below a warning threshold, expressed as a percentage of the total number of Kafka Brokers. The test returns "Bad" health if the number of healthy and "Concerning" Kafka Brokers falls below a critical threshold, expressed as a percentage of the total number of Kafka Brokers. For example, if this test is configured with a warning threshold of 95% and a critical threshold of 90% for a cluster of 100 Kafka Brokers, this test would return "Good" health if 95 or more Kafka Brokers have good health. This test would return "Concerning" health if at least 90 Kafka Brokers have either "Good" or "Concerning" health. If more than 10 Kafka Brokers have bad health, this test would return "Bad" health. A failure of this health test indicates unhealthy Kafka Brokers. Check the status of the individual Kafka Brokers for more information. This test can be configured using the Kafka Kafka service-wide monitoring setting.

Short Name: Kafka Broker Health

Healthy Kafka Broker Monitoring Thresholds

Description

The health test thresholds of the overall Kafka Broker health. The check returns "Concerning" health if the percentage of "Healthy" Kafka Brokers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Kafka Brokers falls below the critical threshold.

Template Name

`KAFKA_KAFKA_BROKER_healthy_thresholds`

Default Value

critical:49.99, warning:94.99

Unit(s)

PERCENT

Kafka Connect Health

This is a Kafka service-level health test that checks that enough of the Kafka Connects in the cluster are healthy. The test returns "Concerning" health if the number of healthy Kafka Connects falls below a warning threshold, expressed as a percentage of the total number of Kafka Connects. The test returns "Bad" health if the number of healthy and "Concerning" Kafka Connects falls below a critical threshold, expressed as a percentage of the total number of Kafka Connects. For example, if this test is configured with a warning threshold of 95% and a critical threshold of 90% for a cluster of 100 Kafka Connects, this test would return "Good" health if 95 or more Kafka Connects have good health. This test would return "Concerning" health if at least 90 Kafka Connects have either "Good" or "Concerning" health. If more than 10 Kafka Connects have bad health, this test would return "Bad" health. A failure of this health test indicates unhealthy Kafka Connects. Check the status of the individual Kafka Connects for more information. This test can be configured using the Kafka Kafka service-wide monitoring setting.

Short Name: Kafka Connect Health

Healthy Kafka Connect Monitoring Thresholds

Description

The health test thresholds of the overall Kafka Connect health. The check returns "Concerning" health if the percentage of "Healthy" Kafka Connects falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Kafka Connects falls below the critical threshold.

Template Name

`KAFKA_KAFKA_CONNECT_healthy_thresholds`

Default Value

critical:49.99, warning:94.99

Unit(s)

PERCENT

Kafka Broker Health Tests

Kafka Broker Audit Pipeline Test

This Kafka Broker health test checks that the Auditing for the Kafka Broker role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Kafka Broker process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Kafka Broker host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Kafka Broker monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Kafka Broker File Descriptors

This Kafka Broker health test checks that the number of file descriptors used does not rise above some percentage of the Kafka Broker file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Kafka Broker monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`kafka_broker_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Kafka Broker Host Health

This Kafka Broker health test factors in the health of the host upon which the Kafka Broker is running. A failure of this test means that the host running the Kafka Broker is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Kafka Broker Host Health Test Kafka Broker monitoring setting.

Short Name: Host Health

Kafka Broker Host Health Test

Description

When computing the overall Kafka Broker health, consider the host's health.

Template Name

`kafka_broker_host_health_enabled`

Default Value

true

Unit(s)

no unit

Kafka Broker Lagging Replicas Test

Short Name: Lagging Replicas Test

Kafka Broker Log Directory Free Space

This Kafka Broker health test checks that the filesystem containing the log directory of this Kafka Broker has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Kafka Broker monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Kafka Broker Offline Directory Test

Short Name: Offline Directory Test

Kafka Broker Offline Partitions Test

Short Name: Offline Partitions Test

Kafka Broker Process Status

This Kafka Broker health test checks that the Cloudera Manager Agent on the Kafka Broker host is heart beating correctly and that the process associated with the Kafka Broker role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Kafka Broker process, a lack of connectivity to the Cloudera Manager Agent on the Kafka Broker host, or a problem with the Cloudera Manager Agent. This test can fail either because the Kafka Broker has crashed or because the Kafka Broker will not start or stop in a timely fashion. Check the Kafka Broker logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Kafka Broker host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Kafka Broker host, or look in the Cloudera Manager Agent logs on the Kafka Broker host for more details. This test can be enabled or disabled using the Kafka Broker Process Health Test Kafka Broker monitoring setting.

Short Name: Process Status

Kafka Broker Process Health Test

Description

Enables the health test that the Kafka Broker's process state is consistent with the role configuration

Template Name

`kafka_broker_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Kafka Broker Swap Memory Usage

This Kafka Broker health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Kafka Broker Unexpected Exits

This Kafka Broker health test checks that the Kafka Broker has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Kafka Broker monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Kafka Connect Health Tests

Kafka Connect Audit Pipeline Test

This Kafka Connect health test checks that the Auditing for the Kafka Connect role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Kafka Connect process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Kafka Connect host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Kafka Connect monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Kafka Connect File Descriptors

This Kafka Connect health test checks that the number of file descriptors used does not rise above some percentage of the Kafka Connect file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Kafka Connect monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`kafka_connect_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Kafka Connect Host Health

This Kafka Connect health test factors in the health of the host upon which the Kafka Connect is running. A failure of this test means that the host running the Kafka Connect is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Kafka Connect Host Health Test Kafka Connect monitoring setting.

Short Name: Host Health

Kafka Connect Host Health Test

Description

When computing the overall Kafka Connect health, consider the host's health.

Template Name

`kafka_connect_host_health_enabled`

Default Value

true

Unit(s)

no unit

Kafka Connect Log Directory Free Space

This Kafka Connect health test checks that the filesystem containing the log directory of this Kafka Connect has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Kafka Connect monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Kafka Connect Process Status

This Kafka Connect health test checks that the Cloudera Manager Agent on the Kafka Connect host is heart beating correctly and that the process associated with the Kafka Connect role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Kafka Connect process, a lack of connectivity to the Cloudera Manager Agent on the Kafka Connect host, or a problem with the Cloudera Manager Agent. This test can fail either because the Kafka Connect has crashed or because the Kafka Connect will not start or stop in a timely fashion. Check the Kafka Connect logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Kafka Connect host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Kafka Connect host, or look in the Cloudera Manager Agent logs on the Kafka Connect host for more details. This test can be enabled or disabled using the Kafka Connect Process Health Test Kafka Connect monitoring setting.

Short Name: Process Status

Kafka Connect Process Health Test

Description

Enables the health test that the Kafka Connect's process state is consistent with the role configuration

Template Name

`kafka_connect_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Kafka Connect Swap Memory Usage

This Kafka Connect health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Kafka Connect Unexpected Exits

This Kafka Connect health test checks that the Kafka Connect has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Kafka Connect monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Kafka MirrorMaker Health Tests

Kafka MirrorMaker Audit Pipeline Test

This Kafka MirrorMaker health test checks that the Auditing for the Kafka MirrorMaker role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Kafka MirrorMaker process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Kafka MirrorMaker host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Kafka MirrorMaker monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Kafka MirrorMaker File Descriptors

This Kafka MirrorMaker health test checks that the number of file descriptors used does not rise above some percentage of the Kafka MirrorMaker file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Kafka MirrorMaker monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`kafka_mirror_maker_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Kafka MirrorMaker Host Health

This Kafka MirrorMaker health test factors in the health of the host upon which the Kafka MirrorMaker is running. A failure of this test means that the host running the Kafka MirrorMaker is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Kafka MirrorMaker Host Health Test Kafka MirrorMaker monitoring setting.

Short Name: Host Health

Kafka MirrorMaker Host Health Test

Description

When computing the overall Kafka MirrorMaker health, consider the host's health.

Template Name

`kafka_mirror_maker_host_health_enabled`

Default Value

true

Unit(s)

no unit

Kafka MirrorMaker Log Directory Free Space

This Kafka MirrorMaker health test checks that the filesystem containing the log directory of this Kafka MirrorMaker has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Kafka MirrorMaker monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Kafka MirrorMaker Process Status

This Kafka MirrorMaker health test checks that the Cloudera Manager Agent on the Kafka MirrorMaker host is heart beating correctly and that the process associated with the Kafka MirrorMaker role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Kafka MirrorMaker process, a lack of connectivity to the Cloudera Manager Agent on the Kafka MirrorMaker host, or a problem with the Cloudera Manager Agent. This test can fail either because the Kafka MirrorMaker has crashed or because the Kafka MirrorMaker will not start or stop in a timely fashion. Check the Kafka MirrorMaker logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Kafka MirrorMaker host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Kafka MirrorMaker host, or look in the Cloudera Manager Agent logs on the Kafka MirrorMaker host for more details. This test can be enabled or disabled using the Kafka MirrorMaker Process Health Test Kafka MirrorMaker monitoring setting.

Short Name: Process Status

Kafka MirrorMaker Process Health Test

Description

Enables the health test that the Kafka MirrorMaker's process state is consistent with the role configuration

Template Name

`kafka_mirror_maker_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Kafka MirrorMaker Swap Memory Usage

This Kafka MirrorMaker health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Kafka MirrorMaker Unexpected Exits

This Kafka MirrorMaker health test checks that the Kafka MirrorMaker has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Kafka MirrorMaker monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Kerberos Ticket Renewer Health Tests

Kerberos Ticket Renewer Audit Pipeline Test

This Kerberos Ticket Renewer health test checks that the Auditing for the Kerberos Ticket Renewer role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Kerberos Ticket Renewer process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Kerberos Ticket Renewer host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Kerberos Ticket Renewer monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Kerberos Ticket Renewer File Descriptors

This Kerberos Ticket Renewer health test checks that the number of file descriptors used does not rise above some percentage of the Kerberos Ticket Renewer file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Kerberos Ticket Renewer monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`kt_renewer_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Kerberos Ticket Renewer Heap Dump Directory Free Space

This Kerberos Ticket Renewer health test checks that the filesystem containing the heap dump directory of this Kerberos Ticket Renewer has sufficient free space. This test can be configured using the Heap Dump Directory Free Space Monitoring Absolute Thresholds and Heap Dump Directory Free Space Monitoring Percentage Thresholds Kerberos Ticket Renewer monitoring settings.

Short Name: Heap Dump Directory Free Space

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Template Name

`heap_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`heap_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Kerberos Ticket Renewer Host Health

This Kerberos Ticket Renewer health test factors in the health of the host upon which the Kerberos Ticket Renewer is running. A failure of this test means that the host running the Kerberos Ticket Renewer is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Kerberos Ticket Renewer Host Health Test Kerberos Ticket Renewer monitoring setting.

Short Name: Host Health

Kerberos Ticket Renewer Host Health Test

Description

When computing the overall Kerberos Ticket Renewer health, consider the host's health.

Template Name

`kt_renewer_host_health_enabled`

Default Value

true

Unit(s)

no unit

Kerberos Ticket Renewer Log Directory Free Space

This Kerberos Ticket Renewer health test checks that the filesystem containing the log directory of this Kerberos Ticket Renewer has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Kerberos Ticket Renewer monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Kerberos Ticket Renewer Process Status

This Kerberos Ticket Renewer health test checks that the Cloudera Manager Agent on the Kerberos Ticket Renewer host is heart beating correctly and that the process associated with the Kerberos Ticket Renewer role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Kerberos Ticket Renewer process, a lack of connectivity to the Cloudera Manager Agent on the Kerberos Ticket Renewer host, or a problem with the Cloudera Manager Agent. This test can fail either because the Kerberos Ticket Renewer has crashed or because the Kerberos Ticket Renewer will not start or stop in a timely fashion. Check the Kerberos Ticket Renewer logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Kerberos Ticket Renewer host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Kerberos Ticket Renewer host, or look in the Cloudera Manager Agent logs on the Kerberos Ticket Renewer host for more details. This test can be enabled or disabled using the Kerberos Ticket Renewer Process Health Test Kerberos Ticket Renewer monitoring setting.

Short Name: Process Status

Kerberos Ticket Renewer Process Health Test

Description

Enables the health test that the Kerberos Ticket Renewer's process state is consistent with the role configuration

Template Name

`kt_renewer_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Kerberos Ticket Renewer Swap Memory Usage

This Kerberos Ticket Renewer health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Kerberos Ticket Renewer Unexpected Exits

This Kerberos Ticket Renewer health test checks that the Kerberos Ticket Renewer has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Kerberos Ticket Renewer monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Key Management Server Health Tests

Key Management Server Audit Pipeline Test

This Key Management Server health test checks that the Auditing for the Key Management Server role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Key Management Server process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Key Management Server host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Key Management Server monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Key Management Server File Descriptors

This Key Management Server health test checks that the number of file descriptors used does not rise above some percentage of the Key Management Server file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Key Management Server monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`kms_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Key Management Server Host Health

This Key Management Server health test factors in the health of the host upon which the Key Management Server is running. A failure of this test means that the host running the Key Management Server is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Key Management Server Host Health Test Key Management Server monitoring setting.

Short Name: Host Health

Key Management Server Host Health Test

Description

When computing the overall Key Management Server health, consider the host's health.

Template Name

`kms_host_health_enabled`

Default Value

true

Unit(s)

no unit

Key Management Server Log Directory Free Space

This Key Management Server health test checks that the filesystem containing the log directory of this Key Management Server has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Key Management Server monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Key Management Server Process Status

This Key Management Server health test checks that the Cloudera Manager Agent on the Key Management Server host is heart beating correctly and that the process associated with the Key Management Server role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Key Management Server process, a lack of connectivity to the Cloudera Manager Agent on the Key Management Server host, or a problem with the Cloudera Manager Agent. This test can fail either because the Key Management Server has crashed or because the Key Management Server will not start or stop in a timely fashion. Check the Key Management Server logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Key Management Server host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Key Management Server host, or look in the Cloudera Manager Agent logs on the Key Management Server host for more details. This test can be enabled or disabled using the Key Management Server Process Health Test Key Management Server monitoring setting.

Short Name: Process Status

Key Management Server Process Health Test

Description

Enables the health test that the Key Management Server's process state is consistent with the role configuration

Template Name

`kms_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Key Management Server Swap Memory Usage

This Key Management Server health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Key Management Server Unexpected Exits

This Key Management Server health test checks that the Key Management Server has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Key Management Server monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Key Management Server Proxy Health Tests

Key Management Server Proxy Audit Pipeline Test

This Key Management Server Proxy health test checks that the Auditing for the Key Management Server Proxy role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Key Management Server Proxy process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Key Management Server Proxy host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Key Management Server Proxy monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Key Management Server Proxy File Descriptors

This Key Management Server Proxy health test checks that the number of file descriptors used does not rise above some percentage of the Key Management Server Proxy file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Key Management Server Proxy monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`kms_keytrustee_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Key Management Server Proxy Host Health

This Key Management Server Proxy health test factors in the health of the host upon which the Key Management Server Proxy is running. A failure of this test means that the host running the Key Management Server Proxy is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Key Management Server Proxy Host Health Test Key Management Server Proxy monitoring setting.

Short Name: Host Health

Key Management Server Proxy Host Health Test

Description

When computing the overall Key Management Server Proxy health, consider the host's health.

Template Name

`kms_keytrustee_host_health_enabled`

Default Value

true

Unit(s)

no unit

Key Management Server Proxy Log Directory Free Space

This Key Management Server Proxy health test checks that the filesystem containing the log directory of this Key Management Server Proxy has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Key Management Server Proxy monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Key Management Server Proxy Process Status

This Key Management Server Proxy health test checks that the Cloudera Manager Agent on the Key Management Server Proxy host is heart beating correctly and that the process associated with the Key Management Server Proxy role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Key Management Server Proxy process, a lack of connectivity to the Cloudera Manager Agent on the Key Management Server Proxy host, or a problem with the Cloudera Manager Agent. This test can fail either because the Key Management Server Proxy has crashed or because the Key Management Server Proxy will not start or stop in a timely fashion. Check the Key Management Server Proxy logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Key Management Server Proxy host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Key Management Server Proxy host, or look in the Cloudera Manager Agent logs on the Key Management Server Proxy host for more details. This test can be enabled or disabled using the Key Management Server Proxy Process Health Test Key Management Server Proxy monitoring setting.

Short Name: Process Status

Key Management Server Proxy Process Health Test

Description

Enables the health test that the Key Management Server Proxy's process state is consistent with the role configuration

Template Name

`kms_keytrustee_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Key Management Server Proxy Swap Memory Usage

This Key Management Server Proxy health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Key Management Server Proxy Unexpected Exits

This Key Management Server Proxy health test checks that the Key Management Server Proxy has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Key Management Server Proxy monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Key-Value Store Indexer Health Tests

Key-Value Store Indexer Lily HBase Indexer Health

This is a Key-Value Store Indexer service-level health test that checks that enough of the Lily HBase Indexers in the cluster are healthy. The test returns "Concerning" health if the number of healthy Lily HBase Indexers falls below a warning threshold, expressed as a percentage of the total number of Lily HBase Indexers. The test returns "Bad" health if the number of healthy and "Concerning" Lily HBase Indexers falls below a critical threshold, expressed as a percentage of the total number of Lily HBase Indexers. For example, if this test is configured with a warning threshold of 95% and a critical threshold of 90% for a cluster of 100 Lily HBase Indexers, this test would return "Good" health if 95 or more Lily HBase Indexers have good health. This test would return "Concerning" health if at least 90 Lily HBase Indexers have either "Good" or "Concerning" health. If more than 10 Lily HBase Indexers have bad health, this test would return "Bad" health. A failure of this health test indicates unhealthy Lily HBase Indexers. Check the status of the individual Lily HBase Indexers for more information. This test can be configured using the Key-Value Store Indexer Key-Value Store Indexer service-wide monitoring setting.

Short Name: Lily HBase Indexer Health

Healthy Lily HBase Indexer Monitoring Thresholds

Description

The health test thresholds of the overall Lily HBase Indexer health. The check returns "Concerning" health if the percentage of "Healthy" Lily HBase Indexers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Lily HBase Indexers falls below the critical threshold.

Template Name

`ks_indexer_indexers_healthy_thresholds`

Default Value

critical:90.0, warning:95.0

Unit(s)

PERCENT

Knox Health Tests

Knox Gateway Health

This is a Knox service-level health test that checks that enough of the Knox Gateways in the cluster are healthy. The test returns "Concerning" health if the number of healthy Knox Gateways falls below a warning threshold, expressed as a percentage of the total number of Knox Gateways. The test returns "Bad" health if the number of healthy and "Concerning" Knox Gateways falls below a critical threshold, expressed as a percentage of the total number of Knox Gateways. For example, if this test is configured with a warning threshold of 95% and a critical threshold of 90% for a cluster of 100 Knox Gateways, this test would return "Good" health if 95 or more Knox Gateways have good

health. This test would return "Concerning" health if at least 90 Knox Gateways have either "Good" or "Concerning" health. If more than 10 Knox Gateways have bad health, this test would return "Bad" health. A failure of this health test indicates unhealthy Knox Gateways. Check the status of the individual Knox Gateways for more information. This test can be configured using the Knox Knox service-wide monitoring setting.

Short Name: Knox Gateway Health

Healthy Knox Gateway Monitoring Thresholds

Description

The health test thresholds of the overall Knox Gateway health. The check returns "Concerning" health if the percentage of "Healthy" Knox Gateways falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Knox Gateways falls below the critical threshold.

Template Name

`KNOX_KNOX_GATEWAY_healthy_thresholds`

Default Value

critical:49.0, warning:99.0

Unit(s)

PERCENT

Knox IDBroker Health

This is a Knox service-level health test that checks that enough of the Knox IDBrokers in the cluster are healthy. The test returns "Concerning" health if the number of healthy Knox IDBrokers falls below a warning threshold, expressed as a percentage of the total number of Knox IDBrokers. The test returns "Bad" health if the number of healthy and "Concerning" Knox IDBrokers falls below a critical threshold, expressed as a percentage of the total number of Knox IDBrokers. For example, if this test is configured with a warning threshold of 95% and a critical threshold of 90% for a cluster of 100 Knox IDBrokers, this test would return "Good" health if 95 or more Knox IDBrokers have good health. This test would return "Concerning" health if at least 90 Knox IDBrokers have either "Good" or "Concerning" health. If more than 10 Knox IDBrokers have bad health, this test would return "Bad" health. A failure of this health test indicates unhealthy Knox IDBrokers. Check the status of the individual Knox IDBrokers for more information. This test can be configured using the Knox Knox service-wide monitoring setting.

Short Name: Knox IDBroker Health

Healthy Knox IDBroker Monitoring Thresholds

Description

The health test thresholds of the overall Knox IDBroker health. The check returns "Concerning" health if the percentage of "Healthy" Knox IDBrokers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Knox IDBrokers falls below the critical threshold.

Template Name

`KNOX_IDBROKER_healthy_thresholds`

Default Value

critical:49.0, warning:99.0

Unit(s)

PERCENT

Knox Gateway Health Tests

Knox Gateway Audit Pipeline Test

This Knox Gateway health test checks that the Auditing for the Knox Gateway role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Knox Gateway process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Knox Gateway host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Knox Gateway monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Knox Gateway File Descriptors

This Knox Gateway health test checks that the number of file descriptors used does not rise above some percentage of the Knox Gateway file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Knox Gateway monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`knox_gateway_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Knox Gateway Host Health

This Knox Gateway health test factors in the health of the host upon which the Knox Gateway is running. A failure of this test means that the host running the Knox Gateway is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Knox Gateway Host Health Test Knox Gateway monitoring setting.

Short Name: Host Health

Knox Gateway Host Health Test

Description

When computing the overall Knox Gateway health, consider the host's health.

Template Name

`knox_gateway_host_health_enabled`

Default Value

true

Unit(s)

no unit

Knox Gateway Log Directory Free Space

This Knox Gateway health test checks that the filesystem containing the log directory of this Knox Gateway has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Knox Gateway monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Knox Gateway Process Status

This Knox Gateway health test checks that the Cloudera Manager Agent on the Knox Gateway host is heart beating correctly and that the process associated with the Knox Gateway role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Knox Gateway process, a lack of connectivity to the Cloudera Manager Agent on the Knox Gateway host, or a problem with the Cloudera Manager Agent. This test can fail either because the Knox Gateway has crashed or because the Knox Gateway will not start or stop in a timely fashion. Check the Knox Gateway logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Knox Gateway host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Knox Gateway host, or look in the Cloudera Manager Agent logs on the Knox Gateway host for more details. This test can be enabled or disabled using the Knox Gateway Process Health Test Knox Gateway monitoring setting.

Short Name: Process Status

Knox Gateway Process Health Test

Description

Enables the health test that the Knox Gateway's process state is consistent with the role configuration

Template Name

`knox_gateway_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Knox Gateway Swap Memory Usage

This Knox Gateway health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Knox Gateway Unexpected Exits

This Knox Gateway health test checks that the Knox Gateway has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Knox Gateway monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Knox IDBroker Health Tests

Knox IDBroker Audit Pipeline Test

This Knox IDBroker health test checks that the Auditing for the Knox IDBroker role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Knox IDBroker process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Knox IDBroker host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Knox IDBroker monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Knox IDBroker File Descriptors

This Knox IDBroker health test checks that the number of file descriptors used does not rise above some percentage of the Knox IDBroker file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Knox IDBroker monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`idbroker_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Knox IDBroker Host Health

This Knox IDBroker health test factors in the health of the host upon which the Knox IDBroker is running. A failure of this test means that the host running the Knox IDBroker is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Knox IDBroker Host Health Test Knox IDBroker monitoring setting.

Short Name: Host Health

Knox IDBroker Host Health Test

Description

When computing the overall Knox IDBroker health, consider the host's health.

Template Name

`idbroker_host_health_enabled`

Default Value

true

Unit(s)

no unit

Knox IDBroker Log Directory Free Space

This Knox IDBroker health test checks that the filesystem containing the log directory of this Knox IDBroker has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Knox IDBroker monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Knox IDBroker Process Status

This Knox IDBroker health test checks that the Cloudera Manager Agent on the Knox IDBroker host is heart beating correctly and that the process associated with the Knox IDBroker role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Knox IDBroker process, a lack of connectivity to the Cloudera Manager Agent on the Knox IDBroker host, or a problem with the Cloudera Manager Agent. This test can fail either because the Knox IDBroker has crashed or because the Knox IDBroker will not start or stop in a timely fashion. Check the Knox IDBroker logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Knox IDBroker host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Knox IDBroker host, or look in the Cloudera Manager Agent logs on the Knox IDBroker host for more details. This test can be enabled or disabled using the Knox IDBroker Process Health Test Knox IDBroker monitoring setting.

Short Name: Process Status

Knox IDBroker Process Health Test

Description

Enables the health test that the Knox IDBroker's process state is consistent with the role configuration

Template Name

`idbroker_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Knox IDBroker Swap Memory Usage

This Knox IDBroker health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Knox IDBroker Unexpected Exits

This Knox IDBroker health test checks that the Knox IDBroker has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Knox IDBroker monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Kudu Health Tests

Kudu Master Health

This is a Kudu service-level health test that checks that enough of the Masters in the cluster are healthy. The test returns "Concerning" health if the number of healthy Masters falls below a warning threshold, expressed as a percentage of the total number of Masters. The test returns "Bad" health if the number of healthy and "Concerning" Masters falls below a critical threshold, expressed as a percentage of the total number of Masters. For example, if this test is configured with a warning threshold of 95% and a critical threshold of 90% for a cluster of 100 Masters, this test would return "Good" health if 95 or more Masters have good health. This test would return "Concerning" health

if at least 90 Masters have either "Good" or "Concerning" health. If more than 10 Masters have bad health, this test would return "Bad" health. A failure of this health test indicates unhealthy Masters. Check the status of the individual Masters for more information. This test can be configured using the Kudu Kudu service-wide monitoring setting.

Short Name: Master Health

Healthy Master Monitoring Thresholds

Description

The health test thresholds of the overall Master health. The check returns "Concerning" health if the percentage of "Healthy" Masters falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Masters falls below the critical threshold.

Template Name

`KUDU_KUDU_MASTER_healthy_thresholds`

Default Value

critical:60.0, warning:80.1

Unit(s)

PERCENT

Kudu Tablet Server Health

This is a Kudu service-level health test that checks that enough of the Tablet Servers in the cluster are healthy. The test returns "Concerning" health if the number of healthy Tablet Servers falls below a warning threshold, expressed as a percentage of the total number of Tablet Servers. The test returns "Bad" health if the number of healthy and "Concerning" Tablet Servers falls below a critical threshold, expressed as a percentage of the total number of Tablet Servers. For example, if this test is configured with a warning threshold of 95% and a critical threshold of 90% for a cluster of 100 Tablet Servers, this test would return "Good" health if 95 or more Tablet Servers have good health. This test would return "Concerning" health if at least 90 Tablet Servers have either "Good" or "Concerning" health. If more than 10 Tablet Servers have bad health, this test would return "Bad" health. A failure of this health test indicates unhealthy Tablet Servers. Check the status of the individual Tablet Servers for more information. This test can be configured using the Kudu Kudu service-wide monitoring setting.

Short Name: Tablet Server Health

Healthy Tablet Server Monitoring Thresholds

Description

The health test thresholds of the overall Tablet Server health. The check returns "Concerning" health if the percentage of "Healthy" Tablet Servers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Tablet Servers falls below the critical threshold.

Template Name

`KUDU_KUDU_TSERVER_healthy_thresholds`

Default Value

critical:50.0, warning:75.0

Unit(s)

PERCENT

LLAP Proxy Health Tests

LLAP Proxy Audit Pipeline Test

This LLAP Proxy health test checks that the Auditing for the LLAP Proxy role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of LLAP Proxy process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the LLAP Proxy host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check LLAP Proxy monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

LLAP Proxy File Descriptors

This LLAP Proxy health test checks that the number of file descriptors used does not rise above some percentage of the LLAP Proxy file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds LLAP Proxy monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`llapproxy_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

LLAP Proxy Heap Dump Directory Free Space

This LLAP Proxy health test checks that the filesystem containing the heap dump directory of this LLAP Proxy has sufficient free space. This test can be configured using the Heap Dump Directory Free Space Monitoring Absolute Thresholds and Heap Dump Directory Free Space Monitoring Percentage Thresholds LLAP Proxy monitoring settings.

Short Name: Heap Dump Directory Free Space

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Template Name

`heap_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`heap_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

LLAP Proxy Host Health

This LLAP Proxy health test factors in the health of the host upon which the LLAP Proxy is running. A failure of this test means that the host running the LLAP Proxy is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the LLAP Proxy Host Health Test LLAP Proxy monitoring setting.

Short Name: Host Health

LLAP Proxy Host Health Test

Description

When computing the overall LLAP Proxy health, consider the host's health.

Template Name

`llapproxy_host_health_enabled`

Default Value

true

Unit(s)

no unit

LLAP Proxy LLAP Daemons Ready Check

This is an LLAP daemons health test that checks whether LLAP daemons are ready to process queries. This test can be configured using the LLAP Proxy and Hive LLAP Daemons Ready Status Thresholds llap_proxy monitoring settings.

Short Name: LLAP Daemons Ready Check

Hive LLAP Daemons Ready Status Startup Tolerance

Description

Bad health state will be shown if, after this amount of time (after starting LLAP proxy role), 0 LLAP daemons are running.

Template Name

`llapd_ready_status_check_daemon_startup_tolerance`

Default Value

300

Unit(s)

SECONDS

Hive LLAP Daemons Ready Status Thresholds

Description

The health test thresholds for monitoring the number of active LLAP daemons.

Template Name

`llapd_ready_status_thresholds`

Default Value

critical:25.0, warning:75.0

Unit(s)

no unit

Hive LLAP Proxy Role Ready Status Startup Tolerance

Description

Startup Tolerance time of the LLAP proxy role in which no health test is run. This is recommended to be kept minimal.

Template Name

`llapd_ready_status_check_role_startup_tolerance`

Default Value

1

Unit(s)

SECONDS

LLAP Proxy Log Directory Free Space

This LLAP Proxy health test checks that the filesystem containing the log directory of this LLAP Proxy has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds LLAP Proxy monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

LLAP Proxy Pause Duration

This LLAP Proxy health test checks that the LLAP Proxy threads are not experiencing long scheduling pauses. The test uses a pause monitoring thread in the LLAP Proxy that tracks scheduling delay by noting if it is run on its requested schedule. If the thread is not run on its requested schedule, the delay is noted and considered pause time. The health test checks that no more than some percentage of recent time is spent paused. A failure of this health test may indicate that the LLAP Proxy is not getting enough CPU resources, or that it is spending too much time doing garbage collection. Inspect the LLAP Proxy logs for any pause monitor output and check garbage collection metrics exposed by the LLAP Proxy. This test can be configured using the Pause Duration Thresholds and Pause Duration Monitoring Period LLAP Proxy monitoring settings.

Short Name: Pause Duration

Pause Duration Monitoring Period

Description

The period to review when computing the moving average of extra time the pause monitor spent paused.

Template Name

`llapproxy_pause_duration_window`

Default Value

5

Unit(s)

MINUTES

Pause Duration Thresholds

Description

The health test thresholds for the weighted average extra time the pause monitor spent paused. Specified as a percentage of elapsed wall clock time.

Template Name

`llapproxy_pause_duration_thresholds`

Default Value

critical:60.0, warning:30.0

Unit(s)

no unit

LLAP Proxy Process Status

This LLAP Proxy health test checks that the Cloudera Manager Agent on the LLAP Proxy host is heart beating correctly and that the process associated with the LLAP Proxy role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the LLAP Proxy process, a lack of connectivity to the Cloudera Manager Agent on the LLAP Proxy host, or a problem with the Cloudera Manager Agent. This test can fail either because the LLAP Proxy has crashed or because the LLAP Proxy will not start or stop in a timely fashion. Check the LLAP Proxy logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the LLAP Proxy host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the LLAP Proxy host, or look in the Cloudera Manager Agent logs on the LLAP Proxy host for more details. This test can be enabled or disabled using the LLAP Proxy Process Health Test LLAP Proxy monitoring setting.

Short Name: Process Status

LLAP Proxy Process Health Test

Description

Enables the health test that the LLAP Proxy's process state is consistent with the role configuration

Template Name

`llapproxy_scm_health_enabled`

Default Value

true

Unit(s)

no unit

LLAP Proxy Swap Memory Usage

This LLAP Proxy health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

LLAP Proxy Unexpected Exits

This LLAP Proxy health test checks that the LLAP Proxy has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period LLAP Proxy monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Lily HBase Indexer Health Tests

Lily HBase Indexer Audit Pipeline Test

This Lily HBase Indexer health test checks that the Auditing for the Lily HBase Indexer role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Lily HBase Indexer process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Lily HBase Indexer host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Lily HBase Indexer monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Lily HBase Indexer File Descriptors

This Lily HBase Indexer health test checks that the number of file descriptors used does not rise above some percentage of the Lily HBase Indexer file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Lily HBase Indexer monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`hbase_indexer_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Lily HBase Indexer Heap Dump Directory Free Space

This Lily HBase Indexer health test checks that the filesystem containing the heap dump directory of this Lily HBase Indexer has sufficient free space. This test can be configured using the Heap Dump Directory Free Space Monitoring Absolute Thresholds and Heap Dump Directory Free Space Monitoring Percentage Thresholds Lily HBase Indexer monitoring settings.

Short Name: Heap Dump Directory Free Space

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Template Name

`heap_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`heap_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Lily HBase Indexer Host Health

This Lily HBase Indexer health test factors in the health of the host upon which the Lily HBase Indexer is running. A failure of this test means that the host running the Lily HBase Indexer is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Lily HBase Indexer Host Health Test Lily HBase Indexer monitoring setting.

Short Name: Host Health

Lily HBase Indexer Host Health Test

Description

When computing the overall Lily HBase Indexer health, consider the host's health.

Template Name

`hbase_indexer_host_health_enabled`

Default Value

true

Unit(s)

no unit

Lily HBase Indexer Log Directory Free Space

This Lily HBase Indexer health test checks that the filesystem containing the log directory of this Lily HBase Indexer has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Lily HBase Indexer monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Lily HBase Indexer Process Status

This Lily HBase Indexer health test checks that the Cloudera Manager Agent on the Lily HBase Indexer host is heart beating correctly and that the process associated with the Lily HBase Indexer role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Lily HBase Indexer process, a lack of connectivity to the Cloudera Manager Agent on the Lily HBase Indexer host, or a problem with the Cloudera

Manager Agent. This test can fail either because the Lily HBase Indexer has crashed or because the Lily HBase Indexer will not start or stop in a timely fashion. Check the Lily HBase Indexer logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Lily HBase Indexer host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Lily HBase Indexer host, or look in the Cloudera Manager Agent logs on the Lily HBase Indexer host for more details. This test can be enabled or disabled using the Lily HBase Indexer Process Health Test Lily HBase Indexer monitoring setting.

Short Name: Process Status

Lily HBase Indexer Process Health Test

Description

Enables the health test that the Lily HBase Indexer's process state is consistent with the role configuration

Template Name

`hbase_indexer_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Lily HBase Indexer Swap Memory Usage

This Lily HBase Indexer health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Lily HBase Indexer Unexpected Exits

This Lily HBase Indexer health test checks that the Lily HBase Indexer has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Lily HBase Indexer monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Livy Health Tests

Livy Server Health

This Livy service-level health test checks for the presence of a running, healthy Livy Server. The test returns "Bad" health if the service is running and the Livy Server is not running. In all other cases it returns the health of the Livy Server. A failure of this health test indicates a stopped or unhealthy Livy Server. Check the status of the Livy Server for more information. This test can be enabled or disabled using the Livy Server Role Health Test Livy Server service-wide monitoring setting.

Short Name: Livy Server Health

Livy Server Role Health Test

Description

When computing the overall LIVY health, consider Livy Server's health

Template Name

`LIVY_LIVY_SERVER_health_enabled`

Default Value

true

Unit(s)

no unit

Livy Server Health Tests

Livy Server Audit Pipeline Test

This Livy Server health test checks that the Auditing for the Livy Server role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Livy Server process. This test

can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Livy Server host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Livy Server monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Livy Server File Descriptors

This Livy Server health test checks that the number of file descriptors used does not rise above some percentage of the Livy Server file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Livy Server monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`livy_server_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Livy Server Host Health

This Livy Server health test factors in the health of the host upon which the Livy Server is running. A failure of this test means that the host running the Livy Server is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Livy Server Host Health Test Livy Server monitoring setting.

Short Name: Host Health

Livy Server Host Health Test

Description

When computing the overall Livy Server health, consider the host's health.

Template Name

`livy_server_host_health_enabled`

Default Value

true

Unit(s)

no unit

Livy Server Log Directory Free Space

This Livy Server health test checks that the filesystem containing the log directory of this Livy Server has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Livy Server monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Livy Server Process Status

This Livy Server health test checks that the Cloudera Manager Agent on the Livy Server host is heart beating correctly and that the process associated with the Livy Server role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Livy Server process, a lack of connectivity to the Cloudera Manager Agent on the Livy Server host, or a problem with the Cloudera Manager Agent. This test can fail either because the Livy Server has crashed or because the Livy Server will not start or stop in a timely fashion. Check the Livy Server logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Livy Server host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Livy Server host, or look in the Cloudera Manager Agent logs on the Livy Server host for more details. This test can be enabled or disabled using the Livy Server Process Health Test Livy Server monitoring setting.

Short Name: Process Status

Livy Server Process Health Test

Description

Enables the health test that the Livy Server's process state is consistent with the role configuration

Template Name

`livy_server_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Livy Server Swap Memory Usage

This Livy Server health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Livy Server Unexpected Exits

This Livy Server health test checks that the Livy Server has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Livy Server monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Load Balancer Health Tests

Load Balancer Audit Pipeline Test

This Load Balancer health test checks that the Auditing for the Load Balancer role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Load Balancer process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Load Balancer host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Load Balancer monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Load Balancer File Descriptors

This Load Balancer health test checks that the number of file descriptors used does not rise above some percentage of the Load Balancer file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Load Balancer monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`hue_load_balancer_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Load Balancer Heap Dump Directory Free Space

This Load Balancer health test checks that the filesystem containing the heap dump directory of this Load Balancer has sufficient free space. This test can be configured using the Heap Dump Directory Free Space Monitoring Absolute Thresholds and Heap Dump Directory Free Space Monitoring Percentage Thresholds Load Balancer monitoring settings.

Short Name: Heap Dump Directory Free Space

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Template Name

`heap_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`heap_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Load Balancer Host Health

This Load Balancer health test factors in the health of the host upon which the Load Balancer is running. A failure of this test means that the host running the Load Balancer is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Load Balancer Host Health Test Load Balancer monitoring setting.

Short Name: Host Health

Load Balancer Host Health Test

Description

When computing the overall Load Balancer health, consider the host's health.

Template Name

`hue_load_balancer_host_health_enabled`

Default Value

true

Unit(s)

no unit

Load Balancer Log Directory Free Space

This Load Balancer health test checks that the filesystem containing the log directory of this Load Balancer has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Load Balancer monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Load Balancer Process Status

This Load Balancer health test checks that the Cloudera Manager Agent on the Load Balancer host is heart beating correctly and that the process associated with the Load Balancer role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Load Balancer process, a lack of connectivity to the Cloudera Manager Agent on the Load Balancer host, or a problem with the Cloudera Manager Agent. This test can fail either because the Load Balancer has crashed or because the Load Balancer will not start or stop in a timely fashion. Check the Load Balancer logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Load Balancer host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Load Balancer host, or look in the Cloudera Manager Agent logs on the Load Balancer host for more details. This test can be enabled or disabled using the Load Balancer Process Health Test Load Balancer monitoring setting.

Short Name: Process Status

Load Balancer Process Health Test

Description

Enables the health test that the Load Balancer's process state is consistent with the role configuration

Template Name

`hue_load_balancer_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Load Balancer Swap Memory Usage

This Load Balancer health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Load Balancer Unexpected Exits

This Load Balancer health test checks that the Load Balancer has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Load Balancer monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

MapReduce Health Tests

MapReduce Failover Controllers Health

This is a MapReduce service-level health test that checks that all the Failover Controllers associated with this service are healthy and running. The test returns "Bad" health if any of Failover Controllers that the service depends on is unhealthy or not running. Check the Failover Controllers logs for more details This test can be enabled or disabled using the Failover Controllers Healthy service-wide monitoring setting.

Short Name: Failover Controllers Health

Failover Controllers Healthy

Description

Enables the health check that verifies that the failover controllers associated with this service are healthy and running.

Template Name

`failover_controllers_healthy_enabled`

Default Value

true

Unit(s)

no unit

MapReduce JobTracker Health

This is a MapReduce service-level health test that checks for and active, healthy JobTracker. The test returns "Bad" health if the service is running and an active JobTracker cannot be found. If an active JobTracker is found, then the test checks the health of that JobTracker as well as the health of any standby JobTracker configured. A "Good" health result will only be returned if both the active and Standby JobTrackers are healthy. A failure of this health test may indicate stopped or unhealthy JobTracker roles, or it may indicate a problem with communication between the Cloudera Manager Service Monitor and the JobTrackers. Check the status of the MapReduce service's JobTracker roles and look in the Cloudera Manager Service Monitor's log files for more information when this test fails. This test can be enabled or disabled using the JobTracker Role Health Test MapReduce service-wide monitoring setting. The check for a healthy standby JobTracker can be enabled or disabled with Standby JobTracker Health Test. In addition, the Active JobTracker Detection Window can be used to adjust the amount of time that the Cloudera Manager Service Monitor has to detect the active JobTracker before this health test fails, and the JobTracker Activation Startup Tolerance can be used to adjust the amount of time around JobTracker startup that the test allows for the JobTracker to be made active.

Short Name: JobTracker Health

Active JobTracker Detection Window

Description

The tolerance window that will be used in Mapreduce service tests that depend on detection of the active JobTracker.

Template Name

`mapreduce_active_jobtracker_detection_window`

Default Value

3

Unit(s)

MINUTES

JobTracker Activation Startup Tolerance

Description

The amount of time after JobTracker(s) start that the lack of an active JobTracker will be tolerated. This is intended to allow either the auto-failover daemon to make a JobTracker active, or a specifically issued failover command to take effect. This is an advanced option that does not often need to be changed.

Template Name

`mapreduce_jobtracker_activation_startup_tolerance`

Default Value

180

Unit(s)

SECONDS

JobTracker Role Health Test

Description

When computing the overall MapReduce cluster health, consider the JobTracker's health

Template Name

`mapreduce_jobtracker_health_enabled`

Default Value

true

Unit(s)

no unit

Standby JobTracker Health Test

Description

When computing the overall cluster health, consider the health of the standby JobTracker.

Template Name

`mapreduce_standby_jobtrackers_health_enabled`

Default Value

true

Unit(s)

no unit

MapReduce TaskTracker Health

This is a MapReduce service-level health test that checks that enough of the TaskTrackers in the cluster are healthy. The test returns "Concerning" health if the number of healthy TaskTrackers falls below a warning threshold, expressed as a percentage of the total number of TaskTrackers. The test returns "Bad" health if the number of healthy and "Concerning" TaskTrackers falls below a critical threshold, expressed as a percentage of the total number of TaskTrackers. For example, if this test is configured with a warning threshold of 95% and a critical threshold of 90% for a cluster of 100 TaskTrackers, this test would return "Good" health if 95 or more TaskTrackers have good health. This test would return "Concerning" health if at least 90 TaskTrackers have either "Good" or "Concerning" health. If more than 10 TaskTrackers have bad health, this test would return "Bad" health. A failure of this health test indicates unhealthy TaskTrackers. Check the status of the individual TaskTrackers for more information. This test can be configured using the MapReduce MapReduce service-wide monitoring setting.

Short Name: TaskTracker Health

Healthy TaskTracker Monitoring Thresholds

Description

The health test thresholds of the overall TaskTracker health. The check returns "Concerning" health if the percentage of "Healthy" TaskTrackers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" TaskTrackers falls below the critical threshold.

Template Name

`mapreduce_tasktrackers_healthy_thresholds`

Default Value

critical:90.0, warning:95.0

Unit(s)

PERCENT

Master Health Tests

Master Audit Pipeline Test

This Master health test checks that the Auditing for the Master role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Master process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Master host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Master monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Master Failed Data Directories

Short Name: Failed Data Directories

Master File Descriptors

This Master health test checks that the number of file descriptors used does not rise above some percentage of the Master file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Master monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`master_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Master Full Data Directories

Short Name: Full Data Directories

Master GC Duration

This Master health test checks that the Master is not spending too much time performing Java garbage collection. It checks that no more than some percentage of recent time is spent performing Java garbage collection. A failure of this health test may indicate a capacity planning problem or misconfiguration of the Master. This test can be configured using the Garbage Collection Duration Thresholds and Garbage Collection Duration Monitoring Period Master monitoring settings.

Short Name: GC Duration

Garbage Collection Duration Monitoring Period

Description

The period to review when computing the moving average of garbage collection time.

Template Name

`master_gc_duration_window`

Default Value

5

Unit(s)

MINUTES

Garbage Collection Duration Thresholds

Description

The health test thresholds for the weighted average time spent in Java garbage collection. Specified as a percentage of elapsed wall clock time.

Template Name

`master_gc_duration_thresholds`

Default Value

critical:60.0, warning:30.0

Unit(s)

no unit

Master HBase Master Canary

This is an HBase Master health test that checks that a client can connect to and get basic information from the Master in a reasonable amount of time. The test returns "Bad" health if the connection to or basic queries of the Master fail. The test returns "Concerning" health if the connection attempt or queries do not complete in a reasonable time. A failure of this health test may indicate that the Master is failing to satisfy basic client requests correctly or in a timely fashion. Check the status of the Master, and look in the Master logs for more details. This test can be enabled or disabled using the HBase Master Canary Health Test HBase Master monitoring setting.

Short Name: HBase Master Canary

HBase Master Canary Health Test

Description

Enables the health test that a client can connect to the HBase Master

Template Name

`master_canary_health_enabled`

Default Value

true

Unit(s)

no unit

Master HBase Regions In Transition Over Threshold

This is an HBase Master health test that checks whether there are regions staying in transition state for a duration longer than the configured threshold in HBase. The test returns "Bad" health if there are regions in transition over the threshold. A failure of this health test may indicate configuration errors or corrupted hfiles. Check the status of the Master, and look into the Master UI for more details. This test can be enabled or disabled using the HBase Regions In Transition Over Threshold Health Test HBase Master monitoring setting.

Short Name: HBase Regions In Transition Over Threshold

HBase Regions In Transition Over Threshold Health Test

Description

Enable the health test that checks if there are regions in transition over the threshold configured in HBase.

Template Name

`master_regions_in_transition_health_enabled`

Default Value

CDH=[[CDH 5.0.0..CDH 8.0.0)=true]

Unit(s)

no unit

Master Heap Dump Directory Free Space

This Master health test checks that the filesystem containing the heap dump directory of this Master has sufficient free space. This test can be configured using the Heap Dump Directory Free Space Monitoring Absolute Thresholds and Heap Dump Directory Free Space Monitoring Percentage Thresholds Master monitoring settings.

Short Name: Heap Dump Directory Free Space

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Template Name

`heap_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`heap_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Master Host Health

This Master health test factors in the health of the host upon which the Master is running. A failure of this test means that the host running the Master is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Master Host Health Test Master monitoring setting.

Short Name: Host Health

Master Host Health Test

Description

When computing the overall Master health, consider the host's health.

Template Name

`master_host_health_enabled`

Default Value

true

Unit(s)

no unit

Master Log Directory Free Space

This Master health test checks that the filesystem containing the log directory of this Master has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Master monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Master Process Status

This Master health test checks that the Cloudera Manager Agent on the Master host is heart beating correctly and that the process associated with the Master role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Master process, a lack of connectivity to the Cloudera Manager Agent on the Master host, or a problem with the Cloudera Manager Agent. This test can fail either because the Master has crashed or because the Master will not start or stop in a timely fashion. Check the Master logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Master host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Master host, or look in the Cloudera Manager Agent logs on the Master host for more details. This test can be enabled or disabled using the Master Process Health Test Master monitoring setting.

Short Name: Process Status

Master Process Health Test

Description

Enables the health test that the Master's process state is consistent with the role configuration

Template Name

`master_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Master Swap Memory Usage

This Master health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Master Unexpected Exits

This Master health test checks that the Master has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical

threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Master monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Master Web Server Status

This health test checks that the role's web server is responding quickly to requests by the Cloudera Manager Agent, and that the Cloudera Manager Agent can collect metrics from the web server. Failure of this health test may indicate a problem with the web server of the Master, a misconfiguration of the Master, or a problem with the Cloudera Manager Agent. Consult the Cloudera Manager Agent logs and the logs of the Master for more detail. If the test failure message indicates a communication problem, the Cloudera Manager Agent's HTTP requests to the Master's web server are failing or timing out. If the test's failure message indicates an unexpected response, the Master's web server responded to the Cloudera Manager Agent's request, but the response could not be interpreted for some reason. This test can be configured using the Web Metric Collection Master monitoring setting.

Short Name: Web Server Status

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Template Name

`master_web_metric_collection_enabled`

Default Value

true

Unit(s)

no unit

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Template Name

`master_web_metric_collection_thresholds`

Default Value

critical:never, warning:10000.0

Unit(s)

MILLISECONDS

Monitor Health Tests

Monitor Audit Pipeline Test

This Monitor health test checks that the Auditing for the Monitor role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Monitor process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Monitor host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Monitor monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Monitor File Descriptors

This Monitor health test checks that the number of file descriptors used does not rise above some percentage of the Monitor file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Monitor monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`accumulo_monitor_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Monitor Host Health

This Monitor health test factors in the health of the host upon which the Monitor is running. A failure of this test means that the host running the Monitor is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Monitor Host Health Test Monitor monitoring setting.

Short Name: Host Health

Monitor Host Health Test

Description

When computing the overall Monitor health, consider the host's health.

Template Name

`accumulo_monitor_host_health_enabled`

Default Value

true

Unit(s)

no unit

Monitor Log Directory Free Space

This Monitor health test checks that the filesystem containing the log directory of this Monitor has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Monitor monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Monitor Process Status

This Monitor health test checks that the Cloudera Manager Agent on the Monitor host is heart beating correctly and that the process associated with the Monitor role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Monitor process, a lack of connectivity to the Cloudera Manager Agent on the Monitor host, or a problem with the Cloudera Manager Agent. This test can fail either because the Monitor has crashed or because the Monitor will not start or stop in a timely fashion. Check the Monitor logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Monitor host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Monitor host, or look in the Cloudera Manager Agent logs on the Monitor host for more details. This test can be enabled or disabled using the Monitor Process Health Test Monitor monitoring setting.

Short Name: Process Status

Monitor Process Health Test

Description

Enables the health test that the Monitor's process state is consistent with the role configuration

Template Name

`accumulo_monitor_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Monitor Swap Memory Usage

This Monitor health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Monitor Unexpected Exits

This Monitor health test checks that the Monitor has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Monitor monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

NFS Gateway Health Tests

NFS Gateway Audit Pipeline Test

This NFS Gateway health test checks that the Auditing for the NFS Gateway role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of NFS Gateway process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the NFS Gateway host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check NFS Gateway monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

NFS Gateway File Descriptors

This NFS Gateway health test checks that the number of file descriptors used does not rise above some percentage of the NFS Gateway file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds NFS Gateway monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`nfsgateway_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

NFS Gateway Heap Dump Directory Free Space

This NFS Gateway health test checks that the filesystem containing the heap dump directory of this NFS Gateway has sufficient free space. This test can be configured using the Heap Dump Directory Free Space Monitoring Absolute Thresholds and Heap Dump Directory Free Space Monitoring Percentage Thresholds NFS Gateway monitoring settings.

Short Name: Heap Dump Directory Free Space

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Template Name

`heap_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`heap_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

NFS Gateway Host Health

This NFS Gateway health test factors in the health of the host upon which the NFS Gateway is running. A failure of this test means that the host running the NFS Gateway is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the NFS Gateway Host Health Test NFS Gateway monitoring setting.

Short Name: Host Health

NFS Gateway Host Health Test

Description

When computing the overall NFS Gateway health, consider the host's health.

Template Name

`nfsgateway_host_health_enabled`

Default Value

true

Unit(s)

no unit

NFS Gateway Log Directory Free Space

This NFS Gateway health test checks that the filesystem containing the log directory of this NFS Gateway has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds NFS Gateway monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

NFS Gateway Process Status

This NFS Gateway health test checks that the Cloudera Manager Agent on the NFS Gateway host is heart beating correctly and that the process associated with the NFS Gateway role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the NFS Gateway process, a lack of connectivity to the Cloudera Manager Agent on the NFS Gateway host, or a problem with the Cloudera Manager Agent. This test can fail either because the NFS Gateway has crashed or because the NFS Gateway will not start or stop in a timely fashion. Check the NFS Gateway logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the NFS Gateway host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the NFS Gateway host, or look in the Cloudera Manager Agent logs on the NFS Gateway host for more details. This test can be enabled or disabled using the NFS Gateway Process Health Test NFS Gateway monitoring setting.

Short Name: Process Status

NFS Gateway Process Health Test

Description

Enables the health test that the NFS Gateway's process state is consistent with the role configuration

Template Name

`nfsgateway_scm_health_enabled`

Default Value

true

Unit(s)

no unit

NFS Gateway Swap Memory Usage

This NFS Gateway health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

NFS Gateway Temporary Dump Directory Free Space

This is a NFS Gateway health test that checks that the filesystem containing the Temporary Dump Directory of this NFS Gateway has sufficient free space. See the Temporary Dump Directory description on the NFS Gateway configuration page for more information on this directory type. This test can be configured using the Temporary Dump Directory Free Space Monitoring Absolute Thresholds and Temporary Dump Directory Free Space Monitoring Percentage Thresholds NFS Gateway monitoring settings.

Short Name: Temporary Dump Directory Free Space

Temporary Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Temporary Dump Directory.

Template Name

`nfsgateway_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Temporary Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Temporary Dump Directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Temporary Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`nfsgateway_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

NFS Gateway Unexpected Exits

This NFS Gateway health test checks that the NFS Gateway has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period NFS Gateway monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

NameNode Health Tests

NameNode Audit Pipeline Test

This NameNode health test checks that the Auditing for the NameNode role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of NameNode process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the NameNode host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check NameNode monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

NameNode Checkpoint Status

This is a NameNode health test that checks the NameNode's filesystem checkpoint is no older than some percentage of the Filesystem Checkpoint Period and that the number of transactions that have occurred since the last filesystem checkpoint does not exceed some percentage of the Filesystem Checkpoint Transaction Limit. A failure of this health test may indicate a problem with the active NameNode or its configured checkpointing role, i.e. either a standby NameNode or a SecondaryNameNode. Check the NameNode logs or the logs of the checkpointing role for more details. This test can be configured using the Filesystem Checkpoint Age Monitoring Thresholds and Filesystem Checkpoint Transactions Monitoring Thresholds NameNode monitoring setting.

Short Name: Checkpoint Status

Filesystem Checkpoint Age Monitoring Thresholds

Description

The health test thresholds of the age of the HDFS namespace checkpoint. Specified as a percentage of the configured checkpoint interval.

Template Name

`namenode_checkpoint_age_thresholds`

Default Value

critical:400.0, warning:200.0

Unit(s)

PERCENT

Filesystem Checkpoint Transactions Monitoring Thresholds

Description

The health test thresholds of the number of transactions since the last HDFS namespace checkpoint. Specified as a percentage of the configured checkpointing transaction limit.

Template Name

`namenode_checkpoint_transactions_thresholds`

Default Value

critical:400.0, warning:200.0

Unit(s)

PERCENT

NameNode File Descriptors

This NameNode health test checks that the number of file descriptors used does not rise above some percentage of the NameNode file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds NameNode monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`namenode_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

NameNode Heap Dump Directory Free Space

This NameNode health test checks that the filesystem containing the heap dump directory of this NameNode has sufficient free space. This test can be configured using the Heap Dump Directory Free Space Monitoring Absolute Thresholds and Heap Dump Directory Free Space Monitoring Percentage Thresholds NameNode monitoring settings.

Short Name: Heap Dump Directory Free Space

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Template Name

`heap_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`heap_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

NameNode Host Health

This NameNode health test factors in the health of the host upon which the NameNode is running. A failure of this test means that the host running the NameNode is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the NameNode Host Health Test NameNode monitoring setting.

Short Name: Host Health

NameNode Host Health Test

Description

When computing the overall NameNode health, consider the host's health.

Template Name

`namenode_host_health_enabled`

Default Value

true

Unit(s)

no unit

NameNode JournalNode Sync Status

This is a NameNode health test that checks that the NameNode is not out-of-sync with too many JournalNodes. This test is disabled if Quorum-based storage is not in use.A failure of this health test may indicate a problem with the JournalNodes or a communication problem between the NameNode and the JournalNodes. Check the NameNode and the JournalNode logs for more details.This test can be configured using the NameNode Out-Of-Sync JournalNodes Thresholds NameNode monitoring setting.

Short Name: JournalNode Sync Status

NameNode Out-Of-Sync JournalNodes Thresholds

Description

The health check thresholds for the number of out-of-sync JournalNodes for this NameNode.

Template Name

`namenode_out_of_sync_journal_nodes_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

NameNode Log Directory Free Space

This NameNode health test checks that the filesystem containing the log directory of this NameNode has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds NameNode monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

NameNode Name Directory Status

This is a NameNode health test that checks for whether the NameNode has reported any failed data directories. A failure of this health test indicates that there is a problem with one or more data directories on the NameNode. See the NameNode system web UI for more information. Note that unless the configuration dfs.namenode.name.dir.restore is configured to true, the NameNode will require a restart to recognize data directories that have been restored (e.g., after an NFS outage). This test can be configured using the NameNode Directory Failures Thresholds NameNode monitoring setting.

Short Name: Name Directory Status

NameNode Directory Failures Thresholds

Description

The health test thresholds of failed status directories in a NameNode.

Template Name

`namenode_directory_failures_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

NameNode NameNode Data Directories Free Space

This is a NameNode health test that checks that the filesystem containing the NameNode Data Directories of this NameNode has sufficient free space. See the NameNode Data Directories description on the NameNode configuration page for more information on this directory type. This test can be configured using the NameNode Data Directories Free Space Monitoring Absolute Thresholds and NameNode Data Directories Free Space Monitoring Percentage Thresholds NameNode monitoring settings.

Short Name: NameNode Data Directories Free Space

NameNode Data Directories Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's NameNode Data Directories.

Template Name

`namenode_data_directories_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

NameNode Data Directories Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's NameNode Data Directories. Specified as a percentage of the capacity on that filesystem. This setting is not used if a NameNode Data Directories Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`namenode_data_directories_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

NameNode Pause Duration

This NameNode health test checks that the NameNode threads are not experiencing long scheduling pauses. The test uses a pause monitoring thread in the NameNode that tracks scheduling delay by noting if it is run on its requested schedule. If the thread is not run on its requested schedule, the delay is noted and considered pause time. The health test checks that no more than some percentage of recent time is spent paused. A failure of this health test may indicate that the NameNode is not getting enough CPU resources, or that it is spending too much time doing garbage collection. Inspect the NameNode logs for any pause monitor output and check garbage collection metrics exposed by the NameNode. This test can be configured using the Pause Duration Thresholds and Pause Duration Monitoring Period NameNode monitoring settings.

Short Name: Pause Duration

Pause Duration Monitoring Period

Description

The period to review when computing the moving average of extra time the pause monitor spent paused.

Template Name

`namenode_pause_duration_window`

Default Value

5

Unit(s)

MINUTES

Pause Duration Thresholds

Description

The health test thresholds for the weighted average extra time the pause monitor spent paused. Specified as a percentage of elapsed wall clock time.

Template Name

`namenode_pause_duration_thresholds`

Default Value

critical:60.0, warning:30.0

Unit(s)

no unit

NameNode Process Status

This NameNode health test checks that the Cloudera Manager Agent on the NameNode host is heart beating correctly and that the process associated with the NameNode role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the NameNode process, a lack of connectivity to the Cloudera Manager Agent on the NameNode host, or a problem with the Cloudera Manager Agent. This test can fail either because the NameNode has crashed or because the NameNode will not start or stop in a timely fashion. Check the NameNode logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the NameNode host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the NameNode host, or look in the Cloudera Manager Agent logs on the NameNode host for more details. This test can be enabled or disabled using the NameNode Process Health Test NameNode monitoring setting.

Short Name: Process Status

NameNode Process Health Test

Description

Enables the health test that the NameNode's process state is consistent with the role configuration

Template Name

`namenode_scm_health_enabled`

Default Value

true

Unit(s)

no unit

NameNode RPC Latency

This is a NameNode health test that checks that a moving average of the average time it takes for the NameNode to respond to requests does not exceed some value. A failure of this health test could indicate misconfiguration of the NameNode, that the NameNode is having a problem writing to one of its data directories, or may indicate a capacity planning problem. Check the NameNode's RpcQueueTime_avg_time and if this indicates that the bulk of the RPC latency is spent with requests queued, try increasing the NameNode Handler Count. If the NameNode's RpcProcessingTime_avg_time indicates the bulk of the RPC latency is due to request processing, check to see that each of the directories in which the HDFS metadata is being stored is performing adequately. This test can be configured using the NameNode RPC Latency Thresholds and NameNode RPC Latency Monitoring Window NameNode monitoring settings.

Short Name: RPC Latency

NameNode RPC Latency Monitoring Window

Description

The period to review when computing the moving average of the NameNode's RPC latency.

Template Name

`namenode_rpc_latency_window`

Default Value

5

Unit(s)

MINUTES

NameNode RPC Latency Thresholds

Description

The health check thresholds of the NameNode's RPC latency.

Template Name

`namenode_rpc_latency_thresholds`

Default Value

critical:5000.0, warning:1000.0

Unit(s)

MILLISECONDS

NameNode Rolling Upgrade Status

This is a NameNode health test that checks for the presence of an unfinalized HDFS rolling metadata upgrade. If an unfinalized HDFS rolling meatadata upgrade is detected, this test returns "Concerning" health. A failure of this health test indicates that a previously performed rolling metadata upgrade needs to be finalized. This can be done via HDFS Finalize Rolling Metadata Upgrade command. This test can be enabled or disabled using the HDFS Rolling Metadata Upgrade Status Health Test NameNode monitoring setting.

Short Name: Rolling Upgrade Status

HDFS Rolling Metadata Upgrade Status Health Test

Description

Enables the health test of the rolling metadata upgrade status of the NameNode. This covers rolling metadata upgrades. Nonrolling metadata upgrades are covered in a separate health test.

Template Name

`namenode_rolling_upgrade_status_enabled`

Default Value

true

Unit(s)

no unit

NameNode Safe Mode Status

This is a NameNode health test that checks that the NameNode is not in safemode. A failure of this health test indicates that the NameNode is in safemode. Look in the NameNode logs for more details. This test can be enabled or disabled using the NameNode Safemode Health Test NameNode monitoring setting. The Health Test Startup Tolerance NameNode monitoring setting also controls the amount of time at NameNode start up to tolerate safemode.

Short Name: Safe Mode Status

Health Test Startup Tolerance

Description

The amount of time allowed after this role is started that failures of health tests that rely on communication with this role will be tolerated.

Template Name

`namenode_startup_tolerance`

Default Value

5

Unit(s)

MINUTES

NameNode Safemode Health Test

Description

Enables the health test that the NameNode is not in safemode

Template Name

`namenode_safe_mode_enabled`

Default Value

true

Unit(s)

no unit

NameNode Swap Memory Usage

This NameNode health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

NameNode Unexpected Exits

This NameNode health test checks that the NameNode has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period NameNode monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

NameNode Upgrade Status

This is a NameNode health test that checks for the presence of an unfinalized HDFS metadata upgrade. If an unfinalized HDFS metadata upgrade is detected, this test returns "Concerning" health. A failure of this health test indicates that a previously performed HDFS upgrade needs to be finalized. This can be done via the Finalize Metadata Upgrade NameNode command linked above. This test can be enabled or disabled using the HDFS Metadata Upgrade Status Health Test NameNode monitoring setting.

Short Name: Upgrade Status

HDFS Metadata Upgrade Status Health Test

Description

Enables the health test of the metadata upgrade status of the NameNode. This covers nonrolling metadata upgrades. Rolling metadata upgrades are covered in a separate health test.

Template Name

`namenode_upgrade_status_enabled`

Default Value

true

Unit(s)

no unit

NameNode Web Server Status

This health test checks that the role's web server is responding quickly to requests by the Cloudera Manager Agent, and that the Cloudera Manager Agent can collect metrics from the web server. Failure of this health test may indicate a problem with the web server of the NameNode, a misconfiguration of the NameNode, or a problem with the Cloudera Manager Agent. Consult the Cloudera Manager Agent logs and the logs of the NameNode for more detail. If the test failure message indicates a communication problem, the Cloudera Manager Agent's HTTP requests to the NameNode's web server are failing or timing out. If the test's failure message indicates an unexpected response, the NameNode's web server responded to the Cloudera Manager Agent's request, but the response could not be interpreted for some reason. This test can be configured using the Web Metric Collection NameNode monitoring setting.

Short Name: Web Server Status

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Template Name

`namenode_web_metric_collection_enabled`

Default Value

true

Unit(s)

no unit

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Template Name

`namenode_web_metric_collection_thresholds`

Default Value

critical:never, warning:10000.0

Unit(s)

MILLISECONDS

Navigator Audit Server Health Tests

Navigator Audit Server Audit Pipeline Test

This Navigator Audit Server health test checks that the Auditing for the Navigator Audit Server role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Navigator Audit Server process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Navigator Audit Server host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Navigator Audit Server monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Navigator Audit Server File Descriptors

This Navigator Audit Server health test checks that the number of file descriptors used does not rise above some percentage of the Navigator Audit Server file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Navigator Audit Server monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`navigator_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Navigator Audit Server GC Duration

This Navigator Audit Server health test checks that the Navigator Audit Server is not spending too much time performing Java garbage collection. It checks that no more than some percentage of recent time is spent performing Java garbage collection. A failure of this health test may indicate a capacity planning problem or misconfiguration of the Navigator Audit Server. This test can be configured using the Garbage Collection Duration Thresholds and Garbage Collection Duration Monitoring Period Navigator Audit Server monitoring settings.

Short Name: GC Duration

Garbage Collection Duration Monitoring Period

Description

The period to review when computing the moving average of garbage collection time.

Template Name

`navigator_gc_duration_window`

Default Value

5

Unit(s)

MINUTES

Garbage Collection Duration Thresholds

Description

The health test thresholds for the weighted average time spent in Java garbage collection. Specified as a percentage of elapsed wall clock time.

Template Name

`navigator_gc_duration_thresholds`

Default Value

critical:60.0, warning:30.0

Unit(s)

no unit

Navigator Audit Server Heap Dump Directory Free Space

This Navigator Audit Server health test checks that the filesystem containing the heap dump directory of this Navigator Audit Server has sufficient free space. This test can be configured using the Heap Dump Directory Free Space Monitoring Absolute Thresholds and Heap Dump Directory Free Space Monitoring Percentage Thresholds Navigator Audit Server monitoring settings.

Short Name: Heap Dump Directory Free Space

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Template Name

`heap_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`heap_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Navigator Audit Server Host Health

This Navigator Audit Server health test factors in the health of the host upon which the Navigator Audit Server is running. A failure of this test means that the host running the Navigator Audit Server is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Navigator Audit Server Host Health Test Navigator Audit Server monitoring setting.

Short Name: Host Health

Navigator Audit Server Host Health Test

Description

When computing the overall Navigator Audit Server health, consider the host's health.

Template Name

`navigator_host_health_enabled`

Default Value

true

Unit(s)

no unit

Navigator Audit Server Log Directory Free Space

This Navigator Audit Server health test checks that the filesystem containing the log directory of this Navigator Audit Server has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Navigator Audit Server monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Navigator Audit Server Process Status

This Navigator Audit Server health test checks that the Cloudera Manager Agent on the Navigator Audit Server host is heart beating correctly and that the process associated with the Navigator Audit Server role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Navigator Audit Server process, a lack of connectivity to the Cloudera Manager Agent on the Navigator Audit Server host, or a problem with the Cloudera Manager Agent. This test can fail either because the Navigator Audit Server has crashed or because the Navigator Audit Server will not start or stop in a timely fashion. Check the Navigator Audit Server logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Navigator Audit Server host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Navigator Audit Server host, or look in the Cloudera Manager Agent logs on the Navigator Audit Server host for more details. This test can be enabled or disabled using the Navigator Audit Server Process Health Test Navigator Audit Server monitoring setting.

Short Name: Process Status

Navigator Audit Server Process Health Test

Description

Enables the health test that the Navigator Audit Server's process state is consistent with the role configuration

Template Name

`navigator_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Navigator Audit Server Swap Memory Usage

This Navigator Audit Server health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Navigator Audit Server Unexpected Exits

This Navigator Audit Server health test checks that the Navigator Audit Server has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Navigator Audit Server monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Navigator Audit Server Web Server Status

This health test checks that the role's web server is responding quickly to requests by the Cloudera Manager Agent, and that the Cloudera Manager Agent can collect metrics from the web server. Failure of this health test may indicate a problem with the web server of the Navigator Audit Server, a misconfiguration of the Navigator Audit Server, or a problem with the Cloudera Manager Agent. Consult the Cloudera Manager Agent logs and the logs of the Navigator Audit Server for more detail. If the test failure message indicates a communication problem, the Cloudera Manager Agent's HTTP requests to the Navigator Audit Server's web server are failing or timing out. If the test's failure message indicates an unexpected response, the Navigator Audit Server's web server responded to the Cloudera Manager Agent's request, but the response could not be interpreted for some reason. This test can be configured using the Web Metric Collection Navigator Audit Server monitoring setting.

Short Name: Web Server Status

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Template Name

`navigator_web_metric_collection_enabled`

Default Value

true

Unit(s)

no unit

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Template Name

`navigator_web_metric_collection_thresholds`

Default Value

critical:never, warning:10000.0

Unit(s)

MILLISECONDS

Navigator Luna KMS Metastore Health Tests

Navigator Luna KMS Metastore Audit Pipeline Test

This Navigator Luna KMS Metastore health test checks that the Auditing for the Navigator Luna KMS Metastore role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Navigator Luna KMS Metastore process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Navigator Luna KMS Metastore host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Navigator Luna KMS Metastore monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Navigator Luna KMS Metastore File Descriptors

This Navigator Luna KMS Metastore health test checks that the number of file descriptors used does not rise above some percentage of the Navigator Luna KMS Metastore file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Navigator Luna KMS Metastore monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`hsmkp_metastore_luna_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Navigator Luna KMS Metastore Host Health

This Navigator Luna KMS Metastore health test factors in the health of the host upon which the Navigator Luna KMS Metastore is running. A failure of this test means that the host running the Navigator Luna KMS Metastore is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Navigator Luna KMS Metastore Host Health Test Navigator Luna KMS Metastore monitoring setting.

Short Name: Host Health

Navigator Luna KMS Metastore Host Health Test

Description

When computing the overall Navigator Luna KMS Metastore health, consider the host's health.

Template Name

`hsmkp_metastore_luna_host_health_enabled`

Default Value

true

Unit(s)

no unit

Navigator Luna KMS Metastore Process Status

This Navigator Luna KMS Metastore health test checks that the Cloudera Manager Agent on the Navigator Luna KMS Metastore host is heart beating correctly and that the process associated with the Navigator Luna KMS Metastore role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Navigator Luna KMS Metastore process, a lack of connectivity to the Cloudera Manager Agent on the Navigator Luna KMS Metastore host, or a problem with the Cloudera Manager Agent. This test can fail either because the Navigator Luna KMS Metastore has crashed or because the Navigator Luna KMS Metastore will not start or stop in a timely fashion. Check the Navigator Luna KMS Metastore logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Navigator Luna KMS Metastore host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Navigator Luna KMS Metastore host, or look in the Cloudera Manager Agent logs on the Navigator Luna KMS Metastore host for more details. This test can be enabled or disabled using the Navigator Luna KMS Metastore Process Health Test Navigator Luna KMS Metastore monitoring setting.

Short Name: Process Status

Navigator Luna KMS Metastore Process Health Test

Description

Enables the health test that the Navigator Luna KMS Metastore's process state is consistent with the role configuration

Template Name

`hsmkp_metastore_luna_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Navigator Luna KMS Metastore Swap Memory Usage

This Navigator Luna KMS Metastore health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Navigator Luna KMS Metastore Unexpected Exits

This Navigator Luna KMS Metastore health test checks that the Navigator Luna KMS Metastore has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Navigator Luna KMS Metastore monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Navigator Luna KMS Proxy Health Tests

Navigator Luna KMS Proxy Audit Pipeline Test

This Navigator Luna KMS Proxy health test checks that the Auditing for the Navigator Luna KMS Proxy role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Navigator Luna KMS Proxy process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Navigator Luna KMS Proxy host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Navigator Luna KMS Proxy monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Navigator Luna KMS Proxy File Descriptors

This Navigator Luna KMS Proxy health test checks that the number of file descriptors used does not rise above some percentage of the Navigator Luna KMS Proxy file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Navigator Luna KMS Proxy monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`hsmkp_luna_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Navigator Luna KMS Proxy Host Health

This Navigator Luna KMS Proxy health test factors in the health of the host upon which the Navigator Luna KMS Proxy is running. A failure of this test means that the host running the Navigator Luna KMS Proxy is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Navigator Luna KMS Proxy Host Health Test Navigator Luna KMS Proxy monitoring setting.

Short Name: Host Health

Navigator Luna KMS Proxy Host Health Test

Description

When computing the overall Navigator Luna KMS Proxy health, consider the host's health.

Template Name

`hsmkp_luna_host_health_enabled`

Default Value

true

Unit(s)

no unit

Navigator Luna KMS Proxy Log Directory Free Space

This Navigator Luna KMS Proxy health test checks that the filesystem containing the log directory of this Navigator Luna KMS Proxy has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Navigator Luna KMS Proxy monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Navigator Luna KMS Proxy Process Status

This Navigator Luna KMS Proxy health test checks that the Cloudera Manager Agent on the Navigator Luna KMS Proxy host is heart beating correctly and that the process associated with the Navigator Luna KMS Proxy role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Navigator Luna KMS Proxy process, a lack of connectivity to the Cloudera Manager Agent on the Navigator Luna KMS Proxy host, or a problem with the Cloudera Manager Agent. This test can fail either because the Navigator Luna KMS Proxy has crashed or because the Navigator Luna KMS Proxy will not start or stop in a timely fashion. Check the Navigator Luna KMS Proxy logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Navigator Luna KMS Proxy host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Navigator Luna KMS Proxy host, or look in the Cloudera Manager Agent logs on the Navigator Luna KMS Proxy host for more details. This test can be enabled or disabled using the Navigator Luna KMS Proxy Process Health Test Navigator Luna KMS Proxy monitoring setting.

Short Name: Process Status

Navigator Luna KMS Proxy Process Health Test

Description

Enables the health test that the Navigator Luna KMS Proxy's process state is consistent with the role configuration

Template Name

`hsmkp_luna_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Navigator Luna KMS Proxy Swap Memory Usage

This Navigator Luna KMS Proxy health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Navigator Luna KMS Proxy Unexpected Exits

This Navigator Luna KMS Proxy health test checks that the Navigator Luna KMS Proxy has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Navigator Luna KMS Proxy monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Navigator Metadata Server Health Tests

Navigator Metadata Server Audit Log Directory Free Space

This is a Navigator Metadata Server health test that checks that the filesystem containing the Audit Log Directory of this Navigator Metadata Server has sufficient free space. See the Audit Log Directory description on the Navigator Metadata Server configuration page for more information on this directory type. This test can be configured using the Audit Log Directory Free Space Monitoring Absolute Thresholds and Audit Log Directory Free Space Monitoring Percentage Thresholds Navigator Metadata Server monitoring settings.

Short Name: Audit Log Directory Free Space

Audit Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Audit Log Directory.

Template Name

`navigatormetaserver_audit_event_log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Audit Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Audit Log Directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Audit Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`navigatormetaserver_audit_event_log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Navigator Metadata Server Audit Pipeline Test

This Navigator Metadata Server health test checks that the Auditing for the Navigator Metadata Server role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Navigator Metadata Server process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Navigator Metadata Server host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Navigator Metadata Server monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Navigator Metadata Server File Descriptors

This Navigator Metadata Server health test checks that the number of file descriptors used does not rise above some percentage of the Navigator Metadata Server file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Navigator Metadata Server monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`navigatormetaserver_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Navigator Metadata Server Heap Dump Directory Free Space

This Navigator Metadata Server health test checks that the filesystem containing the heap dump directory of this Navigator Metadata Server has sufficient free space. This test can be configured using the Heap Dump Directory Free Space Monitoring Absolute Thresholds and Heap Dump Directory Free Space Monitoring Percentage Thresholds Navigator Metadata Server monitoring settings.

Short Name: Heap Dump Directory Free Space

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Template Name

`heap_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`heap_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Navigator Metadata Server Host Health

This Navigator Metadata Server health test factors in the health of the host upon which the Navigator Metadata Server is running. A failure of this test means that the host running the Navigator Metadata Server is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Navigator Metadata Server Host Health Test Navigator Metadata Server monitoring setting.

Short Name: Host Health

Navigator Metadata Server Host Health Test

Description

When computing the overall Navigator Metadata Server health, consider the host's health.

Template Name

`navigatormetaserver_host_health_enabled`

Default Value

true

Unit(s)

no unit

Navigator Metadata Server Log Directory Free Space

This Navigator Metadata Server health test checks that the filesystem containing the log directory of this Navigator Metadata Server has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Navigator Metadata Server monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Navigator Metadata Server Navigator Metadata Server Storage Dir Free Space

This is a Navigator Metadata Server health test that checks that the filesystem containing the Navigator Metadata Server Storage Dir of this Navigator Metadata Server has sufficient free space. See the Navigator Metadata Server Storage Dir description on the Navigator Metadata Server configuration page for more information on this directory type. This test can be configured using the Navigator Metadata Server Storage Dir Free Space Monitoring Absolute Thresholds and Navigator Metadata Server Storage Dir Free Space Monitoring Percentage Thresholds Navigator Metadata Server monitoring settings.

Short Name: Navigator Metadata Server Storage Dir Free Space

Navigator Metadata Server Storage Dir Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Navigator Metadata Server Storage Dir.

Template Name

`navigatormetaserver_data_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Navigator Metadata Server Storage Dir Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Navigator Metadata Server Storage Dir. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Navigator Metadata Server Storage Dir Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`navigatormetaserver_data_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Navigator Metadata Server Process Status

This Navigator Metadata Server health test checks that the Cloudera Manager Agent on the Navigator Metadata Server host is heart beating correctly and that the process associated with the Navigator Metadata Server role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Navigator Metadata Server process, a lack of connectivity to the Cloudera Manager Agent on the Navigator Metadata Server host, or a problem with the Cloudera Manager Agent. This test can fail either because the Navigator Metadata Server has crashed or because the Navigator Metadata Server will not start or stop in a timely fashion. Check the Navigator Metadata Server logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Navigator Metadata Server host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Navigator Metadata Server host, or look in the Cloudera Manager Agent logs on the Navigator Metadata Server host for more details. This test can be enabled or disabled using the Navigator Metadata Server Process Health Test Navigator Metadata Server monitoring setting.

Short Name: Process Status

Navigator Metadata Server Process Health Test

Description

Enables the health test that the Navigator Metadata Server's process state is consistent with the role configuration

Template Name

`navigatormetaserver_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Navigator Metadata Server Solr Element Count Threshold Test

This alert indicates when the document count in the Navigator Elements Solr core is reaching Solrs maximum limit. Typically, the maximum number of documents in a Solr core is around 2 billion. When the document count reaches the critical threshold, Navigator Metadata Server will stop working. The warning threshold is set to give administrators time to reduce the volume of documents before Navigator can no longer function. Consider changing these thresholds if you want to give more time between when the alerts are triggered and when Navigator Metadata Server stops working. To reduce the number of documents, make sure Navigator purge is running regularly. For more information, see *Troubleshooting Cloudera Navigator Metadata Server*.

Short Name: Solr Element Count Threshold Test

Solr Element Count Threshold

Description

Threshold for throwing alert when the Solr Element Count reaches

Template Name

`navigatormetaserver_solr_element_count_threshold`

Default Value

critical:1.0E9, warning:5.0E8

Unit(s)

no unit

Navigator Metadata Server Solr Relation Count Threshold Test

This alert indicates when the document count in the Navigator Relations Solr core is reaching Solrs maximum limit. Typically, the maximum number of documents in a Solr core is around 2 billion. When the document count reaches the critical threshold, Navigator Metadata Server will stop working. The warning threshold is set to give administrators time to reduce the volume of documents before Navigator can no longer function. Consider changing these thresholds if you want to give more time between when the alerts are triggered and when Navigator Metadata Server stops working. To reduce the number of documents, make sure Navigator purge is running regularly. For more information, see *Troubleshooting Cloudera Navigator Metadata Server*.

Short Name: Solr Relation Count Threshold Test

Solr Relation Count Threshold

Description

Threshold for throwing alert when the Solr Relation Count reaches

Template Name

`navigatormetaserver_solr_relation_count_threshold`

Default Value

critical:1.0E9, warning:5.0E8

Unit(s)

no unit

Navigator Metadata Server Swap Memory Usage

This Navigator Metadata Server health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Navigator Metadata Server Unexpected Exits

This Navigator Metadata Server health test checks that the Navigator Metadata Server has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Navigator Metadata Server monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Navigator Thales KMS Metastore Health Tests

Navigator Thales KMS Metastore Audit Pipeline Test

This Navigator Thales KMS Metastore health test checks that the Auditing for the Navigator Thales KMS Metastore role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Navigator Thales KMS Metastore process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Navigator Thales KMS Metastore host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Navigator Thales KMS Metastore monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Navigator Thales KMS Metastore File Descriptors

This Navigator Thales KMS Metastore health test checks that the number of file descriptors used does not rise above some percentage of the Navigator Thales KMS Metastore file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Navigator Thales KMS Metastore monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`hsmkp_metastore_thales_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Navigator Thales KMS Metastore Host Health

This Navigator Thales KMS Metastore health test factors in the health of the host upon which the Navigator Thales KMS Metastore is running. A failure of this test means that the host running the Navigator Thales KMS Metastore is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Navigator Thales KMS Metastore Host Health Test Navigator Thales KMS Metastore monitoring setting.

Short Name: Host Health

Navigator Thales KMS Metastore Host Health Test

Description

When computing the overall Navigator Thales KMS Metastore health, consider the host's health.

Template Name

`hsmkp_metastore_thales_host_health_enabled`

Default Value

true

Unit(s)

no unit

Navigator Thales KMS Metastore Process Status

This Navigator Thales KMS Metastore health test checks that the Cloudera Manager Agent on the Navigator Thales KMS Metastore host is heart beating correctly and that the process associated with the Navigator Thales KMS Metastore role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Navigator Thales KMS Metastore process, a lack of connectivity to the Cloudera Manager Agent on the Navigator Thales KMS Metastore host, or a problem with the Cloudera Manager Agent. This test can fail either because the Navigator Thales KMS Metastore has crashed or because the Navigator Thales KMS Metastore will not start or stop in a timely fashion. Check the Navigator Thales KMS Metastore logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Navigator Thales KMS Metastore host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Navigator Thales KMS Metastore host, or look in the Cloudera Manager Agent logs on the Navigator Thales KMS Metastore host for more details. This test can be enabled or disabled using the Navigator Thales KMS Metastore Process Health Test Navigator Thales KMS Metastore monitoring setting.

Short Name: Process Status

Navigator Thales KMS Metastore Process Health Test

Description

Enables the health test that the Navigator Thales KMS Metastore's process state is consistent with the role configuration

Template Name

`hsmkp_metastore_thales_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Navigator Thales KMS Metastore Swap Memory Usage

This Navigator Thales KMS Metastore health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Navigator Thales KMS Metastore Unexpected Exits

This Navigator Thales KMS Metastore health test checks that the Navigator Thales KMS Metastore has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Navigator Thales KMS Metastore monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Navigator Thales KMS Proxy Health Tests

Navigator Thales KMS Proxy Audit Pipeline Test

This Navigator Thales KMS Proxy health test checks that the Auditing for the Navigator Thales KMS Proxy role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Navigator Thales KMS Proxy process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Navigator Thales KMS Proxy host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Navigator Thales KMS Proxy monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Navigator Thales KMS Proxy File Descriptors

This Navigator Thales KMS Proxy health test checks that the number of file descriptors used does not rise above some percentage of the Navigator Thales KMS Proxy file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Navigator Thales KMS Proxy monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`hsmkp_thales_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Navigator Thales KMS Proxy Host Health

This Navigator Thales KMS Proxy health test factors in the health of the host upon which the Navigator Thales KMS Proxy is running. A failure of this test means that the host running the Navigator Thales KMS Proxy is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Navigator Thales KMS Proxy Host Health Test Navigator Thales KMS Proxy monitoring setting.

Short Name: Host Health

Navigator Thales KMS Proxy Host Health Test

Description

When computing the overall Navigator Thales KMS Proxy health, consider the host's health.

Template Name

`hsmkp_thales_host_health_enabled`

Default Value

true

Unit(s)

no unit

Navigator Thales KMS Proxy Log Directory Free Space

This Navigator Thales KMS Proxy health test checks that the filesystem containing the log directory of this Navigator Thales KMS Proxy has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Navigator Thales KMS Proxy monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Navigator Thales KMS Proxy Process Status

This Navigator Thales KMS Proxy health test checks that the Cloudera Manager Agent on the Navigator Thales KMS Proxy host is heart beating correctly and that the process associated with the Navigator Thales KMS Proxy role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Navigator Thales KMS Proxy process, a lack of connectivity to the Cloudera Manager Agent on the Navigator Thales KMS Proxy host, or a problem with the Cloudera Manager Agent. This test can fail either because the Navigator Thales KMS Proxy has crashed or because the Navigator Thales KMS Proxy will not start or stop in a timely fashion. Check the Navigator Thales KMS Proxy logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Navigator Thales KMS Proxy host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Navigator Thales KMS Proxy host, or look in the Cloudera Manager Agent logs on the Navigator Thales KMS Proxy host for more details. This test can be enabled or disabled using the Navigator Thales KMS Proxy Process Health Test Navigator Thales KMS Proxy monitoring setting.

Short Name: Process Status

Navigator Thales KMS Proxy Process Health Test

Description

Enables the health test that the Navigator Thales KMS Proxy's process state is consistent with the role configuration

Template Name

`hsmkp_thales_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Navigator Thales KMS Proxy Swap Memory Usage

This Navigator Thales KMS Proxy health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Navigator Thales KMS Proxy Unexpected Exits

This Navigator Thales KMS Proxy health test checks that the Navigator Thales KMS Proxy has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Navigator Thales KMS Proxy monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

NodeManager Health Tests

NodeManager Audit Pipeline Test

This NodeManager health test checks that the Auditing for the NodeManager role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of NodeManager process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the NodeManager host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check NodeManager monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

NodeManager File Descriptors

This NodeManager health test checks that the number of file descriptors used does not rise above some percentage of the NodeManager file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds NodeManager monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`nodemanager_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

NodeManager GC Duration

This NodeManager health test checks that the NodeManager is not spending too much time performing Java garbage collection. It checks that no more than some percentage of recent time is spent performing Java garbage collection. A failure of this health test may indicate a capacity planning problem or misconfiguration of the NodeManager. This test can be configured using the Garbage Collection Duration Thresholds and Garbage Collection Duration Monitoring Period NodeManager monitoring settings.

Short Name: GC Duration

Garbage Collection Duration Monitoring Period

Description

The period to review when computing the moving average of garbage collection time.

Template Name

`nodemanager_gc_duration_window`

Default Value

5

Unit(s)

MINUTES

Garbage Collection Duration Thresholds

Description

The health test thresholds for the weighted average time spent in Java garbage collection. Specified as a percentage of elapsed wall clock time.

Template Name

`nodemanager_gc_duration_thresholds`

Default Value

critical:60.0, warning:30.0

Unit(s)

no unit

NodeManager Heap Dump Directory Free Space

This NodeManager health test checks that the filesystem containing the heap dump directory of this NodeManager has sufficient free space. This test can be configured using the Heap Dump Directory Free Space Monitoring Absolute Thresholds and Heap Dump Directory Free Space Monitoring Percentage Thresholds NodeManager monitoring settings.

Short Name: Heap Dump Directory Free Space

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Template Name

`heap_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`heap_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

NodeManager Host Health

This NodeManager health test factors in the health of the host upon which the NodeManager is running. A failure of this test means that the host running the NodeManager is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the NodeManager Host Health Test NodeManager monitoring setting.

Short Name: Host Health

NodeManager Host Health Test

Description

When computing the overall NodeManager health, consider the host's health.

Template Name

`nodemanager_host_health_enabled`

Default Value

true

Unit(s)

no unit

NodeManager Log Directory Free Space

This NodeManager health test checks that the filesystem containing the log directory of this NodeManager has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds NodeManager monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

NodeManager NodeManager Container Log Directories Free Space

This is a NodeManager health test that checks that the filesystem containing the NodeManager Container Log Directories of this NodeManager has sufficient free space. See the NodeManager Container Log Directories description on the NodeManager configuration page for more information on this directory type. This test can be configured using the NodeManager Container Log Directories Free Space Monitoring Absolute Thresholds and NodeManager Container Log Directories Free Space Monitoring Percentage Thresholds NodeManager monitoring settings.

Short Name: NodeManager Container Log Directories Free Space

NodeManager Container Log Directories Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's NodeManager Container Log Directories.

Template Name

`nodemanager_log_directories_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

NodeManager Container Log Directories Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's NodeManager Container Log Directories. Specified as a percentage of the capacity on that filesystem. This setting is not used if a NodeManager Container Log Directories Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`nodemanager_log_directories_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

NodeManager NodeManager Health Checker

This is a NodeManager health test that checks whether the ResourceManager considers the NodeManager healthly. A failure of this health test indicates that the NodeManager disk health checker or a health check script, if one is configured, reported an unhealthy condition. The NodeManager health report may include more details about the failure. Look in the NodeManager logs for more details. This test may return an unknown result if the Service Monitor is not able to communicate with the ResourceManager web server. Check the status of the ResourceManager web server and the Service Monitor logs if this test is returning an unknown result. This test can be enabled or disabled using the NodeManager Health Checker Health Check NodeManager monitoring setting. The NodeManager Connectivity Tolerance at Startup Node Manager monitoring setting and the Health Test Startup Tolerance ResourceManager monitor setting can be used to control the test's tolerance windows around NodeManager and ResourceManager restarts, respectively. The NodeManager disk health checker configuration can be configured using Disk Health Checker Minimum Health Disks Fraction, Disk Health Checker Minimum Health Disk Space, and Dish Health Checker Max Disk Utilization Percent.

Short Name: NodeManager Health Checker

Dish Health Checker Max Disk Utilization Percent

Description

The maximum percentage of disk space utilization allowed after which a disk is marked as bad. Values can range from 0.0 to 100.0. If the value is greater than or equal to 100, the NodeManager will check for full disk. This applies to local directories and log directories.

Template Name

`yarn_nodemanager_disk_health_checker_max_disk_utilization_per_disk_percentage`

Default Value

CDH=[[CDH 5.2.0..CDH 8.0.0)=90.0]

Unit(s)

PERCENT

Disk Health Checker Minimum Health Disk Space

Description

The minimum space that must be available on a disk for it to be used. This applies to local directories and log directories.

Template Name

`yarn_nodemanager_disk_health_checker_min_free_space_per_disk_mb`

Default Value

CDH=[[CDH 5.2.0..CDH 8.0.0)=0]

Unit(s)

MEGABYTES

Disk Health Checker Minimum Health Disks Fraction

Description

The minimum fraction of number of disks to be healthy for the NodeManager to launch new containers. This correspond to both local directories and log directories; that is, if there are fewer healthy local directories (or log directories) available, then new containers will not be launched on this node.

Template Name

`yarn_nodemanager_disk_health_checker_min_healthy_disks`

Default Value

0.25

Unit(s)

no unit

Health Test Startup Tolerance

Description

The amount of time allowed after this role is started that failures of health tests that rely on communication with this role will be tolerated.

Template Name

`resourcemanager_startup_tolerance_minutes`

Default Value

5

Unit(s)

MINUTES

NodeManager Connectivity Tolerance at Startup

Description

The amount of time to wait for the NodeManager to fully start up and connect to the ResourceManager before enforcing the connectivity check.

Template Name

`nodemanager_connectivity_tolerance_seconds`

Default Value

180

Unit(s)

SECONDS

NodeManager Health Checker Health Check

Description

Enables the health check that verifies the NodeManager is seen as healthy by the ResourceManager.

Template Name

`nodemanager_health_checker_health_enabled`

Default Value

true

Unit(s)

no unit

NodeManager NodeManager Local Directories Free Space

This is a NodeManager health test that checks that the filesystem containing the NodeManager Local Directories of this NodeManager has sufficient free space. See the NodeManager Local Directories description on the NodeManager configuration page for more information on this directory type. This test can be configured using the NodeManager Local Directories Free Space Monitoring Absolute Thresholds and NodeManager Local Directories Free Space Monitoring Percentage Thresholds NodeManager monitoring settings.

Short Name: NodeManager Local Directories Free Space

NodeManager Local Directories Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's NodeManager Local Directories.

Template Name

`nodemanager_local_data_directories_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

NodeManager Local Directories Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's NodeManager Local Directories. Specified as a percentage of the capacity on that filesystem. This setting is not used if a NodeManager Local Directories Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`nodemanager_local_data_directories_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

NodeManager NodeManager Recovery Directory Free Space

This is a NodeManager health test that checks that the filesystem containing the NodeManager Recovery Directory of this NodeManager has sufficient free space. See the NodeManager Recovery Directory description on the NodeManager configuration page for more information on this directory type. This test can be configured using the NodeManager Recovery Directory Free Space Monitoring Absolute Thresholds and NodeManager Recovery Directory Free Space Monitoring Percentage Thresholds NodeManager monitoring settings.

Short Name: NodeManager Recovery Directory Free Space

NodeManager Recovery Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's NodeManager Recovery Directory.

Template Name

`nodemanager_recovery_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

NodeManager Recovery Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's NodeManager Recovery Directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a NodeManager Recovery Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`nodemanager_recovery_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

NodeManager Process Status

This NodeManager health test checks that the Cloudera Manager Agent on the NodeManager host is heart beating correctly and that the process associated with the NodeManager role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the NodeManager process, a lack of connectivity to the Cloudera Manager Agent on the NodeManager host, or a problem with the Cloudera Manager Agent. This test can fail either because the NodeManager has crashed or because the NodeManager will not start or stop in a timely fashion. Check the NodeManager logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the NodeManager host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the NodeManager host, or look in the Cloudera Manager Agent logs on the NodeManager host for more details. This test can be enabled or disabled using the NodeManager Process Health Test NodeManager monitoring setting.

Short Name: Process Status

NodeManager Process Health Test

Description

Enables the health test that the NodeManager's process state is consistent with the role configuration

Template Name

`nodemanager_scm_health_enabled`

Default Value

true

Unit(s)

no unit

NodeManager ResourceManager Connectivity

This is a NodeManager health test that checks whether the ResourceManager considers the NodeManager alive. A failure of this health test may indicate that the NodeManager is having trouble communicating with the ResourceManager. Look in the NodeManager logs for more details. This test may return an unknown result if the Service Monitor is not able to communicate with the ResourceManager web server. Check the status of the ResourceManager web server and the Service Monitor logs if this test is returning an unknown result. This test can be enabled or disabled using the NodeManager Connectivity Health Check NodeManager monitoring setting. The NodeManager Connectivity Tolerance at Startup NodeManager monitoring setting and the Health Test Startup Tolerance ResourceManager monitoring setting can be used to control the test's tolerance windows around NodeManager and ResourceManager restarts respectively.

Short Name: ResourceManager Connectivity

Health Test Startup Tolerance

Description

The amount of time allowed after this role is started that failures of health tests that rely on communication with this role will be tolerated.

Template Name

`resourcemanager_startup_tolerance_minutes`

Default Value

5

Unit(s)

MINUTES

NodeManager Connectivity Health Check

Description

Enables the health check that verifies the NodeManager is connected to the ResourceManager.

Template Name

`nodemanager_connectivity_health_enabled`

Default Value

true

Unit(s)

no unit

NodeManager Connectivity Tolerance at Startup

Description

The amount of time to wait for the NodeManager to fully start up and connect to the ResourceManager before enforcing the connectivity check.

Template Name

`nodemanager_connectivity_tolerance_seconds`

Default Value

180

Unit(s)

SECONDS

NodeManager Swap Memory Usage

This NodeManager health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

NodeManager Unexpected Exits

This NodeManager health test checks that the NodeManager has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits

were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period NodeManager monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

NodeManager Web Server Status

This health test checks that the role's web server is responding quickly to requests by the Cloudera Manager Agent, and that the Cloudera Manager Agent can collect metrics from the web server. Failure of this health test may indicate a problem with the web server of the NodeManager, a misconfiguration of the NodeManager, or a problem with the Cloudera Manager Agent. Consult the Cloudera Manager Agent logs and the logs of the NodeManager for more detail. If the test failure message indicates a communication problem, the Cloudera Manager Agent's HTTP requests to the NodeManager's web server are failing or timing out. If the test's failure message indicates an unexpected response, the NodeManager's web server responded to the Cloudera Manager Agent's request, but the response could not be interpreted for some reason. This test can be configured using the Web Metric Collection NodeManager monitoring setting.

Short Name: Web Server Status

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Template Name

`nodemanager_web_metric_collection_enabled`

Default Value

true

Unit(s)

no unit

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Template Name

`nodemanager_web_metric_collection_thresholds`

Default Value

critical:never, warning:10000.0

Unit(s)

MILLISECONDS

Oozie Health Tests

Oozie Server Health

This is a Oozie service-level health test that checks that enough of the Oozie Servers in the cluster are healthy. The test returns "Concerning" health if the number of healthy Oozie Servers falls below a warning threshold, expressed as a percentage of the total number of Oozie Servers. The test returns "Bad" health if the number of healthy and "Concerning" Oozie Servers falls below a critical threshold, expressed as a percentage of the total number of Oozie Servers. For example, if this test is configured with a warning threshold of 95% and a critical threshold of 90% for a cluster of 100 Oozie Servers, this test would return "Good" health if 95 or more Oozie Servers have good health. This test would return "Concerning" health if at least 90 Oozie Servers have either "Good" or "Concerning" health. If more than 10 Oozie Servers have bad health, this test would return "Bad" health. A failure of this health test indicates unhealthy Oozie Servers. Check the status of the individual Oozie Servers for more information. This test can be configured using the Oozie Oozie service-wide monitoring setting.

Short Name: Oozie Server Health

Healthy Oozie Server Monitoring Thresholds

Description

The health test thresholds of the overall Oozie Server health. The check returns "Concerning" health if the percentage of "Healthy" Oozie Servers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Oozie Servers falls below the critical threshold.

Template Name

`oozie_servers_healthy_thresholds`

Default Value

critical:51.0, warning:99.0

Unit(s)

PERCENT

Oozie Server Health Tests

Oozie Server Audit Pipeline Test

This Oozie Server health test checks that the Auditing for the Oozie Server role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Oozie Server process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on

the Oozie Server host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Oozie Server monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Oozie Server Callable Queue Size

This is an Oozie Server health test that checks that a moving average of the size of the Oozie Server's callable queue does not exceed some percentage of the configured maximum size for the queue. The callable queue contains tasks (e.g., StartCommand task, ActionCommand task) for asynchronous execution. When the queue is full the callable queue service stops queuing tasks. This may cause running jobs and submissions of new jobs to fail. A failure of this health test indicates a high load on the Oozie Server. Make sure the Oozie server has enough heap and is not running out of memory. You can also increase the number of threads handling the callable queue items by changing Number Threads For Executing Callables and the max size of the callable queue by changing Maximum Callable Queue Size.

This test can be configured using the Oozie Server Callable Queue Monitoring Threshold and Oozie Server Callable Queue Monitoring Period Oozie Server monitoring settings.

Short Name: Callable Queue Size

Maximum Callable Queue Size

Description

Maximum callable queue size

Template Name

`oozie_service_callablequeueservice_queue_size`

Default Value

10000

Unit(s)

no unit

Number Threads For Executing Callables

Description

Number of threads used for executing callables

Template Name

`oozie_service_callablequeueservice_threads`

Default Value

50

Unit(s)

no unit

Oozie Server Callable Queue Monitoring Period

Description

The period over which to compute the moving average of the callable queue size.

Template Name

`oozie_server_callable_queue_window`

Default Value

5

Unit(s)

MINUTES

Oozie Server Callable Queue Monitoring Threshold

Description

The health test thresholds of the weighted average size of the Oozie Server callable queue over a recent period. See also Oozie Server Callable Queue Monitoring Period.

Template Name

`oozie_server_callable_queue_threshold`

Default Value

critical:95.0, warning:80.0

Unit(s)

PERCENT

Oozie Server File Descriptors

This Oozie Server health test checks that the number of file descriptors used does not rise above some percentage of the Oozie Server file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Oozie Server monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`oozie_server_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Oozie Server Heap Dump Directory Free Space

This Oozie Server health test checks that the filesystem containing the heap dump directory of this Oozie Server has sufficient free space. This test can be configured using the Heap Dump Directory Free Space Monitoring Absolute Thresholds and Heap Dump Directory Free Space Monitoring Percentage Thresholds Oozie Server monitoring settings.

Short Name: Heap Dump Directory Free Space

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Template Name

`heap_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`heap_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Oozie Server Host Health

This Oozie Server health test factors in the health of the host upon which the Oozie Server is running. A failure of this test means that the host running the Oozie Server is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Oozie Server Host Health Test Oozie Server monitoring setting.

Short Name: Host Health

Oozie Server Host Health Test

Description

When computing the overall Oozie Server health, consider the host's health.

Template Name

`oozie_server_host_health_enabled`

Default Value

true

Unit(s)

no unit

Oozie Server Log Directory Free Space

This Oozie Server health test checks that the filesystem containing the log directory of this Oozie Server has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Oozie Server monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Oozie Server Oozie Server Shared Library Check

This is an Oozie Server health test that verifies that the installed shared library is correct. If the shared library is missing, is out-of-sync with the Oozie build version, or does not match the Oozie MapReduce service dependency, the check will return "Bad" health. Follow the instructions in the Cloudera Manager documentation to install or upgrade it. For other failures of this health test, consult the Cloudera Manager Service Monitor logs. This test can be enabled or disabled using the Enable Oozie Server Shared Libraries Version Check Oozie Server monitoring setting.

Short Name: Oozie Server Shared Library Check

Enable Oozie Server Shared Libraries Version Check

Description

If true, enables version check for Oozie Server and installed shared libraries.

Template Name

`oozie_server_shared_lib_version_check_enabled`

Default Value

CDH=[[CDH 5.0.0..CDH 8.0.0)=true]

Unit(s)

no unit

Oozie Server Pause Duration

This Oozie Server health test checks that the Oozie Server threads are not experiencing long scheduling pauses. The test uses a pause monitoring thread in the Oozie Server that tracks scheduling delay by noting if it is run on its requested schedule. If the thread is not run on its requested schedule, the delay is noted and considered pause time. The health test checks that no more than some percentage of recent time is spent paused. A failure of this health test may indicate that the Oozie Server is not getting enough CPU resources, or that it is spending too much time doing garbage collection. Inspect the Oozie Server logs for any pause monitor output and check garbage collection metrics exposed by the Oozie Server. This test can be configured using the Pause Duration Thresholds and Pause Duration Monitoring Period Oozie Server monitoring settings.

Short Name: Pause Duration

Pause Duration Monitoring Period

Description

The period to review when computing the moving average of extra time the pause monitor spent paused.

Template Name

`oozie_server_pause_duration_window`

Default Value

5

Unit(s)

MINUTES

Pause Duration Thresholds

Description

The health test thresholds for the weighted average extra time the pause monitor spent paused. Specified as a percentage of elapsed wall clock time.

Template Name

`oozie_server_pause_duration_thresholds`

Default Value

critical:60.0, warning:30.0

Unit(s)

no unit

Oozie Server Process Status

This Oozie Server health test checks that the Cloudera Manager Agent on the Oozie Server host is heart beating correctly and that the process associated with the Oozie Server role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Oozie Server process, a lack of connectivity to the Cloudera Manager Agent on the Oozie Server host, or a problem with the Cloudera Manager Agent. This test can fail either because the Oozie Server has crashed or because the Oozie Server will not start or stop in a timely fashion. Check the Oozie Server logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Oozie Server host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Oozie Server host, or look in the Cloudera Manager Agent logs on the Oozie Server host for more details. This test can be enabled or disabled using the Oozie Server Process Health Test Oozie Server monitoring setting.

Short Name: Process Status

Oozie Server Process Health Test

Description

Enables the health test that the Oozie Server's process state is consistent with the role configuration

Template Name

`oozie_server_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Oozie Server Swap Memory Usage

This Oozie Server health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Oozie Server Unexpected Exits

This Oozie Server health test checks that the Oozie Server has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured

with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Oozie Server monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Oozie Server Web Server Status

This health test checks that the role's web server is responding quickly to requests by the Cloudera Manager Service Monitor, and that the Cloudera Manager Service Monitor can collect metrics from the web server. Failure of this health test may indicate a problem with the web server of the Oozie Server, a misconfiguration of the Oozie Server, or a problem with the Cloudera Manager Service Monitor. Consult the Cloudera Manager Service Monitor logs and the logs of the Oozie Server for more detail. If the test failure message indicates a communication problem, the Cloudera Manager Service Monitor's HTTP requests to the Oozie Server's web server are failing or timing out. If the test's failure message indicates an unexpected response, the Oozie Server's web server responded to the Cloudera Manager Service Monitor's request, but the response could not be interpreted for some reason. This test can be configured using the Web Metric Collection Oozie Server monitoring setting.

Short Name: Web Server Status

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Template Name

`oozie_server_web_metric_collection_enabled`

Default Value

true

Unit(s)

no unit

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Template Name

`oozie_server_web_metric_collection_thresholds`

Default Value

critical:never, warning:10000.0

Unit(s)

MILLISECONDS

Ozone DataNode Health Tests

Ozone DataNode Audit Pipeline Test

This Ozone DataNode health test checks that the Auditing for the Ozone DataNode role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Ozone DataNode process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Ozone DataNode host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Ozone DataNode monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Ozone DataNode File Descriptors

This Ozone DataNode health test checks that the number of file descriptors used does not rise above some percentage of the Ozone DataNode file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Ozone DataNode monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`ozone_datanode_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Ozone DataNode Host Health

This Ozone DataNode health test factors in the health of the host upon which the Ozone DataNode is running. A failure of this test means that the host running the Ozone DataNode is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Ozone DataNode Host Health Test Ozone DataNode monitoring setting.

Short Name: Host Health

Ozone DataNode Host Health Test

Description

When computing the overall Ozone DataNode health, consider the host's health.

Template Name

`ozone_datanode_host_health_enabled`

Default Value

true

Unit(s)

no unit

Ozone DataNode Log Directory Free Space

This Ozone DataNode health test checks that the filesystem containing the log directory of this Ozone DataNode has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Ozone DataNode monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Ozone DataNode Process Status

This Ozone DataNode health test checks that the Cloudera Manager Agent on the Ozone DataNode host is heart beating correctly and that the process associated with the Ozone DataNode role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Ozone DataNode process, a lack of connectivity to the Cloudera Manager Agent on the Ozone DataNode host, or a problem with the Cloudera Manager Agent. This test can fail either because the Ozone DataNode has crashed or because the Ozone DataNode will not start or stop in a timely fashion. Check the Ozone DataNode logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Ozone DataNode host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Ozone DataNode host, or look in the Cloudera Manager Agent logs on the Ozone DataNode host for more details. This test can be enabled or disabled using the Ozone DataNode Process Health Test Ozone DataNode monitoring setting.

Short Name: Process Status

Ozone DataNode Process Health Test

Description

Enables the health test that the Ozone DataNode's process state is consistent with the role configuration

Template Name

`ozone_datanode_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Ozone DataNode Swap Memory Usage

This Ozone DataNode health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Ozone DataNode Unexpected Exits

This Ozone DataNode health test checks that the Ozone DataNode has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Ozone DataNode monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Ozone Manager Health Tests

Ozone Manager Audit Pipeline Test

This Ozone Manager health test checks that the Auditing for the Ozone Manager role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Ozone Manager process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Ozone Manager host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Ozone Manager monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Ozone Manager File Descriptors

This Ozone Manager health test checks that the number of file descriptors used does not rise above some percentage of the Ozone Manager file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Ozone Manager monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`ozone_manager_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Ozone Manager Host Health

This Ozone Manager health test factors in the health of the host upon which the Ozone Manager is running. A failure of this test means that the host running the Ozone Manager is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Ozone Manager Host Health Test Ozone Manager monitoring setting.

Short Name: Host Health

Ozone Manager Host Health Test

Description

When computing the overall Ozone Manager health, consider the host's health.

Template Name

`ozone_manager_host_health_enabled`

Default Value

true

Unit(s)

no unit

Ozone Manager Log Directory Free Space

This Ozone Manager health test checks that the filesystem containing the log directory of this Ozone Manager has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Ozone Manager monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Ozone Manager Process Status

This Ozone Manager health test checks that the Cloudera Manager Agent on the Ozone Manager host is heart beating correctly and that the process associated with the Ozone Manager role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Ozone Manager process, a lack of connectivity to the Cloudera Manager Agent on the Ozone Manager host, or a problem with the Cloudera Manager Agent. This test can fail either because the Ozone Manager has crashed or because the Ozone Manager will not start or stop in a timely fashion. Check the Ozone Manager logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Ozone Manager host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Ozone Manager host, or look in the Cloudera Manager Agent logs on the Ozone Manager host for more details. This test can be enabled or disabled using the Ozone Manager Process Health Test Ozone Manager monitoring setting.

Short Name: Process Status

Ozone Manager Process Health Test

Description

Enables the health test that the Ozone Manager's process state is consistent with the role configuration

Template Name

`ozone_manager_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Ozone Manager Swap Memory Usage

This Ozone Manager health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Ozone Manager Unexpected Exits

This Ozone Manager health test checks that the Ozone Manager has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Ozone Manager monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Ozone Prometheus Health Tests

Ozone Prometheus Audit Pipeline Test

This Ozone Prometheus health test checks that the Auditing for the Ozone Prometheus role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Ozone Prometheus process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Ozone Prometheus host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Ozone Prometheus monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Ozone Prometheus File Descriptors

This Ozone Prometheus health test checks that the number of file descriptors used does not rise above some percentage of the Ozone Prometheus file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Ozone Prometheus monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`ozone_prometheus_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Ozone Prometheus Host Health

This Ozone Prometheus health test factors in the health of the host upon which the Ozone Prometheus is running. A failure of this test means that the host running the Ozone Prometheus is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Ozone Prometheus Host Health Test Ozone Prometheus monitoring setting.

Short Name: Host Health

Ozone Prometheus Host Health Test

Description

When computing the overall Ozone Prometheus health, consider the host's health.

Template Name

`ozone_prometheus_host_health_enabled`

Default Value

true

Unit(s)

no unit

Ozone Prometheus Process Status

This Ozone Prometheus health test checks that the Cloudera Manager Agent on the Ozone Prometheus host is heart beating correctly and that the process associated with the Ozone Prometheus role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Ozone Prometheus process, a lack of connectivity to the Cloudera Manager Agent on the Ozone Prometheus host, or a problem with the Cloudera Manager Agent. This test can fail either because the Ozone Prometheus has crashed or because the Ozone Prometheus will not start or stop in a timely fashion. Check the Ozone Prometheus logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Ozone Prometheus host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Ozone Prometheus host, or look

in the Cloudera Manager Agent logs on the Ozone Prometheus host for more details. This test can be enabled or disabled using the Ozone Prometheus Process Health Test Ozone Prometheus monitoring setting.

Short Name: Process Status

Ozone Prometheus Process Health Test

Description

Enables the health test that the Ozone Prometheus's process state is consistent with the role configuration

Template Name

`ozone_prometheus_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Ozone Prometheus Swap Memory Usage

This Ozone Prometheus health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Ozone Prometheus Unexpected Exits

This Ozone Prometheus health test checks that the Ozone Prometheus has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Ozone Prometheus monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Ozone Recon Health Tests

Ozone Recon Audit Pipeline Test

This Ozone Recon health test checks that the Auditing for the Ozone Recon role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Ozone Recon process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Ozone Recon host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Ozone Recon monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Ozone Recon File Descriptors

This Ozone Recon health test checks that the number of file descriptors used does not rise above some percentage of the Ozone Recon file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Ozone Recon monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`ozone_recon_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Ozone Recon Host Health

This Ozone Recon health test factors in the health of the host upon which the Ozone Recon is running. A failure of this test means that the host running the Ozone Recon is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Ozone Recon Host Health Test Ozone Recon monitoring setting.

Short Name: Host Health

Ozone Recon Host Health Test

Description

When computing the overall Ozone Recon health, consider the host's health.

Template Name

`ozone_recon_host_health_enabled`

Default Value

true

Unit(s)

no unit

Ozone Recon Log Directory Free Space

This Ozone Recon health test checks that the filesystem containing the log directory of this Ozone Recon has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Ozone Recon monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Ozone Recon Process Status

This Ozone Recon health test checks that the Cloudera Manager Agent on the Ozone Recon host is heart beating correctly and that the process associated with the Ozone Recon role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Ozone Recon process, a lack of connectivity to the Cloudera Manager Agent on the Ozone Recon host, or a problem with the Cloudera Manager Agent. This test can fail either because the Ozone Recon has crashed or because the Ozone Recon will not start or stop in a timely fashion. Check the Ozone Recon logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Ozone Recon host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Ozone Recon host, or look in the Cloudera Manager Agent logs on the Ozone Recon host for more details. This test can be enabled or disabled using the Ozone Recon Process Health Test Ozone Recon monitoring setting.

Short Name: Process Status

Ozone Recon Process Health Test

Description

Enables the health test that the Ozone Recon's process state is consistent with the role configuration

Template Name

`ozone_recon_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Ozone Recon Swap Memory Usage

This Ozone Recon health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Ozone Recon Unexpected Exits

This Ozone Recon health test checks that the Ozone Recon has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Ozone Recon monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Passive Database Health Tests

Passive Database Audit Pipeline Test

This Passive Database health test checks that the Auditing for the Passive Database role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Passive Database process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Passive Database host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Passive Database monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Passive Database File Descriptors

This Passive Database health test checks that the number of file descriptors used does not rise above some percentage of the Passive Database file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Passive Database monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`db_passive_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Passive Database Host Health

This Passive Database health test factors in the health of the host upon which the Passive Database is running. A failure of this test means that the host running the Passive Database is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Passive Database Host Health Test Passive Database monitoring setting.

Short Name: Host Health

Passive Database Host Health Test

Description

When computing the overall Passive Database health, consider the host's health.

Template Name

`db_passive_host_health_enabled`

Default Value

true

Unit(s)

no unit

Passive Database Process Status

This Passive Database health test checks that the Cloudera Manager Agent on the Passive Database host is heart beating correctly and that the process associated with the Passive Database role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Passive Database process, a lack of

connectivity to the Cloudera Manager Agent on the Passive Database host, or a problem with the Cloudera Manager Agent. This test can fail either because the Passive Database has crashed or because the Passive Database will not start or stop in a timely fashion. Check the Passive Database logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Passive Database host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Passive Database host, or look in the Cloudera Manager Agent logs on the Passive Database host for more details. This test can be enabled or disabled using the Passive Database Process Health Test Passive Database monitoring setting.

Short Name: Process Status

Passive Database Process Health Test

Description

Enables the health test that the Passive Database's process state is consistent with the role configuration

Template Name

`db_passive_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Passive Database Swap Memory Usage

This Passive Database health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Passive Database Unexpected Exits

This Passive Database health test checks that the Passive Database has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Passive Database monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Passive Key Trustee Server Health Tests

Passive Key Trustee Server Audit Pipeline Test

This Passive Key Trustee Server health test checks that the Auditing for the Passive Key Trustee Server role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Passive Key Trustee Server process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Passive Key Trustee Server host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Passive Key Trustee Server monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Passive Key Trustee Server File Descriptors

This Passive Key Trustee Server health test checks that the number of file descriptors used does not rise above some percentage of the Passive Key Trustee Server file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Passive Key Trustee Server monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`keytrustee_passive_server_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Passive Key Trustee Server Host Health

This Passive Key Trustee Server health test factors in the health of the host upon which the Passive Key Trustee Server is running. A failure of this test means that the host running the Passive Key Trustee Server is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Passive Key Trustee Server Host Health Test Passive Key Trustee Server monitoring setting.

Short Name: Host Health

Passive Key Trustee Server Host Health Test

Description

When computing the overall Passive Key Trustee Server health, consider the host's health.

Template Name

`keytrustee_passive_server_host_health_enabled`

Default Value

true

Unit(s)

no unit

Passive Key Trustee Server Log Directory Free Space

This Passive Key Trustee Server health test checks that the filesystem containing the log directory of this Passive Key Trustee Server has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Passive Key Trustee Server monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Passive Key Trustee Server Process Status

This Passive Key Trustee Server health test checks that the Cloudera Manager Agent on the Passive Key Trustee Server host is heart beating correctly and that the process associated with the Passive Key Trustee Server role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Passive Key Trustee Server process, a lack of connectivity to the Cloudera Manager Agent on the Passive Key Trustee Server host, or a problem with the Cloudera Manager Agent. This test can fail either because the Passive Key Trustee Server has crashed or because the Passive Key Trustee Server will not start or stop in a timely fashion. Check the Passive Key

Trustee Server logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Passive Key Trustee Server host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Passive Key Trustee Server host, or look in the Cloudera Manager Agent logs on the Passive Key Trustee Server host for more details. This test can be enabled or disabled using the Passive Key Trustee Server Process Health Test Passive Key Trustee Server monitoring setting.

Short Name: Process Status

Passive Key Trustee Server Process Health Test

Description

Enables the health test that the Passive Key Trustee Server's process state is consistent with the role configuration

Template Name

`keytrustee_passive_server_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Passive Key Trustee Server Swap Memory Usage

This Passive Key Trustee Server health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Passive Key Trustee Server Unexpected Exits

This Passive Key Trustee Server health test checks that the Passive Key Trustee Server has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Passive Key Trustee Server monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Phoenix Health Tests

Phoenix Query Server Health

This is a Phoenix service-level health test that checks that enough of the Query Servers in the cluster are healthy. The test returns "Concerning" health if the number of healthy Query Servers falls below a warning threshold, expressed as a percentage of the total number of Query Servers. The test returns "Bad" health if the number of healthy and "Concerning" Query Servers falls below a critical threshold, expressed as a percentage of the total number of Query Servers. For example, if this test is configured with a warning threshold of 95% and a critical threshold of 90% for a cluster of 100 Query Servers, this test would return "Good" health if 95 or more Query Servers have good health. This test would return "Concerning" health if at least 90 Query Servers have either "Good" or "Concerning" health. If more than 10 Query Servers have bad health, this test would return "Bad" health. A failure of this health test indicates unhealthy Query Servers. Check the status of the individual Query Servers for more information. This test can be configured using the Phoenix Phoenix service-wide monitoring setting.

Short Name: Query Server Health

Healthy Query Server Monitoring Thresholds

Description

The health test thresholds of the overall Query Server health. The check returns "Concerning" health if the percentage of "Healthy" Query Servers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Query Servers falls below the critical threshold.

Template Name

`PHOENIX_PHOENIX_QUERY_SERVER_healthy_thresholds`

Default Value

critical:90.0, warning:99.0

Unit(s)

PERCENT

Query Server Health Tests

Query Server Audit Pipeline Test

This Query Server health test checks that the Auditing for the Query Server role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Query Server process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Query Server host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Query Server monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Query Server File Descriptors

This Query Server health test checks that the number of file descriptors used does not rise above some percentage of the Query Server file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Query Server monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`phoenix_query_server_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Query Server Host Health

This Query Server health test factors in the health of the host upon which the Query Server is running. A failure of this test means that the host running the Query Server is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Query Server Host Health Test Query Server monitoring setting.

Short Name: Host Health

Query Server Host Health Test

Description

When computing the overall Query Server health, consider the host's health.

Template Name

`phoenix_query_server_host_health_enabled`

Default Value

true

Unit(s)

no unit

Query Server Log Directory Free Space

This Query Server health test checks that the filesystem containing the log directory of this Query Server has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Query Server monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Query Server Process Status

This Query Server health test checks that the Cloudera Manager Agent on the Query Server host is heart beating correctly and that the process associated with the Query Server role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Query Server process, a lack of connectivity to the Cloudera Manager Agent on the Query Server host, or a problem with the Cloudera Manager Agent. This test can fail either because the Query Server has crashed or because the Query Server will not start or stop in a timely fashion. Check the Query Server logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Query Server host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Query Server host, or look in the Cloudera Manager Agent logs on the Query Server host for more details. This test can be enabled or disabled using the Query Server Process Health Test Query Server monitoring setting.

Short Name: Process Status

Query Server Process Health Test

Description

Enables the health test that the Query Server's process state is consistent with the role configuration

Template Name

`phoenix_query_server_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Query Server Swap Memory Usage

This Query Server health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Query Server Unexpected Exits

This Query Server health test checks that the Query Server has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Query Server monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Ranger Health Tests

Ranger Admin Health

This is a Ranger service-level health test that checks that enough of the Ranger Admins in the cluster are healthy. The test returns "Concerning" health if the number of healthy Ranger Admins falls below a warning threshold, expressed as a percentage of the total number of Ranger Admins. The test returns "Bad" health if the number of healthy and "Concerning" Ranger Admins falls below a critical threshold, expressed as a percentage of the total number of Ranger Admins. For example, if this test is configured with a warning threshold of 95% and a critical threshold of 90% for a cluster of 100 Ranger Admins, this test would return "Good" health if 95 or more Ranger Admins have good health. This test would return "Concerning" health if at least 90 Ranger Admins have either "Good" or "Concerning" health. If more than 10 Ranger Admins have bad health, this test would return "Bad" health. A failure of this health test indicates unhealthy Ranger Admins. Check the status of the individual Ranger Admins for more information. This test can be configured using the Ranger Ranger service-wide monitoring setting.

Short Name: Ranger Admin Health

Healthy Ranger Admin Monitoring Thresholds

Description

The health test thresholds of the overall Ranger Admin health. The check returns "Concerning" health if the percentage of "Healthy" Ranger Admins falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Ranger Admins falls below the critical threshold.

Template Name

`RANGER_RANGER_ADMIN_healthy_thresholds`

Default Value

critical:49.0, warning:99.0

Unit(s)

PERCENT

Ranger Tagsync Health

This Ranger service-level health test checks for the presence of a running, healthy Ranger Tagsync. The test returns "Bad" health if the service is running and the Ranger Tagsync is not running. In all other cases it returns the health of the Ranger Tagsync. A failure of this health test indicates a stopped or unhealthy Ranger Tagsync. Check the status of the Ranger Tagsync for more information. This test can be enabled or disabled using the Ranger Tagsync Role Health Test Ranger Tagsync service-wide monitoring setting.

Short Name: Ranger Tagsync Health

Ranger Tagsync Role Health Test

Description

When computing the overall RANGER health, consider Ranger Tagsync's health

Template Name

`RANGER_RANGER_TAGSYNC_health_enabled`

Default Value

true

Unit(s)

no unit

Ranger Usersync Health

This Ranger service-level health test checks for the presence of a running, healthy Ranger Usersync. The test returns "Bad" health if the service is running and the Ranger Usersync is not running. In all other cases it returns the health of the Ranger Usersync. A failure of this health test indicates a stopped or unhealthy Ranger Usersync. Check the status

of the Ranger Usersync for more information. This test can be enabled or disabled using the Ranger Usersync Role Health Test Ranger Usersync service-wide monitoring setting.

Short Name: Ranger Usersync Health

Ranger Usersync Role Health Test

Description

When computing the overall RANGER health, consider Ranger Usersync's health

Template Name

`RANGER_RANGER_USERSYNC_health_enabled`

Default Value

true

Unit(s)

no unit

Ranger Admin Health Tests

Ranger Admin Audit Pipeline Test

This Ranger Admin health test checks that the Auditing for the Ranger Admin role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Ranger Admin process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Ranger Admin host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Ranger Admin monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Ranger Admin File Descriptors

This Ranger Admin health test checks that the number of file descriptors used does not rise above some percentage of the Ranger Admin file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Ranger Admin monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`ranger_admin_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Ranger Admin Host Health

This Ranger Admin health test factors in the health of the host upon which the Ranger Admin is running. A failure of this test means that the host running the Ranger Admin is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Ranger Admin Host Health Test Ranger Admin monitoring setting.

Short Name: Host Health

Ranger Admin Host Health Test

Description

When computing the overall Ranger Admin health, consider the host's health.

Template Name

`ranger_admin_host_health_enabled`

Default Value

true

Unit(s)

no unit

Ranger Admin Log Directory Free Space

This Ranger Admin health test checks that the filesystem containing the log directory of this Ranger Admin has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Ranger Admin monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Ranger Admin Process Status

This Ranger Admin health test checks that the Cloudera Manager Agent on the Ranger Admin host is heart beating correctly and that the process associated with the Ranger Admin role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Ranger Admin process, a lack of connectivity to the Cloudera Manager Agent on the Ranger Admin host, or a problem with the Cloudera Manager Agent. This test can fail either because the Ranger Admin has crashed or because the Ranger Admin will not start or stop in a timely fashion. Check the Ranger Admin logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Ranger Admin host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Ranger Admin host, or look in the Cloudera Manager Agent logs on the Ranger Admin host for more details. This test can be enabled or disabled using the Ranger Admin Process Health Test Ranger Admin monitoring setting.

Short Name: Process Status

Ranger Admin Process Health Test

Description

Enables the health test that the Ranger Admin's process state is consistent with the role configuration

Template Name

`ranger_admin_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Ranger Admin Swap Memory Usage

This Ranger Admin health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Ranger Admin Unexpected Exits

This Ranger Admin health test checks that the Ranger Admin has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Ranger Admin monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Ranger KMS Health Tests

Ranger KMS Server Health

This is a Ranger KMS service-level health test that checks that enough of the Ranger KMS Servers in the cluster are healthy. The test returns "Concerning" health if the number of healthy Ranger KMS Servers falls below a warning threshold, expressed as a percentage of the total number of Ranger KMS Servers. The test returns "Bad" health if the number of healthy and "Concerning" Ranger KMS Servers falls below a critical threshold, expressed as a percentage of the total number of Ranger KMS Servers. For example, if this test is configured with a warning threshold of 95% and a critical threshold of 90% for a cluster of 100 Ranger KMS Servers, this test would return "Good" health if 95 or more Ranger KMS Servers have good health. This test would return "Concerning" health if at least 90 Ranger KMS Servers have either "Good" or "Concerning" health. If more than 10 Ranger KMS Servers have bad health, this test would return "Bad" health. A failure of this health test indicates unhealthy Ranger KMS Servers. Check the status of the individual Ranger KMS Servers for more information. This test can be configured using the Ranger KMS Ranger KMS service-wide monitoring setting.

Short Name: Ranger KMS Server Health

Healthy Ranger KMS Server Monitoring Thresholds

Description

The health test thresholds of the overall Ranger KMS Server health. The check returns "Concerning" health if the percentage of "Healthy" Ranger KMS Servers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Ranger KMS Servers falls below the critical threshold.

Template Name

`RANGER_KMS_RANGER_KMS_SERVER_healthy_thresholds`

Default Value

critical:49.0, warning:99.0

Unit(s)

PERCENT

Ranger KMS Server Health Tests

Ranger KMS Server Audit Pipeline Test

This Ranger KMS Server health test checks that the Auditing for the Ranger KMS Server role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Ranger KMS Server process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Ranger KMS Server host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Ranger KMS Server monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Ranger KMS Server File Descriptors

This Ranger KMS Server health test checks that the number of file descriptors used does not rise above some percentage of the Ranger KMS Server file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Ranger KMS Server monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`ranger_kms_server_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Ranger KMS Server Host Health

This Ranger KMS Server health test factors in the health of the host upon which the Ranger KMS Server is running. A failure of this test means that the host running the Ranger KMS Server is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Ranger KMS Server Host Health Test Ranger KMS Server monitoring setting.

Short Name: Host Health

Ranger KMS Server Host Health Test

Description

When computing the overall Ranger KMS Server health, consider the host's health.

Template Name

`ranger_kms_server_host_health_enabled`

Default Value

true

Unit(s)

no unit

Ranger KMS Server Log Directory Free Space

This Ranger KMS Server health test checks that the filesystem containing the log directory of this Ranger KMS Server has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Ranger KMS Server monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Ranger KMS Server Process Status

This Ranger KMS Server health test checks that the Cloudera Manager Agent on the Ranger KMS Server host is heart beating correctly and that the process associated with the Ranger KMS Server role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Ranger KMS Server process, a lack of connectivity to the Cloudera Manager Agent on the Ranger KMS Server host, or a problem with the Cloudera Manager Agent. This test can fail either because the Ranger KMS Server has crashed or because the Ranger KMS Server will not start or stop in a timely fashion. Check the Ranger KMS Server logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Ranger KMS Server host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Ranger KMS Server host, or look in the Cloudera Manager Agent logs on the Ranger KMS Server host for more details. This test can be enabled or disabled using the Ranger KMS Server Process Health Test Ranger KMS Server monitoring setting.

Short Name: Process Status

Ranger KMS Server Process Health Test

Description

Enables the health test that the Ranger KMS Server's process state is consistent with the role configuration

Template Name

`ranger_kms_server_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Ranger KMS Server Swap Memory Usage

This Ranger KMS Server health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Ranger KMS Server Unexpected Exits

This Ranger KMS Server health test checks that the Ranger KMS Server has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Ranger KMS Server monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Ranger KMS Server with KTS Health Tests

Ranger KMS Server with KTS Audit Pipeline Test

This Ranger KMS Server with KTS health test checks that the Auditing for the Ranger KMS Server with KTS role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Ranger KMS Server with KTS process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Ranger KMS Server with KTS host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Ranger KMS Server with KTS monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Ranger KMS Server with KTS File Descriptors

This Ranger KMS Server with KTS health test checks that the number of file descriptors used does not rise above some percentage of the Ranger KMS Server with KTS file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Ranger KMS Server with KTS monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`ranger_kms_server_kts_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Ranger KMS Server with KTS Host Health

This Ranger KMS Server with KTS health test factors in the health of the host upon which the Ranger KMS Server with KTS is running. A failure of this test means that the host running the Ranger KMS Server with KTS is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Ranger KMS Server with KTS Host Health Test Ranger KMS Server with KTS monitoring setting.

Short Name: Host Health

Ranger KMS Server with KTS Host Health Test

Description

When computing the overall Ranger KMS Server with KTS health, consider the host's health.

Template Name

`ranger_kms_server_kts_host_health_enabled`

Default Value

true

Unit(s)

no unit

Ranger KMS Server with KTS Log Directory Free Space

This Ranger KMS Server with KTS health test checks that the filesystem containing the log directory of this Ranger KMS Server with KTS has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Ranger KMS Server with KTS monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Ranger KMS Server with KTS Process Status

This Ranger KMS Server with KTS health test checks that the Cloudera Manager Agent on the Ranger KMS Server with KTS host is heart beating correctly and that the process associated with the Ranger KMS Server with KTS role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Ranger KMS Server with KTS process, a lack of connectivity to the Cloudera Manager Agent on the Ranger KMS Server with KTS host, or a problem with the Cloudera Manager Agent. This test can fail either because the Ranger KMS Server with KTS has crashed or because the Ranger KMS Server with KTS will not start or stop in a timely fashion. Check the Ranger KMS Server with KTS logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Ranger KMS Server with KTS host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Ranger KMS Server with KTS host, or look in the Cloudera Manager Agent logs on the Ranger KMS Server with KTS host for more details. This test can be enabled or disabled using the Ranger KMS Server with KTS Process Health Test Ranger KMS Server with KTS monitoring setting.

Short Name: Process Status

Ranger KMS Server with KTS Process Health Test

Description

Enables the health test that the Ranger KMS Server with KTS's process state is consistent with the role configuration

Template Name

`ranger_kms_server_kts_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Ranger KMS Server with KTS Swap Memory Usage

This Ranger KMS Server with KTS health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Ranger KMS Server with KTS Unexpected Exits

This Ranger KMS Server with KTS health test checks that the Ranger KMS Server with KTS has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Ranger KMS Server with KTS monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Ranger KMS with Key Trustee Server Health Tests

Ranger KMS with Key Trustee Server Ranger KMS Server with KTS Health

This is a Ranger KMS with Key Trustee Server service-level health test that checks that enough of the Ranger KMS Server with KTSs in the cluster are healthy. The test returns "Concerning" health if the number of healthy Ranger KMS Server with KTSs falls below a warning threshold, expressed as a percentage of the total number of Ranger KMS Server with KTSs. The test returns "Bad" health if the number of healthy and "Concerning" Ranger KMS Server with KTSs falls below a critical threshold, expressed as a percentage of the total number of Ranger KMS Server with KTSs. For example, if this test is configured with a warning threshold of 95% and a critical threshold of 90% for a cluster of 100 Ranger KMS Server with KTSs, this test would return "Good" health if 95 or more Ranger KMS Server with KTSs have good health. This test would return "Concerning" health if at least 90 Ranger KMS Server with KTSs have either "Good" or "Concerning" health. If more than 10 Ranger KMS Server with KTSs have bad health, this test would return "Bad" health. A failure of this health test indicates unhealthy Ranger KMS Server with KTSs. Check the status of the individual Ranger KMS Server with KTSs for more information. This test can be configured using the Ranger KMS with Key Trustee Server Ranger KMS with Key Trustee Server service-wide monitoring setting.

Short Name: Ranger KMS Server with KTS Health

Healthy Ranger KMS Server with KTS Monitoring Thresholds

Description

The health test thresholds of the overall Ranger KMS Server with KTS health. The check returns "Concerning" health if the percentage of "Healthy" Ranger KMS Server with KTSs falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Ranger KMS Server with KTSs falls below the critical threshold.

Template Name

`RANGER_KMS_KTS_RANGER_KMS_SERVER_KTS_healthy_thresholds`

Default Value

critical:49.0, warning:99.0

Unit(s)

PERCENT

Ranger RMS Health Tests

Ranger RMS Server Health

This is a Ranger RMS service-level health test that checks that enough of the Ranger RMS Servers in the cluster are healthy. The test returns "Concerning" health if the number of healthy Ranger RMS Servers falls below a warning threshold, expressed as a percentage of the total number of Ranger RMS Servers. The test returns "Bad" health if the number of healthy and "Concerning" Ranger RMS Servers falls below a critical threshold, expressed as a percentage of the total number of Ranger RMS Servers. For example, if this test is configured with a warning threshold of 95% and a critical threshold of 90% for a cluster of 100 Ranger RMS Servers, this test would return "Good" health if 95 or more Ranger RMS Servers have good health. This test would return "Concerning" health if at least 90 Ranger RMS Servers have either "Good" or "Concerning" health. If more than 10 Ranger RMS Servers have bad health, this test would return "Bad" health. A failure of this health test indicates unhealthy Ranger RMS Servers. Check the status of the individual Ranger RMS Servers for more information. This test can be configured using the Ranger RMS Ranger RMS service-wide monitoring setting.

Short Name: Ranger RMS Server Health

Healthy Ranger RMS Server Monitoring Thresholds

Description

The health test thresholds of the overall Ranger RMS Server health. The check returns "Concerning" health if the percentage of "Healthy" Ranger RMS Servers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Ranger RMS Servers falls below the critical threshold.

Template Name

`RANGER_RMS_RANGER_RMS_SERVER_healthy_thresholds`

Default Value

critical:49.0, warning:99.0

Unit(s)

PERCENT

Ranger RMS Server Health Tests

Ranger RMS Server Audit Pipeline Test

This Ranger RMS Server health test checks that the Auditing for the Ranger RMS Server role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Ranger RMS Server process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Ranger RMS Server host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Ranger RMS Server monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Ranger RMS Server File Descriptors

This Ranger RMS Server health test checks that the number of file descriptors used does not rise above some percentage of the Ranger RMS Server file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Ranger RMS Server monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`ranger_rms_server_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Ranger RMS Server Host Health

This Ranger RMS Server health test factors in the health of the host upon which the Ranger RMS Server is running. A failure of this test means that the host running the Ranger RMS Server is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Ranger RMS Server Host Health Test Ranger RMS Server monitoring setting.

Short Name: Host Health

Ranger RMS Server Host Health Test

Description

When computing the overall Ranger RMS Server health, consider the host's health.

Template Name

`ranger_rms_server_host_health_enabled`

Default Value

true

Unit(s)

no unit

Ranger RMS Server Log Directory Free Space

This Ranger RMS Server health test checks that the filesystem containing the log directory of this Ranger RMS Server has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Ranger RMS Server monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Ranger RMS Server Process Status

This Ranger RMS Server health test checks that the Cloudera Manager Agent on the Ranger RMS Server host is heart beating correctly and that the process associated with the Ranger RMS Server role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Ranger RMS Server process, a lack of connectivity to the Cloudera Manager Agent on the Ranger RMS Server host, or a problem with the Cloudera Manager Agent. This test can fail either because the Ranger RMS Server has crashed or because the Ranger RMS Server will not start or stop in a timely fashion. Check the Ranger RMS Server logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Ranger RMS Server host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Ranger RMS Server host, or look in the Cloudera Manager Agent logs on the Ranger RMS Server host for more details. This test can be enabled or disabled using the Ranger RMS Server Process Health Test Ranger RMS Server monitoring setting.

Short Name: Process Status

Ranger RMS Server Process Health Test

Description

Enables the health test that the Ranger RMS Server's process state is consistent with the role configuration

Template Name

`ranger_rms_server_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Ranger RMS Server Swap Memory Usage

This Ranger RMS Server health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Ranger RMS Server Unexpected Exits

This Ranger RMS Server health test checks that the Ranger RMS Server has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Ranger RMS Server monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Ranger Raz Health Tests

Ranger Raz Server Health

This is a Ranger Raz service-level health test that checks that enough of the Ranger Raz Servers in the cluster are healthy. The test returns "Concerning" health if the number of healthy Ranger Raz Servers falls below a warning threshold, expressed as a percentage of the total number of Ranger Raz Servers. The test returns "Bad" health if the number of healthy and "Concerning" Ranger Raz Servers falls below a critical threshold, expressed as a percentage of the total number of Ranger Raz Servers. For example, if this test is configured with a warning threshold of 95% and a critical threshold of 90% for a cluster of 100 Ranger Raz Servers, this test would return "Good" health if 95

or more Ranger Raz Servers have good health. This test would return "Concerning" health if at least 90 Ranger Raz Servers have either "Good" or "Concerning" health. If more than 10 Ranger Raz Servers have bad health, this test would return "Bad" health. A failure of this health test indicates unhealthy Ranger Raz Servers. Check the status of the individual Ranger Raz Servers for more information. This test can be configured using the Ranger Raz Ranger Raz service-wide monitoring setting.

Short Name: Ranger Raz Server Health

Healthy Ranger Raz Server Monitoring Thresholds

Description

The health test thresholds of the overall Ranger Raz Server health. The check returns "Concerning" health if the percentage of "Healthy" Ranger Raz Servers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Ranger Raz Servers falls below the critical threshold.

Template Name

`RANGER_RAZ_RANGER_RAZ_SERVER_healthy_thresholds`

Default Value

critical:49.0, warning:99.0

Unit(s)

PERCENT

Ranger Raz Server Health Tests

Ranger Raz Server Audit Pipeline Test

This Ranger Raz Server health test checks that the Auditing for the Ranger Raz Server role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Ranger Raz Server process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Ranger Raz Server host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Ranger Raz Server monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Ranger Raz Server File Descriptors

This Ranger Raz Server health test checks that the number of file descriptors used does not rise above some percentage of the Ranger Raz Server file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Ranger Raz Server monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`ranger_raz_server_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Ranger Raz Server Host Health

This Ranger Raz Server health test factors in the health of the host upon which the Ranger Raz Server is running. A failure of this test means that the host running the Ranger Raz Server is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Ranger Raz Server Host Health Test Ranger Raz Server monitoring setting.

Short Name: Host Health

Ranger Raz Server Host Health Test

Description

When computing the overall Ranger Raz Server health, consider the host's health.

Template Name

`ranger_raz_server_host_health_enabled`

Default Value

true

Unit(s)

no unit

Ranger Raz Server Log Directory Free Space

This Ranger Raz Server health test checks that the filesystem containing the log directory of this Ranger Raz Server has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Ranger Raz Server monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Ranger Raz Server Process Status

This Ranger Raz Server health test checks that the Cloudera Manager Agent on the Ranger Raz Server host is heart beating correctly and that the process associated with the Ranger Raz Server role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Ranger Raz Server process, a lack of connectivity to the Cloudera Manager Agent on the Ranger Raz Server host, or a problem with the Cloudera Manager Agent. This test can fail either because the Ranger Raz Server has crashed or because the Ranger Raz Server will not start or stop in a timely fashion. Check the Ranger Raz Server logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Ranger Raz Server host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Ranger Raz Server host, or look in the Cloudera Manager Agent logs on the Ranger Raz Server host for more details. This test can be enabled or disabled using the Ranger Raz Server Process Health Test Ranger Raz Server monitoring setting.

Short Name: Process Status

Ranger Raz Server Process Health Test

Description

Enables the health test that the Ranger Raz Server's process state is consistent with the role configuration

Template Name

`ranger_raz_server_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Ranger Raz Server Swap Memory Usage

This Ranger Raz Server health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Ranger Raz Server Unexpected Exits

This Ranger Raz Server health test checks that the Ranger Raz Server has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Ranger Raz Server monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Ranger Tagsync Health Tests

Ranger Tagsync Audit Pipeline Test

This Ranger Tagsync health test checks that the Auditing for the Ranger Tagsync role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Ranger Tagsync process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Ranger Tagsync host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Ranger Tagsync monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Ranger Tagsync File Descriptors

This Ranger Tagsync health test checks that the number of file descriptors used does not rise above some percentage of the Ranger Tagsync file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Ranger Tagsync monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`ranger_tagsync_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Ranger Tagsync Host Health

This Ranger Tagsync health test factors in the health of the host upon which the Ranger Tagsync is running. A failure of this test means that the host running the Ranger Tagsync is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Ranger Tagsync Host Health Test Ranger Tagsync monitoring setting.

Short Name: Host Health

Ranger Tagsync Host Health Test

Description

When computing the overall Ranger Tagsync health, consider the host's health.

Template Name

`ranger_tagsync_host_health_enabled`

Default Value

true

Unit(s)

no unit

Ranger Tagsync Log Directory Free Space

This Ranger Tagsync health test checks that the filesystem containing the log directory of this Ranger Tagsync has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Ranger Tagsync monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Ranger Tagsync Process Status

This Ranger Tagsync health test checks that the Cloudera Manager Agent on the Ranger Tagsync host is heart beating correctly and that the process associated with the Ranger Tagsync role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Ranger Tagsync process, a lack of connectivity to the Cloudera Manager Agent on the Ranger Tagsync host, or a problem with the Cloudera Manager Agent. This test can fail either because the Ranger Tagsync has crashed or because the Ranger Tagsync will not start or stop in a timely fashion. Check the Ranger Tagsync logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Ranger Tagsync host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Ranger Tagsync host, or look in the Cloudera Manager Agent logs on the Ranger Tagsync host for more details. This test can be enabled or disabled using the Ranger Tagsync Process Health Test Ranger Tagsync monitoring setting.

Short Name: Process Status

Ranger Tagsync Process Health Test

Description

Enables the health test that the Ranger Tagsync's process state is consistent with the role configuration

Template Name

`ranger_tagsync_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Ranger Tagsync Swap Memory Usage

This Ranger Tagsync health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Ranger Tagsync Unexpected Exits

This Ranger Tagsync health test checks that the Ranger Tagsync has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Ranger Tagsync monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Ranger Usersync Health Tests

Ranger Usersync Audit Pipeline Test

This Ranger Usersync health test checks that the Auditing for the Ranger Usersync role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Ranger Usersync process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Ranger Usersync host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Ranger Usersync monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Ranger Usersync File Descriptors

This Ranger Usersync health test checks that the number of file descriptors used does not rise above some percentage of the Ranger Usersync file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Ranger Usersync monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`ranger_usersync_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Ranger Usersync Host Health

This Ranger Usersync health test factors in the health of the host upon which the Ranger Usersync is running. A failure of this test means that the host running the Ranger Usersync is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Ranger Usersync Host Health Test Ranger Usersync monitoring setting.

Short Name: Host Health

Ranger Usersync Host Health Test

Description

When computing the overall Ranger Usersync health, consider the host's health.

Template Name

`ranger_usersync_host_health_enabled`

Default Value

true

Unit(s)

no unit

Ranger Usersync Log Directory Free Space

This Ranger Usersync health test checks that the filesystem containing the log directory of this Ranger Usersync has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Ranger Usersync monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Ranger Usersync Process Status

This Ranger Usersync health test checks that the Cloudera Manager Agent on the Ranger Usersync host is heart beating correctly and that the process associated with the Ranger Usersync role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Ranger Usersync process, a lack of connectivity to the Cloudera Manager Agent on the Ranger Usersync host, or a problem with the Cloudera Manager Agent. This test can fail either because the Ranger Usersync has crashed or because the Ranger Usersync will not start or stop in a timely fashion. Check the Ranger Usersync logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Ranger Usersync host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Ranger Usersync host, or look in the Cloudera Manager Agent logs on the Ranger Usersync host for more details. This test can be enabled or disabled using the Ranger Usersync Process Health Test Ranger Usersync monitoring setting.

Short Name: Process Status

Ranger Usersync Process Health Test

Description

Enables the health test that the Ranger Usersync's process state is consistent with the role configuration

Template Name

`ranger_usersync_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Ranger Usersync Swap Memory Usage

This Ranger Usersync health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Ranger Usersync Unexpected Exits

This Ranger Usersync health test checks that the Ranger Usersync has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Ranger Usersync monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

RegionServer Health Tests

RegionServer Audit Pipeline Test

This RegionServer health test checks that the Auditing for the RegionServer role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of RegionServer process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the RegionServer host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check RegionServer monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

RegionServer Cluster Connectivity

This is a RegionServer health test that checks whether the Master considers the RegionServer alive. A failure of this health test may indicate that the RegionServer is having trouble communicating with at least the HBase Master and possibly the entire HBase cluster. Look in the RegionServer logs for more details. This test can be enabled or disabled using the HBase RegionServer to Master Connectivity Test RegionServer monitoring setting. The HBase Region Server Connectivity Tolerance at Startup RegionServer monitoring setting and the Health Test Startup Tolerance Master monitoring setting can be used to control the test's tolerance windows around RegionServer and Master restarts respectively.

Short Name: Cluster Connectivity

HBase Region Server Connectivity Tolerance at Startup

Description

The amount of time to wait for the HBase Region Server to fully start up and connect to the HBase Master before enforcing the connectivity check.

Template Name

`regionserver_connectivity_tolerance`

Default Value

180

Unit(s)

SECONDS

HBase RegionServer to Master Connectivity Test

Description

Enables the health test that the RegionServer is connected to the Master

Template Name

`regionserver_master_connectivity_enabled`

Default Value

true

Unit(s)

no unit

Health Test Startup Tolerance

Description

The amount of time allowed after this role is started that failures of health tests that rely on communication with this role will be tolerated.

Template Name

`master_startup_tolerance`

Default Value

5

Unit(s)

MINUTES

RegionServer Compaction Queue Size

This is a RegionServer health test that checks that a moving average of the size of the RegionServer's compaction queue does not exceed some value. A failure of this health test indicates a high write load on the RegionServer. Try reducing the write load on the RegionServer, increasing capacity by adding additional disks to the RegionServer, or adding additional RegionServers. This test can be configured using the HBase RegionServer Compaction Queue Monitoring Thresholds and HBase RegionServer Compaction Queue Monitoring Period RegionServer monitoring settings.

Short Name: Compaction Queue Size

HBase RegionServer Compaction Queue Monitoring Period

Description

The period over which to compute the moving average of the compaction queue size.

Template Name

`regionserver_compaction_queue_window`

Default Value

5

Unit(s)

MINUTES

HBase RegionServer Compaction Queue Monitoring Thresholds

Description

The health test thresholds of the weighted average size of the HBase RegionServer compaction queue over a recent period. See HBase RegionServer Compaction Queue Monitoring Period.

Template Name

`regionserver_compaction_queue_thresholds`

Default Value

critical:never, warning:10.0

Unit(s)

no unit

RegionServer File Descriptors

This RegionServer health test checks that the number of file descriptors used does not rise above some percentage of the RegionServer file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds RegionServer monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`regionserver_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

RegionServer Flush Queue Size

This is a RegionServer health test that checks that a moving average of the size of the RegionServer's flush queue does not exceed some value. A failure of this health test indicates a high write load on the RegionServer. Try reducing the write load on the RegionServer, increasing capacity by adding additional disks to the RegionServer, or adding additional RegionServers. This test can be configured using the HBase RegionServer Flush Queue Monitoring Thresholds and HBase RegionServer Flush Queue Monitoring Period RegionServer monitoring settings.

Short Name: Flush Queue Size

HBase RegionServer Flush Queue Monitoring Period

Description

The period over which to compute the moving average of the flush queue size.

Template Name

`regionserver_flush_queue_window`

Default Value

5

Unit(s)

MINUTES

HBase RegionServer Flush Queue Monitoring Thresholds

Description

The health test thresholds of the average size of the HBase RegionServer flush queue over a recent period. See HBase RegionServer Flush Queue Monitoring Period.

Template Name

`regionserver_flush_queue_thresholds`

Default Value

critical:never, warning:10.0

Unit(s)

no unit

RegionServer GC Duration

This RegionServer health test checks that the RegionServer is not spending too much time performing Java garbage collection. It checks that no more than some percentage of recent time is spent performing Java garbage collection. A failure of this health test may indicate a capacity planning problem or misconfiguration of the RegionServer. This test can be configured using the Garbage Collection Duration Thresholds and Garbage Collection Duration Monitoring Period RegionServer monitoring settings.

Short Name: GC Duration

Garbage Collection Duration Monitoring Period

Description

The period to review when computing the moving average of garbage collection time.

Template Name

`regionserver_gc_duration_window`

Default Value

5

Unit(s)

MINUTES

Garbage Collection Duration Thresholds

Description

The health test thresholds for the weighted average time spent in Java garbage collection. Specified as a percentage of elapsed wall clock time.

Template Name

`regionserver_gc_duration_thresholds`

Default Value

critical:60.0, warning:30.0

Unit(s)

no unit

RegionServer Heap Dump Directory Free Space

This RegionServer health test checks that the filesystem containing the heap dump directory of this RegionServer has sufficient free space. This test can be configured using the Heap Dump Directory Free Space Monitoring Absolute Thresholds and Heap Dump Directory Free Space Monitoring Percentage Thresholds RegionServer monitoring settings.

Short Name: Heap Dump Directory Free Space

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Template Name

`heap_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`heap_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

RegionServer Host Health

This RegionServer health test factors in the health of the host upon which the RegionServer is running. A failure of this test means that the host running the RegionServer is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the RegionServer Host Health Test RegionServer monitoring setting.

Short Name: Host Health

RegionServer Host Health Test

Description

When computing the overall RegionServer health, consider the host's health.

Template Name

`regionserver_host_health_enabled`

Default Value

true

Unit(s)

no unit

RegionServer Log Directory Free Space

This RegionServer health test checks that the filesystem containing the log directory of this RegionServer has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds RegionServer monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

RegionServer Memstore Size

This is a RegionServer health test that checks that the amount of the RegionServer's memory devoted to memstores does not exceed some percentage of the RegionServer's configured hbase.regionserver.global.memstore.upperLimit. When a RegionServer's memstores reach this maximum size, new updates are blocked while the RegionServer flushes. A failure of this health test indicates a high write load on the RegionServer. Try reducing the write load

on the RegionServer, increasing capacity by adding additional disks to the RegionServer, or adding additional RegionServers. This test can be configured using the HBase RegionServer Memstore Size Thresholds RegionServer monitoring setting.

Short Name: Memstore Size

HBase RegionServer Memstore Size Thresholds

Description

The health test thresholds of the total size of RegionServer's memstores. Specified as a percentage of the configured upper limit. See Maximum Size of All Memstores in RegionServer.

Template Name

`regionserver_memstore_size_thresholds`

Default Value

critical:100.0, warning:95.0

Unit(s)

PERCENT

RegionServer Process Status

This RegionServer health test checks that the Cloudera Manager Agent on the RegionServer host is heart beating correctly and that the process associated with the RegionServer role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the RegionServer process, a lack of connectivity to the Cloudera Manager Agent on the RegionServer host, or a problem with the Cloudera Manager Agent. This test can fail either because the RegionServer has crashed or because the RegionServer will not start or stop in a timely fashion. Check the RegionServer logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the RegionServer host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the RegionServer host, or look in the Cloudera Manager Agent logs on the RegionServer host for more details. This test can be enabled or disabled using the RegionServer Process Health Test RegionServer monitoring setting.

Short Name: Process Status

RegionServer Process Health Test

Description

Enables the health test that the RegionServer's process state is consistent with the role configuration

Template Name

`regionserver_scm_health_enabled`

Default Value

true

Unit(s)

no unit

RegionServer Store File Index Size

This is a RegionServer health test that checks that the sum of the sizes of all store file indexes does not exceed some percentage of the RegionServer's maximum heap size. A failure of this health test indicates that the RegionServer is using a significant portion of its memory for store file indexes. If the amount of memory devoted to these indexes is undesirably high, the size of indexes can be reduced by increasing the HBase block size, by using smaller key values, or by using fewer columns. Each of these choices involves trade-offs. Contact Cloudera Support for more information on this topic. This test can be configured using the Percentage of Heap Used by HStoreFile Index RegionServer monitoring setting.

Short Name: Store File Index Size

Percentage of Heap Used by HStoreFile Index

Description

The health test thresholds of the size used by the HStoreFile index. Specified as a percentage of the total heap size.

Template Name

`regionserver_store_file_idx_size_thresholds`

Default Value

critical:never, warning:10.0

Unit(s)

PERCENT

RegionServer Swap Memory Usage

This RegionServer health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

RegionServer Unexpected Exits

This RegionServer health test checks that the RegionServer has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period RegionServer monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

RegionServer Web Server Status

This health test checks that the role's web server is responding quickly to requests by the Cloudera Manager Agent, and that the Cloudera Manager Agent can collect metrics from the web server. Failure of this health test may indicate a problem with the web server of the RegionServer, a misconfiguration of the RegionServer, or a problem with the Cloudera Manager Agent. Consult the Cloudera Manager Agent logs and the logs of the RegionServer for more detail. If the test failure message indicates a communication problem, the Cloudera Manager Agent's HTTP requests to the RegionServer's web server are failing or timing out. If the test's failure message indicates an unexpected response, the RegionServer's web server responded to the Cloudera Manager Agent's request, but the response could not be interpreted for some reason. This test can be configured using the Web Metric Collection RegionServer monitoring setting.

Short Name: Web Server Status

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Template Name

`regionserver_web_metric_collection_enabled`

Default Value

true

Unit(s)

no unit

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Template Name

`regionserver_web_metric_collection_thresholds`

Default Value

critical:never, warning:10000.0

Unit(s)

MILLISECONDS

Reports Manager Health Tests

Reports Manager Audit Pipeline Test

This Reports Manager health test checks that the Auditing for the Reports Manager role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Reports Manager process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Reports Manager host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Reports Manager monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Reports Manager Cloudera Manager Descriptor Age

This is a Reports Manager health test that checks if the Cloudera Manager descriptor has been refreshed recently. The Cloudera Manager descriptor is used to pass configuration information from the Cloudera Manager Server to the Reports Manager. If the descriptor becomes stale, Reports Manager operation may be impacted because the Reports Manager will receive information about new hosts, roles, and services, or changes to existing hosts, roles, and services. A stale descriptor usually indicates problems communicating with the Cloudera Manager Server but can also indicate performance problems or a bug. Consult the Reports Manager log and the Cloudera Manager Server log for more information. This test can be configured using the Cloudera Manager Descriptor Age Thresholds Cloudera Manager Reports Manager setting.

Short Name: Cloudera Manager Descriptor Age

Cloudera Manager Descriptor Age Thresholds

Description

The health test thresholds for monitoring the time since the Cloudera Manager descriptor was last refreshed.

Template Name

`scm_descriptor_age_thresholds`

Default Value

critical:120000.0, warning:60000.0

Unit(s)

no unit

Reports Manager File Descriptors

This Reports Manager health test checks that the number of file descriptors used does not rise above some percentage of the Reports Manager file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Reports Manager monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`reportsmanager_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Reports Manager Heap Dump Directory Free Space

This Reports Manager health test checks that the filesystem containing the heap dump directory of this Reports Manager has sufficient free space. This test can be configured using the Heap Dump Directory Free Space Monitoring Absolute Thresholds and Heap Dump Directory Free Space Monitoring Percentage Thresholds Reports Manager monitoring settings.

Short Name: Heap Dump Directory Free Space

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Template Name

`heap_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`heap_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Reports Manager Host Health

This Reports Manager health test factors in the health of the host upon which the Reports Manager is running. A failure of this test means that the host running the Reports Manager is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Reports Manager Host Health Test Reports Manager monitoring setting.

Short Name: Host Health

Reports Manager Host Health Test

Description

When computing the overall Reports Manager health, consider the host's health.

Template Name

`reportsmanager_host_health_enabled`

Default Value

true

Unit(s)

no unit

Reports Manager Log Directory Free Space

This Reports Manager health test checks that the filesystem containing the log directory of this Reports Manager has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Reports Manager monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Reports Manager Pause Duration

This Reports Manager health test checks that the Reports Manager threads are not experiencing long scheduling pauses. The test uses a pause monitoring thread in the Reports Manager that tracks scheduling delay by noting if it is run on its requested schedule. If the thread is not run on its requested schedule, the delay is noted and considered pause time. The health test checks that no more than some percentage of recent time is spent paused. A failure of this health test may indicate that the Reports Manager is not getting enough CPU resources, or that it is spending too much time doing garbage collection. Inspect the Reports Manager logs for any pause monitor output and check garbage collection metrics exposed by the Reports Manager. This test can be configured using the Pause Duration Thresholds and Pause Duration Monitoring Period Reports Manager monitoring settings.

Short Name: Pause Duration

Pause Duration Monitoring Period

Description

The period to review when computing the moving average of extra time the pause monitor spent paused.

Template Name

`reportsmanager_pause_duration_window`

Default Value

5

Unit(s)

MINUTES

Pause Duration Thresholds

Description

The health test thresholds for the weighted average extra time the pause monitor spent paused. Specified as a percentage of elapsed wall clock time.

Template Name

`reportsmanager_pause_duration_thresholds`

Default Value

critical:60.0, warning:30.0

Unit(s)

no unit

Reports Manager Process Status

This Reports Manager health test checks that the Cloudera Manager Agent on the Reports Manager host is heart beating correctly and that the process associated with the Reports Manager role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Reports Manager process, a lack of connectivity to the Cloudera Manager Agent on the Reports Manager host, or a problem with the Cloudera Manager Agent. This test can fail either because the Reports Manager has crashed or because the Reports Manager will not start or stop in a timely fashion. Check the Reports Manager logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Reports Manager host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Reports Manager host, or look in the Cloudera Manager Agent logs on the Reports Manager host for more details. This test can be enabled or disabled using the Reports Manager Process Health Test Reports Manager monitoring setting.

Short Name: Process Status

Reports Manager Process Health Test

Description

Enables the health test that the Reports Manager's process state is consistent with the role configuration

Template Name

`reportsmanager_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Reports Manager Reports Manager Working Directory Free Space

This is a Reports Manager health test that checks that the filesystem containing the Reports Manager Working Directory of this Reports Manager has sufficient free space. See the Reports Manager Working Directory description on the Reports Manager configuration page for more information on this directory type. This test can be configured using the Reports Manager Working Directory Free Space Monitoring Absolute Thresholds and Reports Manager Working Directory Free Space Monitoring Percentage Thresholds Reports Manager monitoring settings.

Short Name: Reports Manager Working Directory Free Space

Reports Manager Working Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Reports Manager Working Directory.

Template Name

`reportsmanager_scratch_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Reports Manager Working Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Reports Manager Working Directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Reports Manager Working Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`reportsmanager_scratch_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Reports Manager Swap Memory Usage

This Reports Manager health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Reports Manager Unexpected Exits

This Reports Manager health test checks that the Reports Manager has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Reports Manager monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

ResourceManager Health Tests

ResourceManager Audit Pipeline Test

This ResourceManager health test checks that the Auditing for the ResourceManager role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of ResourceManager process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the ResourceManager host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check ResourceManager monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

ResourceManager File Descriptors

This ResourceManager health test checks that the number of file descriptors used does not rise above some percentage of the ResourceManager file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds ResourceManager monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`resourcemanager_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

ResourceManager GC Duration

This ResourceManager health test checks that the ResourceManager is not spending too much time performing Java garbage collection. It checks that no more than some percentage of recent time is spent performing Java garbage collection. A failure of this health test may indicate a capacity planning problem or misconfiguration of the ResourceManager. This test can be configured using the Garbage Collection Duration Thresholds and Garbage Collection Duration Monitoring Period ResourceManager monitoring settings.

Short Name: GC Duration

Garbage Collection Duration Monitoring Period

Description

The period to review when computing the moving average of garbage collection time.

Template Name

`resourcemanager_gc_duration_window`

Default Value

5

Unit(s)

MINUTES

Garbage Collection Duration Thresholds

Description

The health test thresholds for the weighted average time spent in Java garbage collection. Specified as a percentage of elapsed wall clock time.

Template Name

`resourcemanager_gc_duration_thresholds`

Default Value

critical:60.0, warning:30.0

Unit(s)

no unit

ResourceManager Heap Dump Directory Free Space

This ResourceManager health test checks that the filesystem containing the heap dump directory of this ResourceManager has sufficient free space. This test can be configured using the Heap Dump Directory Free Space Monitoring Absolute Thresholds and Heap Dump Directory Free Space Monitoring Percentage Thresholds ResourceManager monitoring settings.

Short Name: Heap Dump Directory Free Space

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Template Name

`heap_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`heap_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

ResourceManager Host Health

This ResourceManager health test factors in the health of the host upon which the ResourceManager is running. A failure of this test means that the host running the ResourceManager is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the ResourceManager Host Health Test ResourceManager monitoring setting.

Short Name: Host Health

ResourceManager Host Health Test

Description

When computing the overall ResourceManager health, consider the host's health.

Template Name

`resourcemanager_host_health_enabled`

Default Value

true

Unit(s)

no unit

ResourceManager Log Directory Free Space

This ResourceManager health test checks that the filesystem containing the log directory of this ResourceManager has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds ResourceManager monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

ResourceManager Process Status

This ResourceManager health test checks that the Cloudera Manager Agent on the ResourceManager host is heart beating correctly and that the process associated with the ResourceManager role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the ResourceManager process, a lack of connectivity to the Cloudera Manager Agent on the ResourceManager host, or a problem with the Cloudera Manager Agent. This test can fail either because the ResourceManager has crashed or because the ResourceManager will not start or stop in a timely fashion. Check the ResourceManager logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the ResourceManager host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the ResourceManager host, or look in the Cloudera Manager Agent logs on the ResourceManager host for more details. This test can be enabled or disabled using the ResourceManager Process Health Test ResourceManager monitoring setting.

Short Name: Process Status

ResourceManager Process Health Test

Description

Enables the health test that the ResourceManager's process state is consistent with the role configuration

Template Name

`resourcemanager_scm_health_enabled`

Default Value

true

Unit(s)

no unit

ResourceManager Swap Memory Usage

This ResourceManager health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

ResourceManager Unexpected Exits

This ResourceManager health test checks that the ResourceManager has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory

monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period ResourceManager monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

ResourceManager Web Server Status

This health test checks that the role's web server is responding quickly to requests by the Cloudera Manager Agent, and that the Cloudera Manager Agent can collect metrics from the web server. Failure of this health test may indicate a problem with the web server of the ResourceManager, a misconfiguration of the ResourceManager, or a problem with the Cloudera Manager Agent. Consult the Cloudera Manager Agent logs and the logs of the ResourceManager for more detail. If the test failure message indicates a communication problem, the Cloudera Manager Agent's HTTP requests to the ResourceManager's web server are failing or timing out. If the test's failure message indicates an unexpected response, the ResourceManager's web server responded to the Cloudera Manager Agent's request, but the response could not be interpreted for some reason. This test can be configured using the Web Metric Collection ResourceManager monitoring setting.

Short Name: Web Server Status

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Template Name

`resourcemanager_web_metric_collection_enabled`

Default Value

true

Unit(s)

no unit

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Template Name

`resourcemanager_web_metric_collection_thresholds`

Default Value

critical:never, warning:10000.0

Unit(s)

MILLISECONDS

S3 Gateway Health Tests

S3 Gateway Audit Pipeline Test

This S3 Gateway health test checks that the Auditing for the S3 Gateway role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of S3 Gateway process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the S3 Gateway host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check S3 Gateway monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

S3 Gateway File Descriptors

This S3 Gateway health test checks that the number of file descriptors used does not rise above some percentage of the S3 Gateway file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds S3 Gateway monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`s3_gateway_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

S3 Gateway Host Health

This S3 Gateway health test factors in the health of the host upon which the S3 Gateway is running. A failure of this test means that the host running the S3 Gateway is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the S3 Gateway Host Health Test S3 Gateway monitoring setting.

Short Name: Host Health

S3 Gateway Host Health Test

Description

When computing the overall S3 Gateway health, consider the host's health.

Template Name

`s3_gateway_host_health_enabled`

Default Value

true

Unit(s)

no unit

S3 Gateway Log Directory Free Space

This S3 Gateway health test checks that the filesystem containing the log directory of this S3 Gateway has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds S3 Gateway monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

S3 Gateway Process Status

This S3 Gateway health test checks that the Cloudera Manager Agent on the S3 Gateway host is heart beating correctly and that the process associated with the S3 Gateway role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the S3 Gateway process, a lack of connectivity to the Cloudera Manager Agent on the S3 Gateway host, or a problem with the Cloudera Manager Agent. This test can fail either because the S3 Gateway has crashed or because the S3 Gateway will not start or stop in a timely fashion. Check the S3 Gateway logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the S3 Gateway host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the S3 Gateway host, or look in the Cloudera Manager Agent logs on the S3 Gateway host for more details. This test can be enabled or disabled using the S3 Gateway Process Health Test S3 Gateway monitoring setting.

Short Name: Process Status

S3 Gateway Process Health Test

Description

Enables the health test that the S3 Gateway's process state is consistent with the role configuration

Template Name

`s3_gateway_scm_health_enabled`

Default Value

true

Unit(s)

no unit

S3 Gateway Swap Memory Usage

This S3 Gateway health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

S3 Gateway Unexpected Exits

This S3 Gateway health test checks that the S3 Gateway has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period S3 Gateway monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

SRM Driver Health Tests

SRM Driver Audit Pipeline Test

This SRM Driver health test checks that the Auditing for the SRM Driver role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of SRM Driver process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the SRM Driver host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check SRM Driver monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

SRM Driver File Descriptors

This SRM Driver health test checks that the number of file descriptors used does not rise above some percentage of the SRM Driver file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds SRM Driver monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`streams_replication_manager_driver_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

SRM Driver Host Health

This SRM Driver health test factors in the health of the host upon which the SRM Driver is running. A failure of this test means that the host running the SRM Driver is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the SRM Driver Host Health Test SRM Driver monitoring setting.

Short Name: Host Health

SRM Driver Host Health Test

Description

When computing the overall SRM Driver health, consider the host's health.

Template Name

`streams_replication_manager_driver_host_health_enabled`

Default Value

true

Unit(s)

no unit

SRM Driver Log Directory Free Space

This SRM Driver health test checks that the filesystem containing the log directory of this SRM Driver has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds SRM Driver monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

SRM Driver Process Status

This SRM Driver health test checks that the Cloudera Manager Agent on the SRM Driver host is heart beating correctly and that the process associated with the SRM Driver role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the SRM Driver process, a lack of connectivity to the Cloudera Manager Agent on the SRM Driver host, or a problem with the Cloudera Manager Agent. This test can fail either because the SRM Driver has crashed or because the SRM Driver will not start or stop in a timely fashion. Check the SRM Driver logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the SRM Driver host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the SRM Driver host, or look in the Cloudera Manager Agent logs on the SRM Driver host for more details. This test can be enabled or disabled using the SRM Driver Process Health Test SRM Driver monitoring setting.

Short Name: Process Status

SRM Driver Process Health Test

Description

Enables the health test that the SRM Driver's process state is consistent with the role configuration

Template Name

`streams_replication_manager_driver_scm_health_enabled`

Default Value

true

Unit(s)

no unit

SRM Driver Swap Memory Usage

This SRM Driver health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

SRM Driver Unexpected Exits

This SRM Driver health test checks that the SRM Driver has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period SRM Driver monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

SRM Service Health Tests

SRM Service Audit Pipeline Test

This SRM Service health test checks that the Auditing for the SRM Service role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of SRM Service process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the SRM Service host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check SRM Service monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

SRM Service File Descriptors

This SRM Service health test checks that the number of file descriptors used does not rise above some percentage of the SRM Service file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds SRM Service monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`streams_replication_manager_service_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

SRM Service Host Health

This SRM Service health test factors in the health of the host upon which the SRM Service is running. A failure of this test means that the host running the SRM Service is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the SRM Service Host Health Test SRM Service monitoring setting.

Short Name: Host Health

SRM Service Host Health Test

Description

When computing the overall SRM Service health, consider the host's health.

Template Name

`streams_replication_manager_service_host_health_enabled`

Default Value

true

Unit(s)

no unit

SRM Service Log Directory Free Space

This SRM Service health test checks that the filesystem containing the log directory of this SRM Service has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds SRM Service monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

SRM Service Process Status

This SRM Service health test checks that the Cloudera Manager Agent on the SRM Service host is heart beating correctly and that the process associated with the SRM Service role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the SRM Service process, a lack of connectivity to the Cloudera Manager Agent on the SRM Service host, or a problem with the Cloudera Manager Agent. This test can fail either because the SRM Service has crashed or because the SRM Service will not start or stop in a timely fashion. Check the SRM Service logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the SRM Service host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the SRM Service host, or look in the Cloudera Manager Agent logs on the SRM Service host for more details. This test can be enabled or disabled using the SRM Service Process Health Test SRM Service monitoring setting.

Short Name: Process Status

SRM Service Process Health Test

Description

Enables the health test that the SRM Service's process state is consistent with the role configuration

Template Name

`streams_replication_manager_service_scm_health_enabled`

Default Value

true

Unit(s)

no unit

SRM Service Swap Memory Usage

This SRM Service health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

SRM Service Unexpected Exits

This SRM Service health test checks that the SRM Service has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period SRM Service monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Schema Registry Health Tests

Schema Registry Server Health

This is a Schema Registry service-level health test that checks that enough of the Schema Registry Servers in the cluster are healthy. The test returns "Concerning" health if the number of healthy Schema Registry Servers falls below a warning threshold, expressed as a percentage of the total number of Schema Registry Servers. The test returns "Bad" health if the number of healthy and "Concerning" Schema Registry Servers falls below a critical threshold, expressed as a percentage of the total number of Schema Registry Servers. For example, if this test is configured with a warning threshold of 95% and a critical threshold of 90% for a cluster of 100 Schema Registry Servers, this test would return "Good" health if 95 or more Schema Registry Servers have good health. This test would return "Concerning" health if at least 90 Schema Registry Servers have either "Good" or "Concerning" health. If more than 10 Schema Registry Servers have bad health, this test would return "Bad" health. A failure of this health test indicates unhealthy Schema Registry Servers. Check the status of the individual Schema Registry Servers for more information. This test can be configured using the Schema Registry Schema Registry service-wide monitoring setting.

Short Name: Schema Registry Server Health

Healthy Schema Registry Server Monitoring Thresholds

Description

The health test thresholds of the overall Schema Registry Server health. The check returns "Concerning" health if the percentage of "Healthy" Schema Registry Servers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Schema Registry Servers falls below the critical threshold.

Template Name

`SCHEMAREGISTRY_SCHEMA_REGISTRY_SERVER_healthy_thresholds`

Default Value

critical:49.99, warning:99.99

Unit(s)

PERCENT

Schema Registry Server Health Tests

Schema Registry Server Audit Pipeline Test

This Schema Registry Server health test checks that the Auditing for the Schema Registry Server role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Schema Registry Server process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Schema Registry Server host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Schema Registry Server monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Schema Registry Server File Descriptors

This Schema Registry Server health test checks that the number of file descriptors used does not rise above some percentage of the Schema Registry Server file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Schema Registry Server monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`schema_registry_server_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Schema Registry Server Host Health

This Schema Registry Server health test factors in the health of the host upon which the Schema Registry Server is running. A failure of this test means that the host running the Schema Registry Server is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Schema Registry Server Host Health Test Schema Registry Server monitoring setting.

Short Name: Host Health

Schema Registry Server Host Health Test

Description

When computing the overall Schema Registry Server health, consider the host's health.

Template Name

`schema_registry_server_host_health_enabled`

Default Value

true

Unit(s)

no unit

Schema Registry Server Log Directory Free Space

This Schema Registry Server health test checks that the filesystem containing the log directory of this Schema Registry Server has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Schema Registry Server monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Schema Registry Server Process Status

This Schema Registry Server health test checks that the Cloudera Manager Agent on the Schema Registry Server host is heart beating correctly and that the process associated with the Schema Registry Server role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Schema Registry Server

process, a lack of connectivity to the Cloudera Manager Agent on the Schema Registry Server host, or a problem with the Cloudera Manager Agent. This test can fail either because the Schema Registry Server has crashed or because the Schema Registry Server will not start or stop in a timely fashion. Check the Schema Registry Server logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Schema Registry Server host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Schema Registry Server host, or look in the Cloudera Manager Agent logs on the Schema Registry Server host for more details. This test can be enabled or disabled using the Schema Registry Server Process Health Test Schema Registry Server monitoring setting.

Short Name: Process Status

Schema Registry Server Process Health Test

Description

Enables the health test that the Schema Registry Server's process state is consistent with the role configuration

Template Name

`schema_registry_server_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Schema Registry Server Swap Memory Usage

This Schema Registry Server health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Schema Registry Server Unexpected Exits

This Schema Registry Server health test checks that the Schema Registry Server has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Schema Registry Server monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

SecondaryNameNode Health Tests

SecondaryNameNode Audit Pipeline Test

This SecondaryNameNode health test checks that the Auditing for the SecondaryNameNode role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of SecondaryNameNode process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the SecondaryNameNode host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check SecondaryNameNode monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

SecondaryNameNode File Descriptors

This SecondaryNameNode health test checks that the number of file descriptors used does not rise above some percentage of the SecondaryNameNode file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds SecondaryNameNode monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`secondarynamenode_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

SecondaryNameNode GC Duration

This SecondaryNameNode health test checks that the SecondaryNameNode is not spending too much time performing Java garbage collection. It checks that no more than some percentage of recent time is spent performing Java garbage collection. A failure of this health test may indicate a capacity planning problem or misconfiguration of the SecondaryNameNode. This test can be configured using the Garbage Collection Duration Thresholds and Garbage Collection Duration Monitoring Period SecondaryNameNode monitoring settings.

Short Name: GC Duration

Garbage Collection Duration Monitoring Period

Description

The period to review when computing the moving average of garbage collection time.

Template Name

`secondarynamenode_gc_duration_window`

Default Value

5

Unit(s)

MINUTES

Garbage Collection Duration Thresholds

Description

The health test thresholds for the weighted average time spent in Java garbage collection. Specified as a percentage of elapsed wall clock time.

Template Name

`secondarynamenode_gc_duration_thresholds`

Default Value

critical:60.0, warning:30.0

Unit(s)

no unit

SecondaryNameNode HDFS Checkpoint Directories Free Space

This is a SecondaryNameNode health test that checks that the filesystem containing the HDFS Checkpoint Directories of this SecondaryNameNode has sufficient free space. See the HDFS Checkpoint Directories description on the SecondaryNameNode configuration page for more information on this directory type. This test can be configured using the HDFS Checkpoint Directories Free Space Monitoring Absolute Thresholds and HDFS Checkpoint Directories Free Space Monitoring Percentage Thresholds SecondaryNameNode monitoring settings.

Short Name: HDFS Checkpoint Directories Free Space

HDFS Checkpoint Directories Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's HDFS Checkpoint Directories.

Template Name

`secondarynamenode_checkpoint_directories_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

HDFS Checkpoint Directories Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's HDFS Checkpoint Directories. Specified as a percentage of the capacity on that filesystem. This setting is not used if a HDFS Checkpoint Directories Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`secondarynamenode_checkpoint_directories_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

SecondaryNameNode Heap Dump Directory Free Space

This SecondaryNameNode health test checks that the filesystem containing the heap dump directory of this SecondaryNameNode has sufficient free space. This test can be configured using the Heap Dump Directory Free Space Monitoring Absolute Thresholds and Heap Dump Directory Free Space Monitoring Percentage Thresholds SecondaryNameNode monitoring settings.

Short Name: Heap Dump Directory Free Space

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Template Name

`heap_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`heap_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

SecondaryNameNode Host Health

This SecondaryNameNode health test factors in the health of the host upon which the SecondaryNameNode is running. A failure of this test means that the host running the SecondaryNameNode is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the SecondaryNameNode Host Health Test SecondaryNameNode monitoring setting.

Short Name: Host Health

SecondaryNameNode Host Health Test

Description

When computing the overall SecondaryNameNode health, consider the host's health.

Template Name

`secondarynamenode_host_health_enabled`

Default Value

true

Unit(s)

no unit

SecondaryNameNode Log Directory Free Space

This SecondaryNameNode health test checks that the filesystem containing the log directory of this SecondaryNameNode has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds SecondaryNameNode monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

SecondaryNameNode Process Status

This SecondaryNameNode health test checks that the Cloudera Manager Agent on the SecondaryNameNode host is heart beating correctly and that the process associated with the SecondaryNameNode role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the SecondaryNameNode process, a lack of connectivity to the Cloudera Manager Agent on the SecondaryNameNode host, or a problem with the Cloudera Manager Agent. This test can fail either because the SecondaryNameNode has crashed or because the SecondaryNameNode will not start or stop in a timely fashion. Check the SecondaryNameNode logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the SecondaryNameNode host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the SecondaryNameNode host, or look in the Cloudera Manager Agent logs on the SecondaryNameNode

host for more details. This test can be enabled or disabled using the SecondaryNameNode Process Health Test SecondaryNameNode monitoring setting.

Short Name: Process Status

SecondaryNameNode Process Health Test

Description

Enables the health test that the SecondaryNameNode's process state is consistent with the role configuration

Template Name

`secondarynamenode_scm_health_enabled`

Default Value

true

Unit(s)

no unit

SecondaryNameNode Swap Memory Usage

This SecondaryNameNode health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

SecondaryNameNode Unexpected Exits

This SecondaryNameNode health test checks that the SecondaryNameNode has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period SecondaryNameNode monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

SecondaryNameNode Web Server Status

This health test checks that the role's web server is responding quickly to requests by the Cloudera Manager Agent, and that the Cloudera Manager Agent can collect metrics from the web server. Failure of this health test may indicate a problem with the web server of the SecondaryNameNode, a misconfiguration of the SecondaryNameNode, or a problem with the Cloudera Manager Agent. Consult the Cloudera Manager Agent logs and the logs of the SecondaryNameNode for more detail. If the test failure message indicates a communication problem, the Cloudera Manager Agent's HTTP requests to the SecondaryNameNode's web server are failing or timing out. If the test's failure message indicates an unexpected response, the SecondaryNameNode's web server responded to the Cloudera Manager Agent's request, but the response could not be interpreted for some reason. This test can be configured using the Web Metric Collection SecondaryNameNode monitoring setting.

Short Name: Web Server Status

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Template Name

`secondarynamenode_web_metric_collection_enabled`

Default Value

true

Unit(s)

no unit

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Template Name

`secondarynamenode_web_metric_collection_thresholds`

Default Value

critical:never, warning:10000.0

Unit(s)

MILLISECONDS

Sentry Health Tests

Sentry Server Health

This is a Sentry service-level health test that checks that enough of the Sentry Servers in the cluster are healthy. The test returns "Concerning" health if the number of healthy Sentry Servers falls below a warning threshold, expressed as a percentage of the total number of Sentry Servers. The test returns "Bad" health if the number of healthy and "Concerning" Sentry Servers falls below a critical threshold, expressed as a percentage of the total number of Sentry Servers. For example, if this test is configured with a warning threshold of 95% and a critical threshold of 90% for a cluster of 100 Sentry Servers, this test would return "Good" health if 95 or more Sentry Servers have good health. This test would return "Concerning" health if at least 90 Sentry Servers have either "Good" or "Concerning" health. If more than 10 Sentry Servers have bad health, this test would return "Bad" health. A failure of this health test indicates unhealthy Sentry Servers. Check the status of the individual Sentry Servers for more information. This test can be configured using the Sentry Sentry service-wide monitoring setting.

Short Name: Sentry Server Health

Healthy Sentry Server Monitoring Thresholds

Description

The health test thresholds of the overall Sentry Server health. The check returns "Concerning" health if the percentage of "Healthy" Sentry Servers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Sentry Servers falls below the critical threshold.

Template Name

`sentry_sentry_server_healthy_thresholds`

Default Value

critical:51.0, warning:99.0

Unit(s)

PERCENT

Sentry Server Health Tests

Sentry Server Audit Pipeline Test

This Sentry Server health test checks that the Auditing for the Sentry Server role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Sentry Server process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Sentry Server host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Sentry Server monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Sentry Server File Descriptors

This Sentry Server health test checks that the number of file descriptors used does not rise above some percentage of the Sentry Server file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Sentry Server monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`sentry_server_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Sentry Server Heap Dump Directory Free Space

This Sentry Server health test checks that the filesystem containing the heap dump directory of this Sentry Server has sufficient free space. This test can be configured using the Heap Dump Directory Free Space Monitoring Absolute Thresholds and Heap Dump Directory Free Space Monitoring Percentage Thresholds Sentry Server monitoring settings.

Short Name: Heap Dump Directory Free Space

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Template Name

`heap_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`heap_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Sentry Server Host Health

This Sentry Server health test factors in the health of the host upon which the Sentry Server is running. A failure of this test means that the host running the Sentry Server is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Sentry Server Host Health Test Sentry Server monitoring setting.

Short Name: Host Health

Sentry Server Host Health Test

Description

When computing the overall Sentry Server health, consider the host's health.

Template Name

`sentry_server_host_health_enabled`

Default Value

true

Unit(s)

no unit

Sentry Server Log Directory Free Space

This Sentry Server health test checks that the filesystem containing the log directory of this Sentry Server has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Sentry Server monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Sentry Server Process Status

This Sentry Server health test checks that the Cloudera Manager Agent on the Sentry Server host is heart beating correctly and that the process associated with the Sentry Server role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Sentry Server process, a lack of connectivity to the Cloudera Manager Agent on the Sentry Server host, or a problem with the Cloudera Manager Agent. This test can fail either because the Sentry Server has crashed or because the Sentry Server will not start or stop in a timely fashion. Check the Sentry Server logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Sentry Server host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Sentry Server host, or look in the Cloudera Manager Agent logs on the Sentry Server host for more details. This test can be enabled or disabled using the Sentry Server Process Health Test Sentry Server monitoring setting.

Short Name: Process Status

Sentry Server Process Health Test

Description

Enables the health test that the Sentry Server's process state is consistent with the role configuration

Template Name

`sentry_server_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Sentry Server Swap Memory Usage

This Sentry Server health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Sentry Server Unexpected Exits

This Sentry Server health test checks that the Sentry Server has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Sentry Server monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Service Monitor Health Tests

Service Monitor Audit Pipeline Test

This Service Monitor health test checks that the Auditing for the Service Monitor role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Service Monitor process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Service Monitor host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Service Monitor monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Service Monitor Cloudera Manager Descriptor Age

This is a Service Monitor health test that checks if the Cloudera Manager descriptor has been refreshed recently. The Cloudera Manager descriptor is used to pass configuration information from the Cloudera Manager Server to the Service Monitor. If the descriptor becomes stale, Service Monitor operation may be impacted because the Service Monitor will receive information about new hosts, roles, and services, or changes to existing hosts, roles, and services. A stale descriptor usually indicates problems communicating with the Cloudera Manager Server but can also indicate performance problems or a bug. Consult the Service Monitor log and the Cloudera Manager Server log for more information. This test can be configured using the Cloudera Manager Descriptor Age Thresholds Cloudera Manager Service Monitor setting.

Short Name: Cloudera Manager Descriptor Age

Cloudera Manager Descriptor Age Thresholds

Description

The health test thresholds for monitoring the time since the Cloudera Manager descriptor was last refreshed.

Template Name

`scm_descriptor_age_thresholds`

Default Value

critical:120000.0, warning:60000.0

Unit(s)

no unit

Service Monitor Cloudera Manager Metric Schema Age

This is a Service Monitor health test that checks if the Cloudera Manager metric schema has been refreshed recently. If the metric schema becomes stale, Service Monitor operation may be impacted because the Service Monitor will not receive information about new metrics and changes to existing metrics. A stale metric schema usually indicates problems communicating with the Cloudera Manager Server but can also indicate performance problems or a bug. Consult the Service Monitor log and the Cloudera Manager Server log for more information. This test can be configured using the Cloudera Manager Metric Schema Age Thresholds Cloudera Manager Service Monitor setting.

Short Name: Cloudera Manager Metric Schema Age

Cloudera Manager Metric Schema Age Thresholds

Description

The health test thresholds for monitoring the time since the Cloudera Manager metric schema was last refreshed.

Template Name

`metric_schema_age_thresholds_name`

Default Value

critical:120000.0, warning:60000.0

Unit(s)

no unit

Service Monitor File Descriptors

This Service Monitor health test checks that the number of file descriptors used does not rise above some percentage of the Service Monitor file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Service Monitor monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`servicemonitor_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Service Monitor Heap Dump Directory Free Space

This Service Monitor health test checks that the filesystem containing the heap dump directory of this Service Monitor has sufficient free space. This test can be configured using the Heap Dump Directory Free Space Monitoring Absolute Thresholds and Heap Dump Directory Free Space Monitoring Percentage Thresholds Service Monitor monitoring settings.

Short Name: Heap Dump Directory Free Space

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Template Name

`heap_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`heap_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Service Monitor Heap Size

This Service Monitor health test checks that the Service Monitor heap size is adequate for the role. Consider increasing the heap when it is in critical state A failure of this health test may indicate that the Service Monitor is not getting the optimal heap size. Inspect the Service Monitor logs for any pause monitor output, check garbage collection metrics exposed by the Service Monitor and check the number of entities monitored by Service Monitor on Cloudera Management Service Status page This test can be configured using the Heap Size Thresholds Service Monitor monitoring settings.

Short Name: Heap Size

Heap Size Thresholds

Description

The health test thresholds for the heap used.

Template Name

`servicemonitor_heap_size_thresholds`

Default Value

critical:95.0, warning:90.0

Unit(s)

PERCENT

Service Monitor Host Health

This Service Monitor health test factors in the health of the host upon which the Service Monitor is running. A failure of this test means that the host running the Service Monitor is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Service Monitor Host Health Test Service Monitor monitoring setting.

Short Name: Host Health

Service Monitor Host Health Test

Description

When computing the overall Service Monitor health, consider the host's health.

Template Name

`servicemonitor_host_health_enabled`

Default Value

true

Unit(s)

no unit

Service Monitor Log Directory Free Space

This Service Monitor health test checks that the filesystem containing the log directory of this Service Monitor has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Service Monitor monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Service Monitor Metrics Aggregation Run Duration Test

This is a Service Monitor health test that checks whether Cloudera Manager's aggregation run durations are within the thresholds. If the test fails, Service Monitor operation may be impacted because the Service Monitor is not able to process the metrics fast enough. You can also turn off "Enable Metric Collection" setting for services that generate lot of metrics such as Hbase, Solr etc.. This test can be configured using the Metrics Aggregation Run Duration Thresholds Cloudera Manager Service Monitor setting.

It is safe to increase these thresholds if a Concerning or Bad status is reported often, as long as they remain less than or equal to the aggregation period (one minute by default). If other measures have failed to address the issue satisfactorily, then Cloudera recommends setting the critical threshold to 60 seconds, and the warning threshold to 45 seconds.

Short Name: Metrics Aggregation Run Duration Test

Metrics Aggregation Run Duration Thresholds

Description

The health test thresholds for monitoring the metrics aggregation run duration.

Template Name

`aggregation_run_duration_thresholds`

Default Value

critical:30000.0, warning:10000.0

Unit(s)

MILLISECONDS

Service Monitor Pause Duration

This Service Monitor health test checks that the Service Monitor threads are not experiencing long scheduling pauses. The test uses a pause monitoring thread in the Service Monitor that tracks scheduling delay by noting if it is run on its requested schedule. If the thread is not run on its requested schedule, the delay is noted and considered pause time. The health test checks that no more than some percentage of recent time is spent paused. A failure of this health test may indicate that the Service Monitor is not getting enough CPU resources, or that it is spending too much time doing garbage collection. Inspect the Service Monitor logs for any pause monitor output and check garbage collection metrics exposed by the Service Monitor. This test can be configured using the Pause Duration Thresholds and Pause Duration Monitoring Period Service Monitor monitoring settings.

Short Name: Pause Duration

Pause Duration Monitoring Period

Description

The period to review when computing the moving average of extra time the pause monitor spent paused.

Template Name

`servicemonitor_pause_duration_window`

Default Value

5

Unit(s)

MINUTES

Pause Duration Thresholds

Description

The health test thresholds for the weighted average extra time the pause monitor spent paused. Specified as a percentage of elapsed wall clock time.

Template Name

`servicemonitor_pause_duration_thresholds`

Default Value

critical:60.0, warning:30.0

Unit(s)

no unit

Service Monitor Process Status

This Service Monitor health test checks that the Cloudera Manager Agent on the Service Monitor host is heart beating correctly and that the process associated with the Service Monitor role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Service Monitor process, a lack of connectivity to the Cloudera Manager Agent on the Service Monitor host, or a problem with the Cloudera Manager Agent. This test can fail either because the Service Monitor has crashed or because the Service Monitor will not start or stop in a timely fashion. Check the Service Monitor logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Service Monitor host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Service Monitor host, or look in the Cloudera Manager Agent logs on the Service Monitor host for more details. This test can be enabled or disabled using the Service Monitor Process Health Test Service Monitor monitoring setting.

Short Name: Process Status

Service Monitor Process Health Test

Description

Enables the health test that the Service Monitor's process state is consistent with the role configuration

Template Name

`servicemonitor_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Service Monitor Role Pipeline

This Service Monitor health test checks that no messages are being dropped by the role stage of the Service Monitor pipeline. A failure of this health test indicates a problem with the Service Monitor. This may indicate a configuration problem or a bug in the Service Monitor. This test can be configured using the Service Monitor Role Pipeline Monitoring Time Period monitoring setting.

Short Name: Role Pipeline

Service Monitor Role Pipeline Monitoring Thresholds

Description

The health test thresholds for monitoring the Service Monitor role pipeline. This specifies the number of dropped messages that will be tolerated over the monitoring time period.

Template Name

`servicemonitor_role_pipeline_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Service Monitor Role Pipeline Monitoring Time Period

Description

The time period over which the Service Monitor role pipeline will be monitored for dropped messages.

Template Name

`servicemonitor_role_pipeline_window`

Default Value

5

Unit(s)

MINUTES

Service Monitor Service Monitor Storage Directory Free Space

This is a Service Monitor health test that checks that the filesystem containing the Service Monitor Storage Directory of this Service Monitor has sufficient free space. See the Service Monitor Storage Directory description on the Service Monitor configuration page for more information on this directory type. This test can be configured using the Service Monitor Storage Directory Free Space Monitoring Absolute Thresholds and Service Monitor Storage Directory Free Space Monitoring Percentage Thresholds Service Monitor monitoring settings.

Short Name: Service Monitor Storage Directory Free Space

Service Monitor Storage Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Service Monitor Storage Directory.

Template Name

`firehose_storage_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Service Monitor Storage Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Service Monitor Storage Directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Service Monitor Storage Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`firehose_storage_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Service Monitor Swap Memory Usage

This Service Monitor health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Service Monitor Unexpected Exits

This Service Monitor health test checks that the Service Monitor has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Service Monitor monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Service Monitor Web Server Status

This health test checks that the role's web server is responding quickly to requests by the Cloudera Manager Agent, and that the Cloudera Manager Agent can collect metrics from the web server. Failure of this health test may indicate a problem with the web server of the Service Monitor, a misconfiguration of the Service Monitor, or a problem with the Cloudera Manager Agent. Consult the Cloudera Manager Agent logs and the logs of the Service Monitor for more detail. If the test failure message indicates a communication problem, the Cloudera Manager Agent's HTTP requests to the Service Monitor's web server are failing or timing out. If the test's failure message indicates an unexpected response, the Service Monitor's web server responded to the Cloudera Manager Agent's request, but the response could not be interpreted for some reason. This test can be configured using the Web Metric Collection Service Monitor monitoring setting.

Short Name: Web Server Status

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Template Name

`servicemonitor_web_metric_collection_enabled`

Default Value

true

Unit(s)

no unit

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Template Name

`servicemonitor_web_metric_collection_thresholds`

Default Value

critical:never, warning:10000.0

Unit(s)

MILLISECONDS

Solr Health Tests

Solr Server Health

This is a Solr service-level health test that checks that enough of the Solr Servers in the cluster are healthy. The test returns "Concerning" health if the number of healthy Solr Servers falls below a warning threshold, expressed as a percentage of the total number of Solr Servers. The test returns "Bad" health if the number of healthy and "Concerning" Solr Servers falls below a critical threshold, expressed as a percentage of the total number of Solr Servers. For example, if this test is configured with a warning threshold of 95% and a critical threshold of 90% for a cluster of 100 Solr Servers, this test would return "Good" health if 95 or more Solr Servers have good health. This test would return "Concerning" health if at least 90 Solr Servers have either "Good" or "Concerning" health. If more than 10 Solr Servers have bad health, this test would return "Bad" health. A failure of this health test indicates unhealthy Solr Servers. Check the status of the individual Solr Servers for more information. This test can be configured using the Solr Solr service-wide monitoring setting.

Short Name: Solr Server Health

Healthy Solr Server Monitoring Thresholds

Description

The health test thresholds of the overall Solr Server health. The check returns "Concerning" health if the percentage of "Healthy" Solr Servers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Solr Servers falls below the critical threshold.

Template Name

`solr_solr_servers_healthy_thresholds`

Default Value

critical:90.0, warning:95.0

Unit(s)

PERCENT

Solr Server Health Tests

Solr Server Audit Pipeline Test

This Solr Server health test checks that the Auditing for the Solr Server role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Solr Server process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Solr Server host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Solr Server monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Solr Server File Descriptors

This Solr Server health test checks that the number of file descriptors used does not rise above some percentage of the Solr Server file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Solr Server monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`solr_server_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Solr Server GC Duration

This Solr Server health test checks that the Solr Server is not spending too much time performing Java garbage collection. It checks that no more than some percentage of recent time is spent performing Java garbage collection. A failure of this health test may indicate a capacity planning problem or misconfiguration of the Solr Server. This test can be configured using the Garbage Collection Duration Thresholds and Garbage Collection Duration Monitoring Period Solr Server monitoring settings.

Short Name: GC Duration

Garbage Collection Duration Monitoring Period

Description

The period to review when computing the moving average of garbage collection time.

Template Name

`solr_server_gc_duration_window`

Default Value

5

Unit(s)

MINUTES

Garbage Collection Duration Thresholds

Description

The health test thresholds for the weighted average time spent in Java garbage collection. Specified as a percentage of elapsed wall clock time.

Template Name

`solr_server_gc_duration_thresholds`

Default Value

critical:60.0, warning:30.0

Unit(s)

no unit

Solr Server Heap Dump Directory Free Space

This Solr Server health test checks that the filesystem containing the heap dump directory of this Solr Server has sufficient free space. This test can be configured using the Heap Dump Directory Free Space Monitoring Absolute Thresholds and Heap Dump Directory Free Space Monitoring Percentage Thresholds Solr Server monitoring settings.

Short Name: Heap Dump Directory Free Space

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Template Name

`heap_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`heap_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Solr Server Host Health

This Solr Server health test factors in the health of the host upon which the Solr Server is running. A failure of this test means that the host running the Solr Server is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Solr Server Host Health Test Solr Server monitoring setting.

Short Name: Host Health

Solr Server Host Health Test

Description

When computing the overall Solr Server health, consider the host's health.

Template Name

`solr_server_host_health_enabled`

Default Value

true

Unit(s)

no unit

Solr Server Log Directory Free Space

This Solr Server health test checks that the filesystem containing the log directory of this Solr Server has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Solr Server monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Solr Server Process Status

This Solr Server health test checks that the Cloudera Manager Agent on the Solr Server host is heart beating correctly and that the process associated with the Solr Server role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Solr Server process, a lack of connectivity to the Cloudera Manager Agent on the Solr Server host, or a problem with the Cloudera Manager Agent. This test can fail either because the Solr Server has crashed or because the Solr Server will not start or stop in a timely fashion. Check the Solr Server logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Solr Server host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Solr Server host, or look in the Cloudera Manager Agent logs on the Solr Server host for more details. This test can be enabled or disabled using the Solr Server Process Health Test Solr Server monitoring setting.

Short Name: Process Status

Solr Server Process Health Test

Description

Enables the health test that the Solr Server's process state is consistent with the role configuration

Template Name

`solr_server_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Solr Server Solr Server API Liveness

This is a Solr Server health test that checks that the Solr Server is responding quickly to API requests by the Cloudera Manager Agent to collect the status of the Solr Server's Solr cores. A failure of this health test may indicate a problem with the Solr Server, a misconfiguration of the Solr Server or a problem with the Cloudera Manager Agent. Consult the Cloudera Manager Agent logs and the logs of the Solr Server for more details. If the test's failure message indicates a communication problem, this means that the Cloudera Manager Agent's HTTP requests to the Solr Server are failing or timing out. These requests are completely local to the Solr Server's host, and so should never fail under

normal conditions. If the test's failure message indicates an unexpected response, then the Solr Server responded to the Cloudera Manager Agent's request, but the Cloudera Manager Agent could not interpret the response for some reason. This test can be enabled or disabled using the Solr Server API Liveness Solr Server monitoring setting and can be configured using the Solr Server API Liveness Request Duration monitoring setting.

Short Name: Solr Server API Liveness

Solr Server API Liveness

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather status of Solr Cores from the Solr Server with a simple API request.

Template Name

`solr_core_status_collection_health_enabled`

Default Value

true

Unit(s)

no unit

Solr Server API Liveness Request Duration

Description

The health test thresholds on the duration of the Solr Server API request.

Template Name

`solr_core_status_collection_thresholds`

Default Value

critical:never, warning:10000.0

Unit(s)

MILLISECONDS

Solr Server Swap Memory Usage

This Solr Server health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Solr Server Unexpected Exits

This Solr Server health test checks that the Solr Server has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Solr Server monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Solr Server Web Server Status

This health test checks that the role's web server is responding quickly to requests by the Cloudera Manager Agent, and that the Cloudera Manager Agent can collect metrics from the web server. Failure of this health test may indicate a problem with the web server of the Solr Server, a misconfiguration of the Solr Server, or a problem with the Cloudera Manager Agent. Consult the Cloudera Manager Agent logs and the logs of the Solr Server for more detail. If the test failure message indicates a communication problem, the Cloudera Manager Agent's HTTP requests to the Solr Server's web server are failing or timing out. If the test's failure message indicates an unexpected response, the Solr Server's web server responded to the Cloudera Manager Agent's request, but the response could not be interpreted for some reason. This test can be configured using the Web Metric Collection Solr Server monitoring setting.

Short Name: Web Server Status

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Template Name

`solr_server_web_metric_collection_enabled`

Default Value

true

Unit(s)

no unit

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Template Name

`solr_server_web_metric_collection_thresholds`

Default Value

critical:never, warning:10000.0

Unit(s)

MILLISECONDS

Spark Health Tests

Spark History Server Health

This Spark service-level health test checks for the presence of a running, healthy History Server. The test returns "Bad" health if the service is running and the History Server is not running. In all other cases it returns the health of the History Server. A failure of this health test indicates a stopped or unhealthy History Server. Check the status of the History Server for more information. This test can be enabled or disabled using the History Server Role Health Test History Server service-wide monitoring setting.

Short Name: History Server Health

History Server Role Health Test

Description

When computing the overall SPARK_ON_YARN health, consider History Server's health

Template Name

`SPARK_ON_YARN_SPARK_YARN_HISTORY_SERVER_health_enabled`

Default Value

true

Unit(s)

no unit

Sqoop 2 Health Tests

Sqoop 2 Server Health

This Sqoop 2 service-level health test checks for the presence of a running, healthy Sqoop 2 Server. The test returns "Bad" health if the service is running and the Sqoop 2 Server is not running. In all other cases it returns the health of the Sqoop 2 Server. A failure of this health test indicates a stopped or unhealthy Sqoop 2 Server. Check the status of the Sqoop 2 Server for more information. This test can be enabled or disabled using the Sqoop 2 Server Role Health Test Sqoop 2 Server service-wide monitoring setting.

Short Name: Sqoop 2 Server Health

Sqoop 2 Server Role Health Test

Description

When computing the overall SQOOP health, consider Sqoop 2 Server's health

Template Name

`sqoop_sqoop_server_health_enabled`

Default Value

true

Unit(s)

no unit

Sqoop 2 Server Health Tests

Sqoop 2 Server Audit Pipeline Test

This Sqoop 2 Server health test checks that the Auditing for the Sqoop 2 Server role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Sqoop 2 Server process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Sqoop 2 Server host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Sqoop 2 Server monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Sqoop 2 Server File Descriptors

This Sqoop 2 Server health test checks that the number of file descriptors used does not rise above some percentage of the Sqoop 2 Server file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Sqoop 2 Server monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`sqoop_server_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Sqoop 2 Server Heap Dump Directory Free Space

This Sqoop 2 Server health test checks that the filesystem containing the heap dump directory of this Sqoop 2 Server has sufficient free space. This test can be configured using the Heap Dump Directory Free Space Monitoring Absolute Thresholds and Heap Dump Directory Free Space Monitoring Percentage Thresholds Sqoop 2 Server monitoring settings.

Short Name: Heap Dump Directory Free Space

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Template Name

`heap_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`heap_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Sqoop 2 Server Host Health

This Sqoop 2 Server health test factors in the health of the host upon which the Sqoop 2 Server is running. A failure of this test means that the host running the Sqoop 2 Server is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Sqoop 2 Server Host Health Test Sqoop 2 Server monitoring setting.

Short Name: Host Health

Sqoop 2 Server Host Health Test

Description

When computing the overall Sqoop 2 Server health, consider the host's health.

Template Name

`sqoop_server_host_health_enabled`

Default Value

true

Unit(s)

no unit

Sqoop 2 Server Log Directory Free Space

This Sqoop 2 Server health test checks that the filesystem containing the log directory of this Sqoop 2 Server has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Sqoop 2 Server monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Sqoop 2 Server Process Status

This Sqoop 2 Server health test checks that the Cloudera Manager Agent on the Sqoop 2 Server host is heart beating correctly and that the process associated with the Sqoop 2 Server role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Sqoop 2 Server process, a lack of connectivity to the Cloudera Manager Agent on the Sqoop 2 Server host, or a problem with the Cloudera Manager Agent. This test can fail either because the Sqoop 2 Server has crashed or because the Sqoop 2 Server will not start or stop in a timely fashion. Check the Sqoop 2 Server logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Sqoop 2 Server host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Sqoop 2 Server host, or look in the Cloudera Manager Agent logs on the Sqoop 2 Server host for more details. This test can be enabled or disabled using the Sqoop 2 Server Process Health Test Sqoop 2 Server monitoring setting.

Short Name: Process Status

Sqoop 2 Server Process Health Test

Description

Enables the health test that the Sqoop 2 Server's process state is consistent with the role configuration

Template Name

`sqoop_server_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Sqoop 2 Server Swap Memory Usage

This Sqoop 2 Server health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Sqoop 2 Server Unexpected Exits

This Sqoop 2 Server health test checks that the Sqoop 2 Server has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Sqoop 2 Server monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Storage Container Manager Health Tests

Storage Container Manager Audit Pipeline Test

This Storage Container Manager health test checks that the Auditing for the Storage Container Manager role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Storage Container Manager process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Storage Container Manager host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details.

This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Storage Container Manager monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Storage Container Manager File Descriptors

This Storage Container Manager health test checks that the number of file descriptors used does not rise above some percentage of the Storage Container Manager file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Storage Container Manager monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`storage_container_manager_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Storage Container Manager Host Health

This Storage Container Manager health test factors in the health of the host upon which the Storage Container Manager is running. A failure of this test means that the host running the Storage Container Manager is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Storage Container Manager Host Health Test Storage Container Manager monitoring setting.

Short Name: Host Health

Storage Container Manager Host Health Test

Description

When computing the overall Storage Container Manager health, consider the host's health.

Template Name

`storage_container_manager_host_health_enabled`

Default Value

true

Unit(s)

no unit

Storage Container Manager Log Directory Free Space

This Storage Container Manager health test checks that the filesystem containing the log directory of this Storage Container Manager has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Storage Container Manager monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Storage Container Manager Process Status

This Storage Container Manager health test checks that the Cloudera Manager Agent on the Storage Container Manager host is heart beating correctly and that the process associated with the Storage Container Manager role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Storage Container Manager process, a lack of connectivity to the Cloudera Manager Agent on the Storage Container Manager host, or a problem with the Cloudera Manager Agent. This test can fail either because the Storage Container Manager has crashed or because the Storage Container Manager will not start or stop in a timely fashion. Check the Storage Container Manager logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Storage Container Manager host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Storage Container Manager host, or look in the Cloudera Manager Agent logs on the Storage Container Manager host for more details. This test can be enabled or disabled using the Storage Container Manager Process Health Test Storage Container Manager monitoring setting.

Short Name: Process Status

Storage Container Manager Process Health Test

Description

Enables the health test that the Storage Container Manager's process state is consistent with the role configuration

Template Name

`storage_container_manager_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Storage Container Manager Swap Memory Usage

This Storage Container Manager health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Storage Container Manager Unexpected Exits

This Storage Container Manager health test checks that the Storage Container Manager has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Storage Container Manager monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Streams Messaging Manager Health Tests

Streams Messaging Manager Rest Admin Server Health

This Streams Messaging Manager service-level health test checks for the presence of a running, healthy Streams Messaging Manager Rest Admin Server. The test returns "Bad" health if the service is running and the Streams Messaging Manager Rest Admin Server is not running. In all other cases it returns the health of the Streams Messaging Manager Rest Admin Server. A failure of this health test indicates a stopped or unhealthy Streams Messaging Manager Rest Admin Server. Check the status of the Streams Messaging Manager Rest Admin Server for more information. This test can be enabled or disabled using the Streams Messaging Manager Rest Admin Server Role Health Test Streams Messaging Manager Rest Admin Server service-wide monitoring setting.

Short Name: Streams Messaging Manager Rest Admin Server Health

Streams Messaging Manager Rest Admin Server Role Health Test

Description

When computing the overall STREAMS_MESSAGING_MANAGER health, consider Streams Messaging Manager Rest Admin Server's health

Template Name

`STREAMS_MESSAGING_MANAGER_STREAMS_MESSAGING_MANAGER_SERVER_health_enabled`

Default Value

true

Unit(s)

no unit

Streams Messaging Manager UI Server Health

This Streams Messaging Manager service-level health test checks for the presence of a running, healthy Streams Messaging Manager UI Server. The test returns "Bad" health if the service is running and the Streams Messaging Manager UI Server is not running. In all other cases it returns the health of the Streams Messaging Manager UI Server. A failure of this health test indicates a stopped or unhealthy Streams Messaging Manager UI Server. Check the status of the Streams Messaging Manager UI Server for more information. This test can be enabled or disabled using the Streams Messaging Manager UI Server Role Health Test Streams Messaging Manager UI Server service-wide monitoring setting.

Short Name: Streams Messaging Manager UI Server Health

Streams Messaging Manager UI Server Role Health Test

Description

When computing the overall STREAMS_MESSAGING_MANAGER health, consider Streams Messaging Manager UI Server's health

Template Name

`STREAMS_MESSAGING_MANAGER_STREAMS_MESSAGING_MANAGER_UI_health_enabled`

Default Value

true

Unit(s)

no unit

Streams Messaging Manager Rest Admin Server Health Tests

Streams Messaging Manager Rest Admin Server Audit Pipeline Test

This Streams Messaging Manager Rest Admin Server health test checks that the Auditing for the Streams Messaging Manager Rest Admin Server role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Streams Messaging Manager Rest Admin Server process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Streams Messaging Manager Rest Admin Server host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Streams Messaging Manager Rest Admin Server monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Streams Messaging Manager Rest Admin Server File Descriptors

This Streams Messaging Manager Rest Admin Server health test checks that the number of file descriptors used does not rise above some percentage of the Streams Messaging Manager Rest Admin Server file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Streams Messaging Manager Rest Admin Server monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`streams_messaging_manager_server_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Streams Messaging Manager Rest Admin Server Host Health

This Streams Messaging Manager Rest Admin Server health test factors in the health of the host upon which the Streams Messaging Manager Rest Admin Server is running. A failure of this test means that the host running the Streams Messaging Manager Rest Admin Server is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Streams Messaging Manager Rest Admin Server Host Health Test Streams Messaging Manager Rest Admin Server monitoring setting.

Short Name: Host Health

Streams Messaging Manager Rest Admin Server Host Health Test

Description

When computing the overall Streams Messaging Manager Rest Admin Server health, consider the host's health.

Template Name

`streams_messaging_manager_server_host_health_enabled`

Default Value

true

Unit(s)

no unit

Streams Messaging Manager Rest Admin Server Log Directory Free Space

This Streams Messaging Manager Rest Admin Server health test checks that the filesystem containing the log directory of this Streams Messaging Manager Rest Admin Server has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Streams Messaging Manager Rest Admin Server monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Streams Messaging Manager Rest Admin Server Process Status

This Streams Messaging Manager Rest Admin Server health test checks that the Cloudera Manager Agent on the Streams Messaging Manager Rest Admin Server host is heart beating correctly and that the process associated with the Streams Messaging Manager Rest Admin Server role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Streams Messaging Manager Rest Admin Server process, a lack of connectivity to the Cloudera Manager Agent on the Streams Messaging Manager Rest Admin Server host, or a problem with the Cloudera Manager Agent. This test can fail either because the Streams Messaging Manager Rest Admin Server has crashed or because the Streams Messaging Manager Rest Admin Server will not start or stop in a timely fashion. Check the Streams Messaging Manager Rest Admin Server logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Streams Messaging Manager Rest Admin Server host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Streams Messaging Manager Rest Admin Server host, or look in the Cloudera Manager Agent logs on the Streams Messaging Manager Rest Admin Server host for more details. This test can be enabled or disabled using the Streams Messaging Manager Rest Admin Server Process Health Test Streams Messaging Manager Rest Admin Server monitoring setting.

Short Name: Process Status

Streams Messaging Manager Rest Admin Server Process Health Test

Description

Enables the health test that the Streams Messaging Manager Rest Admin Server's process state is consistent with the role configuration

Template Name

`streams_messaging_manager_server_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Streams Messaging Manager Rest Admin Server Swap Memory Usage

This Streams Messaging Manager Rest Admin Server health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Streams Messaging Manager Rest Admin Server Unexpected Exits

This Streams Messaging Manager Rest Admin Server health test checks that the Streams Messaging Manager Rest Admin Server has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Streams Messaging Manager Rest Admin Server monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Streams Messaging Manager UI Server Health Tests

Streams Messaging Manager UI Server Audit Pipeline Test

This Streams Messaging Manager UI Server health test checks that the Auditing for the Streams Messaging Manager UI Server role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Streams Messaging Manager UI Server process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Streams Messaging Manager

UI Server host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Streams Messaging Manager UI Server monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Streams Messaging Manager UI Server File Descriptors

This Streams Messaging Manager UI Server health test checks that the number of file descriptors used does not rise above some percentage of the Streams Messaging Manager UI Server file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Streams Messaging Manager UI Server monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`streams_messaging_manager_ui_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Streams Messaging Manager UI Server Host Health

This Streams Messaging Manager UI Server health test factors in the health of the host upon which the Streams Messaging Manager UI Server is running. A failure of this test means that the host running the Streams Messaging Manager UI Server is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Streams Messaging Manager UI Server Host Health Test Streams Messaging Manager UI Server monitoring setting.

Short Name: Host Health

Streams Messaging Manager UI Server Host Health Test

Description

When computing the overall Streams Messaging Manager UI Server health, consider the host's health.

Template Name

`streams_messaging_manager_ui_host_health_enabled`

Default Value

true

Unit(s)

no unit

Streams Messaging Manager UI Server Log Directory Free Space

This Streams Messaging Manager UI Server health test checks that the filesystem containing the log directory of this Streams Messaging Manager UI Server has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Streams Messaging Manager UI Server monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Streams Messaging Manager UI Server Process Status

This Streams Messaging Manager UI Server health test checks that the Cloudera Manager Agent on the Streams Messaging Manager UI Server host is heart beating correctly and that the process associated with the Streams Messaging Manager UI Server role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Streams Messaging Manager UI Server process, a lack of connectivity to the Cloudera Manager Agent on the Streams Messaging Manager UI Server host, or a problem with the Cloudera Manager Agent. This test can fail either because the Streams Messaging Manager UI Server has crashed or because the Streams Messaging Manager UI Server will not start or stop in a timely fashion. Check the Streams Messaging Manager UI Server logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Streams Messaging Manager UI Server host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Streams Messaging Manager UI Server host, or look in the Cloudera Manager Agent logs on the Streams Messaging Manager UI Server host for more details. This test can be enabled or disabled using the Streams Messaging Manager UI Server Process Health Test Streams Messaging Manager UI Server monitoring setting.

Short Name: Process Status

Streams Messaging Manager UI Server Process Health Test

Description

Enables the health test that the Streams Messaging Manager UI Server's process state is consistent with the role configuration

Template Name

`streams_messaging_manager_ui_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Streams Messaging Manager UI Server Swap Memory Usage

This Streams Messaging Manager UI Server health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Streams Messaging Manager UI Server Unexpected Exits

This Streams Messaging Manager UI Server health test checks that the Streams Messaging Manager UI Server has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Streams Messaging Manager UI Server monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Streams Replication Manager Health Tests

Streams Replication Manager SRM Driver Health

This is a Streams Replication Manager service-level health test that checks that enough of the SRM Drivers in the cluster are healthy. The test returns "Concerning" health if the number of healthy SRM Drivers falls below a warning threshold, expressed as a percentage of the total number of SRM Drivers. The test returns "Bad" health if the number of healthy and "Concerning" SRM Drivers falls below a critical threshold, expressed as a percentage of the total number of SRM Drivers. For example, if this test is configured with a warning threshold of 95% and a critical threshold of 90% for a cluster of 100 SRM Drivers, this test would return "Good" health if 95 or more SRM Drivers have good health. This test would return "Concerning" health if at least 90 SRM Drivers have either "Good" or "Concerning" health. If more than 10 SRM Drivers have bad health, this test would return "Bad" health. A failure of this health test indicates unhealthy SRM Drivers. Check the status of the individual SRM Drivers for more information. This test can be configured using the Streams Replication Manager Streams Replication Manager service-wide monitoring setting.

Short Name: SRM Driver Health

Healthy SRM Driver Monitoring Thresholds

Description

The health test thresholds of the overall SRM Driver health. The check returns "Concerning" health if the percentage of "Healthy" SRM Drivers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" SRM Drivers falls below the critical threshold.

Template Name

`STREAMS_REPLICATION_MANAGER_STREAMS_REPLICATION_MANAGER_DRIVER_healthy_thresholds`

Default Value

critical:49.99, warning:94.99

Unit(s)

PERCENT

Streams Replication Manager SRM Service Health

This Streams Replication Manager service-level health test checks for the presence of a running, healthy SRM Service. The test returns "Bad" health if the service is running and the SRM Service is not running. In all other cases it returns the health of the SRM Service. A failure of this health test indicates a stopped or unhealthy SRM Service. Check the status of the SRM Service for more information. This test can be enabled or disabled using the SRM Service Role Health Test SRM Service service-wide monitoring setting.

Short Name: SRM Service Health

SRM Service Role Health Test

Description

When computing the overall STREAMS_REPLICATION_MANAGER health, consider SRM Service's health

Template Name

`STREAMS_REPLICATION_MANAGER_STREAMS_REPLICATION_MANAGER_SERVICE_health_enabled`

Default Value

true

Unit(s)

no unit

Tablet Server Health Tests

Tablet Server Audit Pipeline Test

This Tablet Server health test checks that the Auditing for the Tablet Server role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Tablet Server process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Tablet Server host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Tablet Server monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Tablet Server Failed Data Directories

Short Name: Failed Data Directories

Tablet Server File Descriptors

This Tablet Server health test checks that the number of file descriptors used does not rise above some percentage of the Tablet Server file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Tablet Server monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`kudu_tserver_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Tablet Server Full Data Directories

Short Name: Full Data Directories

Tablet Server Host Health

This Tablet Server health test factors in the health of the host upon which the Tablet Server is running. A failure of this test means that the host running the Tablet Server is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Tablet Server Host Health Test Tablet Server monitoring setting.

Short Name: Host Health

Tablet Server Host Health Test

Description

When computing the overall Tablet Server health, consider the host's health.

Template Name

`kudu_tserver_host_health_enabled`

Default Value

true

Unit(s)

no unit

Tablet Server Log Directory Free Space

This Tablet Server health test checks that the filesystem containing the log directory of this Tablet Server has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Tablet Server monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Tablet Server Process Status

This Tablet Server health test checks that the Cloudera Manager Agent on the Tablet Server host is heart beating correctly and that the process associated with the Tablet Server role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Tablet Server process, a lack of connectivity to the Cloudera Manager Agent on the Tablet Server host, or a problem with the Cloudera Manager Agent. This test can fail either because the Tablet Server has crashed or because the Tablet Server will not start or stop in a timely fashion. Check the Tablet Server logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Tablet Server host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Tablet Server host, or look in the Cloudera Manager Agent logs on the Tablet Server host for more details. This test can be enabled or disabled using the Tablet Server Process Health Test Tablet Server monitoring setting.

Short Name: Process Status

Tablet Server Process Health Test

Description

Enables the health test that the Tablet Server's process state is consistent with the role configuration

Template Name

`kudu_tserver_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Tablet Server Swap Memory Usage

This Tablet Server health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Tablet Server Unexpected Exits

This Tablet Server health test checks that the Tablet Server has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Tablet Server monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

TaskTracker Health Tests

TaskTracker Audit Pipeline Test

This TaskTracker health test checks that the Auditing for the TaskTracker role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of TaskTracker process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the TaskTracker host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check TaskTracker monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

TaskTracker Blacklisted Status

This is a TaskTracker health test that checks that the JobTracker has not disallowed (blacklisted) the TaskTracker. A failure of this health test indicates that the JobTracker has disallowed the TaskTracker because of the failure rate of tasks on the TaskTracker is significantly higher than the average cluster failure rate. Check the TaskTracker logs for more details. This test can be enabled or disabled using the TaskTracker Blacklisted Health Test TaskTracker monitoring setting.

Short Name: Blacklisted Status

TaskTracker Blacklisted Health Test

Description

Enables the health test that the TaskTracker is not blacklisted

Template Name

`tasktracker_blacklisted_health_enabled`

Default Value

true

Unit(s)

no unit

TaskTracker File Descriptors

This TaskTracker health test checks that the number of file descriptors used does not rise above some percentage of the TaskTracker file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds TaskTracker monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`tasktracker_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

TaskTracker GC Duration

This TaskTracker health test checks that the TaskTracker is not spending too much time performing Java garbage collection. It checks that no more than some percentage of recent time is spent performing Java garbage collection. A failure of this health test may indicate a capacity planning problem or misconfiguration of the TaskTracker. This test can be configured using the Garbage Collection Duration Thresholds and Garbage Collection Duration Monitoring Period TaskTracker monitoring settings.

Short Name: GC Duration

Garbage Collection Duration Monitoring Period

Description

The period to review when computing the moving average of garbage collection time.

Template Name

`tasktracker_gc_duration_window`

Default Value

5

Unit(s)

MINUTES

Garbage Collection Duration Thresholds

Description

The health test thresholds for the weighted average time spent in Java garbage collection. Specified as a percentage of elapsed wall clock time.

Template Name

`tasktracker_gc_duration_thresholds`

Default Value

critical:60.0, warning:30.0

Unit(s)

no unit

TaskTracker Heap Dump Directory Free Space

This TaskTracker health test checks that the filesystem containing the heap dump directory of this TaskTracker has sufficient free space. This test can be configured using the Heap Dump Directory Free Space Monitoring Absolute Thresholds and Heap Dump Directory Free Space Monitoring Percentage Thresholds TaskTracker monitoring settings.

Short Name: Heap Dump Directory Free Space

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Template Name

`heap_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`heap_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

TaskTracker Host Health

This TaskTracker health test factors in the health of the host upon which the TaskTracker is running. A failure of this test means that the host running the TaskTracker is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the TaskTracker Host Health Test TaskTracker monitoring setting.

Short Name: Host Health

TaskTracker Host Health Test

Description

When computing the overall TaskTracker health, consider the host's health.

Template Name

`tasktracker_host_health_enabled`

Default Value

true

Unit(s)

no unit

TaskTracker JobTracker Connectivity

This is a TaskTracker health test that checks whether the JobTracker considers the TaskTracker alive. A failure of this health test may indicate that the TaskTracker is having trouble communicating with the JobTracker. Look in the TaskTracker logs for more details. This test can be enabled or disabled using the TaskTracker Connectivity Health Test TaskTracker monitoring setting. The TaskTracker Connectivity Tolerance at Startup TaskTracker monitoring setting and the Health Test Startup Tolerance JobTracker monitoring setting can be used to control the test's tolerance windows around TaskTracker and JobTracker restarts respectively.

Short Name: JobTracker Connectivity

Health Test Startup Tolerance

Description

The amount of time allowed after this role is started that failures of health tests that rely on communication with this role will be tolerated.

Template Name

`jobtracker_startup_tolerance`

Default Value

5

Unit(s)

MINUTES

TaskTracker Connectivity Health Test

Description

Enables the health test that the TaskTracker is connected to the JobTracker

Template Name

`tasktracker_connectivity_health_enabled`

Default Value

true

Unit(s)

no unit

TaskTracker Connectivity Tolerance at Startup

Description

The amount of time to wait for the TaskTracker to fully start up and connect to the JobTracker before enforcing the connectivity check.

Template Name

`tasktracker_connectivity_tolerance`

Default Value

180

Unit(s)

SECONDS

TaskTracker Log Directory Free Space

This TaskTracker health test checks that the filesystem containing the log directory of this TaskTracker has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds TaskTracker monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

TaskTracker Process Status

This TaskTracker health test checks that the Cloudera Manager Agent on the TaskTracker host is heart beating correctly and that the process associated with the TaskTracker role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the TaskTracker process, a lack of connectivity to the Cloudera Manager Agent on the TaskTracker host, or a problem with the Cloudera Manager Agent. This test can fail either because the TaskTracker has crashed or because the TaskTracker will not start or stop in a timely fashion. Check the TaskTracker logs for more details. If the test fails because of problems communicating with the Cloudera Manager

Agent on the TaskTracker host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the TaskTracker host, or look in the Cloudera Manager Agent logs on the TaskTracker host for more details. This test can be enabled or disabled using the TaskTracker Process Health Test TaskTracker monitoring setting.

Short Name: Process Status

TaskTracker Process Health Test

Description

Enables the health test that the TaskTracker's process state is consistent with the role configuration

Template Name

`tasktracker_scm_health_enabled`

Default Value

true

Unit(s)

no unit

TaskTracker Swap Memory Usage

This TaskTracker health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

TaskTracker TaskTracker Local Data Directories Free Space

This is a TaskTracker health test that checks that the filesystem containing the TaskTracker Local Data Directories of this TaskTracker has sufficient free space. See the TaskTracker Local Data Directories description on the TaskTracker configuration page for more information on this directory type. This test can be configured using the TaskTracker Local Data Directories Free Space Monitoring Absolute Thresholds and TaskTracker Local Data Directories Free Space Monitoring Percentage Thresholds TaskTracker monitoring settings.

Short Name: TaskTracker Local Data Directories Free Space

TaskTracker Local Data Directories Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's TaskTracker Local Data Directories.

Template Name

`tasktracker_local_data_directories_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

TaskTracker Local Data Directories Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's TaskTracker Local Data Directories. Specified as a percentage of the capacity on that filesystem. This setting is not used if a TaskTracker Local Data Directories Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`tasktracker_local_data_directories_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

TaskTracker Unexpected Exits

This TaskTracker health test checks that the TaskTracker has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period TaskTracker monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

TaskTracker Web Server Status

This health test checks that the role's web server is responding quickly to requests by the Cloudera Manager Agent, and that the Cloudera Manager Agent can collect metrics from the web server. Failure of this health test may indicate a problem with the web server of the TaskTracker, a misconfiguration of the TaskTracker, or a problem with the Cloudera Manager Agent. Consult the Cloudera Manager Agent logs and the logs of the TaskTracker for more detail. If the test failure message indicates a communication problem, the Cloudera Manager Agent's HTTP requests to the TaskTracker's web server are failing or timing out. If the test's failure message indicates an unexpected response, the TaskTracker's web server responded to the Cloudera Manager Agent's request, but the response could not be interpreted for some reason. This test can be configured using the Web Metric Collection TaskTracker monitoring setting.

Short Name: Web Server Status

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Template Name

`tasktracker_web_metric_collection_enabled`

Default Value

true

Unit(s)

no unit

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Template Name

`tasktracker_web_metric_collection_thresholds`

Default Value

critical:never, warning:10000.0

Unit(s)

MILLISECONDS

Telemetry Publisher Health Tests

Telemetry Publisher Audit Pipeline Test

This Telemetry Publisher health test checks that the Auditing for the Telemetry Publisher role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Telemetry Publisher process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Telemetry Publisher host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Telemetry Publisher monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Telemetry Publisher Data Export Test For Stream Hive-Query-Audits

This is a Telemetry Publisher health test that checks whether data is exported succesfully for stream HIVE-query-audits. A failure of this check indicates that one or more exports failed.

Short Name: Data Export Test For Stream Hive-Query-Audits

Metrics Data Export Failure Thresholds

Description

The health test thresholds for monitoring the data export failure count.

Template Name

`telemetrypublisher_data_export_failure_thresholds`

Default Value

critical:5.0, warning:3.0

Unit(s)

TIMES

Telemetry Publisher Data Export Monitoring Time Period

Description

The time period over which the telemetry publisher data export for streams will be monitored for failed export.

Template Name

`telemetrypublisher_data_export_failure_window`

Default Value

5

Unit(s)

MINUTES

Telemetry Publisher Data Export Test For Stream Hive-Tez-App

This is a Telemetry Publisher health test that checks whether data is exported succesfully for stream HIVE-tez-app. A failure of this check indicates that one or more exports failed.

Short Name: Data Export Test For Stream Hive-Tez-App

Metrics Data Export Failure Thresholds

Description

The health test thresholds for monitoring the data export failure count.

Template Name

`telemetrypublisher_data_export_failure_thresholds`

Default Value

critical:5.0, warning:3.0

Unit(s)

TIMES

Telemetry Publisher Data Export Monitoring Time Period

Description

The time period over which the telemetry publisher data export for streams will be monitored for failed export.

Template Name

`telemetrypublisher_data_export_failure_window`

Default Value

5

Unit(s)

MINUTES

Telemetry Publisher Data Export Test For Stream Impala-Query-Profile

This is a Telemetry Publisher health test that checks whether data is exported succesfully for stream IMPALA-query-profile. A failure of this check indicates that one or more exports failed.

Short Name: Data Export Test For Stream Impala-Query-Profile

Metrics Data Export Failure Thresholds

Description

The health test thresholds for monitoring the data export failure count.

Template Name

`telemetrypublisher_data_export_failure_thresholds`

Default Value

critical:5.0, warning:3.0

Unit(s)

TIMES

Telemetry Publisher Data Export Monitoring Time Period

Description

The time period over which the telemetry publisher data export for streams will be monitored for failed export.

Template Name

`telemetrypublisher_data_export_failure_window`

Default Value

5

Unit(s)

MINUTES

Telemetry Publisher Data Export Test For Stream Oozie-Workflows

This is a Telemetry Publisher health test that checks whether data is exported succesfully for stream OOZIE-workflows. A failure of this check indicates that one or more exports failed.

Short Name: Data Export Test For Stream Oozie-Workflows

Metrics Data Export Failure Thresholds

Description

The health test thresholds for monitoring the data export failure count.

Template Name

`telemetrypublisher_data_export_failure_thresholds`

Default Value

critical:5.0, warning:3.0

Unit(s)

TIMES

Telemetry Publisher Data Export Monitoring Time Period

Description

The time period over which the telemetry publisher data export for streams will be monitored for failed export.

Template Name

`telemetrypublisher_data_export_failure_window`

Default Value

5

Unit(s)

MINUTES

Telemetry Publisher Data Export Test For Stream Spark2_on_yarn-Event-Log

This is a Telemetry Publisher health test that checks whether data is exported succesfully for stream SPARK2_ON_YARN-event-log. A failure of this check indicates that one or more exports failed.

Short Name: Data Export Test For Stream Spark2_on_yarn-Event-Log

Metrics Data Export Failure Thresholds

Description

The health test thresholds for monitoring the data export failure count.

Template Name

`telemetrypublisher_data_export_failure_thresholds`

Default Value

critical:5.0, warning:3.0

Unit(s)

TIMES

Telemetry Publisher Data Export Monitoring Time Period

Description

The time period over which the telemetry publisher data export for streams will be monitored for failed export.

Template Name

`telemetrypublisher_data_export_failure_window`

Default Value

5

Unit(s)

MINUTES

Telemetry Publisher Data Export Test For Stream Yarn-Apps

This is a Telemetry Publisher health test that checks whether data is exported succesfully for stream YARN-apps. A failure of this check indicates that one or more exports failed.

Short Name: Data Export Test For Stream Yarn-Apps

Metrics Data Export Failure Thresholds

Description

The health test thresholds for monitoring the data export failure count.

Template Name

`telemetrypublisher_data_export_failure_thresholds`

Default Value

critical:5.0, warning:3.0

Unit(s)

TIMES

Telemetry Publisher Data Export Monitoring Time Period

Description

The time period over which the telemetry publisher data export for streams will be monitored for failed export.

Template Name

`telemetrypublisher_data_export_failure_window`

Default Value

5

Unit(s)

MINUTES

Telemetry Publisher Data Export Test For Stream Yarn-Jhist

This is a Telemetry Publisher health test that checks whether data is exported succesfully for stream YARN-jhist. A failure of this check indicates that one or more exports failed.

Short Name: Data Export Test For Stream Yarn-Jhist

Metrics Data Export Failure Thresholds

Description

The health test thresholds for monitoring the data export failure count.

Template Name

`telemetrypublisher_data_export_failure_thresholds`

Default Value

critical:5.0, warning:3.0

Unit(s)

TIMES

Telemetry Publisher Data Export Monitoring Time Period

Description

The time period over which the telemetry publisher data export for streams will be monitored for failed export.

Template Name

`telemetrypublisher_data_export_failure_window`

Default Value

5

Unit(s)

MINUTES

Telemetry Publisher Data Ingest Test For Stream Hive-Query-Audits

This is a Telemetry Publisher health test that checks whether data is ingested succesfully by stream HIVE-query-audits. A failure of this check indicates that one or more ingests failed.

Short Name: Data Ingest Test For Stream Hive-Query-Audits

Metrics Data Ingest Failure Thresholds

Description

The health test thresholds for monitoring the data ingest failure count.

Template Name

`telemetrypublisher_data_ingest_failure_thresholds`

Default Value

critical:5.0, warning:3.0

Unit(s)

TIMES

Telemetry Publisher Data Ingest Monitoring Time Period

Description

The time period over which the telemetry publisher data ingest for streams will be monitored for failed injest.

Template Name

`telemetrypublisher_data_ingest_failure_window`

Default Value

5

Unit(s)

MINUTES

Telemetry Publisher Data Ingest Test For Stream Hive-Tez-App

This is a Telemetry Publisher health test that checks whether data is ingested succesfully by stream HIVE-tez-app. A failure of this check indicates that one or more ingests failed.

Short Name: Data Ingest Test For Stream Hive-Tez-App

Metrics Data Ingest Failure Thresholds

Description

The health test thresholds for monitoring the data ingest failure count.

Template Name

`telemetrypublisher_data_ingest_failure_thresholds`

Default Value

critical:5.0, warning:3.0

Unit(s)

TIMES

Telemetry Publisher Data Ingest Monitoring Time Period

Description

The time period over which the telemetry publisher data ingest for streams will be monitored for failed injest.

Template Name

`telemetrypublisher_data_ingest_failure_window`

Default Value

5

Unit(s)

MINUTES

Telemetry Publisher Data Ingest Test For Stream Impala-Query-Profile

This is a Telemetry Publisher health test that checks whether data is ingested succesfully by stream IMPALA-query-profile. A failure of this check indicates that one or more ingests failed.

Short Name: Data Ingest Test For Stream Impala-Query-Profile

Metrics Data Ingest Failure Thresholds

Description

The health test thresholds for monitoring the data ingest failure count.

Template Name

`telemetrypublisher_data_ingest_failure_thresholds`

Default Value

critical:5.0, warning:3.0

Unit(s)

TIMES

Telemetry Publisher Data Ingest Monitoring Time Period

Description

The time period over which the telemetry publisher data ingest for streams will be monitored for failed injest.

Template Name

`telemetrypublisher_data_ingest_failure_window`

Default Value

5

Unit(s)

MINUTES

Telemetry Publisher Data Ingest Test For Stream Oozie-Workflows

This is a Telemetry Publisher health test that checks whether data is ingested succesfully by stream OOZIE-workflows. A failure of this check indicates that one or more ingests failed.

Short Name: Data Ingest Test For Stream Oozie-Workflows

Metrics Data Ingest Failure Thresholds

Description

The health test thresholds for monitoring the data ingest failure count.

Template Name

`telemetrypublisher_data_ingest_failure_thresholds`

Default Value

critical:5.0, warning:3.0

Unit(s)

TIMES

Telemetry Publisher Data Ingest Monitoring Time Period

Description

The time period over which the telemetry publisher data ingest for streams will be monitored for failed injest.

Template Name

`telemetrypublisher_data_ingest_failure_window`

Default Value

5

Unit(s)

MINUTES

Telemetry Publisher Data Ingest Test For Stream Spark2_on_yarn-Event-Log

This is a Telemetry Publisher health test that checks whether data is ingested succesfully by stream SPARK2_ON_YARN-event-log. A failure of this check indicates that one or more ingests failed.

Short Name: Data Ingest Test For Stream Spark2_on_yarn-Event-Log

Metrics Data Ingest Failure Thresholds

Description

The health test thresholds for monitoring the data ingest failure count.

Template Name

`telemetrypublisher_data_ingest_failure_thresholds`

Default Value

critical:5.0, warning:3.0

Unit(s)

TIMES

Telemetry Publisher Data Ingest Monitoring Time Period

Description

The time period over which the telemetry publisher data ingest for streams will be monitored for failed injest.

Template Name

`telemetrypublisher_data_ingest_failure_window`

Default Value

5

Unit(s)

MINUTES

Telemetry Publisher Data Ingest Test For Stream Yarn-Apps

This is a Telemetry Publisher health test that checks whether data is ingested succesfully by stream YARN-apps. A failure of this check indicates that one or more ingests failed.

Short Name: Data Ingest Test For Stream Yarn-Apps

Metrics Data Ingest Failure Thresholds

Description

The health test thresholds for monitoring the data ingest failure count.

Template Name

`telemetrypublisher_data_ingest_failure_thresholds`

Default Value

critical:5.0, warning:3.0

Unit(s)

TIMES

Telemetry Publisher Data Ingest Monitoring Time Period

Description

The time period over which the telemetry publisher data ingest for streams will be monitored for failed injest.

Template Name

`telemetrypublisher_data_ingest_failure_window`

Default Value

5

Unit(s)

MINUTES

Telemetry Publisher Data Ingest Test For Stream Yarn-Jhist

This is a Telemetry Publisher health test that checks whether data is ingested succesfully by stream YARN-jhist. A failure of this check indicates that one or more ingests failed.

Short Name: Data Ingest Test For Stream Yarn-Jhist

Metrics Data Ingest Failure Thresholds

Description

The health test thresholds for monitoring the data ingest failure count.

Template Name

`telemetrypublisher_data_ingest_failure_thresholds`

Default Value

critical:5.0, warning:3.0

Unit(s)

TIMES

Telemetry Publisher Data Ingest Monitoring Time Period

Description

The time period over which the telemetry publisher data ingest for streams will be monitored for failed injest.

Template Name

`telemetrypublisher_data_ingest_failure_window`

Default Value

5

Unit(s)

MINUTES

Telemetry Publisher File Descriptors

This Telemetry Publisher health test checks that the number of file descriptors used does not rise above some percentage of the Telemetry Publisher file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Telemetry Publisher monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`telemetrypublisher_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Telemetry Publisher GC Duration

This Telemetry Publisher health test checks that the Telemetry Publisher is not spending too much time performing Java garbage collection. It checks that no more than some percentage of recent time is spent performing Java garbage collection. A failure of this health test may indicate a capacity planning problem or misconfiguration of the Telemetry Publisher. This test can be configured using the Garbage Collection Duration Thresholds and Garbage Collection Duration Monitoring Period Telemetry Publisher monitoring settings.

Short Name: GC Duration

Garbage Collection Duration Monitoring Period

Description

The period to review when computing the moving average of garbage collection time.

Template Name

`telemetrypublisher_gc_duration_window`

Default Value

5

Unit(s)

MINUTES

Garbage Collection Duration Thresholds

Description

The health test thresholds for the weighted average time spent in Java garbage collection. Specified as a percentage of elapsed wall clock time.

Template Name

`telemetrypublisher_gc_duration_thresholds`

Default Value

critical:60.0, warning:30.0

Unit(s)

no unit

Telemetry Publisher Heap Dump Directory Free Space

This Telemetry Publisher health test checks that the filesystem containing the heap dump directory of this Telemetry Publisher has sufficient free space. This test can be configured using the Heap Dump Directory Free Space Monitoring Absolute Thresholds and Heap Dump Directory Free Space Monitoring Percentage Thresholds Telemetry Publisher monitoring settings.

Short Name: Heap Dump Directory Free Space

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Template Name

`heap_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`heap_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Telemetry Publisher Host Health

This Telemetry Publisher health test factors in the health of the host upon which the Telemetry Publisher is running. A failure of this test means that the host running the Telemetry Publisher is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Telemetry Publisher Host Health Test Telemetry Publisher monitoring setting.

Short Name: Host Health

Telemetry Publisher Host Health Test

Description

When computing the overall Telemetry Publisher health, consider the host's health.

Template Name

`telemetrypublisher_host_health_enabled`

Default Value

true

Unit(s)

no unit

Telemetry Publisher Log Directory Free Space

This Telemetry Publisher health test checks that the filesystem containing the log directory of this Telemetry Publisher has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Telemetry Publisher monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Telemetry Publisher Process Status

This Telemetry Publisher health test checks that the Cloudera Manager Agent on the Telemetry Publisher host is heart beating correctly and that the process associated with the Telemetry Publisher role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Telemetry Publisher process, a lack of connectivity to the Cloudera Manager Agent on the Telemetry Publisher host, or a problem with the Cloudera Manager Agent. This test can fail either because the Telemetry Publisher has crashed or because the Telemetry Publisher will not start or stop in a timely fashion. Check the Telemetry Publisher logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Telemetry Publisher host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Telemetry Publisher host, or look in the Cloudera Manager Agent logs on the Telemetry Publisher host for more details. This test can be enabled or disabled using the Telemetry Publisher Process Health Test Telemetry Publisher monitoring setting.

Short Name: Process Status

Telemetry Publisher Process Health Test

Description

Enables the health test that the Telemetry Publisher's process state is consistent with the role configuration

Template Name

`telemetrypublisher_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Telemetry Publisher Swap Memory Usage

This Telemetry Publisher health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Telemetry Publisher Telemetry Publisher Data Directory Free Space

This is a Telemetry Publisher health test that checks that the filesystem containing the Telemetry Publisher Data Directory of this Telemetry Publisher has sufficient free space. See the Telemetry Publisher Data Directory description on the Telemetry Publisher configuration page for more information on this directory type. This test can be configured using the Telemetry Publisher Data Directory Free Space Monitoring Absolute Thresholds and Telemetry Publisher Data Directory Free Space Monitoring Percentage Thresholds Telemetry Publisher monitoring settings.

Short Name: Telemetry Publisher Data Directory Free Space

Telemetry Publisher Data Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Telemetry Publisher Data Directory.

Template Name

`telemetrypublisher_data_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Telemetry Publisher Data Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Telemetry Publisher Data Directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Telemetry Publisher Data Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`telemetrypublisher_data_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Telemetry Publisher Unexpected Exits

This Telemetry Publisher health test checks that the Telemetry Publisher has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Telemetry Publisher monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Telemetry Publisher Web Server Status

This health test checks that the role's web server is responding quickly to requests by the Cloudera Manager Agent, and that the Cloudera Manager Agent can collect metrics from the web server. Failure of this health test may indicate a problem with the web server of the Telemetry Publisher, a misconfiguration of the Telemetry Publisher, or a problem with the Cloudera Manager Agent. Consult the Cloudera Manager Agent logs and the logs of the Telemetry Publisher for more detail. If the test failure message indicates a communication problem, the Cloudera Manager Agent's HTTP requests to the Telemetry Publisher's web server are failing or timing out. If the test's failure message indicates an unexpected response, the Telemetry Publisher's web server responded to the Cloudera Manager Agent's request, but the response could not be interpreted for some reason. This test can be configured using the Web Metric Collection Telemetry Publisher monitoring setting.

Short Name: Web Server Status

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Template Name

`telemetrypublisher_web_metric_collection_enabled`

Default Value

true

Unit(s)

no unit

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Template Name

`telemetrypublisher_web_metric_collection_thresholds`

Default Value

critical:never, warning:10000.0

Unit(s)

MILLISECONDS

Tracer Health Tests

Tracer Audit Pipeline Test

This Tracer health test checks that the Auditing for the Tracer role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Tracer process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Tracer host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Tracer monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Tracer File Descriptors

This Tracer health test checks that the number of file descriptors used does not rise above some percentage of the Tracer file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Tracer monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`accumulo_tracer_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Tracer Host Health

This Tracer health test factors in the health of the host upon which the Tracer is running. A failure of this test means that the host running the Tracer is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Tracer Host Health Test Tracer monitoring setting.

Short Name: Host Health

Tracer Host Health Test

Description

When computing the overall Tracer health, consider the host's health.

Template Name

`accumulo_tracer_host_health_enabled`

Default Value

true

Unit(s)

no unit

Tracer Log Directory Free Space

This Tracer health test checks that the filesystem containing the log directory of this Tracer has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Tracer monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Tracer Process Status

This Tracer health test checks that the Cloudera Manager Agent on the Tracer host is heart beating correctly and that the process associated with the Tracer role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Tracer process, a lack of connectivity to the Cloudera Manager Agent on the Tracer host, or a problem with the Cloudera Manager Agent. This test can fail either because the Tracer has crashed or because the Tracer will not start or stop in a timely fashion. Check the Tracer logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Tracer host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Tracer host, or look in the Cloudera

Manager Agent logs on the Tracer host for more details. This test can be enabled or disabled using the Tracer Process Health Test Tracer monitoring setting.

Short Name: Process Status

Tracer Process Health Test

Description

Enables the health test that the Tracer's process state is consistent with the role configuration

Template Name

`accumulo_tracer_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Tracer Swap Memory Usage

This Tracer health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Tracer Unexpected Exits

This Tracer health test checks that the Tracer has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Tracer monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

WebHCat Server Health Tests

WebHCat Server Audit Pipeline Test

This WebHCat Server health test checks that the Auditing for the WebHCat Server role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of WebHCat Server process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the WebHCat Server host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check WebHCat Server monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

WebHCat Server File Descriptors

This WebHCat Server health test checks that the number of file descriptors used does not rise above some percentage of the WebHCat Server file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds WebHCat Server monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`webhcat_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

WebHCat Server Heap Dump Directory Free Space

This WebHCat Server health test checks that the filesystem containing the heap dump directory of this WebHCat Server has sufficient free space. This test can be configured using the Heap Dump Directory Free Space Monitoring Absolute Thresholds and Heap Dump Directory Free Space Monitoring Percentage Thresholds WebHCat Server monitoring settings.

Short Name: Heap Dump Directory Free Space

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Template Name

`heap_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`heap_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

WebHCat Server Host Health

This WebHCat Server health test factors in the health of the host upon which the WebHCat Server is running. A failure of this test means that the host running the WebHCat Server is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the WebHCat Server Host Health Test WebHCat Server monitoring setting.

Short Name: Host Health

WebHCat Server Host Health Test

Description

When computing the overall WebHCat Server health, consider the host's health.

Template Name

`webhcat_host_health_enabled`

Default Value

true

Unit(s)

no unit

WebHCat Server Log Directory Free Space

This WebHCat Server health test checks that the filesystem containing the log directory of this WebHCat Server has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds WebHCat Server monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

WebHCat Server Process Status

This WebHCat Server health test checks that the Cloudera Manager Agent on the WebHCat Server host is heart beating correctly and that the process associated with the WebHCat Server role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the WebHCat Server process, a lack of connectivity to the Cloudera Manager Agent on the WebHCat Server host, or a problem with the Cloudera Manager Agent. This test can fail either because the WebHCat Server has crashed or because the WebHCat Server will not start or stop in a timely fashion. Check the WebHCat Server logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the WebHCat Server host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the WebHCat Server host, or look in the Cloudera Manager Agent logs on the WebHCat Server host for more details. This test can be enabled or disabled using the WebHCat Server Process Health Test WebHCat Server monitoring setting.

Short Name: Process Status

WebHCat Server Process Health Test

Description

Enables the health test that the WebHCat Server's process state is consistent with the role configuration

Template Name

`webhcat_scm_health_enabled`

Default Value

true

Unit(s)

no unit

WebHCat Server Swap Memory Usage

This WebHCat Server health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

WebHCat Server Unexpected Exits

This WebHCat Server health test checks that the WebHCat Server has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period WebHCat Server monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

YARN Health Tests

YARN Container Usage Aggregation

This health test checks whether Cloudera Manager can successfully aggregate YARN container usage metrics by reading them from HDFS and running a MapReduce job to aggregate them and store them in Service Monitor storage. A failure of this health test indicates that Cloudera Manager cannot generate cluster usage metrics for YARN jobs. If this test fails, look at Service Monitor logs for more details. This test can be enabled or disabled using the Enable Container Usage Metrics Collection YARN monitoring setting. .

Short Name: YARN Container Usage Aggregation

Enable Container Usage Metrics Collection

Description

Enables storing YARN container usage metrics in HDFS and periodically running a MapReduce job from Cloudera Service Monitor to aggregate them into per-application metrics. This is required for YARN usage reporting to work.

Template Name

`cm_yarn_enable_container_usage_aggregation`

Default Value

CDH=[[CDH 5.7.0..CDH 8.0.0)=false]

Unit(s)

no unit

YARN JobHistory Server Health

This YARN service-level health test checks for the presence of a running, healthy JobHistory Server. The test returns "Bad" health if the service is running and the JobHistory Server is not running. In all other cases it returns the health of the JobHistory Server. A failure of this health test indicates a stopped or unhealthy JobHistory Server. Check the status of the JobHistory Server for more information. This test can be enabled or disabled using the JobHistory Server Role Health Test JobHistory Server service-wide monitoring setting.

Short Name: JobHistory Server Health

JobHistory Server Role Health Test

Description

When computing the overall YARN health, consider JobHistory Server's health

Template Name

`yarn_jobhistoryserver_health_enabled`

Default Value

true

Unit(s)

no unit

YARN NodeManager Health

This is a YARN service-level health test that checks that enough of the NodeManagers in the cluster are healthy. The test returns "Concerning" health if the number of healthy NodeManagers falls below a warning threshold, expressed as a percentage of the total number of NodeManagers. The test returns "Bad" health if the number of healthy and "Concerning" NodeManagers falls below a critical threshold, expressed as a percentage of the total number of NodeManagers. For example, if this test is configured with a warning threshold of 95% and a critical threshold of 90% for a cluster of 100 NodeManagers, this test would return "Good" health if 95 or more NodeManagers have good health. This test would return "Concerning" health if at least 90 NodeManagers have either "Good" or "Concerning" health. If more than 10 NodeManagers have bad health, this test would return "Bad" health. A failure of this health test indicates unhealthy NodeManagers. Check the status of the individual NodeManagers for more information. This test can be configured using the YARN YARN service-wide monitoring setting.

Short Name: NodeManager Health

Healthy NodeManager Monitoring Thresholds

Description

The health test thresholds of the overall NodeManager health. The check returns "Concerning" health if the percentage of "Healthy" NodeManagers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" NodeManagers falls below the critical threshold.

Template Name

`yarn_nodemanagers_healthy_thresholds`

Default Value

critical:90.0, warning:95.0

Unit(s)

PERCENT

YARN ResourceManager Health (HA)

This is a YARN service-level health test that checks for and active, healthy ResourceManager. The test returns "Bad" health if the service is running and an active ResourceManager cannot be found. If an active ResourceManager is found, then the test checks the health of that ResourceManager as well as the health of any standby ResourceManager configured. A "Good" health result will only be returned if both the active and Standby ResourceManagers are healthy. A failure of this health test may indicate stopped or unhealthy ResourceManager roles, or it may indicate a problem with communication between the Cloudera Manager Service Monitor and the ResourceManagers. Check the status of the YARN service's ResourceManager roles and look in the Cloudera Manager Service Monitor's log files for more information when this test fails. This test can be enabled or disabled using the Active ResourceManager Role Health Check YARN service-wide monitoring setting. The check for a healthy standby ResourceManager can be enabled or disabled with Standby ResourceManager Health Check. In addition, the Active ResourceManager Detection Window can be used to adjust the amount of time that the Cloudera Manager Service Monitor has to detect the active ResourceManager before this health test fails, and the ResourceManager Activation Startup Tolerance can be used to adjust the amount of time around ResourceManager startup that the test allows for a ResourceManager to be made active.

Short Name: ResourceManager Health

Active ResourceManager Detection Window

Description

The tolerance window used in YARN service tests that depend on detection of the active ResourceManager.

Template Name

`yarn_active_resourcemanager_detection_window`

Default Value

CDH=[[CDH 5.0.0..CDH 8.0.0)=3]

Unit(s)

MINUTES

Active ResourceManager Role Health Check

Description

When computing the overall YARN service health, whether to consider the active ResourceManager's health.

Template Name

`yarn_resourcemanagers_health_enabled`

Default Value

CDH=[[CDH 5.0.0..CDH 8.0.0)=true]

Unit(s)

no unit

ResourceManager Activation Startup Tolerance

Description

The amount of time after ResourceManager(s) start that the lack of an active ResourceManager will be tolerated. This is an advanced option that does not often need to be changed.

Template Name

`yarn_resourcemanager_activation_startup_tolerance`

Default Value

CDH=[[CDH 5.0.0..CDH 8.0.0)=180]

Unit(s)

SECONDS

Standby ResourceManager Health Check

Description

When computing the overall YARN service health, whether to consider the health of the standby ResourceManager.

Template Name

`yarn_standby_resourcemanager_health_enabled`

Default Value

CDH=[[CDH 5.0.0..CDH 8.0.0)=true]

Unit(s)

no unit

YARN Queue Manager Store Health Tests

YARN Queue Manager Store Audit Pipeline Test

This YARN Queue Manager Store health test checks that the Auditing for the YARN Queue Manager Store role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of YARN Queue Manager Store process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the YARN Queue Manager Store host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check YARN Queue Manager Store monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

YARN Queue Manager Store File Descriptors

This YARN Queue Manager Store health test checks that the number of file descriptors used does not rise above some percentage of the YARN Queue Manager Store file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds YARN Queue Manager Store monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`queuemanager_store_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

YARN Queue Manager Store Host Health

This YARN Queue Manager Store health test factors in the health of the host upon which the YARN Queue Manager Store is running. A failure of this test means that the host running the YARN Queue Manager Store is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the YARN Queue Manager Store Host Health Test YARN Queue Manager Store monitoring setting.

Short Name: Host Health

YARN Queue Manager Store Host Health Test

Description

When computing the overall YARN Queue Manager Store health, consider the host's health.

Template Name

`queuemanager_store_host_health_enabled`

Default Value

true

Unit(s)

no unit

YARN Queue Manager Store Log Directory Free Space

This YARN Queue Manager Store health test checks that the filesystem containing the log directory of this YARN Queue Manager Store has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds YARN Queue Manager Store monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

YARN Queue Manager Store Process Status

This YARN Queue Manager Store health test checks that the Cloudera Manager Agent on the YARN Queue Manager Store host is heart beating correctly and that the process associated with the YARN Queue Manager Store role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the YARN Queue Manager Store process, a lack of connectivity to the Cloudera Manager Agent on the YARN Queue Manager Store host, or a problem with the Cloudera Manager Agent. This test can fail either because the YARN Queue Manager Store has crashed or because the YARN Queue Manager Store will not start or stop in a timely fashion. Check the YARN Queue Manager Store logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the YARN Queue Manager Store host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the YARN Queue Manager Store host, or look in the Cloudera Manager Agent logs on the YARN Queue Manager Store host for more details. This test can be enabled or disabled using the YARN Queue Manager Store Process Health Test YARN Queue Manager Store monitoring setting.

Short Name: Process Status

YARN Queue Manager Store Process Health Test

Description

Enables the health test that the YARN Queue Manager Store's process state is consistent with the role configuration

Template Name

`queuemanager_store_scm_health_enabled`

Default Value

true

Unit(s)

no unit

YARN Queue Manager Store Swap Memory Usage

This YARN Queue Manager Store health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

YARN Queue Manager Store Unexpected Exits

This YARN Queue Manager Store health test checks that the YARN Queue Manager Store has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also

indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period YARN Queue Manager Store monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

YARN Queue Manager Webapp Health Tests

YARN Queue Manager Webapp Audit Pipeline Test

This YARN Queue Manager Webapp health test checks that the Auditing for the YARN Queue Manager Webapp role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of YARN Queue Manager Webapp process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the YARN Queue Manager Webapp host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check YARN Queue Manager Webapp monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

YARN Queue Manager Webapp File Descriptors

This YARN Queue Manager Webapp health test checks that the number of file descriptors used does not rise above some percentage of the YARN Queue Manager Webapp file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds YARN Queue Manager Webapp monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`queuemanager_webapp_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

YARN Queue Manager Webapp Host Health

This YARN Queue Manager Webapp health test factors in the health of the host upon which the YARN Queue Manager Webapp is running. A failure of this test means that the host running the YARN Queue Manager Webapp is

experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the YARN Queue Manager Webapp Host Health Test YARN Queue Manager Webapp monitoring setting.

Short Name: Host Health

YARN Queue Manager Webapp Host Health Test

Description

When computing the overall YARN Queue Manager Webapp health, consider the host's health.

Template Name

`queuemanager_webapp_host_health_enabled`

Default Value

true

Unit(s)

no unit

YARN Queue Manager Webapp Log Directory Free Space

This YARN Queue Manager Webapp health test checks that the filesystem containing the log directory of this YARN Queue Manager Webapp has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds YARN Queue Manager Webapp monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

YARN Queue Manager Webapp Process Status

This YARN Queue Manager Webapp health test checks that the Cloudera Manager Agent on the YARN Queue Manager Webapp host is heart beating correctly and that the process associated with the YARN Queue Manager Webapp role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the YARN Queue Manager Webapp process, a lack of connectivity to the Cloudera Manager Agent on the YARN Queue Manager Webapp host, or a problem with the Cloudera Manager Agent. This test can fail either because the YARN Queue Manager Webapp has crashed or because the YARN Queue Manager Webapp will not start or stop in a timely fashion. Check the YARN Queue Manager Webapp logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the YARN Queue Manager Webapp host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the YARN Queue Manager Webapp host, or look in the Cloudera Manager Agent logs on the YARN Queue Manager Webapp host for more details. This test can be enabled or disabled using the YARN Queue Manager Webapp Process Health Test YARN Queue Manager Webapp monitoring setting.

Short Name: Process Status

YARN Queue Manager Webapp Process Health Test

Description

Enables the health test that the YARN Queue Manager Webapp's process state is consistent with the role configuration

Template Name

`queuemanager_webapp_scm_health_enabled`

Default Value

true

Unit(s)

no unit

YARN Queue Manager Webapp Swap Memory Usage

This YARN Queue Manager Webapp health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

YARN Queue Manager Webapp Unexpected Exits

This YARN Queue Manager Webapp health test checks that the YARN Queue Manager Webapp has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out

of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period YARN Queue Manager Webapp monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

Zeppelin Health Tests

Zeppelin Server Health

This Zeppelin service-level health test checks for the presence of a running, healthy Zeppelin Server. The test returns "Bad" health if the service is running and the Zeppelin Server is not running. In all other cases it returns the health of the Zeppelin Server. A failure of this health test indicates a stopped or unhealthy Zeppelin Server. Check the status of the Zeppelin Server for more information. This test can be enabled or disabled using the Zeppelin Server Role Health Test Zeppelin Server service-wide monitoring setting.

Short Name: Zeppelin Server Health

Zeppelin Server Role Health Test

Description

When computing the overall ZEPPELIN health, consider Zeppelin Server's health

Template Name

`ZEPPELIN_ZEPPELIN_SERVER_health_enabled`

Default Value

true

Unit(s)

no unit

Zeppelin Server Health Tests

Zeppelin Server Audit Pipeline Test

This Zeppelin Server health test checks that the Auditing for the Zeppelin Server role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Zeppelin Server process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Zeppelin Server host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Zeppelin Server monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

Zeppelin Server File Descriptors

This Zeppelin Server health test checks that the number of file descriptors used does not rise above some percentage of the Zeppelin Server file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Zeppelin Server monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`zeppelin_server_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

Zeppelin Server Host Health

This Zeppelin Server health test factors in the health of the host upon which the Zeppelin Server is running. A failure of this test means that the host running the Zeppelin Server is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Zeppelin Server Host Health Test Zeppelin Server monitoring setting.

Short Name: Host Health

Zeppelin Server Host Health Test

Description

When computing the overall Zeppelin Server health, consider the host's health.

Template Name

`zeppelin_server_host_health_enabled`

Default Value

true

Unit(s)

no unit

Zeppelin Server Log Directory Free Space

This Zeppelin Server health test checks that the filesystem containing the log directory of this Zeppelin Server has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Zeppelin Server monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

Zeppelin Server Process Status

This Zeppelin Server health test checks that the Cloudera Manager Agent on the Zeppelin Server host is heart beating correctly and that the process associated with the Zeppelin Server role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Zeppelin Server process, a lack of connectivity to the Cloudera Manager Agent on the Zeppelin Server host, or a problem with the Cloudera Manager Agent. This test can fail either because the Zeppelin Server has crashed or because the Zeppelin Server will not start or stop in a timely fashion. Check the Zeppelin Server logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Zeppelin Server host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Zeppelin Server host, or look in the Cloudera Manager Agent logs on the Zeppelin Server host for more details. This test can be enabled or disabled using the Zeppelin Server Process Health Test Zeppelin Server monitoring setting.

Short Name: Process Status

Zeppelin Server Process Health Test

Description

Enables the health test that the Zeppelin Server's process state is consistent with the role configuration

Template Name

`zeppelin_server_scm_health_enabled`

Default Value

true

Unit(s)

no unit

Zeppelin Server Swap Memory Usage

This Zeppelin Server health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

Zeppelin Server Unexpected Exits

This Zeppelin Server health test checks that the Zeppelin Server has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Zeppelin Server monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit

ZooKeeper Health Tests

ZooKeeper Canary

This is a ZooKeeper service-level health test that checks that basic client operations are working and are completing in a reasonable amount of time. This test reports the results of a periodic "canary" test that performs the following sequence of operations. First, it connects to and establishes a session (the root session) with the ZooKeeper service and creates a permanent znode to serve as the root of all canary operations. The canary test then connects to and establishes sessions (the child sessions) with each ZooKeeper server of the service. Each child session is used to create an ephemeral child znode under the canary root. After the child znodes have been created, watches that await znode deletion events are registered with each of the child znodes for each of the child sessions. The canary test then deletes each of the child znodes and then verifies that each child session has received deletion notifications for each of the child znodes. Finally the canary test closes all the child sessions, deletes the root znode and closes the root session. The test returns "Bad" health if the establishment of the root session to the ZooKeeper service fails, the creation of znodes (permanent or ephemeral) fails, the deletion of znodes fails or the retrieval of child znodes of the root znode fails. The test returns "Concerning" health when the canary test succeeds but has one or more servers that could not participate in the canary test operations or if the canary test runs too slowly. A failure of this health test may indicate that ZooKeeper is failing to satisfy client requests correctly or in a timely fashion. Check the status of the ZooKeeper servers, and look in the ZooKeeper server logs for more details. This test can be enabled or disabled using the ZooKeeper Canary Health Check ZooKeeper service monitoring setting. The ZooKeeper Canary Root Znode Path, ZooKeeper Canary Connection Timeout, ZooKeeper Canary Session Timeout, ZooKeeper Canary Operation Timeout settings control the operation of the canary.

Short Name: ZooKeeper Canary

ZooKeeper Canary Connection Timeout

Description

Configures the timeout used by the canary for connection establishment with ZooKeeper servers

Template Name

`zookeeper_canary_connection_timeout`

Default Value

10000

Unit(s)

MILLISECONDS

ZooKeeper Canary Health Check

Description

Enables the health check that a client can connect to ZooKeeper and perform basic operations

Template Name

`zookeeper_canary_health_enabled`

Default Value

true

Unit(s)

no unit

ZooKeeper Canary Operation Timeout

Description

Configures the timeout used by the canary for ZooKeeper operations

Template Name

`zookeeper_canary_operation_timeout`

Default Value

30000

Unit(s)

MILLISECONDS

ZooKeeper Canary Root Znode Path

Description

Configures the path of the root znode under which all canary updates are performed

Template Name

`zookeeper_canary_root_path`

Default Value

/cloudera_manager_zookeeper_canary

Unit(s)

no unit

ZooKeeper Canary Session Timeout

Description

Configures the timeout used by the canary sessions with ZooKeeper servers

Template Name

`zookeeper_canary_session_timeout`

Default Value

30000

Unit(s)

MILLISECONDS

ZooKeeper Server Health

This is a ZooKeeper service-level health test that checks that enough of the Servers in the cluster are healthy. The test returns "Concerning" health if the number of healthy Servers falls below a warning threshold, expressed as a percentage of the total number of Servers. The test returns "Bad" health if the number of healthy and "Concerning" Servers falls below a critical threshold, expressed as a percentage of the total number of Servers. For example, if this test is configured with a warning threshold of 95% and a critical threshold of 90% for a cluster of 100 Servers, this test would return "Good" health if 95 or more Servers have good health. This test would return "Concerning" health if at least 90 Servers have either "Good" or "Concerning" health. If more than 10 Servers have bad health, this test would return "Bad" health. A failure of this health test indicates unhealthy Servers. Check the status of the individual Servers for more information. This test can be configured using the ZooKeeper ZooKeeper service-wide monitoring setting.

Short Name: Server Health

Healthy Server Monitoring Thresholds

Description

The health test thresholds of the overall Server health. The check returns "Concerning" health if the percentage of "Healthy" Servers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Servers falls below the critical threshold.

Template Name

`zookeeper_servers_healthy_thresholds`

Default Value

critical:51.0, warning:99.0

Unit(s)

PERCENT

ZooKeeper Server Health Tests

ZooKeeper Server Audit Pipeline Test

This Server health test checks that the Auditing for the Server role is getting processed correctly and is not blocked. A failure of this health test may indicate a problem with the audit pipeline of Server process. This test can fail either because the Cloudera Audit Server is not accepting audits, or the Cloudera Manager Agent on the Server host isn't able to send audits because of some network issue. Check the Cloudera Manager Agent logs and Cloudera Audit Server logs for more details. This test can be enabled or disabled using the Navigator Audit Pipeline Health Check Server monitoring setting.

Short Name: Audit Pipeline Test

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Template Name

`mgmt_navigator_failure_window`

Default Value

20

Unit(s)

MINUTES

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Template Name

`mgmt_navigator_failure_thresholds`

Default Value

critical:any, warning:never

Unit(s)

BYTES

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Template Name

`mgmt_navigator_status_check_enabled`

Default Value

true

Unit(s)

no unit

ZooKeeper Server Connection Count

This is a ZooKeeper Server role-level health test that checks that a moving average of the ZooKeeper Server's connection count does not exceed some value. A failure of this health test indicates a high connection load on the ZooKeeper Server. This test can be configured using the ZooKeeper Server Connection Count Thresholds and ZooKeeper Server Connection Count Monitoring Period ZooKeeper Server monitoring settings.

Short Name: Connection Count

ZooKeeper Server Connection Count Monitoring Period

Description

The period to review when computing the moving average of the connection count. Specified in minutes.

Template Name

`zookeeper_server_connection_count_window`

Default Value

3

Unit(s)

MINUTES

ZooKeeper Server Connection Count Thresholds

Description

The health check thresholds of the weighted average size of the ZooKeeper Server connection count over a recent period. See ZooKeeper Server Connection Count Monitoring Period.

Template Name

`zookeeper_server_connection_count_thresholds`

Default Value

critical:never, warning:never

Unit(s)

no unit

ZooKeeper Server Data Directory Free Space

This is a Server health test that checks that the filesystem containing the Data Directory of this Server has sufficient free space. See the Data Directory description on the Server configuration page for more information on this directory type. This test can be configured using the Data Directory Free Space Monitoring Absolute Thresholds and Data Directory Free Space Monitoring Percentage Thresholds Server monitoring settings.

Short Name: Data Directory Free Space

Data Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Data Directory.

Template Name

`zookeeper_server_data_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Data Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Data Directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Data Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`zookeeper_server_data_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

ZooKeeper Server File Descriptors

This Server health test checks that the number of file descriptors used does not rise above some percentage of the Server file descriptor limit. A failure of this health test may indicate a bug in either Hadoop or Cloudera Manager. Contact Cloudera support. This test can be configured using the File Descriptor Monitoring Thresholds Server monitoring setting.

Short Name: File Descriptors

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Template Name

`zookeeper_server_fd_thresholds`

Default Value

critical:70.0, warning:50.0

Unit(s)

PERCENT

ZooKeeper Server GC Duration

This Server health test checks that the Server is not spending too much time performing Java garbage collection. It checks that no more than some percentage of recent time is spent performing Java garbage collection. A failure of this health test may indicate a capacity planning problem or misconfiguration of the Server. This test can be configured using the Garbage Collection Duration Thresholds and Garbage Collection Duration Monitoring Period Server monitoring settings.

Short Name: GC Duration

Garbage Collection Duration Monitoring Period

Description

The period to review when computing the moving average of garbage collection time.

Template Name

`zookeeper_server_gc_duration_window`

Default Value

5

Unit(s)

MINUTES

Garbage Collection Duration Thresholds

Description

The health test thresholds for the weighted average time spent in Java garbage collection. Specified as a percentage of elapsed wall clock time.

Template Name

`zookeeper_server_gc_duration_thresholds`

Default Value

critical:60.0, warning:30.0

Unit(s)

no unit

ZooKeeper Server Heap Dump Directory Free Space

This Server health test checks that the filesystem containing the heap dump directory of this Server has sufficient free space. This test can be configured using the Heap Dump Directory Free Space Monitoring Absolute Thresholds and Heap Dump Directory Free Space Monitoring Percentage Thresholds Server monitoring settings.

Short Name: Heap Dump Directory Free Space

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Template Name

`heap_dump_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`heap_dump_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

ZooKeeper Server Host Health

This Server health test factors in the health of the host upon which the Server is running. A failure of this test means that the host running the Server is experiencing some problem. See that host's status page for more details.This test can be enabled or disabled using the Server Host Health Test Server monitoring setting.

Short Name: Host Health

Server Host Health Test

Description

When computing the overall Server health, consider the host's health.

Template Name

`zookeeper_server_host_health_enabled`

Default Value

true

Unit(s)

no unit

ZooKeeper Server Log Directory Free Space

This Server health test checks that the filesystem containing the log directory of this Server has sufficient free space. This test can be configured using the Log Directory Free Space Monitoring Absolute Thresholds and Log Directory Free Space Monitoring Percentage Thresholds Server monitoring settings.

Short Name: Log Directory Free Space

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Template Name

`log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

ZooKeeper Server Maximum Request Latency

This is a ZooKeeper server health test that checks that the ratio of the maximum request latency to the maximum client-negotiable session timeout does not exceed some value. Note that the maximum client-negotiable timeout need not be the actual session timeout used by a client but is the upper bound of such client session timeouts. As a result, this test being in "Good" health does not preclude clients from experiencing timeouts based on the particular

session timeout value they have negotiated with the server. A failure of this health test likely indicates a high load on the ZooKeeper Server. This test can be configured using the Maximum Latency Monitoring Thresholds ZooKeeper Server monitoring setting.

Short Name: Maximum Request Latency

Maximum Latency Monitoring Thresholds

Description

The percentage thresholds of the ratio of the maximum request latency to the maximum client-negotiable session timeout since the server was started.

Template Name

`zookeeper_server_max_latency_thresholds`

Default Value

critical:100.0, warning:75.0

Unit(s)

PERCENT

ZooKeeper Server Outstanding Requests

This is a ZooKeeper Server role-level health test that checks that a moving average of the size of the ZooKeeper Server's outstanding requests does not exceed some value. Outstanding requests are the number of queued requests in the server. It increases when the server is under load and is receiving more sustained requests than it can process. A failure of this health test indicates a high connection load on the ZooKeeper Server. This test can be configured using the ZooKeeper Server Outstanding Requests Thresholds and ZooKeeper Server Outstanding Requests Monitoring Period ZooKeeper Server monitoring settings.

Short Name: Outstanding Requests

ZooKeeper Server Outstanding Requests Monitoring Period

Description

The period to review when computing the moving average of the outstanding requests queue size. Specified in minutes.

Template Name

`zookeeper_server_outstanding_requests_window`

Default Value

3

Unit(s)

MINUTES

ZooKeeper Server Outstanding Requests Thresholds

Description

The health check thresholds of the weighted average size of the ZooKeeper Server outstanding requests queue over a recent period. See ZooKeeper Server Outstanding Requests Monitoring Period.

Template Name

`zookeeper_server_outstanding_requests_thresholds`

Default Value

critical:never, warning:never

Unit(s)

no unit

ZooKeeper Server Process Status

This Server health test checks that the Cloudera Manager Agent on the Server host is heart beating correctly and that the process associated with the Server role is in the state expected by Cloudera Manager. A failure of this health test may indicate a problem with the Server process, a lack of connectivity to the Cloudera Manager Agent on the Server host, or a problem with the Cloudera Manager Agent. This test can fail either because the Server has crashed or because the Server will not start or stop in a timely fashion. Check the Server logs for more details. If the test fails because of problems communicating with the Cloudera Manager Agent on the Server host, check the status of the Cloudera Manager Agent by running /etc/init.d/cloudera-scm-agent status on the Server host, or look in the Cloudera Manager Agent logs on the Server host for more details. This test can be enabled or disabled using the Server Process Health Test Server monitoring setting.

Short Name: Process Status

Server Process Health Test

Description

Enables the health test that the Server's process state is consistent with the role configuration

Template Name

`zookeeper_server_scm_health_enabled`

Default Value

true

Unit(s)

no unit

ZooKeeper Server Quorum Membership

This is a ZooKeeper server role-level health test to verify that the server is part of a quorum. This check is disabled if the ZooKeeper Server is in standalone mode. The test returns "Concerning" health as long as the quorum membership status for the ZooKeeper Server was determined within the detection window and it is in leader election. The test returns "Bad" health if the ZooKeeper Server is not part of a quorum or the quorum status of the ZooKeeper Server could not be determined for the entire detection window. A failure of this health test may indicate a communication problem between this ZooKeeper Server and the rest of its peers or between the Cloudera Manager Service Monitor and the ZooKeeper Server. Check the ZooKeeper Server and Cloudera Manager Service Monitor logs for additional information. This test can be enabled or disabled using the Enable the Quorum Membership Check ZooKeeper Server monitoring setting. In addition, the Quorum Membership Detection Window setting can be used to adjust the time that the Cloudera Manager Service Monitor has to detect the ZooKeeper Server quorum membership status before this health test fails.

Short Name: Quorum Membership

Enable the Quorum Membership Check

Description

Enables the quorum membership check for this ZooKeeper Server.

Template Name

`zookeeper_server_quorum_membership_enabled`

Default Value

true

Unit(s)

no unit

Quorum Membership Detection Window

Description

The tolerance window that will be used in the detection of a ZooKeeper server's membership in a quorum. Specified in minutes.

Template Name

`zookeeper_server_quorum_membership_detection_window`

Default Value

3

Unit(s)

MINUTES

ZooKeeper Server Swap Memory Usage

This Server health test checks the amount of swap memory in use by the role. A failure of this health test may indicate that your machine is overloaded. This test can be configured using the Process Swap Memory Thresholds monitoring settings.

Short Name: Swap Memory Usage

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Template Name

`process_swap_memory_thresholds`

Default Value

critical:never, warning:200.0

Unit(s)

BYTES

ZooKeeper Server Transaction Log Directory Free Space

This is a Server health test that checks that the filesystem containing the Transaction Log Directory of this Server has sufficient free space. See the Transaction Log Directory description on the Server configuration page for more information on this directory type. This test can be configured using the Transaction Log Directory Free Space Monitoring Absolute Thresholds and Transaction Log Directory Free Space Monitoring Percentage Thresholds Server monitoring settings.

Short Name: Transaction Log Directory Free Space

Transaction Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Transaction Log Directory.

Template Name

`zookeeper_server_data_log_directory_free_space_absolute_thresholds`

Default Value

critical:5.36870912E9, warning:1.073741824E10

Unit(s)

BYTES

Transaction Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Transaction Log Directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Transaction Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Template Name

`zookeeper_server_data_log_directory_free_space_percentage_thresholds`

Default Value

critical:never, warning:never

Unit(s)

PERCENT

ZooKeeper Server Unexpected Exits

This Server health test checks that the Server has not recently exited unexpectedly. The test returns "Bad" health if the number of unexpected exits exceeds a critical threshold. For example, if this test is configured with a critical threshold of 1, this test returns "Good" health if there have been no unexpected exits recently. If 1 or more unexpected exits occured recently, this test returns "Bad" health. The test also indicates whether any of the exits were caused by an OutOfMemory error if the Cloudera Manager Kill When Out of Memory monitoring setting is enabled. This test can be configured using the Unexpected Exits Thresholds and Unexpected Exits Monitoring Period Server monitoring settings.

Short Name: Unexpected Exits

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Template Name

`unexpected_exits_window`

Default Value

5

Unit(s)

MINUTES

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Template Name

`unexpected_exits_thresholds`

Default Value

critical:any, warning:never

Unit(s)

no unit