MapReduce Service (MRS)
3.3.1-LTS

Fault Management

Issue	01
Date	2024-04-30

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2024. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions

HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 Alarm Handling.....1
1.1 Overview.....1
1.2 Alarms of the MRS Management and Control Plane.....2
1.2.1 PAAS_MRS_00101 Failed to Create a Cluster.....2
1.2.2 PAAS_MRS_00102 Failed to Delete a Cluster.....4
1.2.3 PAAS_MRS_00103 Failed to Scale Out a Cluster.....6
1.2.4 PAAS_MRS_00105 Failed to Scale In a Cluster.....8
1.2.5 PAAS_MRS_00124 Cluster Exception.....10
1.2.6 PAAS_MRS_00135 Heartbeat Task Failed.....15
1.2.7 PAAS_MRS_00308 Too Many Auto Scaling Threads.....17
1.2.8 PAAS_MRS_00309 Too Many Waiting Auto Scaling Tasks.....18
1.2.9 PAAS_MRS_00310 Auto Scale-Out Failed.....20
1.2.10 PAAS_MRS_00311 Auto Scale-In Failed.....22
1.2.11 PAAS_MRS_00313 Failed to Deliver Auto Scale-Out Tasks.....24
1.2.12 PAAS_MRS_00604 Cluster Node Information Is Not Synchronized.....26
1.2.13 PAAS_MRS_00605 ECS Status of the Cluster Node Is Abnormal.....29
1.2.14 PAAS_MRS_00801 Cluster Security Risks.....31
1.2.15 PAAS_MRS_00804 MRS Secure Communications Is Disabled.....34
1.2.16 PAAS_MRS_00806 Usage Is About to Exceed the Threshold Allowed by the License.....36
1.2.17 PAAS_MRS_00807 Usage Exceeds the Threshold Allowed by the License.....39
1.2.18 PAAS_MRS_00905 Manager Failed to Respond to Auto Scaling Monitoring Tasks.....41
1.2.19 PAAS_MRS_00909 Too Many Alarms on the Console.....46
1.2.20 PAAS_MRS_00910 Cluster Scale-Out Partially Succeeded.....48
1.2.21 PAAS_MRS_00911 Node Scaling on Manager Takes a Long Time.....50
1.2.22 PAAS_MRS_00916 Roles Deployed on Non-Master Nodes in a Group Are Inconsistent.....52
1.2.23 PAAS_MRS_00917 Role Information on the Console Is Inconsistent with That on Manager.....55
1.2.24 PAAS_MRS_01001 MRS API Gateway Is Abnormal.....58
1.2.25 PAAS_MRS_01002 MRS Deployer Is Abnormal.....60
1.2.26 PAAS_MRS_01003 MRS ZooKeeper Service Is Abnormal.....63
1.2.27 PAAS_MRS_01004 MRS DB Service Is Faulty.....65
1.2.28 PAAS_MRS_01005 MRS API Gateway Instance Is Abnormal.....68
1.2.29 PAAS_MRS_01006 MRS Deployer Instance Is Abnormal.....71
1.2.30 PAAS_MRS_01007 MRS ZooKeeper Instance Is Abnormal.....73

1.2.31 PAAS_MRS_01008 MRS DB Instance Is Abnormal.....76
1.2.32 PAAS_MRS_01009 Low Response Success Rate of MRS Cluster List.....78
1.2.33 PAAS_MRS_01010 Low Response Success Rate of MRS Job Addition.....81
1.2.34 PAAS_MRS_01011 Low Response Success Rate of MRS Job Execution Result Obtaining.....83
1.2.35 PAAS_MRS_01012 Low Response Success Rate of MRS Query Job List.....85
1.2.36 PAAS_MRS_01013 Low Response Success Rate of MRS Job Stopping.....87
1.2.37 PAAS_MRS_01014 Low Response Success Rate of Batch MRS Job Deletion.....89
1.2.38 PAAS_MRS_01015 Low Response Success Rate of MRS SQL Result Obtaining.....91
1.3 Alarms of the MRS Tenant Plane.....93
1.3.1 ALM-12001 Audit Log Dumping Failure.....94
1.3.2 ALM-12004 Manager OLdap Resource Abnormal.....97
1.3.3 ALM-12005 Manager OKerberos Resource Abnormal.....99
1.3.4 ALM-12006 NodeAgent Process Is Abnormal.....102
1.3.5 ALM-12007 Process Fault.....107
1.3.6 ALM-12010 Manager Heartbeat Interruption Between the Active and Standby Nodes.....111
1.3.7 ALM-12011 Manager Data Synchronization Exception Between the Active and Standby Nodes.....114
1.3.8 ALM-12012 NTP Service Is Abnormal.....118
1.3.9 ALM-12014 Device Partition Lost.....126
1.3.10 ALM-12015 Partition Filesystem Readonly.....129
1.3.11 ALM-12016 CPU Usage Exceeds the Threshold.....132
1.3.12 ALM-12017 Insufficient Disk Capacity.....135
1.3.13 ALM-12018 Memory Usage Exceeds the Threshold.....138
1.3.14 ALM-12027 Host PID Usage Exceeds the Threshold.....141
1.3.15 ALM-12028 Number of Processes in the D State and Z State on a Host Exceeds the Threshold.....144
1.3.16 ALM-12033 Slow Disk Fault.....146
1.3.17 ALM-12034 Periodical Backup Failure.....154
1.3.18 ALM-12035 Unknown Data Status After Recovery Task Failure.....157
1.3.19 ALM-12037 NTP Server Abnormal.....160
1.3.20 ALM-12038 Monitoring Indicator Dumping Failure.....163
1.3.21 ALM-12039 Active/Standby OMS Databases Not Synchronized.....166
1.3.22 ALM-12040 Insufficient OS Entropy.....170
1.3.23 ALM-12041 Incorrect Permission on Key Files.....174
1.3.24 ALM-12042 Incorrect Configuration of Key Files.....177
1.3.25 ALM-12045 Read Packet Dropped Rate Exceeds the Threshold.....180
1.3.26 ALM-12046 Write Packet Dropped Rate Exceeds the Threshold.....185
1.3.27 ALM-12047 Read Packet Error Rate Exceeds the Threshold.....188
1.3.28 ALM-12048 Write Packet Error Rate Exceeds the Threshold.....191
1.3.29 ALM-12049 Network Read Throughput Rate Exceeds the Threshold.....194
1.3.30 ALM-12050 Network Write Throughput Rate Exceeds the Threshold.....197
1.3.31 ALM-12051 Disk Inode Usage Exceeds the Threshold.....200
1.3.32 ALM-12052 TCP Temporary Port Usage Exceeds the Threshold.....203
1.3.33 ALM-12053 Host File Handle Usage Exceeds the Threshold.....206

1.3.34 ALM-12054 Invalid Certificate File 210
1.3.35 ALM-12055 The Certificate File Is About to Expire 215
1.3.36 ALM-12057 Metadata Not Configured with the Task to Periodically Back Up Data to a Third-Party Server 221
1.3.37 ALM-12061 Process Usage Exceeds the Threshold 223
1.3.38 ALM-12062 OMS Parameter Configurations Mismatch with the Cluster Scale 227
1.3.39 ALM-12063 Unavailable Disk 230
1.3.40 ALM-12064 Host Random Port Range Conflicts with Cluster Used Port 233
1.3.41 ALM-12066 Trust Relationships Between Nodes Become Invalid 235
1.3.42 ALM-12067 Abnormal Tomcat Resources of Manager 238
1.3.43 ALM-12068 Abnormal ACS Resources of Manager 241
1.3.44 ALM-12069 Abnormal AOS Resources of Manager 243
1.3.45 ALM-12070 Controller Resource Is Abnormal 246
1.3.46 ALM-12071 Httpd Resource Is Abnormal 249
1.3.47 ALM-12072 FloatIP Resource Is Abnormal 251
1.3.48 ALM-12074 FMS Resource Is Abnormal 254
1.3.49 ALM-12075 PMS Resource Is Abnormal 256
1.3.50 ALM-12076 GaussDB Resource Is Abnormal 259
1.3.51 ALM-12077 User omm Expired 262
1.3.52 ALM-12078 Password of User omm Expired 264
1.3.53 ALM-12079 User omm Is About to Expire 267
1.3.54 ALM-12080 Password of User omm Is About to Expire 269
1.3.55 ALM-12081 User ommdba Expired 271
1.3.56 ALM-12082 User ommdba Is About to Expire 273
1.3.57 ALM-12083 Password of User ommdba Is About to Expire 276
1.3.58 ALM-12084 Password of User ommdba Expired 278
1.3.59 ALM-12085 Service Audit Log Dump Failure 280
1.3.60 ALM-12087 System Is in the Upgrade Observation Period 284
1.3.61 ALM-12089 Network Connections Between Nodes Are Abnormal 286
1.3.62 ALM-12091 Abnormal disaster Resources 289
1.3.63 ALM-12099 Core Dump for Cluster Processes 292
1.3.64 ALM-12100 AD Service Connection Failed 294
1.3.65 ALM-12101 AZ Unhealthy 297
1.3.66 ALM-12102 AZ HA Component Is Not Deployed Based on DR Requirements 300
1.3.67 ALM-12103 Executor Resource Exception 302
1.3.68 ALM-12104 Abnormal Knox Resources 304
1.3.69 ALM-12110 Failed to get ECS temporary AK/SK 307
1.3.70 ALM-12150 Disconnection Between the Active and DR Clusters 309
1.3.71 ALM-12151 Failed to Synchronize Ranger Permission Information for Cluster DR 312
1.3.72 ALM-12160 RPO of Streaming Data Synchronization of the Cluster DR Protection Group Exceeds the Threshold 315
1.3.73 ALM-12161 Periodic Synchronization Duration of Cluster DR Data Exceeds the Threshold 317
1.3.74 ALM-12162 Streaming Data Synchronization Failed During Cluster DR 320

1.3.75 ALM-12163 Periodical Data Synchronization Failed During Cluster DR 322
1.3.76 ALM-12164 Cluster DR Data Verification Failed 325
1.3.77 ALM-12165 Cluster DR User Information Synchronization Failure 328
1.3.78 ALM-12166 Cluster DR Protection Group Disabled for a Long Time 331
1.3.79 ALM-12167 Cluster DR Configuration Check Failed 333
1.3.80 ALM-12168 Key Service Configuration Check for Cluster DR Failed 338
1.3.81 ALM-12169 Historical Data Synchronization Failed During Cluster DR 343
1.3.82 ALM-12180 Suspended Disk I/O 346
1.3.83 ALM-12186 CGroup Task Usage Exceeds the Threshold 351
1.3.84 ALM-12187 Failed to Expand Disk Partition Capacity 353
1.3.85 ALM-12188 diskmgt Disk Monitoring Unavailable 357
1.3.86 ALM-12190 Number of Knox Connections Exceeds the Threshold 359
1.3.87 ALM-12191 Disk I/O Usage Exceeds the Threshold 361
1.3.88 ALM-12192 Host Load Exceeds the Threshold 364
1.3.89 ALM-12200 Password Is About to Expire 367
1.3.90 ALM-12201 Process CPU Usage Exceeds the Threshold 370
1.3.91 ALM-12202 Process Memory Usage Exceeds the Threshold 373
1.3.92 ALM-12203 Process Full GC Duration Exceeds the Threshold 375
1.3.93 ALM-12204 Wait Duration of a Disk Read Exceeds the Threshold 378
1.3.94 ALM-12205 Wait Duration of a Disk Write Exceeds the Threshold 381
1.3.95 ALM-12206 Password Has Expired 384
1.3.96 ALM-13000 ZooKeeper Service Unavailable 386
1.3.97 ALM-13001 Available ZooKeeper Connections Are Insufficient 390
1.3.98 ALM-13002 ZooKeeper Direct Memory Usage Exceeds the Threshold 393
1.3.99 ALM-13003 GC Duration of the ZooKeeper Process Exceeds the Threshold 396
1.3.100 ALM-13004 ZooKeeper Heap Memory Usage Exceeds the Threshold 399
1.3.101 ALM-13005 Failed to Set the Quota of Top Directories of ZooKeeper Components 402
1.3.102 ALM-13006 Znode Number or Capacity Exceeds the Threshold 405
1.3.103 ALM-13007 Available ZooKeeper Client Connections Are Insufficient 408
1.3.104 ALM-13008 ZooKeeper Znode Usage Exceeds the Threshold 410
1.3.105 ALM-13009 ZooKeeper Znode Capacity Usage Exceeds the Threshold 413
1.3.106 ALM-13010 Znode Usage of a Directory with Quota Configured Exceeds the Threshold 416
1.3.107 ALM-14000 HDFS Service Unavailable 419
1.3.108 ALM-14001 HDFS Disk Usage Exceeds the Threshold 422
1.3.109 ALM-14002 DataNode Disk Usage Exceeds the Threshold 425
1.3.110 ALM-14003 Number of Lost HDFS Blocks Exceeds the Threshold 429
1.3.111 ALM-14006 Number of HDFS Files Exceeds the Threshold 432
1.3.112 ALM-14007 NameNode Heap Memory Usage Exceeds the Threshold 436
1.3.113 ALM-14008 DataNode Heap Memory Usage Exceeds the Threshold 440
1.3.114 ALM-14009 Number of Dead DataNodes Exceeds the Threshold 443
1.3.115 ALM-14010 NameService Service Is Abnormal 447
1.3.116 ALM-14011 DataNode Data Directory Is Not Configured Properly 451

1.3.117 ALM-14012 JournalNode Is Out of Synchronization 455
1.3.118 ALM-14013 Failed to Update the NameNode FsImage File 458
1.3.119 ALM-14014 NameNode GC Time Exceeds the Threshold 463
1.3.120 ALM-14015 DataNode GC Time Exceeds the Threshold 466
1.3.121 ALM-14016 DataNode Direct Memory Usage Exceeds the Threshold 469
1.3.122 ALM-14017 NameNode Direct Memory Usage Exceeds the Threshold 472
1.3.123 ALM-14018 NameNode Non-heap Memory Usage Exceeds the Threshold 475
1.3.124 ALM-14019 DataNode Non-heap Memory Usage Exceeds the Threshold 478
1.3.125 ALM-14020 Number of Entries in the HDFS Directory Exceeds the Threshold 482
1.3.126 ALM-14021 NameNode Average RPC Processing Time Exceeds the Threshold 485
1.3.127 ALM-14022 NameNode Average RPC Queuing Time Exceeds the Threshold 489
1.3.128 ALM-14023 Percentage of Total Reserved Disk Space for Replicas Exceeds the Threshold 493
1.3.129 ALM-14024 Tenant Space Usage Exceeds the Threshold 497
1.3.130 ALM-14025 Tenant File Object Usage Exceeds the Threshold 500
1.3.131 ALM-14026 Blocks on DataNode Exceed the Threshold 503
1.3.132 ALM-14027 DataNode Disk Fault 506
1.3.133 ALM-14028 Number of Blocks to Be Supplemented Exceeds the Threshold 509
1.3.134 ALM-14029 Number of Blocks in a Replica Exceeds the Threshold 512
1.3.135 ALM-14030 HDFS Allows Write of Single-Replica Data 515
1.3.136 ALM-14031 DataNode Process Is Abnormal 518
1.3.137 ALM-14032 JournalNode Process Is Abnormal 520
1.3.138 ALM-14033 ZKFC Process Is Abnormal 523
1.3.139 ALM-14034 Router Process Is Abnormal 525
1.3.140 ALM-14035 HttpFS Process Is Abnormal 528
1.3.141 ALM-14036 NameNode Is In Safe Mode 530
1.3.142 ALM-14037 DataNodes Outside the Cluster 533
1.3.143 ALM-16000 Percentage of Sessions Connected to the HiveServer to Maximum Number Allowed Exceeds the Threshold 536
1.3.144 ALM-16001 Hive Warehouse Space Usage Exceeds the Threshold 538
1.3.145 ALM-16002 Hive SQL Execution Success Rate Is Lower Than the Threshold 542
1.3.146 ALM-16003 Background Thread Usage Exceeds the Threshold 545
1.3.147 ALM-16004 Hive Service Unavailable 548
1.3.148 ALM-16005 The Heap Memory Usage of the Hive Process Exceeds the Threshold 553
1.3.149 ALM-16006 The Direct Memory Usage of the Hive Process Exceeds the Threshold 557
1.3.150 ALM-16007 Hive GC Time Exceeds the Threshold 560
1.3.151 ALM-16008 Non-Heap Memory Usage of the Hive Process Exceeds the Threshold 563
1.3.152 ALM-16009 Map Number Exceeds the Threshold 566
1.3.153 ALM-16045 Hive Data Warehouse Is Deleted 568
1.3.154 ALM-16046 Hive Data Warehouse Permission Is Modified 570
1.3.155 ALM-16047 HiveServer Has Been Deregistered from ZooKeeper 573
1.3.156 ALM-16048 Tez or Spark Library Path Does Not Exist 576
1.3.157 ALM-16049 Connection Between Hive MetaStore and Redis Is Abnormal 578
1.3.158 ALM-16050 Redis Cache of Hive MetaStore Is Unavailable 581

1.3.159 ALM-16051 Percentage of Sessions Connected to MetaStore Exceeds the Threshold 585
1.3.160 ALM-17003 Oozie Service Unavailable 588
1.3.161 ALM-17004 Oozie Heap Memory Usage Exceeds the Threshold 592
1.3.162 ALM-17005 Oozie Non Heap Memory Usage Exceeds the Threshold 595
1.3.163 ALM-17006 Oozie Direct Memory Usage Exceeds the Threshold 597
1.3.164 ALM-17007 Garbage Collection (GC) Time of the Oozie Process Exceeds the Threshold 600
1.3.165 ALM-17008 Abnormal Connection Between Oozie and ZooKeeper 602
1.3.166 ALM-17009 Abnormal Connection Between Oozie and DBService 605
1.3.167 ALM-17010 Abnormal Connection Between Oozie and HDFS 607
1.3.168 ALM-17011 Abnormal Connection Between Oozie and Yarn 610
1.3.169 ALM-18000 Yarn Service Unavailable 612
1.3.170 ALM-18002 NodeManager Heartbeat Lost 615
1.3.171 ALM-18003 NodeManager Unhealthy 618
1.3.172 ALM-18008 Heap Memory Usage of ResourceManager Exceeds the Threshold 622
1.3.173 ALM-18009 Heap Memory Usage of JobHistoryServer Exceeds the Threshold 625
1.3.174 ALM-18010 ResourceManager GC Time Exceeds the Threshold 628
1.3.175 ALM-18011 NodeManager GC Time Exceeds the Threshold 632
1.3.176 ALM-18012 JobHistoryServer GC Time Exceeds the Threshold 634
1.3.177 ALM-18013 ResourceManager Direct Memory Usage Exceeds the Threshold 637
1.3.178 ALM-18014 NodeManager Direct Memory Usage Exceeds the Threshold 640
1.3.179 ALM-18015 JobHistoryServer Direct Memory Usage Exceeds the Threshold 643
1.3.180 ALM-18016 Non Heap Memory Usage of ResourceManager Exceeds the Threshold 646
1.3.181 ALM-18017 Non Heap Memory Usage of NodeManager Exceeds the Threshold 650
1.3.182 ALM-18018 NodeManager Heap Memory Usage Exceeds the Threshold 653
1.3.183 ALM-18019 Non Heap Memory Usage of JobHistoryServer Exceeds the Threshold 656
1.3.184 ALM-18020 Yarn Task Execution Timeout 659
1.3.185 ALM-18021 Mapreduce Service Unavailable 662
1.3.186 ALM-18022 Insufficient YARN Queue Resources 665
1.3.187 ALM-18023 Number of Pending Yarn Tasks Exceeds the Threshold 669
1.3.188 ALM-18024 Pending Yarn Memory Usage Exceeds the Threshold 672
1.3.189 ALM-18025 Number of Terminated Yarn Tasks Exceeds the Threshold 675
1.3.190 ALM-18026 Number of Failed Yarn Tasks Exceeds the Threshold 677
1.3.191 ALM-18027 JobHistoryServer Process Is Abnormal 679
1.3.192 ALM-18028 TimeLineServer Process Is Abnormal 682
1.3.193 ALM-19000 HBase Service Unavailable 685
1.3.194 ALM-19006 HBase Replication Sync Failed 691
1.3.195 ALM-19007 HBase GC Time Exceeds the Threshold 695
1.3.196 ALM-19008 Heap Memory Usage of the HBase Process Exceeds the Threshold 699
1.3.197 ALM-19009 Direct Memory Usage of the HBase Process Exceeds the Threshold 702
1.3.198 ALM-19011 RegionServer Region Number Exceeds the Threshold 705
1.3.199 ALM-19012 HBase System Table Directory or File Lost 710
1.3.200 ALM-19013 Duration of Regions in transaction State Exceeds the Threshold 712

1.3.201 ALM-19014 Capacity Quota Usage on ZooKeeper Exceeds the Threshold Severely 715
1.3.202 ALM-19015 Quantity Quota Usage on ZooKeeper Exceeds the Threshold 718
1.3.203 ALM-19016 Quantity Quota Usage on ZooKeeper Exceeds the Threshold Severely 722
1.3.204 ALM-19017 Capacity Quota Usage on ZooKeeper Exceeds the Threshold 725
1.3.205 ALM-19018 HBase Compaction Queue Size Exceeds the Threshold 728
1.3.206 ALM-19019 Number of HBase HFiles to Be Synchronized Exceeds the Threshold 731
1.3.207 ALM-19020 Number of HBase WAL Files to Be Synchronized Exceeds the Threshold 734
1.3.208 ALM-19021 Handler Usage of RegionServer Exceeds the Threshold 738
1.3.209 ALM-19022 HBase Hotspot Detection Is Unavailable 742
1.3.210 ALM-19023 Region Traffic Restriction for HBase 745
1.3.211 ALM-19024 RPC Requests P99 Latency on RegionServer Exceeds the Threshold 748
1.3.212 ALM-19025 Damaged StoreFile in HBase 751
1.3.213 ALM-19026 Damaged WAL Files in HBase 754
1.3.214 ALM-19030 P99 Latency of RegionServer RPC Request Exceeds the Threshold 756
1.3.215 ALM-19031 Number of RegionServer RPC Connections Exceeds the Threshold 760
1.3.216 ALM-19032 Number of Tasks in the RegionServer RPC Write Queue Exceeds the Threshold 763
1.3.217 ALM-19033 Number of Tasks in the RegionServer RPC Read Queue Exceeds the Threshold 767
1.3.218 ALM-19034 Number of RegionServer WAL Write Timesouts Exceeds the Threshold 773
1.3.219 ALM-19035 Size of the RegionServer Call Queue Exceeds the Threshold 776
1.3.220 ALM-20002 Hue Service Unavailable 781
1.3.221 ALM-23001 Loader Service Unavailable 784
1.3.222 ALM-23003 Loader Task Execution Failed 789
1.3.223 ALM-23004 Loader Heap Memory Usage Exceeds the Threshold 792
1.3.224 ALM-23005 Loader Non-Heap Memory Usage Exceeds the Threshold 795
1.3.225 ALM-23006 Loader Direct Memory Usage Exceeds the Threshold 797
1.3.226 ALM-23007 GC Duration of the Loader Process Exceeds the Threshold 800
1.3.227 ALM-24000 Flume Service Unavailable 803
1.3.228 ALM-24001 Flume Agent Exception 805
1.3.229 ALM-24003 Flume Client Connection Interrupted 810
1.3.230 ALM-24004 Exception Occurs When Flume Reads Data 812
1.3.231 ALM-24005 Exception Occurs When Flume Transmits Data 815
1.3.232 ALM-24006 Heap Memory Usage of Flume Server Exceeds the Threshold 819
1.3.233 ALM-24007 Flume Server Direct Memory Usage Exceeds the Threshold 822
1.3.234 ALM-24008 Flume Server Non Heap Memory Usage Exceeds the Threshold 825
1.3.235 ALM-24009 Flume Server Garbage Collection (GC) Duration Exceeds the Threshold 828
1.3.236 ALM-24010 Flume Certificate File Is Invalid or Damaged 831
1.3.237 ALM-24011 Flume Certificate File Is About to Expire 833
1.3.238 ALM-24012 Flume Certificate File Has Expired 836
1.3.239 ALM-24013 Flume MonitorServer Certificate File Is Invalid or Damaged 839
1.3.240 ALM-24014 Flume MonitorServer Certificate Is About to Expire 842
1.3.241 ALM-24015 Flume MonitorServer Certificate File Has Expired 845
1.3.242 ALM-25000 LdapServer Service Unavailable 848

1.3.243 ALM-25004 Abnormal LdapServer Data Synchronization 850
1.3.244 ALM-25005 nscd Service Exception 854
1.3.245 ALM-25006 Sssd Service Exception 858
1.3.246 ALM-25007 Number of SlapdServer Connections Exceeds the Threshold 862
1.3.247 ALM-25008 SlapdServer CPU Usage Exceeds the Threshold 865
1.3.248 ALM-25500 KrbServer Service Unavailable 868
1.3.249 ALM-25501 Too Many KerberosServer Requests 871
1.3.250 ALM-27001 DBService Is Unavailable 874
1.3.251 ALM-27003 DBService Heartbeat Interruption Between the Active and Standby Nodes 877
1.3.252 ALM-27004 Data Inconsistency Between Active and Standby DBServices 880
1.3.253 ALM-27005 Database Connection Usage Exceeds the Threshold 883
1.3.254 ALM-27006 Data Directory Disk Usage Exceeds the Threshold 888
1.3.255 ALM-27007 Database Enters the Read-Only Mode 891
1.3.256 ALM-32000 Solr Service Unavailable 894
1.3.257 ALM-32002 SolrServerAdmin Heartbeat Interruption Between the Active and Standby Nodes 898
1.3.258 ALM-32003 Solr Heap Memory Usage Exceeds the Threshold 901
1.3.259 ALM-32005 Down Replicas Exist in Solr 904
1.3.260 ALM-32006 Solr Instance GC Time Exceeds the Threshold 906
1.3.261 ALM-32007 Solr Has Collections Without Replicas 910
1.3.262 ALM-32008 Solr Stored Shard Data Volume Exceeds the Threshold 912
1.3.263 ALM-32009 Solr Shard Document Number Exceeds the Threshold 916
1.3.264 ALM-32010 Invalid Solr HA Certificate File 920
1.3.265 ALM-32011 Solr HA Certificate Is About to Expire 922
1.3.266 ALM-32012 Solr HA Certificate File Has Expired 925
1.3.267 ALM-33004 BLU Instance Health Status of Containers Is Abnormal 927
1.3.268 ALM-33005 Maximum Number of Concurrent Containers Requests Exceeds the Threshold 930
1.3.269 ALM-33006 Failure Rate of Containers Calls Exceeds the Threshold 932
1.3.270 ALM-33007 ALB TPS of Containers Exceeds the Threshold 936
1.3.271 ALM-33008 Average Latency of Containers Exceeds the Threshold 939
1.3.272 ALM-33009 Containers Heap Memory Usage Exceeds the Threshold 943
1.3.273 ALM-33010 Containers Non-Heap Memory Usage Exceeds the Threshold 945
1.3.274 ALM-33011 Containers Metaspace Usage Exceeds the Threshold 948
1.3.275 ALM-33012 Containers' ZooKeeper Client Is Disconnected 951
1.3.276 ALM-35000 FTP-Server Service Unavailable 953
1.3.277 ALM-35001 FTP-Server Heap Memory Usage Exceeds the Threshold 956
1.3.278 ALM-35002 FTP-Server Direct Buffer Usage Exceeds the Threshold 959
1.3.279 ALM-35003 FTP-Server NonHeap Memory Usage Exceeds the Threshold 961
1.3.280 ALM-35004 FTP-Server Garbage Collection (GC) Time Exceeds the Threshold 964
1.3.281 ALM-38000 Kafka Service Unavailable 967
1.3.282 ALM-38001 Insufficient Kafka Disk Space 970
1.3.283 ALM-38002 Kafka Heap Memory Usage Exceeds the Threshold 976
1.3.284 ALM-38004 Kafka Direct Memory Usage Exceeds the Threshold 978

1.3.285 ALM-38005 GC Duration of the Broker Process Exceeds the Threshold....981
1.3.286 ALM-38006 Percentage of Kafka Partitions That Are Not Completely Synchronized Exceeds the Threshold....984
1.3.287 ALM-38007 Status of Kafka Default User Is Abnormal....987
1.3.288 ALM-38008 Abnormal Kafka Data Directory Status....989
1.3.289 ALM-38009 Busy Broker Disk I/Os....992
1.3.290 ALM-38010 Topics with Single Replica....995
1.3.291 ALM-38011 User Connection Usage on Broker Exceeds the Threshold....998
1.3.292 ALM-39000 AOF Persistence Exception....1002
1.3.293 ALM-39001 RDB Persistence Exception....1005
1.3.294 ALM-39002 Abnormal Redis Cluster....1008
1.3.295 ALM-39004 Redis Service Unavailable....1011
1.3.296 ALM-39005 Single Master Redis Instance....1014
1.3.297 ALM-39006 Too Many Redis Master Instances Are on the Same Host....1016
1.3.298 ALM-39007 Inconsistent Maximum Memory Configurations on Redis Master and Slave Instances....1018
1.3.299 ALM-39008 Uneven Slot Distribution of Redis Master Instances....1020
1.3.300 ALM-39009 Redis Slot Migration Exception....1023
1.3.301 ALM-39010 Redis Instance Connections Are Abnormal....1025
1.3.302 ALM-39011 Exceeded Redis Instance Memory Usage....1028
1.3.303 ALM-39012 Excessive Redis Client Connections....1031
1.3.304 ALM-39013 Abnormal Synchronization Between the Active and Standby Redis Nodes....1034
1.3.305 ALM-41007 RTDService Unavailable....1037
1.3.306 ALM-43001 Spark Service Unavailable....1040
1.3.307 ALM-43006 Heap Memory Usage of the JobHistory Process Exceeds the Threshold....1044
1.3.308 ALM-43007 Non-Heap Memory Usage of the JobHistory Process Exceeds the Threshold....1047
1.3.309 ALM-43008 Direct Memory Usage of the JobHistory Process Exceeds the Threshold....1050
1.3.310 ALM-43009 JobHistory Process GC Duration Exceeds the Threshold....1053
1.3.311 ALM-43010 Heap Memory Usage of the JDBCServer Process Exceeds the Threshold....1055
1.3.312 ALM-43011 Non-Heap Memory Usage of the JDBCServer Process Exceeds the Threshold....1058
1.3.313 ALM-43012 Direct Memory Usage of the JDBCServer Process Exceeds the Threshold....1061
1.3.314 ALM-43013 JDBCServer Process GC Duration Exceeds the Threshold....1064
1.3.315 ALM-43017 JDBCServer Process Full GC Times Exceeds the Threshold....1067
1.3.316 ALM-43018 JobHistory Process Full GC Times Exceeds the Threshold....1070
1.3.317 ALM-43019 Heap Memory Usage of the IndexServer Process Exceeds the Threshold....1073
1.3.318 ALM-43020 Non-Heap Memory Usage of the IndexServer Process Exceeds the Threshold....1076
1.3.319 ALM-43021 Direct Memory Usage of the IndexServer Process Exceeds the Threshold....1079
1.3.320 ALM-43022 IndexServer Process GC Time Exceeds the Threshold....1082
1.3.321 ALM-43023 IndexServer Process Full GC Number Exceeds the Threshold....1084
1.3.322 ALM-43028 JDBCServer Process Session Overload....1087
1.3.323 ALM-43200 Elasticsearch Service Unavailable....1090
1.3.324 ALM-43201 Heap Memory Usage of Elasticsearch Exceeds the Threshold....1093
1.3.325 ALM-43202 Indices in the Yellow State Exist in Elasticsearch....1097

1.3.326 ALM-43203 Indices in the Red State Exist in Elasticsearch....1100
1.3.327 ALM-43204 GC Duration of the Elasticsearch Process Exceeds the Threshold....1104
1.3.328 ALM-43205 Elasticsearch Stored Shard Data Volume Exceeds the Threshold....1108
1.3.329 ALM-43206 Elasticsearch Shard Document Number Exceeds the Threshold....1111
1.3.330 ALM-43207 Elasticsearch Has Indexes Without Replicas....1114
1.3.331 ALM-43208 Elasticsearch Data Directory Usage Exceeds the Threshold....1117
1.3.332 ALM-43209 Total Number of Elasticsearch Instance Shards Exceeds the Threshold....1121
1.3.333 ALM-43210 Total Number of Elasticsearch Shards Exceeds the Threshold....1124
1.3.334 ALM-43600 GraphBase Service Unavailable....1127
1.3.335 ALM-43605 Number of Real-Time Requests on a GraphBase Node Exceeds the Threshold....1130
1.3.336 ALM-43607 Nginx Fault in GraphBase....1132
1.3.337 ALM-43608 Floating IP Address of GraphBase Is Faulty....1134
1.3.338 ALM-43609 TaskManager of GraphBase Is Faulty....1137
1.3.339 ALM-43610 GC Time of the Old-Generation GraphServer Process Exceeds the Threshold....1139
1.3.340 ALM-43611 Number of GC Times of the Old-Generation GraphServer Process Exceeds the Threshold....1142
1.3.341 ALM-43612 GC Duration of the Young-Generation GraphServer Process Exceeds the Threshold1145
1.3.342 ALM-43613 Number of GC Times of the Young-Generation GraphServer Process Exceeds the Threshold....1147
1.3.343 ALM-43614 Time Spent on a GraphBase Path Query Request Exceeds the Threshold....1150
1.3.344 ALM-43615 Time Spent on a Line Expansion Query Request in GraphBase Exceeds the Threshold....1153
1.3.345 ALM-43616 GraphBase-related Yarn Jobs Are Abnormal....1155
1.3.346 ALM-43617 Number of Waiting Queues for Real-Time Data Import to GraphBase Exceeds the Threshold....1157
1.3.347 ALM-43618 GraphServer Heap Memory Usage Exceeds the Threshold....1160
1.3.348 ALM-43619 Invalid GraphBase HA Certificate Files....1162
1.3.349 ALM-43620 GraphBase HA Certificates Are About to Expire....1166
1.3.350 ALM-43621 GraphBase HA Certificate Files Have Expired....1169
1.3.351 ALM-43850 KMS Service Unavailable....1172
1.3.352 ALM-43853 KMS Process Is Abnormal....1175
1.3.353 ALM-45000 HetuEngine Service Unavailable....1177
1.3.354 ALM-45001 Faulty HetuEngine Compute Instances....1182
1.3.355 ALM-45003 HetuEngine QAS Disk Capacity Is Insufficient....1185
1.3.356 ALM-45004 Tasks Stacked on HetuEngine Compute Instance....1188
1.3.357 ALM-45005 CPU Usage of HetuEngine Compute Instance Exceeded the Threshold....1191
1.3.358 ALM-45006 Memory Usage of a HetuEngine Compute Instance Exceeded the Threshold....1194
1.3.359 ALM-45007 Number of Workers of a HetuEngine Compute Instance Is Less Than the Threshold....1198
1.3.360 ALM-45179 Number of Failed OBS readFully API Calls Exceeds the Threshold....1201
1.3.361 ALM-45180 Number of Failed OBS read API Calls Exceeds the Threshold....1203
1.3.362 ALM-45181 Number of Failed OBS write API Calls Exceeds the Threshold....1206
1.3.363 ALM-45182 Number of Throttled OBS Operations Exceeds the Threshold....1209

1.3.364 ALM-45183 Total Number of FileNotFoundException Errors Reported by OBS Exceeds the Threshold....1211
1.3.365 ALM-45184 Total Number of OBSIllegalArgumentException Errors Reported by OBS Exceeds the Threshold....1214
1.3.366 ALM-45185 Total Number of AccessControlException Errors Reported by OBS Exceeds the Threshold....1216
1.3.367 ALM-45186 Total Number of OBSMethodNotAllowedException Errors Reported by OBS Exceeds the Threshold....1219
1.3.368 ALM-45187 Total Number of OBSFileConflictException Errors Reported by OBS Exceeds the Threshold....1222
1.3.369 ALM-45188 Total Number of OBSIOException Errors Reported by OBS Exceeds the Threshold 1224
1.3.370 ALM-45189 Total Number of EOFException Errors Reported by OBS Exceeds the Threshold.... 1227
1.3.371 ALM-45190 Total Number of Other OBS Exceptions Exceeds the Threshold....1229
1.3.372 ALM-45191 Failed to Obtain ECS Metadata.... 1232
1.3.373 ALM-45192 Failed to Obtain the IAM Security Token.... 1235
1.3.374 ALM-45275 Ranger Service Unavailable.... 1237
1.3.375 ALM-45276 Abnormal RangerAdmin Status....1240
1.3.376 ALM-45277 RangerAdmin Heap Memory Usage Exceeds the Threshold....1242
1.3.377 ALM-45278 RangerAdmin Direct Memory Usage Exceeds the Threshold....1245
1.3.378 ALM-45279 RangerAdmin Non-Heap Memory Usage Exceeds the Threshold....1247
1.3.379 ALM-45280 RangerAdmin GC Duration Exceeds the Threshold.... 1250
1.3.380 ALM-45281 UserSync Heap Memory Usage Exceeds the Threshold....1253
1.3.381 ALM-45282 UserSync Direct Memory Usage Exceeds the Threshold....1255
1.3.382 ALM-45283 UserSync Non-Heap Memory Usage Exceeds the Threshold....1258
1.3.383 ALM-45284 UserSync Garbage Collection (GC) Time Exceeds the Threshold.... 1260
1.3.384 ALM-45285 TagSync Heap Memory Usage Exceeds the Threshold....1263
1.3.385 ALM-45286 TagSync Direct Memory Usage Exceeds the Threshold....1266
1.3.386 ALM-45287 TagSync Non-Heap Memory Usage Exceeds the Threshold....1268
1.3.387 ALM-45288 TagSync Garbage Collection (GC) Time Exceeds the Threshold.... 1271
1.3.388 ALM-45289 PolicySync Heap Memory Usage Exceeds the Threshold.... 1273
1.3.389 ALM-45290 PolicySync Direct Memory Usage Exceeds the Threshold.... 1276
1.3.390 ALM-45291 PolicySync Non-Heap Memory Usage Exceeds the Threshold.... 1278
1.3.391 ALM-45292 PolicySync GC Duration Exceeds the Threshold....1281
1.3.392 ALM-45293 Ranger User Synchronization Exception....1283
1.3.393 ALM-45294 RangerKMS Process Is Abnormal.... 1286
1.3.394 ALM-45425 ClickHouse Service Unavailable....1289
1.3.395 ALM-45426 ClickHouse Service Quantity Quota Usage in ZooKeeper Exceeds the Threshold....1293
1.3.396 ALM-45427 ClickHouse Service Capacity Quota Usage in ZooKeeper Exceeds the Threshold.... 1296
1.3.397 ALM-45428 ClickHouse Disk I/O Exception....1299
1.3.398 ALM-45429 Table Metadata Synchronization Failed on the Added ClickHouse Node.... 1302
1.3.399 ALM-45430 Permission Metadata Synchronization Failed on the Added ClickHouse Node....1304
1.3.400 ALM-45431 Improper ClickHouse Instance Distribution for Topology Allocation.... 1307
1.3.401 ALM-45432 ClickHouse User Synchronization Process Fails....1310
1.3.402 ALM-45433 ClickHouse AZ Topology Exception.... 1313

1.3.403 ALM-45434 A Single Replica Exists in the ClickHouse Data Table.....1316
1.3.404 ALM-45435 Inconsistent Metadata of ClickHouse Tables.....1318
1.3.405 ALM-45436 Skew ClickHouse Table Data.....1321
1.3.406 ALM-45437 Excessive Parts in the ClickHouse Table.....1324
1.3.407 ALM-45438 ClickHouse Disk Usage Exceeds 80%.....1327
1.3.408 ALM-45439 ClickHouse Node Enters the Read-Only Mode.....1329
1.3.409 ALM-45440 Inconsistency Between ClickHouse Replicas.....1331
1.3.410 ALM-45441 Zookeeper Disconnected.....1335
1.3.411 ALM-45442 Too Many Concurrent SQL Statements.....1338
1.3.412 ALM-45443 Slow SQL Queries in the Cluster.....1340
1.3.413 ALM-45444 Abnormal ClickHouse Process.....1343
1.3.414 ALM-45445 Failed to Send Data Files to Remote Shards When ClickHouse Writes Data to a Distributed Table.....1346
1.3.415 ALM-45446 Mutation Task of ClickHouse Is Not Complete for a Long Time.....1349
1.3.416 ALM-45447 ClickHouse Table Read-Only.....1352
1.3.417 ALM-45448 Rapid Increase of Znodes Used by ClickHouse.....1355
1.3.418 ALM-45449 The Counter Number of zxid Used by ClickHouse Exceeds the Threshold.....1358
1.3.419 ALM-45450 ClickHouse Failed to Obtain a Temporary Agency Credential.....1360
1.3.420 ALM-45451 ClickHouse Failed to Access OBS.....1362
1.3.421 ALM-45452 ClickHouse's Local Disk Space Is Below the Cold-Hot Separation Threshold.....1365
1.3.422 ALM-45585 IoTDB Service Unavailable.....1367
1.3.423 ALM-45586 IoTDBServer Heap Memory Usage Exceeds the Threshold.....1370
1.3.424 ALM-45587 IoTDBServer GC Duration Exceeds the Threshold.....1373
1.3.425 ALM-45588 IoTDBServer Direct Memory Usage Exceeds the Threshold.....1375
1.3.426 ALM-45589 ConfigNode Heap Memory Usage Exceeds the Threshold.....1378
1.3.427 ALM-45590 ConfigNode GC Duration Exceeds the Threshold.....1381
1.3.428 ALM-45591 ConfigNode Direct Memory Usage Exceeds the Threshold.....1384
1.3.429 ALM-45592 IoTDBServer RPC Execution Duration Exceeds the Threshold.....1387
1.3.430 ALM-45593 IoTDBServer Flush Execution Duration Exceeds the Threshold.....1390
1.3.431 ALM-45594 IoTDBServer Intra-Space Merge Duration Exceeds the Threshold.....1392
1.3.432 ALM-45595 IoTDBServer Cross-Space Merge Duration Exceeds the Threshold.....1394
1.3.433 ALM-45596 Procedure Execution Failed.....1396
1.3.434 ALM-45615 CDL Service Unavailable.....1398
1.3.435 ALM-45616 CDL Job Execution Exception.....1401
1.3.436 ALM-45617 Data Queued in the CDL Replication Slot Exceeds the Threshold.....1404
1.3.437 ALM-45635 FlinkServer Job Execution Failure.....1406
1.3.438 ALM-45636 Number of Consecutive Checkpoint Failures of a Flink Job Exceeds the Threshold 1409
1.3.439 ALM-45637 Continuous Back Pressure Time of a Flink Job Exceeds the Threshold.....1412
1.3.440 ALM-45638 Number of Restarts After Flink Job Failures Exceeds the Threshold.....1416
1.3.441 ALM-45639 Checkpointing of a Flink Job Times Out.....1419
1.3.442 ALM-45640 FlinkServer Heartbeat Interruption Between the Active and Standby Nodes.....1422
1.3.443 ALM-45641 Data Synchronization Exception Between the Active and Standby FlinkServer Nodes.....1425

1.3.444 ALM-45642 RocksDB Continuously Triggers Write Traffic Limiting.....1429
1.3.445 ALM-45643 MemTable Size of RocksDB Continuously Exceeds the Threshold.....1434
1.3.446 ALM-45644 Number of SST Files at Level 0 of RocksDB Continuously Exceeds the Threshold...1438
1.3.447 ALM-45645 Pending Flush Size of RocksDB Continuously Exceeds the Threshold.....1442
1.3.448 ALM-45646 Pending Compaction Size of RocksDB Continuously Exceeds the Threshold.....1446
1.3.449 ALM-45647 Estimated Pending Compaction Size of RocksDB Continuously Exceeds the Threshold 1450
1.3.450 ALM-45648 RocksDB Frequently Encounters Write-Stopped.....1454
1.3.451 ALM-45649 P95 Latency of RocksDB Get Requests Continuously Exceeds the Threshold.....1458
1.3.452 ALM-45650 P95 Latency of RocksDB Write Requests Continuously Exceeds the Threshold.....1463
1.3.453 ALM-45652 Flink Service Unavailable.....1467
1.3.454 ALM-45653 Invalid Flink HA Certificate File.....1470
1.3.455 ALM-45654 Flink HA Certificate Is About to Expire.....1473
1.3.456 ALM-45655 Flink HA Certificate File Has Expired.....1475
1.3.457 ALM-45736 Guardian Service Unavailable.....1478
1.3.458 ALM-45737 Guardian TokenServer Heap Memory Usage Exceeds the Threshold.....1481
1.3.459 ALM-45738 Guardian TokenServer Direct Memory Usage Exceeds the Threshold.....1483
1.3.460 ALM-45739 Guardian TokenServer Non-Heap Memory Usage Exceeds the Threshold.....1486
1.3.461 ALM-45740 Guardian TokenServer GC Duration Exceeds the Threshold.....1489
1.3.462 ALM-45741 Guardian Failed to Call the ECS securitykey API.....1492
1.3.463 ALM-45742 Guardian Failed to Call the ECS Metadata API.....1494
1.3.464 ALM-45743 Guardian Failed to Call the IAM API.....1496
1.3.465 ALM-46001 MOTService Unavailable.....1497
1.3.466 ALM-46003 MOTService Heartbeat Interruption Between the Active and Standby Nodes.....1501
1.3.467 ALM-46004 Data Inconsistency Between Active and Standby MOTService Nodes.....1503
1.3.468 ALM-46005 MOTService Database Connection Usage Exceeds the Threshold.....1507
1.3.469 ALM-46006 Disk Space Usage of the MOTService Data Directory Exceeds the Threshold.....1510
1.3.470 ALM-46007 MOTService Database Enters the Read-Only Mode.....1513
1.3.471 ALM-46008 MOTService Memory Usage Exceeds the Threshold.....1516
1.3.472 ALM-46009 MOTService CPU Usage Exceeds the Threshold.....1519
1.3.473 ALM-46010 MOTService Certificate File Is About to Expire.....1521
1.3.474 ALM-46011 MOTService Certificate File Has Expired.....1525
1.3.475 ALM-46012 Abnormal Nginx of MOTService.....1529
1.3.476 ALM-47001 MemArtsCC Service Unavailable.....1531
1.3.477 ALM-47002 MemArtsCC Disk Fault.....1533
1.3.478 ALM-50201 Doris Service Unavailable.....1535
1.3.479 ALM-50202 Doris FE CPU Usage Exceeds the Threshold.....1537
1.3.480 ALM-50203 Doris FE Memory Usage Exceeds the Threshold.....1540
1.3.481 ALM-50205 Doris BE CPU Usage Exceeds the Threshold.....1542
1.3.482 ALM-50206 Doris BE Memory Usage Exceeds the Threshold.....1545
1.3.483 ALM-50207 Ratio of Connections to the Doris FE MySQL Port to the Maximum Connections Allowed Exceeds the Threshold.....1547
1.3.484 ALM-50208 Failures to Clear Doris Historical Metadata Images Exceed the Threshold.....1550

1.3.485 ALM-50209 Failures to Generate Doris Metadata Image Files Exceed the Threshold 1552
1.3.486 ALM-50210 Maximum Compaction Score of All Doris BE Nodes Exceeds the Threshold 1554
1.3.487 ALM-50211 Doris FE Queue Length of BE Periodic Report Tasks Exceeds the Threshold 1557
1.3.488 ALM-50212 Accumulated Old-Generation GC Duration of the Doris FE Process Exceeds the Threshold 1560
1.3.489 ALM-50213 Number of Tasks Queuing in the Doris FE Thread Pool for Interacting with BE Exceeds the Threshold 1562
1.3.490 ALM-50214 Number of Tasks Queuing in the Doris FE Thread Pool for Task Processing Exceeds the Threshold 1564
1.3.491 ALM-50215 Longest Duration of RPC Requests Received by Each Doris FE Thrift Method Exceeds the Threshold 1567
1.3.492 ALM-50216 Memory Usage of the Doris FE Node Exceeds the Threshold 1569
1.3.493 ALM-50217 Heap Memory Usage of the Doris FE Node Exceeds the Threshold 1572
1.3.494 ALM-50219 Length of the Queue in the Thread Pool for Doris Query Execution Exceeds the Threshold 1575
1.3.495 ALM-50220 Error Rate of Doris TCP Packet Receiving Exceeds the Threshold 1577
1.3.496 ALM-50221 Doris BE Data Disk Usage Exceeds the Threshold 1579
1.3.497 ALM-50222 Disk Status of a Specified Data Directory on Doris BE Is Abnormal 1581
1.3.498 ALM-50223 Maximum Memory Required by Doris BE Is Greater Than the Remaining Memory of the Machine 1584
1.3.499 ALM-50224 Failures a Certain Task Type on Doris BE Are Increasing 1587
1.3.500 ALM-50225 Unavailable Doris FE Instances 1589
1.3.501 ALM-50226 Unavailable Doris BE Instances 1592
1.3.502 ALM-50227 Concurrent Doris Tenant Queries Exceeds the Threshold 1595
1.3.503 ALM-50228 Memory Usage of a Doris Tenant Exceeds the Threshold 1598
1.3.504 ALM-50229 Doris FE Failed to Connect to OBS 1601
1.3.505 ALM-50230 Doris BE Cannot Connect to OBS 1603
1.3.506 ALM-50401 Number of JobServer Waiting Tasks Exceeds the Threshold 1606
1.3.507 ALM-50402 JobGateway Service Unavailable 1609
1.3.508 ALM-51201 LakeSearch Unavailable 1611
1.3.509 ALM-51202 LakeSearch Heap Memory Usage Exceeds the Threshold 1614
1.3.510 ALM-51203 GC Duration of the LakeSearch Instance Exceeds the Threshold 1617
1.4 Appendix 1620
1.4.1 Logging In to and Out of Service OM 1620
1.4.2 Determining the Active/Standby Status of MRS-DB Nodes 1621
1.4.3 Logging In to an MRS Management Node 1621
2 Troubleshooting 1624
2.1 Troubleshooting Process 1624
2.2 Collecting Information 1626
2.2.1 Statements 1626
2.2.2 Collecting Site Information 1626
2.2.3 Collecting Fault Information 1627
2.2.4 Collecting Log and System Information 1628
2.3 MRS Management and Control Plane Troubleshooting 1631

2.3.1 ServiceDeployer Fault....1631
2.3.2 APIGateway Fault....1632
2.3.3 ManageOne Maintenance Portal Component Alarm Is Not Cleared After a Component Is Deleted from an MRS Cluster....1633
2.3.4 Failed to Create an MRS Cluster....1634
2.4 MRS Tenant Plane Troubleshooting....1638
2.4.1 ClickHouse....1638
2.4.1.1 Error Message "Not enough privileges" Is Displayed When the Client Performs Operations on the ClickHouse Database and Tables....1638
2.4.1.2 Error Message "connect timed out" Is Displayed When the ClickHouse Client Is Being Connected....1640
2.4.1.3 Failed to Start the ClickHouse Service After Changing the Storage Path....1641
2.4.1.4 Failed to Perform Operations as a User That Was Created When the Metadata Disk Was Faulty1643
2.4.2 Containers....1644
2.4.2.1 BLUs Are Successfully Added but Cannot Be Deployed....1644
2.4.2.2 A Message Is Displayed on the SGP Management Page Indicating that the Consumer Contained in a Newly Added BLU Does Not Exist....1645
2.4.2.3 A Message Is Displayed on the SGP Management Page Indicating that the Service Contained in a Newly Added BLU Does Not Exist....1646
2.4.2.4 ZooKeeper Connection Loss Alarm Cannot Be Automatically Cleared After the ZooKeeper SSL Is Modified and the Service Is Restarted....1647
2.4.2.5 RTD Service Is Abnormal After the Cluster Is Powered Off and Restarted....1647
2.4.3 DBService....1648
2.4.3.1 Failed to Configure HA Parameters During the DBService Installation....1648
2.4.3.2 Default Port 20051 Is Occupied....1649
2.4.3.3 Component Depending on DBService Fails to Be Started when the Active and Standby DBService Instances Are Reinstalled....1650
2.4.4 Elasticsearch....1651
2.4.4.1 The group and permission information is normal, but the access to the Elasticsearch service is rejected and permission denied is returned....1651
2.4.4.2 Error Message "max file descriptors [4096] for elasticsearch process is too low, increase to at least [65536]" Is Displayed When an Elasticsearch Instance Fails to Be Started....1652
2.4.4.3 Reindex Operation Fails on Elasticsearch of the Source Version After the MRS Cluster Is Upgraded from 6.5.x to 8.x....1653
2.4.5 Flume....1654
2.4.5.1 Flume Client WCC Encryption Failed and FileNotFound Is Reported....1654
2.4.6 FTP-Server....1655
2.4.6.1 FTP Client Cannot Be Logged In to and Error Message "530 Authentication failed" Is Displayed1655
2.4.6.2 FTP-Server Uploads Data in a Slow Speed....1657
2.4.7 GraphBase....1658
2.4.7.1 Common GraphBase Client Faults....1658
2.4.7.1.1 Error Message "Connection timed out: connect" Is Displayed....1658
2.4.7.1.2 Error Message "Connection refused: connect" Is Displayed....1659
2.4.7.1.3 Data Occasionally Cannot Be Obtained During the Runtime of the Client....1660
2.4.7.1.4 Error Message "cas login fail" Is Displayed....1661

2.4.7.2 Common GraphBase O&M Faults.... 1662
2.4.7.2.1 GraphBase Service Fault Caused by ZooKeeper Faults.... 1662
2.4.7.2.2 GraphBase Service Fault Caused by HBase Faults.... 1663
2.4.7.2.3 GraphBase Index Query Failure Due to Elasticsearch Mode Switching.... 1664
2.4.8 HBase.... 1665
2.4.8.1 Common HBase Client Faults.... 1665
2.4.8.1.1 Client Login Failure.... 1665
2.4.8.1.2 "SASL authentication failed" Displayed on a Client.... 1666
2.4.8.2 Common HBase Operation Faults.... 1666
2.4.8.2.1 hbase:meta Cannot Be Found Because of Network or OS Faults.... 1666
2.4.8.2.2 Active/Standby Switchover of the HMasters Fails.... 1667
2.4.8.2.3 The LoadIncrementalHFiles Tool Failed.... 1668
2.4.8.2.4 No HMaster in the Active State Exists in the Cluster.... 1669
2.4.8.2.5 "OutOfMemoryError: Direct buffer memory" Written in RegionServer Log.... 1670
2.4.8.2.6 Disk Fault Causes Regions to Stay Offline Despite RegionServer Restart.... 1671
2.4.8.2.7 Multiple Regions Are in RIT Status, An Abnormality Occurs in HMaster, and "Packet len6080218 is out of range" Is Displayed in the Log.... 1671
2.4.8.2.8 "Found lingering reference file" Is Displayed in the hbck Command Output.... 1672
2.4.8.2.9 When HBase Is Running the BulkLoad Task, the Error "OutOfMemoryError" Occurs.... 1674
2.4.8.2.10 Replication failed caused by table not found in peer cluster.... 1675
2.4.8.2.11 An Empty Region Is Displayed on the HMaster Web UI and Same Table Fails to Be Created 1677
2.4.8.2.12 Replication Stuck due to CallQueueTooBigException.... 1679
2.4.8.2.13 "Region X on HDFS, but not listed in hbase:meta or deployed on any region server" Is Displayed in the hbck Report.... 1681
2.4.8.2.14 hbck Reports that a Region Is Allocated to Multiple RegionServers.... 1682
2.4.8.2.15 InvalidToken Error Occurs of Network Faults.... 1683
2.4.8.2.16 Rolling Restart Fails When the Balancer Operation of a Service Is Performed.... 1683
2.4.9 HDFS.... 1685
2.4.9.1 Common HDFS Service Faults.... 1685
2.4.9.1.1 HDFS Service Is Always Abnormal.... 1685
2.4.9.1.2 HDFS Block Loss.... 1686
2.4.9.1.3 Failed to Exit the HDFS Safe Mode.... 1687
2.4.9.1.4 Failed to Start HDFS When SafeMode Is On.... 1688
2.4.9.1.5 HDFS Startup Progress Bar Does Not Move.... 1691
2.4.9.1.6 Failed to Add the HDFS Service After Cross-AZ HA Is Enabled for a Cluster.... 1692
2.4.9.2 Common HDFS Client Faults.... 1693
2.4.9.2.1 OutOfMemoryError Exception Occurs on the HDFS Maintenance Client.... 1693
2.4.9.2.2 HDFS Client Cannot Connect to HDFS Cluster.... 1694
2.4.9.3 Common HDFS NameNode Faults.... 1695
2.4.9.3.1 NameNodes Are Always in the Standby State.... 1695
2.4.9.3.2 Failed to Switch Namenode to Active.... 1697
2.4.9.3.3 NameNode Is Always in the Restoring State.... 1699
2.4.9.3.4 HDFS Enters the Safe Mode Due to Resource Exceptions.... 1701

2.4.9.3.5 NameNode Becomes Faulty Because HDFS editlogs Are Damaged....1701
2.4.9.3.6 Client Access to the NameNode Becomes Slow Due to the Shutdown of the Standby NameNode 1704
2.4.9.4 Common HDFS DataNode Faults....1704
2.4.9.4.1 Uneven Distribution of HDFS Data....1704
2.4.9.4.2 DataNode logs InvalidProtocolBufferException....1705
2.4.9.4.3 File Write Operation Failed due to DataNode unavailable for Replication....1706
2.4.10 HetuEngine....1707
2.4.10.1 Message "yarn error with state [FAILED]" Is Displayed on the Client....1707
2.4.10.2 Dynamic Scaling Function of the HetuEngine Compute Instance Does Not Take Effect....1708
2.4.10.3 Residual Yarn Container Process Exists After HetuEngine Is Uninstalled and Reinstalled....1709
2.4.11 Hive....1710
2.4.11.1 "authentication failed" Displayed on a Shell Client....1710
2.4.11.2 "The ZooKeeper client is AuthFailed" Displayed When Client Authentication Failed....1711
2.4.11.3 "Read timed out" Displayed When a Client Fails to Be Connected....1712
2.4.11.4 "Unable to determine if xxx encryptede" Displayed When a Shell Client Accesses a Table....1713
2.4.11.5 Garbled Characters Displayed When the SELECT Statement Is Run for ARC4-encrypted Textfile 1714
2.4.11.6 "File does not exist" Is Displayed in Hive Server Logs....1715
2.4.11.7 Failed to Download a Large Amount of Result Data on the Hue WebUI....1718
2.4.11.8 Hive Table Is Created in a Specified Path....1720
2.4.11.9 No Information Is Displayed When a SQL Statement Fails to Be Run on the Hue WebUI....1722
2.4.11.10 "SemanticException Error while configuring input job properties" Displayed When Operations Are Performed on a Hive_over_HBase Table....1723
2.4.11.11 An Error Is Reported when the rename Operation Is Performed on a Large Partition Table....1724
2.4.11.12 "java.lang.OutOfMemoryError: GC overhead limit exceeded" Is Reported in MapReduce Logs When Partitions Are Inserted Dynamically....1725
2.4.11.13 "Error 10011" Is Displayed on the Client When a UDF Is Used....1727
2.4.11.14 When Permissions Are Granted for a Hive Database on the Interface, a Message Is Displayed Stating "Failed to modify role. Operation failed."....1728
2.4.11.15 Error Message "task timeout set: 600s, taskTimedOut: true; task stuck timeout set: 600s, taskStuck: false" Is Displayed During Hive Task Execution....1729
2.4.11.16 admin User Fails to Submit the Hive on Spark Task in an Insecure Environment....1730
2.4.11.17 "java.lang.IllegalStateException: unread block data" Is Displayed When Running Hive on Spark After Third-Party JAR Files Are Added....1731
2.4.11.18 When HBase Is Not Installed, Hive on Spark Tasks Do Not Respond....1731
2.4.11.19 Query Fails Due to Duplicate Names in the Hive Struct Field....1732
2.4.11.20 Some HBase Classes Fail to Be Loaded When Hive on Spark Executes HBase Data Source....1732
2.4.11.21 An Error Is Reported During LOAD Execution When Hive Interconnects with OBS Using the Wrapper Solution....1733
2.4.11.22 An SQL Error Is Reported When the CBO of Hive Is Disabled....1734
2.4.11.23 Hive on Spark Failed to Insert Data into a Bucketed Table....1735
2.4.11.24 An Error Is Reported When msck repair table table_name Is Run on Hive....1735
2.4.11.25 An Error Message "Invalid ACL: ACL has 33 access entries, which exceeds maximum of 32" Is Displayed When Hive Creates a Table....1736

2.4.11.26 Number of Buckets Is Inconsistent with the Number of Files When a Bucket Table Is Executed on Hive on Spark....1736
2.4.11.27 Connection Timeout During SQL Statement Execution on the Client....1737
2.4.11.28 A UDF Runs Successfully on Hive on MR but Fails on Hive on Tez and Hive on Spark....1738
2.4.12 Hue....1739
2.4.12.1 Hue Page Cannot Be Opened....1739
2.4.12.2 Hue Reports a Document2 Exceeding Error....1740
2.4.12.3 "Proxy Error" Is Displayed When the Hue Page Is Opened....1741
2.4.12.4 Alarm "Hue Service Unavailable" Is Reported and Is Not Cleared for a Long Time....1742
2.4.12.5 Failed to View Job Information in Job Browser....1743
2.4.13 IoTDB....1744
2.4.13.1 Data of a Storage Group Deleted on the IoTDB Client Is Not Deleted from the Data Node....1744
2.4.13.2 ReadOnly Status of the IoTDB Instance Is Triggered and Cannot Be Automatically Restored....1745
2.4.14 Kafka....1747
2.4.14.1 Broker Instance Status Is Restoring After Kafka Node Disk Usage Reaches 100%....1747
2.4.15 KrbServer....1748
2.4.15.1 KrbServer Service Unavailability....1749
2.4.15.2 Running Status of the KrbServer Service Is Unknown....1749
2.4.15.3 An Error Occurred When Changing a Component Password....1750
2.4.15.4 Failed to Update a Ticket....1751
2.4.16 LdapServer....1751
2.4.16.1 System Reports an Alarm Indicating That the LdapServer Service Is Unavailable....1751
2.4.16.2 FusionInsight Manager Is Unavailable Due to LdapServer Data Exception....1752
2.4.16.3 Health Status of the LdapServer Service Is Unknown....1753
2.4.16.4 The OS User Conflicts with the FusionInsight User, Causing a Component Service Authentication Failure....1754
2.4.17 Loader....1756
2.4.17.1 Failed to Obtain a Connection....1756
2.4.17.2 Failed to Import Data by Using HBASE_BULKLOAD....1758
2.4.17.3 Failed to Import or Export Data by Using SFTP....1760
2.4.17.4 Phoenix Table is Empty After Data is Imported....1761
2.4.17.5 Failed to Query Data If the Data Is Imported Before the Hive Table Is Created....1762
2.4.17.6 An Error Occurred When Creating an SFTP Connection....1764
2.4.17.7 Loader Client WCC Encryption Failed and FileNotFound Is Reported....1766
2.4.17.8 Data Is Lost After the Job for Importing Data to HBase Is Successfully Executed....1767
2.4.17.9 Garbled Characters Are Displayed When Loader Reads Rarely-used Oracle Characters....1768
2.4.17.10 sqoop-shell Is Unavailable Due to Encryption and Decryption Errors....1768
2.4.18 Manager....1769
2.4.18.1 Upgrade Faults....1769
2.4.18.1.1 Failed to Upgrade an Manager Due to Abnormal HA-Monitored Resource....1769
2.4.18.1.2 A Message Indicating Upgrade Package Check Error Displayed During Manager Upgrade....1771
2.4.18.1.3 Clearing Redundant Tenant Data....1771
2.4.18.2 Other Faults....1772

2.4.18.2.1 Failed to Install a NameNode Instance.... 1772
2.4.18.2.2 JPA Error Displayed During Instance Adding or Removing.... 1773
2.4.18.2.3 Failed to Start Components Due to Database Connection Failures.... 1774
2.4.18.2.4 Failed to Decommission a DataNode Instance.... 1775
2.4.18.2.5 Failed to Log In to a Native Window.... 1776
2.4.18.2.6 Database User Password Being Forgotten.... 1777
2.4.18.2.7 Abnormality Caused by Component Database User Password Change.... 1778
2.4.18.2.8 Monitoring Indicator Display Error.... 1779
2.4.18.2.9 Failed to Start the GaussDB Due to Inconsistent Logs and Data.... 1781
2.4.18.2.10 Database Connection Error.... 1782
2.4.18.2.11 Slow Manager Page Loading.... 1783
2.4.18.2.12 Incorrect Display on the Manager Portal.... 1784
2.4.18.2.13 Failed to Add a User on the FusionInsight Manager Portal.... 1787
2.4.18.2.14 Failed to Uninstall Manager.... 1788
2.4.18.2.15 Hosts Page of Manager Cannot Monitor Host State Normally.... 1789
2.4.18.2.16 Failed to Change the Password.... 1792
2.4.18.2.17 Kerberos Secondary Authentication Is 20s Slower After the DNS Is Installed.... 1793
2.4.18.2.18 Some Operations on Manager Fail After Standby OMS Power-off.... 1795
2.4.18.2.19 Troubleshooting Dual Active Manager Nodes.... 1796
2.4.18.2.20 Manager Database Is Abnormal Because Directories or Files Are Deleted Incorrectly.... 1798
2.4.18.2.21 Standby Database Is Abnormal Due to Improper Configuration of Transaction Log Parameters in the Manager Database.... 1801
2.4.18.2.22 Trust of User omm Fails Because the expect Process Stops Responding.... 1804
2.4.18.2.23 Installation Package Fails to Be Distributed After OpenSSH Upgrade.... 1805
2.4.18.2.24 Analyzing Failures of the Audit Dump Configuration.... 1806
2.4.18.2.25 Failed to Synchronize Configuration After the IP Address Is Changed.... 1807
2.4.18.2.26 Failed to Add or Reinstall Hosts Because of the Changed HOSTKEY.... 1808
2.4.18.2.27 Authentication of the Peer Domain Users Is Slow After Mutual Trust Is Configured.... 1809
2.4.18.2.28 Some Nodes in the MRS Service Cluster Are Faulty After the MRS Is Powered Off and then Powered On.... 1809
2.4.18.2.29 Login Occasionally Fails After MRS Manager Exits Due to Timeout.... 1810
2.4.18.2.30 Threshold Monitoring Alarms for New Services Are Not Reported.... 1810
2.4.18.2.31 An Error Reported During Client Authentication for a New User.... 1811
2.4.18.2.32 Alarm Faults Are Rectified, but Alarms in the Manager Alarm List Are Not Automatically Cleared.... 1812
2.4.18.2.33 After a Node Is Powered Off and Then Powered On, the OMS Node Cannot Be Automatically Started or an Alarm "Trust Relationships Between Nodes Become Invalid" Is Reported.... 1812
2.4.19 Mapreduce.... 1813
2.4.19.1 JobHistoryServer Node Faults.... 1813
2.4.19.2 HDFS Directory Fails to Be Deleted After the Related Job Is Deleted.... 1814
2.4.19.3 java.io.IOException Error Occurs During Job Execution.... 1815
2.4.19.4 MapReduce Tasks with Large Data Amount Run Slowly.... 1816
2.4.19.5 Map or Reduce Process Being Terminated Due to Memory Overflow.... 1817

2.4.19.6 Many Fetch Failures Occur During Reduce Phase of Running Task....1818
2.4.20 MemArtsCC.... 1819
2.4.20.1 MemArtsCC Reads Data Slowly.... 1820
2.4.20.2 MemArtsCC CCSidecar or CCWorker Process Fault....1820
2.4.21 MOTService.... 1822
2.4.21.1 MOTService Fails to Be Installed During Preinstallation....1822
2.4.21.2 MOTService Fails to Be Installed Due to Service and Instance Startup Failure.... 1823
2.4.21.3 "command not found" Is Displayed If gsql Is Used to Connect to the Database.... 1823
2.4.21.4 An Error Indicating Too Many Client Connections Is Reported When a User Connects to the MOTService Database.... 1824
2.4.21.5 An Error Is Reported During Cluster Connection, Indicating that the Account Is Locked....1825
2.4.21.6 An Error Message Is Reported During Statement Execution, Indicating That the User Does Not Have the Required Permission....1826
2.4.21.7 LOCK_WAIT_TIMEOUT Is Displayed During SQL Execution....1826
2.4.21.8 Database Enters the Read-Only Mode....1828
2.4.22 Redis.... 1828
2.4.22.1 Cluster Instances Are Offline Due to Abnormal Redis Slot Migration.... 1829
2.4.22.2 Master Instances Exist After the Original Master Instance Restarts Due to Abnormal Redis Slot Migration....1830
2.4.22.3 Redis Cluster Becomes Unreliable When a Redis Node or Instance Is Disconnected....1832
2.4.22.4 Redis Cluster Exists in the Newly Added Redis Service....1834
2.4.22.5 Redis Instances Fail to Start After Node Reboot or Fault Recovery....1835
2.4.22.6 Redis Scale-Out Failed But Some Instances Are in the Normal State....1836
2.4.22.7 Error Message "unknown command" Is Displayed When High-Risk Commands Are Executed on the Redis Client.... 1837
2.4.22.8 Frequent Active/Standby Switchover Caused by Insufficient Storage Space of the Redis Buffer1838
2.4.23 RTDService.... 1838
2.4.23.1 RTDService Is Faulty....1839
2.4.23.2 Failed to Add a RTDService Executor BLU....1839
2.4.23.3 Tenant Password Becomes Invalid After DBService Data Is Restored in an Upgrade....1841
2.4.23.4 Model Status Becomes Incorrect Due to a ZooKeeper Fault During Model Creation.... 1841
2.4.23.5 RTDService Becomes Abnormal After It Is Manually Added on the Console.... 1842
2.4.24 Solr.... 1843
2.4.24.1 Solr Client Fails to Write Index in Real Time.... 1843
2.4.24.2 Some cores still running improperly after Overseer is optimized and restarted....1845
2.4.25 Spark....1846
2.4.25.1 Spark Core.... 1846
2.4.25.1.1 Error Message "java.lang.UnsatisfiedLinkError: org.apache.hadoop.util.NativeCodeLoader.buildSupportsSnappy()Z" Is Displayed When the Snappy Compression Algorithm Is Used.... 1846
2.4.25.1.2 Error Message " Not attempting to re-login since the last re-login was attempted less than 600 seconds before" Is Displayed....1847
2.4.25.1.3 Task Is Suspended and "Initial job has not accepted any resources" Error Occurs....1848
2.4.25.1.4 "Address already in use: Service 'SparkUI' failed after 16 retries!" Error Occurs.... 1849

2.4.25.1.5 Task Cannot Be Supported on YARN.....1851
2.4.25.1.6 Failed to Exit the Application Program Due to Insufficient Memory.....1851
2.4.25.1.7 Failed to Run an Application Because of Insufficient Disk Space.....1853
2.4.25.1.8 Out-of-Memory Is Displayed When A Huge Amount of Data Is Returned to the Driver.....1854
2.4.25.1.9 An Application Fails Upon Startup Because Many Executors Are Lost.....1856
2.4.25.1.10 Errors Occur When an Ultra-Large Result Set Is Being Collected to Driver.....1857
2.4.25.1.11 Executor Log Shows that the Physical Memory Usage Exceeds the Maximal Value.....1859
2.4.25.1.12 When the Big data Is Processed, the Error "Channel idle timeout" Occurs.....1861
2.4.25.1.13 Spark Job Fails and Physical Memory Overflow of ApplicationMaster.....1862
2.4.25.1.14 "BlockNotFoundException" Error Occurs and the Stage Retries During the Running of Jobs1862
2.4.25.1.15 JobHistory Restarts Frequently.....1863
2.4.25.1.16 During Shuffle Process, the Broken Pipe Exception or Timeout Causing Application Failure1864
2.4.25.2 Spark SQL and DataFrame.....1865
2.4.25.2.1 Failed to Delete HDFS Data by Running Delete or Drop Command in the Spark SQL.....1865
2.4.25.2.2 The select Command Returns "File Does not Exist" If the location Directory Specified During Partition Creation Is Deleted.....1866
2.4.25.2.3 "Unable to acquire" Exception.....1867
2.4.25.2.4 The joinedRow.isNullAt Exception Occurs When Spark SQL Is Executed.....1870
2.4.25.3 Spark Streaming.....1871
2.4.25.3.1 Out of Memory Error Occurs While Spark Streaming Application Is Running.....1872
2.4.25.4 Incorrect GLIBC Version.....1873
2.4.25.5 Failed to Execute Spark Tasks After the YARN Active/Standby Switchover.....1873
2.4.25.6 "No space left on device" Is Displayed Constantly During the Running of Spark Tasks.....1875
2.4.25.7 Spark yarn-client Task Failure When the Client Is Deployed Outside the Cluster.....1876
2.4.26 Yarn.....1876
2.4.26.1 Link on the ResourceManager Native Page Is Unavailable.....1876
2.4.26.2 ResourceManager Node Faults.....1877
2.4.26.3 NodeManager Node Faults.....1878
2.4.26.4 NodeManager Unable to Start with DBException.....1879
2.4.26.5 Spark Task Failure Caused by OutOfMemoryError on NodeManager.....1880
2.4.26.6 Tenant Functions Become Abnormal When the Yarn Service Is Set to the Superior Scheduler Mode During Installation.....1882
2.4.26.7 A Job Fails to Be Submitted Because the Launcher-job Queue Fails to Be Created During Cluster Provisioning.....1883
2.4.27 ZooKeeper.....1885
2.4.27.1 ZooKeeper Instance Always in Restoring Status.....1885
2.4.27.2 Unavailable ZooKeeper Service.....1886
2.4.27.3 ZooKeeper Client Session is Closed.....1887
2.4.27.4 Failed to Restore a ZooKeeper File That Was Deleted by Mistake.....1888
2.4.27.5 ZooKeeper Service Abnormal After DNS Installation.....1888
2.4.27.6 Emergency Restoration Upon a Service Exception Caused by Metadata Abnormalities (older than the last zxid).....1890
2.4.28 OS.....1891

2.4.28.1 The Operating System Command Execution is Slow in SUSE 12.x.....1891
2.4.28.2 systemd Restarting Services Causes Other Associated Services to Restart in SUSE 12.2.....1892
2.5 Appendix.....1893
2.5.1 Logging In to Service OM.....1893
2.5.2 Logging In to an MRS Management Node.....1894

1 Alarm Handling

1.1 Overview

An alarm alerts users that a fault has been detected. Information about the fault is contained in the alarm. Alarm monitoring enables O&M personnel to monitor and manage the alarms and events reported by the system or managed objects (MOs). It provides various alarm monitoring and handling rules and notifies O&M personnel of faults. This facilitates efficient alarm monitoring and quick fault locating, ensuring smooth service running.

The alarm severity indicates the severity, importance, and urgency of a fault. It allows O&M personnel to quickly identify the importance of an alarm, take corresponding handling measures, and change the severity of an alarm as required.

Severity	Description	Recommended Handling Strategy
Critical	Services are affected, and measures must be taken immediately.	Handle the alarm immediately. Otherwise, services may be interrupted, or the system may break down.
Major	Services are affected. If the alarm is not handled timely, there may be serious consequences.	Handle the alarm timely. Otherwise, important services will be affected.
Minor	This alarm has minor impacts on services, but you need to take corrective measures to avoid more serious faults.	Find out the cause of the alarm and rectify the fault.
Warning	The fault is not currently affecting services but may cause impacts on services later.	Learn the running status of the network and NEs based on the alarm and handle the alarm based on the actual situation.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarms that can be reported include alarms of modules on the MRS management plane and alarms of hosts and components in the MRS cluster at the tenant side. O&M personnel can view and handle all alarms on ManageOne Maintenance Portal.

Tenants can also view alarms generated in the cluster on the MRS management console or FusionInsight Manager of the MRS cluster.

1.2 Alarms of the MRS Management and Control Plane

1.2.1 PAAS_MRS_00101 Failed to Create a Cluster

Alarm Description

This alarm is generated when a cluster creation request is successfully delivered but the cluster fails to be created.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
PAAS_MRS_00101	Major	Operation	Management plane	MapReduce Service	No

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the abnormal cluster.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	ClusterName	Specifies the name of the abnormal cluster.
	ErrorMessage	Specifies the error message for the alarm.

Impact on the System

Clusters created after this alarm is generated are unavailable.

Possible Causes

The network is abnormal, the quota is insufficient, the ECS resources are insufficient, or the ECS initialization fails.

Handling Procedure

Step 1 Use a browser to log in to ManageOne Operation Portal as the VDC administrator who created the cluster.

Step 2 In the navigation pane on the upper left of the page, click ☰.

Step 3 On the **Service List** page, select a region and choose **MapReduce Service** under **EI Enterprise Intelligence**. The MRS console is displayed.

Step 4 Choose **Active Clusters**.

Step 5 Click **Failed Tasks** and view the task status of the cluster that fails to be created to locate the failure cause.

Step 6 Collect alarms, logs, configurations, and user operation logs, and contact technical support.

1. Log in to the ManageOne alarm platform to obtain the alarm information.
   a. Log in to the ManageOne Maintenance Portal and choose **Alarm Management** > **Alarms** > **Current Alarms** in the navigation pane on the top.
   b. Click **Filter** in the upper left corner and click **Location Info**. The **Location Info** dialog box is displayed.
   c. Set **Operator** to **contains** and **Value** to **CloudService=MRS**, and click **OK**. Click **OK** again to filter MRS alarms.
   d. Obtain **Location Info**, **Possible Causes**, and **Other Information**.
2. Collect system logs of the management plane. For details, see "Log Reference" > "Log Reference on the Management Plane" > "Log Collection" in ***MapReduce Service (MRS) 3.3.1-LTS Reference Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Maintenance Guide (for Huawei Cloud Stack 8.3.1)***.

3. Contact technical support engineers and provide alarm and log information for troubleshooting.

----End

Alarm Clearance

After the fault is rectified, the system does not automatically clear this alarm and you need to manually clear it.

Related Information

None

1.2.2 PAAS_MRS_00102 Failed to Delete a Cluster

Alarm Description

This alarm is generated when a cluster deletion request is successfully delivered but the cluster fails to be deleted.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
PAAS_MRS_00102	Minor	Operation	Tenant plane	MapReduce Service	No

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the abnormal cluster.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	UserName	Specifies the user for which the alarm was generated.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	ClusterName	Specifies the name of the abnormal cluster.
	ErrorMessage	Specifies the error message for the alarm.

Impact on the System

Residual resources may exist.

Possible Causes

The network or ECS is abnormal.

Handling Procedure

Step 1 Use a browser to log in to ManageOne Operation Portal as the VDC administrator who created the cluster.

Step 2 In the navigation pane on the upper left of the page, click ☰.

Step 3 On the **Service List** page, select a region and choose **MapReduce Service** under **EI Enterprise Intelligence**. The MRS console is displayed.

Step 4 Choose **Active Clusters**.

Step 5 Click **Failed Tasks** and view the task status of the cluster that fails to be deleted to locate the failure cause.

Step 6 Collect alarms, logs, configurations, and user operation logs, and contact technical support.

1. Log in to the ManageOne alarm platform to obtain the alarm information.
   a. Log in to the ManageOne Maintenance Portal and choose **Alarm Management** > **Alarms** > **Current Alarms** in the navigation pane on the top.
   b. Click **Filter** in the upper left corner and click **Location Info**. The **Location Info** dialog box is displayed.
   c. Set **Operator** to **contains** and **Value** to **CloudService=MRS**, and click **OK**. Click **OK** again to filter MRS alarms.
   d. Obtain **Location Info**, **Possible Causes**, and **Other Information**.
2. Collect system logs of the management plane. For details, see "Log Reference" > "Log Reference on the Management Plane" > "Log Collection" in ***MapReduce Service (MRS) 3.3.1-LTS Reference Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Maintenance Guide (for Huawei Cloud Stack 8.3.1)***.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

3. Contact technical support engineers and provide alarm and log information for troubleshooting.

----End

Alarm Clearance

After the fault is rectified, the system does not automatically clear this alarm and you need to manually clear it.

Related Information

None

1.2.3 PAAS_MRS_00103 Failed to Scale Out a Cluster

Alarm Description

This alarm is generated when a cluster scale-out request is successfully delivered but the scale-out fails.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
PAAS_MRS_00103	Major	Operation	Tenant plane	MapReduce Service	No

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the abnormal cluster.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	UserName	Specifies the user for which the alarm was generated.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	ClusterName	Specifies the name of the abnormal cluster.
	ErrorMessage	Specifies the error message for the alarm.

Impact on the System

The cluster fails to be scaled out, and the cluster load cannot decrease.

Possible Causes

The network is abnormal, the quota is insufficient, the ECS resources are insufficient, the ECS initialization fails, or the Executor or Controller process is restarted or abnormal.

Handling Procedure

Step 1 Use a browser to log in to ManageOne Operation Portal as the VDC administrator who created the cluster.

Step 2 In the navigation pane on the upper left of the page, click ☰.

Step 3 On the **Service List** page, select a region and choose **MapReduce Service** under **EI Enterprise Intelligence**. The MRS console is displayed.

Step 4 Choose **Active Clusters**.

Step 5 Click the cluster for which the alarm is generated. The cluster management page is displayed.

Step 6 View failed tasks of the cluster and check the status of the failed scale-out task to locate the failure cause.

Step 7 Collect alarms, logs, configurations, and user operation logs, and contact technical support.

1. Log in to the ManageOne alarm platform to obtain the alarm information.
   a. Log in to the ManageOne Maintenance Portal and choose **Alarm Management** > **Alarms** > **Current Alarms** in the navigation pane on the top.
   b. Click **Filter** in the upper left corner and click **Location Info**. The **Location Info** dialog box is displayed.
   c. Set **Operator** to **contains** and **Value** to **CloudService=MRS**, and click **OK**. Click **OK** again to filter MRS alarms.
   d. Obtain **Location Info**, **Possible Causes**, and **Other Information**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

2. Collect system logs of the management plane. For details, see "Log Reference" > "Log Reference on the Management Plane" > "Log Collection" in ***MapReduce Service (MRS) 3.3.1-LTS Reference Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Maintenance Guide (for Huawei Cloud Stack 8.3.1)***.
3. Contact technical support engineers and provide alarm and log information for troubleshooting.

----End

Alarm Clearance

After the fault is rectified, the system does not automatically clear this alarm and you need to manually clear it.

Related Information

None

1.2.4 PAAS_MRS_00105 Failed to Scale In a Cluster

Alarm Description

This alarm is generated when a cluster scale-in request is successfully delivered but the scale-in fails.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
PAAS_MRS_00105	Major	Operation	Tenant plane	MapReduce Service	No

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ClusterId	Specifies the ID of the abnormal cluster.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	ClusterName	Specifies the name of the abnormal cluster.
	ErrorMessage	Specifies the error message for the alarm.

Impact on the System

Cluster resources are not released as expected, and the node that fails to be reduced may be abnormal.

Possible Causes

The Executor or Controller process is restarted or abnormal, or the NodeAgent is restarted.

Handling Procedure

Step 1 Use a browser to log in to ManageOne Operation Portal as the VDC administrator who created the cluster.

Step 2 In the navigation pane on the upper left of the page, click ☰.

Step 3 On the **Service List** page, select a region and choose **MapReduce Service** under **EI Enterprise Intelligence**. The MRS console is displayed.

Step 4 Choose **Active Clusters**.

Step 5 Click the cluster for which the alarm is generated. The cluster management page is displayed.

Step 6 View failed tasks of the cluster and check the status of the failed scale-in task to locate the failure cause.

Step 7 Collect alarms, logs, configurations, and user operation logs, and contact technical support.

1. Log in to the ManageOne alarm platform to obtain the alarm information.
   a. Log in to the ManageOne Maintenance Portal and choose **Alarm Management** > **Alarms** > **Current Alarms** in the navigation pane on the top.
   b. Click **Filter** in the upper left corner and click **Location Info**. The **Location Info** dialog box is displayed.

c. Set **Operator** to **contains** and **Value** to **CloudService=MRS**, and click **OK**. Click **OK** again to filter MRS alarms.

d. Obtain **Location Info**, **Possible Causes**, and **Other Information**.

2. Collect system logs of the management plane. For details, see "Log Reference" > "Log Reference on the Management Plane" > "Log Collection" in ***MapReduce Service (MRS) 3.3.1-LTS Reference Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Maintenance Guide (for Huawei Cloud Stack 8.3.1)***.

3. Contact technical support engineers and provide alarm and log information for troubleshooting.

----End

Alarm Clearance

After the fault is rectified, the system does not automatically clear this alarm and you need to manually clear it.

Related Information

None

1.2.5 PAAS_MRS_00124 Cluster Exception

Alarm Description

This alarm is generated when the communication between the Deployer node on the management plane and the active/standby Manager node is abnormal for more than 5 minutes or when the status returned by the cluster status query interface of Manager is **BAD**.

This alarm is cleared when the communication becomes normal.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
PAAS_MRS_00124	Major	Heartbeat	Tenant plane	MapReduce Service	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.

Type	Parameter	Description
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the abnormal cluster.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	ClusterName	Specifies the name of the abnormal cluster.
	ErrorMessage	Specifies the error message for the alarm.

Impact on the System

The cluster display is abnormal, and operations related to the cluster fail.

Possible Causes

The network or ECS is abnormal, or the memory of the active and standby Master nodes in the cluster is used up, causing the Executor service is abnormal.

Handling Procedure

Step 1 Use a browser to log in to ManageOne Operation Portal as the VDC administrator who created the cluster.

Step 2 In the navigation pane on the upper left of the page, click ☰.

Step 3 On the **Service List** page, select a region and choose **MapReduce Service** under **EI Enterprise Intelligence**. The MRS console is displayed.

Step 4 Choose **Active Clusters**.

Step 5 View the cluster whose status is **Abnormal** and copy the cluster ID displayed below the cluster name in the **Name/ID** column.

Step 6 In the navigation pane, click ☰ on the left. Select **Service List** and choose **Computing** > **Elastic Cloud Server**.

Step 7 On the ECS page, enter the cluster ID copied in **Step 5** into the search box and click the search icon.

Step 8 View the search result in the list and check the **Status** column of the ECSs whose name contains **master1** and **master2** in the **Name** column.

- If the status is **Running**, go to **Step 9**.
- Otherwise, go to **Step 12**.

Step 9 Click **Remote Login** corresponding to the names containing **master1** and **master2** and log in as user **omm**.

Step 10 Run the following command to query the Executor service is running properly:

ps -ef | grep executor

If the service runs properly, the following command output is displayed:

```
omm       3441     1 67 19:23 ?        00:00:54 /opt/Bigdata/common/runtime0/jdk-8u201//bin/java -Dnop -
Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager -Xms256m -Xmx768m -
Djdk.tls.ephemeralDHKeySize=2048 -Dorg.apache.catalina.security.SecurityListener.UMASK=0027 -
Djava.security.krb5.conf=/opt/hadoopclient/KrbClient/kerberos/var/krb5kdc/krb5.conf -
Dorg.apache.catalina.connector.RECYCLE_FACADES=true -Dignore.endorsed.dirs= -classpath :/opt/
hadoopclient/Spark/spark/conf/:/opt/executor/bin/bootstrap.jar:/opt/executor/bin/tomcat-juli.jar -
Dcatalina.base=/opt/executor -Dcatalina.home=/opt/executor -Djava.io.tmpdir=/opt/executor/temp
org.apache.catalina.startup.Bootstrap start
```

- If the server is running properly, run the **free -m** command to check whether the free memory in the **Mem** and **free** rows is insufficient.
  - If yes, release the memory. Wait for a while and check whether the alarm is cleared. If the alarm is cleared, no further action is required. If not, go to **Step 12**.
  - If no, go to **Step 12**.
- If the service is abnormal, perform the following steps:
  a. Run the following command to identify the active and standby nodes on Master1 and Master2:

     sh ${BIGDATA_HOME}/om-server/om/sbin/status-oms.sh

     In the command output, the value of **HAActive** for the active management node is **active**, and that for the standby management node is **standby**. In the following example, Master1 is the active management node, and Master2 is the standby management node.

```
HAMode
double
NodeName            HostName      HAVersion        StartTime              HAActive
HAAllResOK          HARunPhase
192-168-0-30        Master1       V100R001C01      2019-05-01 23:43:02    active
normal              Actived
192-168-0-24        Master2       V100R001C01      2019-05-01 07:14:02
standby             normal        Deactived
```

  b. On the active management node, run the **sh /opt/executor/bin/startup.sh** command as user **omm** to start the Executor service.
  c. Run the **ps -ef | grep executor** command to check whether the Executor process exists.
  d. After the Executor process is restarted, check the cluster status on the cluster list page.
     - If the cluster is running, no further action is required.
     - If the cluster is not in running status, go to **Step 11**.

Step 11 Check whether the network between the management plane and the tenant plane is connected.

1. Log in to any EICommon-Region-Master VM whose status is running as user **opsadmin**. For details, see **Logging In to an MRS Management Node**.

   Run the **su - root** command to switch to user **root**.

   Obtain the default password by referring to ***Huawei Cloud Stack 8.3.1 Account List*** or contacting the cluster administrator.

   NOTE

   If **Status** of all VMs is not **Running**, contact the cluster administrator.

2. Run the following command to view the running container information of the host machine:

   kubectl get pod -n mrs -owide

```
NAME                          READY   STATUS    RESTARTS   AGE   IP           NODE           NOMINATED
NODE   READINESS GATES
mrsapigw-777fc766b9-8dwc9      1/1     Running   0          14h   10.16.0.231    10.35.152.220
<none>           <none>
mrsapigw-777fc766b9-8pgrb      1/1     Running   0          14h   10.16.0.153    10.35.152.219
<none>           <none>
mrsdeployer-7b5dff56cc-bxzgc   1/1     Running   0          14h   10.16.0.172    10.35.152.218
<none>           <none>
mrsdeployer-7b5dff56cc-gtvvw   1/1     Running   0          14h   10.16.0.230    10.35.152.220
<none>           <none>
mrsdeployer-7b5dff56cc-vxkjf   1/1     Running   0          14h   10.16.0.154    10.35.152.219
<none>           <none>
```

3. Copy the NAME values of the three data records whose NAME contains **mrsdeployer** in the data queried in **Step 11.2**.

   Perform **Step 11.4** to **Step 11.5** using the three NAME values obtained.

4. Run the following command to access the container (replace **NAME** values with the obtained values in **Step 11.2**):

   kubectl exec -ti -n mrs *NAME value* **bash**

5. Run the following command to query the network connectivity between the management plane and the tenant plane. If 404 is returned, the network connectivity is normal. If "Connection refused" is returned or no result is returned for a long time, contact the cluster administrator to check whether the port matrix is enabled and whether the configuration is correct.

   curl -ik https://*IP addresses of the active and standby nodes in the cluster* **:9022**

   Example: **curl -ik https://10.20.30.40:9022** or **curl -ik https://10.20.30.41:9022**

NOTE

Obtain the IP addresses of the active and standby nodes on the tenant plane:

1. Log in to any MRS_DB VM as the **opsadmin** user. For details, see **Logging In to an MRS Management Node**.

   Run the **su - root** command to switch to user **root**.

   Obtain the default password by referring to ***Huawei Cloud Stack 8.3.1 Account List*** or contacting the cluster administrator.

2. Run the following commands to log in to the MySQL client and obtain the IP address:

   mysql -P7306 -h*Floating IP address of the MRS database* **-udatasightemr -p***Default password of datasightemr*

   use datasightemr;

   select external_ip,external_alternate_ip from cluster_detail where cluster_id='*ID of the cluster for which the alarm is generated***';**

   You can obtain the floating IP address of the MRS database from the LLD during cloud service installation and deployment.

   Contact O&M personnel to obtain the default password of database user **datasightemr**.

Step 12 Collect alarms, logs, configurations, and user operation logs, and contact technical support.

1. Log in to the ManageOne alarm platform to obtain the alarm information.
   a. Log in to the ManageOne Maintenance Portal and choose **Alarm Management** > **Alarms** > **Current Alarms** in the navigation pane on the top.
   b. Click **Filter** in the upper left corner and click **Location Info**. The **Location Info** dialog box is displayed.
   c. Set **Operator** to **contains** and **Value** to **CloudService=MRS**, and click **OK**. Click **OK** again to filter MRS alarms.
   d. Obtain **Location Info**, **Possible Causes**, and **Other Information**.
2. Collect system logs of the management plane. For details, see "Log Reference" > "Log Reference on the Management Plane" > "Log Collection" in ***MapReduce Service (MRS) 3.3.1-LTS Reference Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Maintenance Guide (for Huawei Cloud Stack 8.3.1)***.
3. Contact technical support engineers and provide alarm and log information for troubleshooting.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.2.6 PAAS_MRS_00135 Heartbeat Task Failed

Alarm Description

This alarm is generated when the heartbeat communication task between the Deployer service on the management plane and the active/standby node of the cluster fails.

This alarm is cleared when the heartbeat communication between Deployer and the cluster is successful.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
PAAS_MRS_00135	Major	Heartbeat	Management plane	MapReduce Service	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

Clusters are displayed abnormally and cluster operations cannot be performed.

Possible Causes

The heartbeat task is blocked.

Handling Procedure

Step 1 Log in to any EICommon-Region-Master VM whose status is running as user **opsadmin**. For details, see **Logging In to an MRS Management Node**.

Run the **su - root** command to switch to user **root**.

Obtain the default password by referring to ***Huawei Cloud Stack 8.3.1 Account List*** or contacting the cluster administrator.

NOTE

If **Status** of all VMs is not **Running**, contact the cluster administrator.

Step 2 Run the following command to view the running container information of the host machine:

kubectl get pod -n mrs -owide

Step 3 Copy the NAME values of the two data records whose NAME contains **mrsapigw** in the data queried in **Step 2**.

Perform **Step 4** to **Step 5** using the two NAME values obtained.

Step 4 Run the following command to access the container (replace *NAME* values with the obtained values in **Step 3**):

kubectl exec -ti -n mrs *NAME value* **bash**

Step 5 Go to the **/opt/cloud/logs/apigateway/** directory and view the **api-gateway.log** file.

- If **Failed to scheduler heartbeat job** is displayed, go to **Step 6**.
- If the message "LastHBJob updated at" is displayed, wait until all the clusters on the cluster page of ManageOne Operation Portal change to the non-operation state, and then check whether the alarm is automatically cleared.
  - If yes, no further action is required.
  - If no, go to **Step 6**.

Step 6 Collect alarms, logs, configurations, and user operation logs, and contact technical support.

1. Log in to the ManageOne alarm platform to obtain the alarm information.
   a. Log in to the ManageOne Maintenance Portal and choose **Alarm Management** > **Alarms** > **Current Alarms** in the navigation pane on the top.
   b. Click **Filter** in the upper left corner and click **Location Info**. The **Location Info** dialog box is displayed.
   c. Set **Operator** to **contains** and **Value** to **CloudService=MRS**, and click **OK**. Click **OK** again to filter MRS alarms.
   d. Obtain **Location Info**, **Possible Causes**, and **Other Information**.
2. Collect system logs of the management plane. For details, see "Log Reference" > "Log Reference on the Management Plane" > "Log Collection" in ***MapReduce Service (MRS) 3.3.1-LTS Reference Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Maintenance Guide (for Huawei Cloud Stack 8.3.1)***.
3. Contact technical support engineers and provide alarm and log information for troubleshooting.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.2.7 PAAS_MRS_00308 Too Many Auto Scaling Threads

Alarm Description

This alarm is generated when the number of active threads on the Deployer node where the auto scaling scheduled task of the MRS management plane is located is equal to the number of core threads and the number of core threads exceeds 5.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
PAAS_MRS_00308	Critical	Operation	Management plane	MapReduce Service	No

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	ThresholdValue	Specifies the available threshold of a control item.
	CurrentValue	Specifies the current usage of a control item.

Impact on the System

The processing time for submitting an auto scaling task may exceed 15s, which may cause system exceptions.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Possible Causes

There are many clusters with auto scaling enabled at the current site, and a large number of auto scaling tasks are triggered at the same time.

Handling Procedure

Step 1 Collect alarms, logs, configurations, and user operation logs, and contact technical support.

1. Log in to the ManageOne alarm platform to obtain the alarm information.
   a. Log in to the ManageOne Maintenance Portal and choose **Alarm Management** > **Alarms** > **Current Alarms** in the navigation pane on the top.
   b. Click **Filter** in the upper left corner and click **Location Info**. The **Location Info** dialog box is displayed.
   c. Set **Operator** to **contains** and **Value** to **CloudService=MRS**, and click **OK**. Click **OK** again to filter MRS alarms.
   d. Obtain **Location Info**, **Possible Causes**, and **Other Information**.
2. Collect system logs of the management plane. For details, see "Log Reference" > "Log Reference on the Management Plane" > "Log Collection" in ***MapReduce Service (MRS) 3.3.1-LTS Reference Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Maintenance Guide (for Huawei Cloud Stack 8.3.1)***.
3. Contact technical support engineers and provide alarm and log information for troubleshooting.

----End

Alarm Clearance

After the fault is rectified, the system does not automatically clear this alarm and you need to manually clear it.

Related Information

None

1.2.8 PAAS_MRS_00309 Too Many Waiting Auto Scaling Tasks

Alarm Description

This alarm is generated when more than 300 tasks are waiting on the Deployer node where the auto scaling scheduled task of the MRS management plane is located.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
PAAS_MRS_00309	Critical	Operation	Management plane	MapReduce Service	No

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	ThresholdValue	Specifies the available threshold of a control item.
	CurrentValue	Specifies the current usage of a control item.

Impact on the System

A large number of auto scaling tasks cannot be processed and auto scaling cannot be performed in a timely manner, which may cause system exceptions.

Possible Causes

If the CPU processing performance is insufficient or there are too many auto scaling clusters, a large number of auto scaling tasks cannot be processed within a short period of time. As a result, more and more auto scaling tasks are waiting in the queue.

Handling Procedure

Step 1 Collect alarms, logs, configurations, and user operation logs, and contact technical support.

1. Log in to the ManageOne alarm platform to obtain the alarm information.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

a. Log in to the ManageOne Maintenance Portal and choose **Alarm Management** > **Alarms** > **Current Alarms** in the navigation pane on the top.
b. Click **Filter** in the upper left corner and click **Location Info**. The **Location Info** dialog box is displayed.
c. Set **Operator** to **contains** and **Value** to **CloudService=MRS**, and click **OK**. Click **OK** again to filter MRS alarms.
d. Obtain **Location Info**, **Possible Causes**, and **Other Information**.

2. Collect system logs of the management plane. For details, see "Log Reference" > "Log Reference on the Management Plane" > "Log Collection" in ***MapReduce Service (MRS) 3.3.1-LTS Reference Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Maintenance Guide (for Huawei Cloud Stack 8.3.1)***.
3. Contact technical support engineers and provide alarm and log information for troubleshooting.

----End

Alarm Clearance

After the fault is rectified, the system does not automatically clear this alarm and you need to manually clear it.

Related Information

None

1.2.9 PAAS_MRS_00310 Auto Scale-Out Failed

Alarm Description

This alarm is generated when cluster auto scale-out is successfully triggered but the scale-out fails.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
PAAS_MRS_00310	Critical	Operation	Tenant plane	MapReduce Service	No

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.

Type	Parameter	Description
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the abnormal cluster.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	ClusterName	Specifies the name of the abnormal cluster.
	ErrorMessage	Specifies the error message for the alarm.

Impact on the System

The cluster fails to be scaled out, and the cluster load cannot decrease.

Possible Causes

The network is abnormal, the ECS resources are insufficient, the ECS initialization fails, or the Executor or Controller process is restarted or abnormal.

Handling Procedure

Step 1 Use a browser to log in to ManageOne Operation Portal as the VDC administrator who created the cluster.

Step 2 In the navigation pane on the upper left of the page, click ☰.

Step 3 On the **Service List** page, select a region and choose **MapReduce Service** under **EI Enterprise Intelligence**. The MRS console is displayed.

Step 4 Choose **Active Clusters**.

Step 5 Click the cluster for which the alarm is generated. The cluster management page is displayed.

Step 6 View failed tasks of the cluster and check the status of the failed scale-out task to locate the failure cause.

Step 7 Collect alarms, logs, configurations, and user operation logs, and contact technical support.

1. Log in to the ManageOne alarm platform to obtain the alarm information.
   a. Log in to the ManageOne Maintenance Portal and choose **Alarm Management** > **Alarms** > **Current Alarms** in the navigation pane on the top.
   b. Click **Filter** in the upper left corner and click **Location Info**. The **Location Info** dialog box is displayed.
   c. Set **Operator** to **contains** and **Value** to **CloudService=MRS**, and click **OK**. Click **OK** again to filter MRS alarms.
   d. Obtain **Location Info**, **Possible Causes**, and **Other Information**.
2. Collect system logs of the management plane. For details, see "Log Reference" > "Log Reference on the Management Plane" > "Log Collection" in ***MapReduce Service (MRS) 3.3.1-LTS Reference Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Maintenance Guide (for Huawei Cloud Stack 8.3.1)***.
3. Contact technical support engineers and provide alarm and log information for troubleshooting.

----End

Alarm Clearance

After the fault is rectified, the system does not automatically clear this alarm and you need to manually clear it.

Related Information

None

1.2.10 PAAS_MRS_00311 Auto Scale-In Failed

Alarm Description

This alarm is generated when cluster auto scale-in is successfully triggered but the scale-in fails.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
PAAS_MRS_00311	Critical	Operation	Tenant plane	MapReduce Service	No

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the abnormal cluster.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	ClusterName	Specifies the name of the abnormal cluster.
	ErrorMessage	Specifies the error message for the alarm.

Impact on the System

Cluster resources are not released as expected, and the node that fails to be reduced may be abnormal.

Possible Causes

The Executor or Controller process is restarted or abnormal, or the NodeAgent is restarted.

Handling Procedure

Step 1 Use a browser to log in to ManageOne Operation Portal as the VDC administrator who created the cluster.

Step 2 In the navigation pane on the upper left of the page, click ☰.

Step 3 On the **Service List** page, select a region and choose **MapReduce Service** under **EI Enterprise Intelligence**. The MRS console is displayed.

Step 4 Choose **Active Clusters**.

Step 5 Click the cluster for which the alarm is generated. The cluster management page is displayed.

Step 6 View failed tasks of the cluster and check the status of the failed scale-in task to locate the failure cause.

Step 7 Collect alarms, logs, configurations, and user operation logs, and contact technical support.

1. Log in to the ManageOne alarm platform to obtain the alarm information.
   a. Log in to the ManageOne Maintenance Portal and choose **Alarm Management** > **Alarms** > **Current Alarms** in the navigation pane on the top.
   b. Click **Filter** in the upper left corner and click **Location Info**. The **Location Info** dialog box is displayed.
   c. Set **Operator** to **contains** and **Value** to **CloudService=MRS**, and click **OK**. Click **OK** again to filter MRS alarms.
   d. Obtain **Location Info**, **Possible Causes**, and **Other Information**.
2. Collect system logs of the management plane. For details, see "Log Reference" > "Log Reference on the Management Plane" > "Log Collection" in ***MapReduce Service (MRS) 3.3.1-LTS Reference Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Maintenance Guide (for Huawei Cloud Stack 8.3.1)***.
3. Contact technical support engineers and provide alarm and log information for troubleshooting.

----End

Alarm Clearance

After the fault is rectified, the system does not automatically clear this alarm and you need to manually clear it.

1.2.11 PAAS_MRS_00313 Failed to Deliver Auto Scale-Out Tasks

Alarm Description

This alarm is generated when a cluster that meets auto scaling conditions fails to deliver scale-out requests.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
PAAS_MRS_00313	Critical	Operation	Tenant plane	MapReduce Service	No

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the abnormal cluster.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	ClusterName	Specifies the name of the abnormal cluster.
	ErrorMessage	Specifies the error message for the alarm.

Impact on the System

The cluster cannot be scaled out, and the load cannot decrease.

Possible Causes

The ECS/EVS quota is insufficient, ECS resources are insufficient, ECSs/EVSs are brought offline, or subnet IP addresses are insufficient.

Handling Procedure

Step 1 Rectify the fault based on the alarm information.

1. If the subnet IP addresses are insufficient, check the available IP addresses in the subnet used by the cluster. If the available IP addresses are insufficient for auto scale-out, delete redundant subnet IP addresses or switch to another subnet.
2. If the ECS quota is insufficient, apply for a higher ECS quota or manually add some nodes based on the remaining quota to relieve service pressure.
3. If the EVS quota is insufficient, apply for a higher EVS quota or manually add some nodes based on the remaining quota to relieve service pressure.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

4. If the ECS capacity is insufficient, coordinate ECS resources of the current flavor or select a node group of other flavors with sufficient resources for auto scale-out.
5. If ECS flavors are brought offline, coordinate ECS resources of the current flavor or select a node group of other flavors with sufficient resources for auto scale-out.
6. For other causes, contact technical support engineers and provide the alarm information for troubleshooting.

----End

Alarm Clearance

After the fault is rectified, the system does not automatically clear this alarm and you need to manually clear it.

Related Information

None

1.2.12 PAAS_MRS_00604 Cluster Node Information Is Not Synchronized

Alarm Description

This alarm is generated when the number of nodes in a cluster recorded by DB on management plane is inconsistent with that recorded on MRS Manager.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
PAAS_MRS_00604	Major	Error handling	Tenant plane	MapReduce Service	No

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.

Type	Parameter	Description
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the abnormal cluster.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	ClusterName	Specifies the name of the abnormal cluster.
	ErrorMessage	Specifies the error message for the alarm.

Impact on the System

A VM leakage may occur due to inconsistency between the number of nodes in the database and the number of nodes used by the user.

Possible Causes

- A scale-out or scale-in fails on ManageOne Operation Portal.
- A user has manually scaled out or in the cluster on FusionInsight Manager.

Handling Procedure

Step 1 Use a browser to log in to ManageOne Operation Portal as the VDC administrator who created the cluster.

Step 2 In the navigation pane on the upper left of the page, click ☰.

Step 3 On the **Service List** page, select a region and choose **MapReduce Service** under **EI Enterprise Intelligence**. The MRS console is displayed.

Step 4 Choose **Active Clusters**.

Step 5 Click the name of the cluster whose information is not synchronized and go to the cluster details page.

Step 6 Click the **Nodes** tab to view the total number of nodes in all node groups.

Step 7 On the **Dashboard** tab page, click **Access Manager** next to **MRS Manager**. Enter the username and password to go to the Manager page.

Step 8 On the upper navigation bar, click **Hosts** to view the number of hosts and compare it with the number of nodes in **Step 6**.

- If the number of nodes is the same, go to **Step 9**.
- If the number of nodes is inconsistent, log in to ManageOne Operation Portal, go to the **Elastic Cloud Server** page, query all nodes in the cluster based on the cluster ID, and check whether the number of nodes is the same as that on the **Nodes** tab page of the MapReduce service.
  - If the number of nodes is the same, go to **Step 9**.
  - If the number of nodes is inconsistent, log in to the master node of database **MRS_DB**. For details, see section "Logging In to an MRS Management Node" in ***MapReduce Service (MRS) 3.3.1-LTS Maintenance Guide (for Huawei Cloud Stack 8.3.1)***. Connect to the database and run the following commands:

    mysql -P7306 -h*Floating IP address of the MRS database* **-udatasightemr -p***Default password of datasightemr*

    Contact O&M personnel to obtain the default password of database user **datasightemr**.

    use datasightemr;

    update host set host_status='destroyed' where host_name='*Cluster ID_node name***';**

    Select the alarm on ManageOne and click **Clear** to check whether the alarm will be generated again.

    - If yes, go to **Step 9**.
    - If no, no further action is required.

    NOTE

    The node information on Manager is used.

Step 9 Collect alarms, logs, configurations, and user operation logs, and contact technical support.

1. Log in to the ManageOne alarm platform to obtain the alarm information.
   a. Log in to the ManageOne Maintenance Portal and choose **Alarm Management** > **Alarms** > **Current Alarms** in the navigation pane on the top.
   b. Click **Filter** in the upper left corner and click **Location Info**. The **Location Info** dialog box is displayed.
   c. Set **Operator** to **contains** and **Value** to **CloudService=MRS**, and click **OK**. Click **OK** again to filter MRS alarms.
   d. Obtain **Location Info**, **Possible Causes**, and **Other Information**.
2. Collect system logs of the management plane. For details, see "Log Reference" > "Log Reference on the Management Plane" > "Log Collection" in ***MapReduce Service (MRS) 3.3.1-LTS Reference Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Maintenance Guide (for Huawei Cloud Stack 8.3.1)***.
3. Contact technical support engineers and provide alarm and log information for troubleshooting.

----End

Alarm Clearance

After the fault is rectified, the system does not automatically clear this alarm and you need to manually clear it.

Related Information

None

1.2.13 PAAS_MRS_00605 ECS Status of the Cluster Node Is Abnormal

Alarm Description

The ECS on the cluster node is not in the **Running**, **Stopped**, **Creating**, **Faulty**, **Restarting**, **Rebuilding**, **Soft-deleted**, or **Unknown** state.

This alarm is cleared when the ECS service status becomes normal.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
PAAS_MRS_00605	Critical	Error handling	Tenant plane	MapReduce Service	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the abnormal cluster.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	UserName	Specifies the user for which the alarm was generated.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	ClusterName	Specifies the name of the abnormal cluster.
	ErrorMessage	Specifies the error message for the alarm.

Impact on the System

The cluster node may not be able to work properly.

Possible Causes

The ECS node is abnormal, or operations such as live migration are performed on the ECS service.

Handling Procedure

Step 1 Use a browser to log in to ManageOne Operation Portal as the VDC administrator who created the cluster.

Step 2 In the navigation pane on the upper left of the page, click ☰.

Step 3 On the **Service List** page, select a region and choose **MapReduce Service** under **EI Enterprise Intelligence**. The MRS console is displayed.

Step 4 Choose **Active Clusters**.

Step 5 View the cluster whose status is **Abnormal** and copy the cluster ID displayed below the cluster name in the **Name/ID** column.

Step 6 In the navigation pane, click ☰ on the left. Select **Service List** and choose **Computing** > **Elastic Cloud Server**.

Step 7 On the ECS page, enter the cluster ID copied in **Step 5** into the search box and click the search icon.

Step 8 Check the ECS status of the node in the cluster.

- If the ECS is in the **Running**, **Stopped**, **Creating**, **Faulty**, **Restarting**, **Rebuilding**, **Soft-deleted**, or **Unknown** state, the ECS is normal. This alarm is automatically cleared and will not be reported again. No further action is required.
- If the ECS is not in one of the preceding states, go to **Step 9**.

Step 9 Collect alarms, logs, configurations, and user operation logs, and contact technical support.

1. Log in to the ManageOne alarm platform to obtain the alarm information.

a. Log in to the ManageOne Maintenance Portal and choose **Alarm Management** > **Alarms** > **Current Alarms** in the navigation pane on the top.
b. Click **Filter** in the upper left corner and click **Location Info**. The **Location Info** dialog box is displayed.
c. Set **Operator** to **contains** and **Value** to **CloudService=MRS**, and click **OK**. Click **OK** again to filter MRS alarms.
d. Obtain **Location Info**, **Possible Causes**, and **Other Information**.

2. Collect system logs of the management plane. For details, see "Log Reference" > "Log Reference on the Management Plane" > "Log Collection" in ***MapReduce Service (MRS) 3.3.1-LTS Reference Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Maintenance Guide (for Huawei Cloud Stack 8.3.1)***.
3. Contact technical support engineers and provide alarm and log information for troubleshooting.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.2.14 PAAS_MRS_00801 Cluster Security Risks

Alarm Description

This alarm is generated when the system detects that access from all IP addresses and ports is allowed in the security group rule.

This alarm is cleared when the cluster security group rule limits access from specified IP addresses and ports.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
PAAS_MRS_00801	Major	Operation	Tenant plane	MapReduce Service	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the abnormal cluster.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	ClusterName	Specifies the name of the abnormal cluster.
	ErrorMessage	Specifies the error message for the alarm.

Impact on the System

The cluster may be maliciously attacked.

Possible Causes

The cluster is a non-security cluster and the Master node in the cluster is bound to an EIP. In addition, the inbound direction rule of the security group of the current cluster is not strictly limited.

Handling Procedure

Step 1 Use a browser to log in to ManageOne Operation Portal as the VDC administrator who created the cluster.

Step 2 In the navigation pane on the upper left of the page, click ☰.

Step 3 On the **Service List** page, select a region and choose **MapReduce Service** under **EI Enterprise Intelligence**. The MRS console is displayed.

Step 4 Choose **Active Clusters**.

Step 5 View the cluster whose status is **Abnormal** and copy the cluster ID displayed below the cluster name in the **Name/ID** column.

Step 6 In the navigation pane, click ☰ on the left. Select **Service List** and choose **Computing** > **Elastic Cloud Server**.

Step 7 On the ECS page, enter the cluster ID copied in **Step 5** into the search box and click the search icon.

Step 8 View the search result in the list, check whether the **Name** column contains **master1** and **master2**, and click the name to go to the host information details page.

Step 9 Click the **EIPs** tab and check whether the node is bound to an EIP.

- If an EIP has been bound to the ECS, go to **Step 10**.
- Otherwise, go to **Step 16**.

Step 10 Click the **Security Groups** tab to view the security group to which the node belongs.

Step 11 Check whether the value of **Port Range/ICMP Type** is **Any** or only one upper or lower limit, and whether the value of **Remote End** is **Any** or **0.0.0.0/0** (all IP addresses).

- If the port range and remote IP address are not the values above, go to **Step 12**.
- Otherwise, go to **Step 16**.

Step 12 In the navigation pane, click ☰ on the left. Select **Service List** and choose **Network** > **Virtual Private Cloud**.

Step 13 Choose **Security Groups** on the left. The **Security Groups** tab page is displayed.

Step 14 Locate the security group queried in **Step 10** and click **Manage Rule**. The security group policy configuration page is displayed.

Step 15 On the **Inbound Rules** or **Outbound Rules** tab, click **Modify** in the **Operation** column. Restrict the remote IP address to a specified IP address range or change the port number to a fixed one.

Step 16 Collect alarms, logs, configurations, and user operation logs, and contact technical support.

1. Log in to the ManageOne alarm platform to obtain the alarm information.
   a. Log in to the ManageOne Maintenance Portal and choose **Alarm Management** > **Alarms** > **Current Alarms** in the navigation pane on the top.
   b. Click **Filter** in the upper left corner and click **Location Info**. The **Location Info** dialog box is displayed.
   c. Set **Operator** to **contains** and **Value** to **CloudService=MRS**, and click **OK**. Click **OK** again to filter MRS alarms.
   d. Obtain **Location Info**, **Possible Causes**, and **Other Information**.
2. Collect system logs of the management plane. For details, see "Log Reference" > "Log Reference on the Management Plane" > "Log Collection" in ***MapReduce Service (MRS) 3.3.1-LTS Reference Guide (for Huawei Cloud***

Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Maintenance Guide (for Huawei Cloud Stack 8.3.1).

3. Contact technical support engineers and provide alarm and log information for troubleshooting.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.2.15 PAAS_MRS_00804 MRS Secure Communications Is Disabled

Alarm Description

If **Secure Communications** on the cluster **Dashboard** page is disabled, the cluster status will be abnormal.

This alarm is cleared when the security authorization function of the cluster is enabled.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
PAAS_MRS_00804	Major	Security	Tenant plane	MapReduce Service	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.

Type	Parameter	Description
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the abnormal cluster.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	ClusterName	Specifies the name of the abnormal cluster.
	ErrorMessage	Specifies the error message for the alarm.

Impact on the System

The cluster is unavailable. The service reliability may deteriorate or the service may be unavailable.

Possible Causes

Cluster secure communication is disabled.

Handling Procedure

Step 1 Log in to the ManageOne Maintenance Portal and choose **Alarm Management** > **Alarms** > **Current Alarms** in the navigation pane on the top.

Step 2 Check the ID of the cluster for which the alarm is generated in **Location Info**.

Step 3 Log in to ManageOne Operation Portal as the VDC administrator who created the cluster.

Step 4 In the navigation pane on the upper left of the page, click ☰.

Step 5 On the **Service List** page, select a region and choose **MapReduce Service** under **EI Enterprise Intelligence**. The MRS console is displayed.

Step 6 Choose **Active Clusters** and click the cluster for which the alarm is generated. The cluster management page is displayed.

Step 7 In the **Basic Information** area on the **Dashboard** page, check whether **Secure Communications** is enabled.

- If yes, go to **Step 8**.
- If no, enable **Secure Communications**. Wait for a while and check whether the alarm is cleared. If yes, no further action is required. If no, go to **Step 8**.

Step 8 Collect alarms, logs, configurations, and user operation logs, and contact technical support.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

1. Log in to the ManageOne alarm platform to obtain the alarm information.
   a. Log in to the ManageOne Maintenance Portal and choose **Alarm Management** > **Alarms** > **Current Alarms** in the navigation pane on the top.
   b. Click **Filter** in the upper left corner and click **Location Info**. The **Location Info** dialog box is displayed.
   c. Set **Operator** to **contains** and **Value** to **CloudService=MRS**, and click **OK**. Click **OK** again to filter MRS alarms.
   d. Obtain **Location Info**, **Possible Causes**, and **Other Information**.
2. Collect system logs of the management plane. For details, see "Log Reference" > "Log Reference on the Management Plane" > "Log Collection" in ***MapReduce Service (MRS) 3.3.1-LTS Reference Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Maintenance Guide (for Huawei Cloud Stack 8.3.1)***.
3. Contact technical support engineers and provide alarm and log information for troubleshooting.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.2.16 PAAS_MRS_00806 Usage Is About to Exceed the Threshold Allowed by the License

Alarm Description

The system checks the used capacity every 5 minutes. This alarm is generated when the usage of a license control item exceeds the threshold.

This alarm is automatically cleared when the usage of a license control item falls below the alarm threshold or no license control item whose usage exceeds the alarm threshold exists after a new license file is imported.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
PAAS_MRS_00806	Critical	Operation	Management plane	MapReduce Service	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	LicenseId	Specifies the ID of the license whose usage is about to exceed the threshold.
	ControlScope	Specifies the control scope of the license whose usage is about to exceed the threshold.
	Unit	Specifies the unit of the license whose usage is about to exceed the threshold.
	LicenseVersion	Specifies the version of the license whose usage is about to exceed the threshold.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	ItemName	Describes the control item.
	BbomCode	Specifies the control item code.
	Used	Specifies the current usage of the license.
	Capacity	Specifies the maximum usage of the license.
	AlarmThreshold	Specifies the usage threshold of the license.

Impact on the System

The usage of a license control item is about to exceed the threshold. This may cause system exceptions.

Possible Causes

The usage of a license control item is about to exceed the threshold.

Handling Procedure

Step 1 Log in to the ManageOne Maintenance Portal and choose **System** > **System Settings** > **License Management** in the navigation pane on the top.

Step 2 Choose **Control Items** > **Products and cloud services** to view the license usage of the MapReduce service, as shown in **Figure 1-1**.

Figure 1-1 License page

Step 3 Check whether the used capacity exceeds 90% of the applied capacity.

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 Apply for a new license file, and import and update the license file. For details, see ***Huawei Cloud Stack 8.3.1 License Guide***.

Step 5 Wait for 5 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Step 6 Collect alarms, logs, configurations, and user operation logs, and contact technical support.

1. Log in to the ManageOne alarm platform to obtain the alarm information.
   a. Log in to the ManageOne Maintenance Portal and choose **Alarm Management** > **Alarms** > **Current Alarms** in the navigation pane on the top.
   b. Click **Filter** in the upper left corner and click **Location Info**. The **Location Info** dialog box is displayed.
   c. Set **Operator** to **contains** and **Value** to **CloudService=MRS**, and click **OK**. Click **OK** again to filter MRS alarms.
   d. Obtain **Location Info**, **Possible Causes**, and **Other Information**.
2. Collect system logs of the management plane. For details, see "Log Reference" > "Log Reference on the Management Plane" > "Log Collection" in ***MapReduce Service (MRS) 3.3.1-LTS Reference Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Maintenance Guide (for Huawei Cloud Stack 8.3.1)***.
3. Contact technical support engineers and provide alarm and log information for troubleshooting.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.2.17 PAAS_MRS_00807 Usage Exceeds the Threshold Allowed by the License

Alarm Description

After the cluster is installed, the system checks whether the usage of control items in the license file in the current system exceeds the threshold every 5 minutes. This alarm is generated when the usage of a license control item exceeds the threshold.

This alarm is automatically cleared when the usage of a license control item falls below the threshold or no license control item whose usage exceeds the threshold exists after a new license file is imported.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
PAAS_MRS_00807	Critical	Operation	Management plane	MapReduce Service	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	LicenseId	Specifies the ID of the license whose usage exceeds the threshold.
	ControlScope	Specifies the control scope of the license whose usage exceeds the threshold.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	Unit	Specifies the unit of the license whose usage exceeds the threshold.
	LicenseVersion	Specifies the version of the license whose usage exceeds the threshold.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	ItemName	Describes the control item.
	BbomCode	Specifies the control item code.
	Used	Specifies the current usage of the license.
	Capacity	Specifies the maximum usage of the license.

Impact on the System

The usage of a license control item exceeds the threshold. This may cause system exceptions.

Possible Causes

The usage of a license control item exceeds the threshold.

Handling Procedure

Checking whether the authorized capacity exceeds the upper limit allowed by the license

Step 1 Log in to the ManageOne Maintenance Portal and choose **System** > **System Settings** > **License Management** in the navigation pane on the top.

Step 2 Choose **Control Items** > **Products and cloud services** to view the license usage of the MapReduce service, as shown in **Figure 1-2**.

Figure 1-2 License page

Step 3 Check whether the usage exceeds the threshold allowed by the license file.

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 Apply for a new license file, in which the number of licensed systems must meet the requirements of the current region. Then, import and activate the new license file. For details, see ***Huawei Cloud Stack 8.3.1 License Guide***.

Step 5 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collecting fault information

Step 6 Collect alarms, logs, configurations, and user operation logs, and contact technical support.

1. Log in to the ManageOne alarm platform to obtain the alarm information.
   a. Log in to the ManageOne Maintenance Portal and choose **Alarm Management** > **Alarms** > **Current Alarms** in the navigation pane on the top.
   b. Click **Filter** in the upper left corner and click **Location Info**. The **Location Info** dialog box is displayed.
   c. Set **Operator** to **contains** and **Value** to **CloudService=MRS**, and click **OK**. Click **OK** again to filter MRS alarms.
   d. Obtain **Location Info**, **Possible Causes**, and **Other Information**.
2. Collect system logs of the management plane. For details, see "Log Reference" > "Log Reference on the Management Plane" > "Log Collection" in ***MapReduce Service (MRS) 3.3.1-LTS Reference Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Maintenance Guide (for Huawei Cloud Stack 8.3.1)***.
3. Contact technical support engineers and provide alarm and log information for troubleshooting.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.2.18 PAAS_MRS_00905 Manager Failed to Respond to Auto Scaling Monitoring Tasks

Alarm Description

This alarm is generated when Manager fails to obtain metric information during cluster auto scaling monitoring.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
PAAS_MRS_00905	Critical	Communications	Tenant plane	MapReduce Service	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the abnormal cluster.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	ClusterName	Specifies the name of the abnormal cluster.
	ErrorMessage	Specifies the error message for the alarm.

Impact on the System

The cluster may fail to collect cluster metrics and cannot be scaled based on the auto scaling policy in the metric dimensions.

Possible Causes

The network is abnormal, and the Executor service of the cluster is abnormal.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Handling Procedure

Step 1 Use a browser to log in to ManageOne Operation Portal as the VDC administrator who created the cluster.

Step 2 In the navigation pane on the upper left of the page, click ☰.

Step 3 On the **Service List** page, select a region and choose **MapReduce Service** under **EI Enterprise Intelligence**. The MRS console is displayed.

Step 4 Choose **Active Clusters**.

Step 5 View the cluster whose status is **Abnormal** and copy the cluster ID displayed below the cluster name in the **Name/ID** column.

Step 6 In the navigation pane on the left, click ☰. Choose **Computing** > **Elastic Cloud Server** in **Service List**.

Step 7 On the ECS page, enter the cluster ID copied in **Step 5** into the search box and click the search icon.

Step 8 View the search result in the list and check the **Status** column of the ECSs whose name contains **master1** and **master2** in the **Name** column.

- If the status is **Running**, go to **Step 9**.
- Otherwise, go to **Step 12**.

Step 9 Click **Remote Login** corresponding to the names containing **master1** and **master2** and log in as user **omm**.

Step 10 Run the following command to check whether the Executor service is running properly:

ps -ef | grep executor

If the service is running properly, the following information is displayed:

```
omm       3441     1 67 19:23 ?        00:00:54 /opt/Bigdata/common/runtime0/jdk-8u201//bin/java -Dnop -
Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager -Xms256m -Xmx768m -
Djdk.tls.ephemeralDHKeySize=2048 -Dorg.apache.catalina.security.SecurityListener.UMASK=0027 -
Djava.security.krb5.conf=/opt/hadoopclient/KrbClient/kerberos/var/krb5kdc/krb5.conf -
Dorg.apache.catalina.connector.RECYCLE_FACADES=true -Dignore.endorsed.dirs= -classpath :/opt/
hadoopclient/Spark/spark/conf/:/opt/executor/bin/bootstrap.jar:/opt/executor/bin/tomcat-juli.jar -
Dcatalina.base=/opt/executor -Dcatalina.home=/opt/executor -Djava.io.tmpdir=/opt/executor/temp
org.apache.catalina.startup.Bootstrap start
```

- If the server is running properly, run the **free -m** command to check whether the free memory in the **Mem** and **free** rows is insufficient.
  - If yes, release the memory. Wait for a while and check whether the alarm is cleared. If the alarm is cleared, no further action is required. If not, go to **Step 12**.
  - If no, go to **Step 12**.
- If the service is abnormal, perform the following steps:
  a. Run the following command to determine the active and standby nodes on the nodes whose name contains **master1** and **master2**:

     sh ${BIGDATA_HOME}/om-server/om/sbin/status-oms.sh

     In the command output, the value of **HAActive** for the active management node is **active**, and that for the standby management node

is **standby**. In the following example, **Master1** is the active management node, and **Master2** is the standby management node:

```
HAMode
double
NodeName        HostName      HAVersion       StartTime           HAActive
HAAllResOK      HARunPhase
192-168-0-30      Master1       V100R001C01      2019-05-01 23:43:02     active
normal          Actived
192-168-0-24      Master2       V100R001C01      2019-05-01 07:14:02
standby         normal        Deactived
```

b. On the active management node, run the **sh /opt/executor/bin/startup.sh** command as user **omm** to start the Executor service.

c. Run the **ps -ef | grep executor** command to check whether the Executor process exists.

d. After the Executor process is restarted, check the cluster status on the cluster list page.

- If the cluster is running, no further action is required.
- If the cluster is not in the running state, go to **Step 11**.

Step 11 Check whether the network between the management plane and the tenant plane is connected.

1. Log in to any EICommon-Region-Master VM whose status is running as user **opsadmin**. For details, see **Logging In to an MRS Management Node**.

   Run the **su - root** command to switch to user **root**.

   Obtain the default password by referring to ***Huawei Cloud Stack 8.3.1 Account List*** or contacting the cluster administrator.

   NOTE

   If **Status** of all VMs is not **Running**, contact the cluster administrator.

2. Run the following command to view the running container information of the host machine:

   kubectl get pod -n mrs -owide

```
NAME                          READY   STATUS    RESTARTS   AGE   IP            NODE            NOMINATED
NODE   READINESS GATES
mrsapigw-777fc766b9-8dwc9      1/1     Running   0          14h   10.16.0.231    10.35.152.220
<none>           <none>
mrsapigw-777fc766b9-8pgrb      1/1     Running   0          14h   10.16.0.153    10.35.152.219
<none>           <none>
mrsdeployer-7b5dff56cc-bxzgc   1/1     Running   0          14h   10.16.0.172    10.35.152.218
<none>           <none>
mrsdeployer-7b5dff56cc-gtvvw   1/1     Running   0          14h   10.16.0.230    10.35.152.220
<none>           <none>
mrsdeployer-7b5dff56cc-vxkjf   1/1     Running   0          14h   10.16.0.154    10.35.152.219
<none>           <none>
```

3. Copy the **NAME** values of the three data records whose **NAME** contains **mrsdeployer** in the data obtained in **Step 11.2**.

   Perform **Step 11.4** to **Step 11.5** using the three **NAME** values obtained.

4. Run the following command to access the container (replace **NAME** values with the obtained values in **Step 11.2**):

   kubectl exec -ti -n mrs *NAME value* **bash**

5. Run the following command to query the network connectivity between the management plane and the tenant plane. If 404 is returned, the network

connectivity is normal. If "Connection refused" is returned or no result is returned for a long time, contact the cluster administrator to check whether the port matrix is enabled and whether the configuration is correct.

curl -ik https://*IP addresses of the active and standby nodes in the cluster***:9022**

Example: **curl -ik https://10.20.30.40:9022** or **curl -ik https://10.20.30.41:9022**

NOTE

Obtain the IP addresses of the active and standby nodes on the tenant plane:

1. Log in to any MRS_DB VM as user **opsadmin**. For details, see **Logging In to an MRS Management Node**.

   Run the **su - root** command to switch to user **root**.

   Obtain the default password by referring to ***Huawei Cloud Stack 8.3.1 Account List*** or contacting the cluster administrator.

2. Run the following commands to log in to the MySQL client and obtain the IP address:

   mysql -P7306 -h*Floating IP address of the MRS database* **-udatasightemr -p***Default password of datasightemr*

   use datasightemr;

   select external_ip,external_alternate_ip from cluster_detail where cluster_id='*ID of the cluster for which the alarm is generated***';**

   You can obtain the floating IP address of the MRS database from the LLD during cloud service installation and deployment.

   Contact the O&M personnel to obtain the default password of database user **datasightemr**.

Step 12 Collect alarms, logs, configurations, and user operation logs, and contact technical support.

1. Log in to the ManageOne alarm platform to obtain the alarm information.
   a. Log in to the ManageOne Maintenance Portal and choose **Alarm Management** > **Alarms** > **Current Alarms** in the navigation pane on the top.
   b. Click **Filter** in the upper left corner and click **Location Info**. The **Location Info** dialog box is displayed.
   c. Set **Operator** to **contains** and **Value** to **CloudService=MRS**, and click **OK**. Click **OK** again to filter MRS alarms.
   d. Obtain **Location Info**, **Possible Causes**, and **Other Information**.
2. Collect system logs of the management plane. For details, see "Log Reference" > "Log Reference on the Management Plane" > "Log Collection" in ***MapReduce Service (MRS) 3.3.1-LTS Reference Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Maintenance Guide (for Huawei Cloud Stack 8.3.1)***.
3. Contact technical support engineers and provide alarm and log information for troubleshooting.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.2.19 PAAS_MRS_00909 Too Many Alarms on the Console

Alarm Description

This alarm is generated when the number of alarms that are not cleared or fail to be sent in a cluster exceeds 10,000 on the MRS console.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
PAAS_MRS_00909	Critical	Operation	Tenant plane	MapReduce Service	No

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the abnormal cluster.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ClusterName	Specifies the name of the abnormal cluster.
	ErrorMessage	Specifies the error message for the alarm.

Impact on the System

Alarms that should be automatically cleared on the console may fail to be automatically cleared.

Possible Causes

Cluster components may be abnormal.

Handling Procedure

Step 1 Use a browser to log in to ManageOne Operation Portal as the VDC administrator who created the cluster.

Step 2 In the navigation pane on the upper left of the page, click ☰.

Step 3 On the **Service List** page, select a region and choose **MapReduce Service** under **EI Enterprise Intelligence**. The MRS console is displayed.

Step 4 Choose **Active Clusters**.

Step 5 Click the cluster for which the alarm is generated to go to the cluster management page and log in to its Manager.

Step 6 Check whether abnormal components exist in the cluster. If yes, restore the abnormal components.

Step 7 Collect alarms, logs, configurations, and user operation logs, and contact technical support.

1. Log in to the ManageOne alarm platform to obtain the alarm information.
   a. Log in to the ManageOne Maintenance Portal and choose **Alarm Management** > **Alarms** > **Current Alarms** in the navigation pane on the top.
   b. Click **Filter** in the upper left corner and click **Location Info**. The **Location Info** dialog box is displayed.
   c. Set **Operator** to **contains** and **Value** to **CloudService=MRS**, and click **OK**. Click **OK** again to filter MRS alarms.
   d. Obtain **Location Info**, **Possible Causes**, and **Other Information**.
2. Collect system logs of the management plane. For details, see "Log Reference" > "Log Reference on the Management Plane" > "Log Collection" in ***MapReduce Service (MRS) 3.3.1-LTS Reference Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Maintenance Guide (for Huawei Cloud Stack 8.3.1)***.

3. Contact technical support engineers and provide alarm and log information for troubleshooting.

----End

Alarm Clearance

After the fault is rectified, the system does not automatically clear this alarm and you need to manually clear it.

Related Information

None

1.2.20 PAAS_MRS_00910 Cluster Scale-Out Partially Succeeded

Alarm Description

This alarm is generated when the number of nodes successfully added to a cluster is less than the expected number of nodes to be added.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
PAAS_MRS_00910	Critical	Operation	Tenant plane	MapReduce Service	No

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the abnormal cluster.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	UserName	Specifies the user for which the alarm was generated.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	ClusterName	Specifies the name of the abnormal cluster.
	ErrorMessage	Specifies the error message for the alarm.

Impact on the System

The cluster load cannot decrease to the expected level.

Possible Causes

The network is abnormal, ECS resources are insufficient, ECS initialization fails, or some nodes fail to be deployed.

Handling Procedure

Step 1 Use a browser to log in to ManageOne Operation Portal as the VDC administrator who created the cluster.

Step 2 In the navigation pane on the upper left of the page, click ☰.

Step 3 On the **Service List** page, select a region and choose **MapReduce Service** under **EI Enterprise Intelligence**. The MRS console is displayed.

Step 4 Choose **Active Clusters**.

Step 5 Click the cluster for which the alarm is generated. The cluster management page is displayed.

Step 6 View failed tasks of the cluster and check the status of the failed scale-out task to locate the failure cause.

Step 7 Collect alarms, logs, configurations, and user operation logs, and contact technical support.

1. Log in to the ManageOne alarm platform to obtain the alarm information.
   a. Log in to the ManageOne Maintenance Portal and choose **Alarm Management** > **Alarms** > **Current Alarms** in the navigation pane on the top.
   b. Click **Filter** in the upper left corner and click **Location Info**. The **Location Info** dialog box is displayed.
   c. Set **Operator** to **contains** and **Value** to **CloudService=MRS**, and click **OK**. Click **OK** again to filter MRS alarms.
   d. Obtain **Location Info**, **Possible Causes**, and **Other Information**.
2. Collect system logs of the management plane. For details, see "Log Reference" > "Log Reference on the Management Plane" > "Log Collection" in

MapReduce Service (MRS) 3.3.1-LTS Reference Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Maintenance Guide (for Huawei Cloud Stack 8.3.1).

3. Contact technical support engineers and provide alarm and log information for troubleshooting.

----End

Alarm Clearance

After the fault is rectified, the system does not automatically clear this alarm and you need to manually clear it.

Related Information

None

1.2.21 PAAS_MRS_00911 Node Scaling on Manager Takes a Long Time

Alarm Description

This alarm is generated when nodes to be added to a cluster have been installed on Manager for more than 40 minutes.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
PAAS_MRS_00911	Critical	Operation	Tenant plane	MapReduce Service	No

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ClusterId	Specifies the ID of the abnormal cluster.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	ClusterName	Specifies the name of the abnormal cluster.
	ErrorMessage	Specifies the error message for the alarm.

Impact on the System

The node installation may be blocked on Manager, and the scale-out fails.

Possible Causes

When nodes are being added on Manager, the network for the Executor to access a specified node is disconnected, and obtaining task details on Manager times out.

Handling Procedure

Step 1 Use a browser to log in to ManageOne Operation Portal as the VDC administrator who created the cluster.

Step 2 In the navigation pane on the upper left of the page, click ☰.

Step 3 On the **Service List** page, select a region and choose **MapReduce Service** under **EI Enterprise Intelligence**. The MRS console is displayed.

Step 4 Choose **Active Clusters**.

Step 5 Click the cluster for which the alarm is generated. The cluster management page is displayed.

Step 6 View the Manager task list of the cluster and check the task status of the scale-out task to determine whether the scale-out fails.

Step 7 Collect alarms, logs, configurations, and user operation logs, and contact technical support.

1. Log in to the ManageOne alarm platform to obtain the alarm information.
   a. Log in to the ManageOne Maintenance Portal and choose **Alarm Management** > **Alarms** > **Current Alarms** in the navigation pane on the top.
   b. Click **Filter** in the upper left corner and click **Location Info**. The **Location Info** dialog box is displayed.

c. Set **Operator** to **contains** and **Value** to **CloudService=MRS**, and click **OK**. Click **OK** again to filter MRS alarms.

d. Obtain **Location Info**, **Possible Causes**, and **Other Information**.

2. Collect system logs of the management plane. For details, see "Log Reference" > "Log Reference on the Management Plane" > "Log Collection" in ***MapReduce Service (MRS) 3.3.1-LTS Reference Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Maintenance Guide (for Huawei Cloud Stack 8.3.1)***.

3. Contact technical support engineers and provide alarm and log information for troubleshooting.

----End

Alarm Clearance

After the fault is rectified, the system does not automatically clear this alarm and you need to manually clear it.

Related Information

None

1.2.22 PAAS_MRS_00916 Roles Deployed on Non-Master Nodes in a Group Are Inconsistent

Alarm Description

The number of roles deployed on different nodes in a non-master node group is different.

This alarm is cleared when the roles deployed on nodes in a non-master node group are consistent.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
PAAS_MRS_00916	Major	Quality of service	Tenant plane	MapReduce Service	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.

Type	Parameter	Description
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the abnormal cluster.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	ClusterName	Specifies the name of the abnormal cluster.
	ErrorMessage	Specifies the error message for the alarm.

Impact on the System

The number of roles is incorrectly calculated, affecting the verification of the number of roles during scale-out and instance adding.

Possible Causes

When an instance is added, an isolated node exists in a non-Master node group. The isolated node is regarded as a discarded node and the instance is not deployed on the isolated node. If you cancel the isolation of an isolated node after adding an instance, the roles deployed on the node are different from those deployed on other nodes in the node group.

Handling Procedure

Step 1 Log in to the MRS console. Choose **Active Clusters** and click the name of the target cluster to go to its details page. If the node is not required, go to **Step 2**. If the node is required, go to **Step 4**.

Scaling in nodes

Step 2 Click **Nodes**, select the desired node, and choose **Node Operation** > **Isolate Host**.

Confirm the information about the host to be isolated and click **OK**.

When "Operation successful" is displayed, click **Finish**. The host is isolated successfully, and the value of **Operating Status** becomes **Isolated**.

Step 3 Locate the row that contains the target node group and click **Scale In** in the **Operation** column to go to the **Scale In** page. Set **Scale-In Type** to **Specific node** and select the node to be removed.

Select "I understand the consequences of performing the scale-in operation", and click **OK**.

Deleting and adding an instance again

Step 4 Click **Nodes**, click **View Role** in the **Operation** column of the node group, compare the deployment role of the node with that of other nodes, and record the missing service instances.

Step 5 Click **Components**, select the services recorded in **Step 4**. On the **Instances** page that is displayed, select the instances recorded in **Step 4**, choose **More** > **Delete Instance**, select the related description, and click **OK**.

On the service status page, click **More** and select **Restart Service** or **Rolling Restart Service** to restart the service.

NOTE

- Instances such as HDFS DataNodes, YARN NodeManagers, HBase RegionServers, Elasticsearch EsNodes, ClickHouse ClickHouseServers, and IoTDB IoTDBServers must be decommissioned before being deleted. Otherwise, the deletion will fail.
- Before deleting data instances, you need to migrate data. For details about the impact of instance deletion, see the capacity reduction description in *MapReduce Service (MRS) 3.3.1-LTS Physical Machine Cluster Capacity Expansion Guide (for Huawei Cloud Stack 8.3.1)*.
- Adding or deleting instances to or from job submission-related services such as Flink, Hive, Spark, HDFS, YARN, and MapReduce may interrupt jobs. Before performing this operation, check whether any job is being submitted and select "I understand that this operation will interrupt job submission and confirm to add the instances.".

Step 6 Add the instance deleted in **Step 5** to the node group again.

Choose **Components**, click the service name, click **Instances**, and then **Add Instance**. On the displayed page, add the instance deleted in **Step 5** to the corresponding node group.

On the service status page, click **More** and select **Restart Service** or **Rolling Restart Service** to restart the service.

Step 7 Check whether this alarm is cleared after 5 minutes.

- If yes, no further action is required.
- If no, go to **Step 8**.

Step 8 Collect alarms, logs, configurations, and user operation logs, and contact technical support.

1. Log in to the ManageOne alarm platform to obtain the alarm information.
   a. Log in to the ManageOne Maintenance Portal and choose **Alarm Management** > **Alarms** > **Current Alarms** in the navigation pane on the top.

b. Click **Filter** in the upper left corner and click **Location Info**. The **Location Info** dialog box is displayed.

c. Set **Operator** to **contains** and **Value** to **CloudService=MRS**, and click **OK**. Click **OK** again to filter MRS alarms.

d. Obtain **Location Info**, **Possible Causes**, and **Other Information**.

2. Collect system logs of the management plane. For details, see "Log Reference" > "Log Reference on the Management Plane" > "Log Collection" in ***MapReduce Service (MRS) 3.3.1-LTS Reference Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Maintenance Guide (for Huawei Cloud Stack 8.3.1)***.

3. Contact technical support engineers and provide alarm and log information for troubleshooting.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.2.23 PAAS_MRS_00917 Role Information on the Console Is Inconsistent with That on Manager

Alarm Description

The role deployment information recorded on the console is inconsistent with that deployed on Manager.

This alarm is cleared when the role deployment information recorded on the console becomes consistent with that deployed on Manager.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
PAAS_MRS_00917	Major	Quality of service	Tenant plane	MapReduce Service	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.

Type	Parameter	Description
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the abnormal cluster.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	ClusterName	Specifies the name of the abnormal cluster.
	ErrorMessage	Specifies the error message for the alarm.

Impact on the System

The number of roles is incorrectly calculated, affecting the verification of the number of roles during scale-out and instance adding.

Possible Causes

An exception occurs when a service or an instance is added or deleted. As a result, the data delivered to Manager is incorrect, or an exception occurs when the data on the console is updated. As a result, the role information on the console is inconsistent with that on Manager.

Handling Procedure

Step 1 Log in to any ElCommon-Region-Master VM whose status is running as user **opsadmin**. For details, see **Logging In to an MRS Management Node**.

Run the **su - root** command to switch to user **root**.

Obtain the default password by referring to ***Huawei Cloud Stack 8.3.1 Account List*** or contacting the cluster administrator.

NOTE

If **Status** of all VMs is not **Running**, contact the cluster administrator.

Step 2 Run the following command to check the container status:

kubectl get pod -n mrs -owide

Step 3 Run the following command to access any Deployer container:

kubectl exec -ti -n mrs *Deployer container name* **bash**

Step 4 Run the following commands to synchronize role information:

NOTE

- To synchronize role information, the cluster must be in the running state. Otherwise, the synchronization fails. Cluster management is not involved.
- You can synchronize the role information of a single service, a single cluster, multiple clusters, or all clusters.

- Synchronize a single service.

  sh /opt/cloud/MRS-Deployer/bin/cli.sh -clusterId *Cluster ID -Service service name*
- Synchronize a single cluster.

  sh /opt/cloud/MRS-Deployer/bin/cli.sh -clusterId *Cluster ID*
- Synchronize multiple clusters.

  sh /opt/cloud/MRS-Deployer/bin/cli.sh -clusterIds *Cluster ID1, cluster ID2...*
- Synchronize all clusters.

  sh /opt/cloud/MRS-Deployer/bin/cli.sh -all

Step 5 Check whether this alarm is cleared after 5 minutes.

- If yes, no further action is required.
- If no, go to **Step 6**.

Step 6 Collect alarms, logs, configurations, and user operation logs, and contact technical support.

1. Log in to the ManageOne alarm platform to obtain the alarm information.
   a. Log in to the ManageOne Maintenance Portal and choose **Alarm Management** > **Alarms** > **Current Alarms** in the navigation pane on the top.
   b. Click **Filter** in the upper left corner and click **Location Info**. The **Location Info** dialog box is displayed.
   c. Set **Operator** to **contains** and **Value** to **CloudService=MRS**, and click **OK**. Click **OK** again to filter MRS alarms.
   d. Obtain **Location Info**, **Possible Causes**, and **Other Information**.
2. Collect system logs of the management plane. For details, see "Log Reference" > "Log Reference on the Management Plane" > "Log Collection" in ***MapReduce Service (MRS) 3.3.1-LTS Reference Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Maintenance Guide (for Huawei Cloud Stack 8.3.1)***.
3. Contact technical support engineers and provide alarm and log information for troubleshooting.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.2.24 PAAS_MRS_01001 MRS API Gateway Is Abnormal

Alarm Description

On the active node, the system checks the API Gateway service status every 60 seconds. This alarm is generated when the system detects that the API Gateway service has been abnormal for three consecutive times.

This alarm is cleared when the API Gateway service status has been normal for three consecutive times.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
PAAS_MRS_01001	Critical	Quality of service	Management plane	MapReduce Service	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	MicroServiceInstanceName	Specifies the name of the microservice instance for which the alarm was generated.
	MicroServiceInstanceId	Specifies the ID of the microservice instance for which the alarm was generated.
	IP Address	Specifies the IP address of the microservice for which the alarm was generated.
Additional Information	ThresholdValue	Specifies the service status triggering the alarm.
	CurrentValue	Specifies the current service status.
	ThresholdRulename	Specifies the name of the threshold rule for triggering the alarm.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

The MRS UI pages cannot be accessed. The reliability of some services may deteriorate or some services may be unavailable.

Possible Causes

- The CDK status is abnormal.
- The **mrsapigw** container is abnormal.
- The API Gateway service is abnormal.

Handling Procedure

Step 1 Use a browser to log in to ManageOne Maintenance Portal as an O&M administrator.

Step 2 Choose **Alarm Management** > **Alarms** > **Current Alarms** and check whether the alarm whose ID is **605001** or **605002** exists.

- If these alarms exist, clear them by referring to related alarm documents and go to **Step 3**.
- If these alarms do not exist, go to **Step 3**.

Step 3 Log in to any EICommon-Region-Master VM whose status is running as user **opsadmin**. For details, see **Logging In to an MRS Management Node**.

Run the **su - root** command to switch to user **root**.

Obtain the default password by referring to ***Huawei Cloud Stack 8.3.1 Account List*** or contacting the cluster administrator.

NOTE

If **Status** of all VMs is not **Running**, contact the cluster administrator.

Step 4 Run the following command to check the container status:

kubectl get pod -n mrs -owide

Step 5 Check whether the values in the **READY** and **STATUS** columns for the API Gateway container are **1/1** and **Running**, respectively.

- If yes, go to **Step 10**.
- If no, go to **Step 6**.

Step 6 Run the following commands to access any API Gateway container and view the API Gateway container logs:

kubectl exec -ti -n mrs *API Gateway container name* **bash**

vi /opt/cloud/logs/apigateway/api-gateway.log

Step 7 Repeat **Step 6** to view the logs of all API Gateway containers.

Step 8 Check whether the alarm is caused by a network fault based on the logs. If the logs contain information such as **connect fail**, the network is faulty.

- If yes, go to **Step 9**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If no, go to **Step 10**.

Step 9 Contact network administrators to rectify the network fault. Then, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 10**.

Step 10 Collect alarms, logs, configurations, and user operation logs, and contact technical support.

1. Log in to the ManageOne alarm platform to obtain the alarm information.
   a. Log in to the ManageOne Maintenance Portal and choose **Alarm Management** > **Alarms** > **Current Alarms** in the navigation pane on the top.
   b. Click **Filter** in the upper left corner and click **Location Info**. The **Location Info** dialog box is displayed.
   c. Set **Operator** to **contains** and **Value** to **CloudService=MRS**, and click **OK**. Click **OK** again to filter MRS alarms.
   d. Obtain **Location Info**, **Possible Causes**, and **Other Information**.
2. Collect system logs of the management plane. For details, see "Log Reference" > "Log Reference on the Management Plane" > "Log Collection" in ***MapReduce Service (MRS) 3.3.1-LTS Reference Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Maintenance Guide (for Huawei Cloud Stack 8.3.1)***.
3. Contact technical support engineers and provide alarm and log information for troubleshooting.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.2.25 PAAS_MRS_01002 MRS Deployer Is Abnormal

Alarm Description

On the active node, the system checks the MRS Deployer service status every 60 seconds. This alarm is generated when the system detects that the MRS Deployer service has been abnormal for three consecutive times.

This alarm is cleared when the MRS Deployer service status has been normal for three consecutive times.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
PAAS_MRS_01002	Critical	Quality of service	Management plane	MapReduce Service	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	MicroServiceInstanceName	Specifies the name of the microservice instance for which the alarm was generated.
	MicroServiceInstanceId	Specifies the ID of the microservice instance for which the alarm was generated.
	IP Address	Specifies the IP address of the microservice for which the alarm was generated.
Additional Information	ThresholdValue	Specifies the service status triggering the alarm.
	CurrentValue	Specifies the current service status.
	ThresholdRulename	Specifies the name of the threshold rule for triggering the alarm.

Impact on the System

The service reliability deteriorates or some services are unavailable.

Possible Causes

- The CDK status is abnormal.
- The **mrsdeployer** container is abnormal.
- The Deployer service is abnormal.

Handling Procedure

Step 1 Use a browser to log in to ManageOne Maintenance Portal as an O&M administrator.

Step 2 Choose **Alarm Management** > **Alarms** > **Current Alarms** and check whether the alarm whose ID is **605001** or **605002** exists.

- If these alarms exist, clear them by referring to related alarm documents and go to **Step 3**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If these alarms do not exist, go to **Step 3**.

Step 3 Log in to any EICommon-Region-Master VM whose status is running as user **opsadmin**. For details, see **Logging In to an MRS Management Node**.

Run the **su - root** command to switch to user **root**.

Obtain the default password by referring to ***Huawei Cloud Stack 8.3.1 Account List*** or contacting the cluster administrator.

NOTE

If **Status** of all VMs is not **Running**, contact the cluster administrator.

Step 4 Run the following command to check the container status:

kubectl get pod -n mrs -owide

Step 5 Check whether the values in the **READY** and **STATUS** columns for the Deployer container are **1/1** and **Running**, respectively.

- If yes, go to **Step 10**.
- If no, go to **Step 6**.

Step 6 Run the following commands to access any Deployer container and view the Deployer container logs:

kubectl exec -ti -n mrs *Deployer container name* **bash**

vi /opt/cloud/logs/service-deployer/service-deployer-service-deployer.log

Step 7 Repeat **Step 6** to view the logs of all Deployer containers.

Step 8 Check whether the alarm is caused by a network fault based on the logs. If the logs contain information such as **connect fail**, the network is faulty.

- If yes, go to **Step 9**.
- If no, go to **Step 10**.

Step 9 Contact network administrators to rectify the network fault. Then, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 10**.

Step 10 Collect alarms, logs, configurations, and user operation logs, and contact technical support.

1. Log in to the ManageOne alarm platform to obtain the alarm information.
   a. Log in to the ManageOne Maintenance Portal and choose **Alarm Management** > **Alarms** > **Current Alarms** in the navigation pane on the top.
   b. Click **Filter** in the upper left corner and click **Location Info**. The **Location Info** dialog box is displayed.
   c. Set **Operator** to **contains** and **Value** to **CloudService=MRS**, and click **OK**. Click **OK** again to filter MRS alarms.
   d. Obtain **Location Info**, **Possible Causes**, and **Other Information**.
2. Collect system logs of the management plane. For details, see "Log Reference" > "Log Reference on the Management Plane" > "Log Collection" in

MapReduce Service (MRS) 3.3.1-LTS Reference Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Maintenance Guide (for Huawei Cloud Stack 8.3.1).

3. Contact technical support engineers and provide alarm and log information for troubleshooting.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.2.26 PAAS_MRS_01003 MRS ZooKeeper Service Is Abnormal

Alarm Description

On the active node, the system checks the ZooKeeper service status every 60 seconds. This alarm is generated when the system detects that the ZooKeeper service has been abnormal for three consecutive times.

This alarm is cleared when the ZooKeeper service status has been normal for three consecutive times.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
PAAS_MRS_00103	Critical	Quality of service	Management plane	MapReduce Service	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	MicroServiceInstanceName	Specifies the name of the microservice instance for which the alarm was generated.
	MicroServiceInstanceId	Specifies the ID of the microservice instance for which the alarm was generated.
	IP Address	Specifies the IP address of the microservice for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
Additional Information	ThresholdValue	Specifies the service status triggering the alarm.
	CurrentValue	Specifies the current service status.
	ThresholdRule name	Specifies the name of the threshold rule for triggering the alarm.

Impact on the System

Users cannot manage clusters. MRS reliability deteriorates or MRS is unavailable.

Possible Causes

- The MRS_Region_Node VM is faulty.
- The ZooKeeper service is abnormal.

Handling Procedure

Step 1 Log in to any MRS_Region_Node VM whose status is running as the **opsadmin** user..

Run the following command to switch to user **root**:

su - root

Obtain the default password by referring to ***Huawei Cloud Stack 8.3.1 Account List*** or contacting the cluster administrator.

NOTE

If **Status** of all VMs is not **Running**, contact the cluster administrator.

Step 2 Check whether the **/opt/cloud/zookeeper** directory exists. If the directory does not exist, ZooKeeper is not deployed on the current node. Repeat **Step 1** to select another MRS_Region_Node node.

ll /opt/cloud

Step 3 Run the **ps -ef | grep zookeeper** command to check whether the ZooKeeper process exists.

```
-rw------- 1 service servicegroup [redacted] .log
[root@host-24-69-26-200 zookeeper]# ps -ef |grep zookeeper
root      12812  6855  0 12:03 pts/0    00:00:00 grep --color=auto zookeeper
service   125669     1  0 Feb18 ?        00:12:46 /opt/cloud/3rdComponent/jre/bin/java -Dzookeeper.log.dir=/opt/cloud/logs/zookeeper/server -Dzookeeper.root.logger=INFO,ROLLINGFILE -Dzookeeper.authPr
ris.auth.GTSZKAuthProvider -cp /opt/cloud/zookeeper/bin/../lib/zookeeper-jute-3.4.14.jar:/opt/cloud/zookeeper/bin/../lib/zookeeper-3.4.14.jar:/opt/cloud/zookeeper/bin/../lib/us-file-1.0.9.jar:/opt/cl
tor-1.0.9.jar:/opt/cloud/zookeeper/bin/../lib/us-common-1.0.9.jar:/opt/cloud/zookeeper/bin/../lib/us-certverification-1.0.9.jar:/opt/cloud/zookeeper/bin/../lib/slf4j-api-1.7.26.jar:/opt/cloud/zookeep
ar:/opt/cloud/zookeeper/bin/../lib/log4j-slf4j-impl-2.12.0.jar:/opt/cloud/zookeeper/bin/../lib/log4j-core-2.12.0.jar:/opt/cloud/zookeeper/bin/../lib/log4j-api-2.12.0.jar:/opt/cloud/zookeeper/bin/../l
keeper/bin/../lib/jline-2.14.6.jar:/opt/cloud/zookeeper/bin/../lib/huawei-secure-api-3.0.6.jar:/opt/cloud/zookeeper/bin/../lib/commons-lang3-3.7.jar:/opt/cloud/zookeeper/bin/../lib/bcprov-jdk15on-1.6
lib/audience-annotations-0.5.0.jar:/opt/cloud/zookeeper/bin/../lib/antisamy-1.5.8.jar:/opt/cloud/zookeeper/bin/../lib/zookeeper-jute-3.4.14.jar:/opt/cloud/zookeeper/bin/../lib/zookeeper-3.4.14.jar:/o
ile-1.0.9.jar:/opt/cloud/zookeeper/bin/../lib/us-encryptor-1.0.9.jar:/opt/cloud/zookeeper/bin/../lib/us-common-1.0.9.jar:/opt/cloud/zookeeper/bin/../lib/us-certverification-1.0.9.jar:/opt/cloud/zooke
ar:/opt/cloud/zookeeper/bin/../lib/netty-3.10.6.Final.jar:/opt/cloud/zookeeper/bin/../lib/log4j-slf4j-impl-2.12.0.jar:/opt/cloud/zookeeper/bin/../lib/log4j-core-2.12.0.jar:/opt/cloud/zookeeper/bin/..
ud/zookeeper/bin/../lib/jsr305-3.0.2.jar:/opt/cloud/zookeeper/bin/../lib/jline-2.14.6.jar:/opt/cloud/zookeeper/bin/../lib/huawei-secure-api-3.0.6.jar:/opt/cloud/zookeeper/bin/../lib/commons-lang3-3.7
lib/bcprov-jdk15on-1.60.jar:/opt/cloud/zookeeper/bin/../lib/audience-annotations-0.5.0.jar:/opt/cloud/zookeeper/bin/../lib/antisamy-1.5.8.jar:/opt/cloud/zookeeper/bin/../zookeeper-*.jar:/opt/cloud/zoo
/main/resources/lib/*.jar:/opt/cloud/zookeeper/bin/../conf::/opt/cloud/3rdcomponent/jre/lib/dt.jar:/opt/cloud/3rdcomponent/jre/lib/tools.jar -Xms3072m -Xmx3072m -Xmn2048m -DuSer.timezone=GMT+08 org..
rumPeerMain /opt/cloud/zookeeper/bin/../conf/zoo.cfg
```

- If yes, go to **Step 8**.
- If no, go to **Step 4**.

Step 4 Run the following command to view ZooKeeper logs:

vi /opt/cloud/logs/zookeeper/zookeeper*.log

Step 5 Repeat **Step 1** to **Step 4** to check whether all ZooKeeper service processes and logs are normal.

Step 6 Check whether the alarm is caused by a network fault based on the logs. If the logs contain information such as **connect fail**, the network is faulty.

- If yes, go to **Step 7**.
- If no, go to **Step 8**.

Step 7 Rectify the network fault and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Step 8 Collect alarms, logs, configurations, and user operation logs, and contact technical support.

1. Log in to the ManageOne alarm platform to obtain the alarm information.
   a. Log in to the ManageOne Maintenance Portal and choose **Alarm Management** > **Alarms** > **Current Alarms** in the navigation pane on the top.
   b. Click **Filter** in the upper left corner and click **Location Info**. The **Location Info** dialog box is displayed.
   c. Set **Operator** to **contains** and **Value** to **CloudService=MRS**, and click **OK**. Click **OK** again to filter MRS alarms.
   d. Obtain **Location Info**, **Possible Causes**, and **Other Information**.
2. Collect system logs of the management plane. For details, see "Log Reference" > "Log Reference on the Management Plane" > "Log Collection" in ***MapReduce Service (MRS) 3.3.1-LTS Reference Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Maintenance Guide (for Huawei Cloud Stack 8.3.1)***.
3. Contact technical support engineers and provide alarm and log information for troubleshooting.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.2.27 PAAS_MRS_01004 MRS DB Service Is Faulty

Alarm Description

On the active node, the system checks the MRS DB service status every 60 seconds. This alarm is generated when the system detects that the MRS DB service has been abnormal for three consecutive times.

This alarm is cleared when the MRS DB service status has been normal for three consecutive times.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
PAAS_MRS_00104	Critical	Quality of service	Management plane	MapReduce Service	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	MicroServiceInstanceName	Specifies the name of the microservice instance for which the alarm was generated.
	MicroServiceInstanceId	Specifies the ID of the microservice instance for which the alarm was generated.
	IP Address	Specifies the IP address of the microservice for which the alarm was generated.
Additional Information	ThresholdValue	Specifies the service status triggering the alarm.
	CurrentValue	Specifies the current service status.
	ThresholdRulename	Specifies the name of the threshold rule for triggering the alarm.

Impact on the System

Operations on the database, such as adding, deleting, modifying, and querying, are abnormal. Service reliability deteriorates or some services may be unavailable.

Possible Causes

- The MySQL service is abnormal.
- The MRS-DB node is abnormal.

Handling Procedure

Step 1 Log in to any MRS_DB VM whose status is running as the **opsadmin** user. For details, see **Logging In to an MRS Management Node**.

Run the **su - root** command to switch to user **root**.

Obtain the default password by referring to ***Huawei Cloud Stack 8.3.1 Account List*** or contacting the cluster administrator.

NOTE

If **Status** of all VMs is not **Running**, contact the cluster administrator.

Step 2 Check whether the **/data/mysql** directory exists. If the directory does not exist, MySQL is not deployed on the current VM node. Repeat **Step 1** to select another MRS_DB VM node.

ll /data

Step 3 Run the **netstat -ntlp | grep 7306** command to check whether the port is listened.

```
tcp        0      0 0.0.0.0:7306            0.0.0.0:*               LISTEN      7850/mysqld
```

- If yes, go to **Step 5**.
- If no, go to **Step 4**.

Step 4 Run the following commands to restart MySQL. Wait for a while and check whether the alarm is cleared.

su - mysql

startdb

- If yes, no further action is required.
- If no, go to **Step 5**.

Step 5 Run the following command to check whether the MySQL service is running properly. If the message "mysqld is alive" is displayed, the service is running properly.

/data/mysql/base/bin/mysqladmin -P7306 -h127.0.0.1 -udatasightemr -p*Password of user datasightemr* **ping**

Contact O&M personnel to obtain the default password of database user **datasightemr**.

```
...
mysqld is alive
```

- If yes, go to **Step 10**.
- If no, go to **Step 6**.

Step 6 View the MySQL logs.

vi /data/mysql/logs/error.log

Step 7 Repeat **Step 1** and **Step 6** to check whether all MySQL service processes and logs are normal.

Step 8 Check whether the alarm is caused by a network fault based on the logs. If the logs contain information such as **connect fail**, the network is faulty.

- If yes, go to **Step 9**.
- If no, go to **Step 10**.

Step 9 Rectify the network fault and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 10**.

Step 10 Collect alarms, logs, configurations, and user operation logs, and contact technical support.

1. Log in to the ManageOne alarm platform to obtain the alarm information.
   a. Log in to the ManageOne Maintenance Portal and choose **Alarm Management** > **Alarms** > **Current Alarms** in the navigation pane on the top.
   b. Click **Filter** in the upper left corner and click **Location Info**. The **Location Info** dialog box is displayed.
   c. Set **Operator** to **contains** and **Value** to **CloudService=MRS**, and click **OK**. Click **OK** again to filter MRS alarms.
   d. Obtain **Location Info**, **Possible Causes**, and **Other Information**.
2. Collect system logs of the management plane. For details, see "Log Reference" > "Log Reference on the Management Plane" > "Log Collection" in ***MapReduce Service (MRS) 3.3.1-LTS Reference Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Maintenance Guide (for Huawei Cloud Stack 8.3.1)***.
3. Contact technical support engineers and provide alarm and log information for troubleshooting.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.2.28 PAAS_MRS_01005 MRS API Gateway Instance Is Abnormal

Alarm Description

On the active node, the system checks the API Gateway instance status every 60 seconds. This alarm is generated when the system detects that the API Gateway instance has been abnormal for three consecutive times.

This alarm is cleared when the API Gateway instance status has been normal for three consecutive times.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
PAAS_MRS_01005	Critical	Quality of service	Management plane	MapReduce Service	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	MicroService InstanceName	Specifies the name of the microservice instance for which the alarm was generated.
	MicroService InstanceId	Specifies the ID of the microservice instance for which the alarm was generated.
	IP Address	Specifies the IP address of the microservice for which the alarm was generated.
Additional Information	ThresholdValue	Specifies the service status triggering the alarm.
	CurrentValue	Specifies the current service status.
	ThresholdRule name	Specifies the name of the threshold rule for triggering the alarm.

Impact on the System

For multi-instance API Gateway, services are not significantly affected. For single-instance API Gateway, service reliability may deteriorate or some services may be unavailable.

Possible Causes

The Cloud Development Kit (CDK) status, container of MRS API Gateway, or the API Gateway service is abnormal.

Handling Procedure

Step 1 Log in to any EICommon-Region-Master VM whose status is running as user **opsadmin**. For details, see **Logging In to an MRS Management Node**.

Run the **su - root** command to switch to user **root**.

Obtain the default password by referring to ***Huawei Cloud Stack 8.3.1 Account List*** or contacting the cluster administrator.

NOTE

If **Status** of all VMs is not **Running**, contact the cluster administrator.

Step 2 Run the following command to check the container status:

kubectl get pod -n mrs -owide

Step 3 Check whether the values in the **READY** and **STATUS** columns for the API Gateway container are **1/1** and **Running**, respectively.

- If yes, go to **Step 8**.
- If no, go to **Step 4**.

Step 4 Run the following commands to access any API Gateway container and view the API Gateway container logs:

kubectl exec -ti -n mrs *API Gateway container name* **bash**

vi /opt/cloud/logs/apigateway/api-gateway.log

Step 5 Repeat **Step 4** to view the logs of all API Gateway containers.

Step 6 Check whether the alarm is caused by a network fault based on the logs. If the logs contain information such as **connect fail**, the network is faulty.

- If yes, go to **Step 7**.
- If no, go to **Step 8**.

Step 7 Contact network administrators to rectify the network fault. Then, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Step 8 Collect alarms, logs, configurations, and user operation logs, and contact technical support.

1. Log in to the ManageOne alarm platform to obtain the alarm information.
   a. Log in to the ManageOne Maintenance Portal and choose **Alarm Management** > **Alarms** > **Current Alarms** in the navigation pane on the top.
   b. Click **Filter** in the upper left corner and click **Location Info**. The **Location Info** dialog box is displayed.
   c. Set **Operator** to **contains** and **Value** to **CloudService=MRS**, and click **OK**. Click **OK** again to filter MRS alarms.
   d. Obtain **Location Info**, **Possible Causes**, and **Other Information**.
2. Collect system logs of the management plane. For details, see "Log Reference" > "Log Reference on the Management Plane" > "Log Collection" in ***MapReduce Service (MRS) 3.3.1-LTS Reference Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Maintenance Guide (for Huawei Cloud Stack 8.3.1)***.
3. Contact technical support engineers and provide alarm and log information for troubleshooting.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.2.29 PAAS_MRS_01006 MRS Deployer Instance Is Abnormal

Alarm Description

On the active node, the system checks the MRS Deployer instance status every 60 seconds. This alarm is generated when the system detects that the MRS Deployer instance has been abnormal for three consecutive times.

This alarm is cleared when the MRS Deployer instance status has been normal for three consecutive times.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
PAAS_MRS_01006	Critical	Quality of service	Management plane	MapReduce Service	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	MicroServiceInstanceName	Specifies the name of the microservice instance for which the alarm was generated.
	MicroServiceInstanceId	Specifies the ID of the microservice instance for which the alarm was generated.
	IP Address	Specifies the IP address of the microservice for which the alarm was generated.
Additional Information	ThresholdValue	Specifies the service status triggering the alarm.
	CurrentValue	Specifies the current service status.
	ThresholdRulename	Specifies the name of the threshold rule for triggering the alarm.

Impact on the System

For multi-instance MRS Deployer, services are not significantly affected. For single-instance MRS Deployer, service reliability may deteriorate or some services may be unavailable.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Possible Causes

- The CDK status is abnormal.
- The MRS Deployer container is abnormal.
- The Deployer service is abnormal.

Handling Procedure

Step 1 Log in to any EICommon-Region-Master VM whose status is running as user **opsadmin**. For details, see **Logging In to an MRS Management Node**.

Run the **su - root** command to switch to user **root**.

Obtain the default password by referring to ***Huawei Cloud Stack 8.3.1 Account List*** or contacting the cluster administrator.

NOTE

If **Status** of all VMs is not **Running**, contact the cluster administrator.

Step 2 Run the following command to check the container status:

kubectl get pod -n mrs -owide

Step 3 Check whether the values in the **READY** and **STATUS** columns for the Deployer container are **1/1** and **Running**, respectively.

- If yes, go to **Step 8**.
- If no, go to **Step 4**.

Step 4 Run the following commands to access any Deployer container and view the Deployer container logs:

kubectl exec -ti -n mrs *Deployer container name* **bash**

vi /opt/cloud/logs/service-deployer/service-deployer-service-deployer.log

Step 5 Repeat **Step 4** to view the logs of all Deployer containers.

Step 6 Check whether the alarm is caused by a network fault based on the logs. If the logs contain information such as **connect fail**, the network is faulty.

- If yes, go to **Step 7**.
- If no, go to **Step 8**.

Step 7 Contact network administrators to rectify the network fault. Then, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Step 8 Collect alarms, logs, configurations, and user operation logs, and contact technical support.

1. Log in to the ManageOne alarm platform to obtain the alarm information.
   a. Log in to the ManageOne Maintenance Portal and choose **Alarm Management** > **Alarms** > **Current Alarms** in the navigation pane on the top.

b. Click **Filter** in the upper left corner and click **Location Info**. The **Location Info** dialog box is displayed.

c. Set **Operator** to **contains** and **Value** to **CloudService=MRS**, and click **OK**. Click **OK** again to filter MRS alarms.

d. Obtain **Location Info**, **Possible Causes**, and **Other Information**.

2. Collect system logs of the management plane. For details, see "Log Reference" > "Log Reference on the Management Plane" > "Log Collection" in ***MapReduce Service (MRS) 3.3.1-LTS Reference Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Maintenance Guide (for Huawei Cloud Stack 8.3.1)***.

3. Contact technical support engineers and provide alarm and log information for troubleshooting.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.2.30 PAAS_MRS_01007 MRS ZooKeeper Instance Is Abnormal

Alarm Description

On the active node, the system checks the ZooKeeper instance status every 60 seconds. This alarm is generated when the system detects that the ZooKeeper instance has been abnormal for three consecutive times.

This alarm is cleared when the ZooKeeper instance status has been normal for three consecutive times.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
PAAS_MRS_01007	Critical	Quality of service	Management plane	MapReduce Service	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.

Type	Parameter	Description
	MicroService InstanceName	Specifies the name of the microservice instance for which the alarm was generated.
	MicroService InstanceId	Specifies the ID of the microservice instance for which the alarm was generated.
	IP Address	Specifies the IP address of the microservice for which the alarm was generated.
Additional Information	ThresholdValue	Specifies the service status triggering the alarm.
	CurrentValue	Specifies the current service status.
	ThresholdRule name	Specifies the name of the threshold rule for triggering the alarm.

Impact on the System

Users may fail to manage clusters. Service reliability deteriorates or the service becomes unavailable.

Possible Causes

- The MRS_Region_Node VM is faulty.
- The ZooKeeper service is abnormal.

Handling Procedure

Step 1 Log in to any MRS_Region_Node VM whose status is running as the **opsadmin** user..

Run the following command to switch to user **root**:

su - root

Obtain the default password by referring to ***Huawei Cloud Stack 8.3.1 Account List*** or contacting the cluster administrator.

NOTE

If **Status** of all VMs is not **Running**, contact the cluster administrator.

Step 2 Run the following command to check whether the **/opt/cloud/zookeeper** directory exists: If it does not exist, ZooKeeper is not deployed on the current node. In this case, log in to other MRS_Region_Node nodes by referring to **Step 1** and perform **Step 1** and **Step 2** on the nodes.

ll /opt/cloud

Step 3 Run the **ps -ef | grep zookeeper** command to check whether the ZooKeeper process exists.

```
-rw------- 1 service servicegroup [illegible] [illegible]t.log
[root@host-24-69-26-200 zookeeper]# ps -ef |grep zookeeper
root     12812  6853  0 12:03 pts/0    00:00:00 grep --color=auto zookeeper
service  125669     1  0 Feb18 ?        00:12:46 /opt/cloud/3rdComponent/jre/bin/java -Dzookeeper.log.dir=/opt/cloud/logs/zookeeper/server -Dzookeeper.root.logger=INFO,ROLLINGFILE -Dzookeeper.authPr
ts.auth.GTSZKAuthProvider -cp /opt/cloud/zookeeper/bin/../lib/zookeeper-jute-3.4.14.jar:/opt/cloud/zookeeper/bin/../lib/zookeeper-3.4.14.jar:/opt/cloud/zookeeper/bin/../lib/us-file-1.0.9.jar:/opt/ch
tor-1.0.9.jar:/opt/cloud/zookeeper/bin/../lib/us-common-1.0.9.jar:/opt/cloud/zookeeper/bin/../lib/us-certverification-1.0.9.jar:/opt/cloud/zookeeper/bin/../lib/slf4j-api-1.7.26.jar:/opt/cloud/zookeep
ar:/opt/cloud/zookeeper/bin/../lib/log4j-slf4j-impl-2.12.0.jar:/opt/cloud/zookeeper/bin/../lib/log4j-core-2.12.0.jar:/opt/cloud/zookeeper/bin/../lib/log4j-api-2.12.0.jar:/opt/cloud/zookeeper/bin/../l
keeper/bin/../lib/jline-2.14.6.jar:/opt/cloud/zookeeper/bin/../lib/huawei-secure-api-3.0.6.jar:/opt/cloud/zookeeper/bin/../lib/commons-lang3-3.7.jar:/opt/cloud/zookeeper/bin/../lib/bcprov-jdk15on-1.6
lib/audience-annotations-0.5.0.jar:/opt/cloud/zookeeper/bin/../lib/antlrsamy-1.5.8.jar:/opt/cloud/zookeeper/bin/../lib/zookeeper-jute-3.4.14.jar:/opt/cloud/zookeeper/bin/../lib/zookeeper-3.4.14.jar:/o
ile-1.0.9.jar:/opt/cloud/zookeeper/bin/../lib/us-encryptor-1.0.9.jar:/opt/cloud/zookeeper/bin/../lib/us-common-1.0.9.jar:/opt/cloud/zookeeper/bin/../lib/us-certverification-1.0.9.jar:/opt/cloud/zooke
ar:/opt/cloud/zookeeper/bin/../lib/netty-3.10.6.Final.jar:/opt/cloud/zookeeper/bin/../lib/log4j-slf4j-impl-2.12.0.jar:/opt/cloud/zookeeper/bin/../lib/log4j-core-2.12.0.jar:/opt/cloud/zookeeper/bin/..
ad/zookeeper/bin/../lib/jsr305-3.0.2.jar:/opt/cloud/zookeeper/bin/../lib/jline-2.14.6.jar:/opt/cloud/zookeeper/bin/../lib/huawei-secure-api-3.0.6.jar:/opt/cloud/zookeeper/bin/../lib/commons-lang3-3.7
lib/bcprov-jdk15on-1.60.jar:/opt/cloud/zookeeper/bin/../lib/audience-annotations-0.5.0.jar:/opt/cloud/zookeeper/bin/../lib/antlrsamy-1.5.8.jar:/opt/cloud/zookeeper/bin/../zookeeper-*.jar:/opt/cloud/zoo
/main/resources/lib/*.jar:/opt/cloud/zookeeper/bin/../conf:/opt/cloud/3rdComponent/jre/lib/dt.jar:/opt/cloud/3rdComponent/jre/lib/tools.jar -Xms3072m -Xmx3072m -Xmn204800 -Duser.timezone=GMT+08 org.
rumPeerMain /opt/cloud/zookeeper/bin/../conf/zoo.cfg
[root@host-24-69-26-200 zookeeper]
```

- If yes, go to **Step 8**.
- If no, go to **Step 4**.

Step 4 Run the following command to view ZooKeeper logs:

vi /opt/cloud/logs/zookeeper/zookeeper*.log

Step 5 Repeat **Step 1** and **Step 4** to check whether all ZooKeeper service processes and logs are normal.

Step 6 Check whether the alarm is caused by a network fault based on the logs. If the logs contain information such as **connect fail** or **zookeeper not connected**, the network is faulty.

- If yes, go to **Step 7**.
- If no, go to **Step 8**.

Step 7 Rectify the network fault and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Step 8 Collect alarms, logs, configurations, and user operation logs, and contact technical support.

1. Log in to the ManageOne alarm platform to obtain the alarm information.
   a. Log in to the ManageOne Maintenance Portal and choose **Alarm Management** > **Alarms** > **Current Alarms** in the navigation pane on the top.
   b. Click **Filter** in the upper left corner and click **Location Info**. The **Location Info** dialog box is displayed.
   c. Set **Operator** to **contains** and **Value** to **CloudService=MRS**, and click **OK**. Click **OK** again to filter MRS alarms.
   d. Obtain **Location Info**, **Possible Causes**, and **Other Information**.
2. Collect system logs of the management plane. For details, see "Log Reference" > "Log Reference on the Management Plane" > "Log Collection" in ***MapReduce Service (MRS) 3.3.1-LTS Reference Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Maintenance Guide (for Huawei Cloud Stack 8.3.1)***.
3. Contact technical support engineers and provide alarm and log information for troubleshooting.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.2.31 PAAS_MRS_01008 MRS DB Instance Is Abnormal

Alarm Description

On the active node, the system checks the MRS DB instance status every 60 seconds. This alarm is generated when the system detects that the ZooKeeper instance has been abnormal for three consecutive times.

This alarm is cleared when the MRS DB instance status has been normal for three consecutive times.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
PAAS_MRS_01008	Critical	Quality of service	Management plane	MapReduce Service	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	MicroServiceInstanceName	Specifies the name of the microservice instance for which the alarm was generated.
	MicroServiceInstanceId	Specifies the ID of the microservice instance for which the alarm was generated.
	IP Address	Specifies the IP address of the microservice for which the alarm was generated.
Additional Information	ThresholdValue	Specifies the service status triggering the alarm.
	CurrentValue	Specifies the current service status.
	ThresholdRulename	Specifies the name of the threshold rule for triggering the alarm.

Impact on the System

If the MySQL service fails to be started or the MRS-DB node is faulty, users fail to add, delete, modify, or query clusters. For single-instance MRS DB, MRS reliability deteriorates or MRS becomes unavailable. For multi-instance MRS DB, services are not affected.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Possible Causes

- The MySQL service is abnormal.
- The MRS-DB node is abnormal.

Handling Procedure

Step 1 Log in to any MRS_DB VM whose status is running as the **opsadmin** user. For details, see **Logging In to an MRS Management Node**.

Run the **su - root** command to switch to user **root**.

Obtain the default password by referring to ***Huawei Cloud Stack 8.3.1 Account List*** or contacting the cluster administrator.

NOTE

If **Status** of all VMs is not **Running**, contact the cluster administrator.

Step 2 Run the following commands to switch to user **mysql**:

su - mysql

Step 3 Run the **dbstatus** command to check whether the database on the current node is in the **Online** status.

```
+----------------+-----------+-----------+----------------+-----------+---------+----------------+-----------+------
+-------+---------------------+---------------------+
| node_ip        | ha_status | db_status |      vip       | rep_state | db_role |  master_host   | read_only | sync |
delay |    heartbeat_time   |      check_time     |
+----------------+-----------+-----------+----------------+-----------+---------+----------------+-----------+------
+-------+---------------------+---------------------+
| 10.35.101.101  |   online  |   online  | 10.35.101.103  |   Normal  | Primary |       -        |    OFF    | -  |  -  |
2022-03-23 14:32:13 | 2022-03-23 14:32:14 |
| 10.35.101.102  |   online  |   online  |       -        |   Normal  | Standby | 10.35.101.101  |    ON     | 100 |  0
| 2022-03-23 14:32:08 | 2022-03-23 14:32:09 |
+----------------+-----------+-----------+----------------+-----------+---------+----------------+-----------+------
+-------+---------------------+---------------------+
```

- If yes, check whether the alarm is cleared 5 minutes later. If the alarm is cleared, no further action is required. If the alarm persists, go to **Step 4**.
- If no, go to **Step 7**.

Step 4 Check whether the **/data/dbmha/haprogram/db_tool.py** file exists.

- If yes, go to **Step 5**.
- If no, go to **Step 7**.

Step 5 Run the **python /data/dbmha/haprogram/db_tool.py db_status** command and check whether the value of **ha_status** is **online**.

```
+----------------+-----------+-----------+----------------+-----------+---------+----------------+-----------+------
+-------+---------------------+---------------------+
| node_ip        | ha_status | db_status |      vip       | rep_state | db_role |  master_host   | read_only | sync |
delay |    heartbeat_time   |      check_time     |
+----------------+-----------+-----------+----------------+-----------+---------+----------------+-----------+------
+-------+---------------------+---------------------+
| 10.35.101.101  |   online  |   online  | 10.35.101.103  |   Normal  | Primary |       -        |    OFF    | -  |  -  |
2022-03-23 14:33:31 | 2022-03-23 14:33:31 |
| 10.35.101.102  |   online  |   online  |       -        |   Normal  | Standby | 10.35.101.101  |    ON     | 100 |  0
| 2022-03-23 14:33:25 | 2022-03-23 14:33:31 |
+----------------+-----------+-----------+----------------+-----------+---------+----------------+-----------+------
+-------+---------------------+---------------------+
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If yes, check whether the alarm is cleared 5 minutes later. If the alarm is cleared, no further action is required. If the alarm persists, go to **Step 6**.
- If no, go to **Step 6**.

Step 6 Run the following command as user **root** to perform HA takeover. After a period of time, check whether the alarm is cleared.

python /data/dbmha/haprogram/ha_tool.py attach_ha

- If yes, no further action is required.
- If no, go to **Step 7**.

Step 7 Collect alarms, logs, configurations, and user operation logs, and contact technical support.

1. Log in to the ManageOne alarm platform to obtain the alarm information.
   a. Log in to the ManageOne Maintenance Portal and choose **Alarm Management** > **Alarms** > **Current Alarms** in the navigation pane on the top.
   b. Click **Filter** in the upper left corner and click **Location Info**. The **Location Info** dialog box is displayed.
   c. Set **Operator** to **contains** and **Value** to **CloudService=MRS**, and click **OK**. Click **OK** again to filter MRS alarms.
   d. Obtain **Location Info**, **Possible Causes**, and **Other Information**.
2. Collect system logs of the management plane. For details, see "Log Reference" > "Log Reference on the Management Plane" > "Log Collection" in ***MapReduce Service (MRS) 3.3.1-LTS Reference Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Maintenance Guide (for Huawei Cloud Stack 8.3.1)***.
3. Contact technical support engineers and provide alarm and log information for troubleshooting.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.2.32 PAAS_MRS_01009 Low Response Success Rate of MRS Cluster List

Alarm Description

The system checks the response success rate of the API for querying the MRS cluster list every 60 seconds on the active node. This alarm is generated when the system detects that the response success rate has been lower than 99.99% for three consecutive times.

This alarm is cleared when the response success rate has exceeded 99.99% for three consecutive times.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
PAAS_MRS_01009	Critical	Quality of service	Management plane	MapReduce Service	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	MicroServiceInstanceName	Specifies the name of the microservice instance for which the alarm was generated.
	MicroServiceInstanceId	Specifies the ID of the microservice instance for which the alarm was generated.
	IP Address	Specifies the IP address of the microservice for which the alarm was generated.
Additional Information	ThresholdValue	Specifies the service status triggering the alarm.
	CurrentValue	Specifies the current service status.
	ThresholdRulename	Specifies the name of the threshold rule for triggering the alarm.

Impact on the System

Users may fail to query the cluster list. Service reliability deteriorates or the service becomes unavailable.

Possible Causes

- The MRS API Gateway service is abnormal.
- The MRS Deployer service is abnormal.

Handling Procedure

Step 1 Log in to any EICommon-Region-Master VM whose status is running as user **opsadmin**. For details, see **Logging In to an MRS Management Node**.

Run the **su - root** command to switch to user **root**.

Obtain the default password by referring to ***Huawei Cloud Stack 8.3.1 Account List*** or contacting the cluster administrator.

NOTE

If **Status** of all VMs is not **Running**, contact the cluster administrator.

Step 2 Run the following command to check the container status:

kubectl get pod -n mrs -owide

Step 3 Run the following commands to access any API Gateway container and view the API Gateway container logs:

kubectl exec -ti -n mrs *API Gateway container name* **bash**

vi /opt/cloud/logs/apigateway/api-gateway.log

Step 4 Repeat **Step 2** to **Step 3** to view the logs of all API Gateway containers.

Step 5 Collect alarms, logs, configurations, and user operation logs, and contact technical support.

1. Log in to the ManageOne alarm platform to obtain the alarm information.
   a. Log in to the ManageOne Maintenance Portal and choose **Alarm Management** > **Alarms** > **Current Alarms** in the navigation pane on the top.
   b. Click **Filter** in the upper left corner and click **Location Info**. The **Location Info** dialog box is displayed.
   c. Set **Operator** to **contains** and **Value** to **CloudService=MRS**, and click **OK**. Click **OK** again to filter MRS alarms.
   d. Obtain **Location Info**, **Possible Causes**, and **Other Information**.
2. Collect system logs of the management plane. For details, see "Log Reference" > "Log Reference on the Management Plane" > "Log Collection" in ***MapReduce Service (MRS) 3.3.1-LTS Reference Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Maintenance Guide (for Huawei Cloud Stack 8.3.1)***.
3. Contact technical support engineers and provide alarm and log information for troubleshooting.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.2.33 PAAS_MRS_01010 Low Response Success Rate of MRS Job Addition

Alarm Description

The system checks the response success rate of the API for adding MRS jobs every 60 seconds on the active node. This alarm is generated when the system detects that the response success rate has been lower than 99.99% for three consecutive times.

This alarm is cleared when the response success rate has exceeded 99.99% for three consecutive times.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
PAAS_MRS_01010	Critical	Quality of service	Management plane	MapReduce Service	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	MicroService InstanceName	Specifies the name of the microservice instance for which the alarm was generated.
	MicroService InstanceId	Specifies the ID of the microservice instance for which the alarm was generated.
	IP Address	Specifies the IP address of the microservice for which the alarm was generated.
Additional Information	ThresholdValue	Specifies the service status triggering the alarm.
	CurrentValue	Specifies the current service status.
	ThresholdRule name	Specifies the name of the threshold rule for triggering the alarm.

Impact on the System

Users may fail to add jobs. Service reliability deteriorates or the service becomes unavailable.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Possible Causes

- The MRS API Gateway service is abnormal.
- The MRS Deployer service is abnormal.

Handling Procedure

Step 1 Log in to any EICommon-Region-Master VM whose status is running as user **opsadmin**. For details, see **Logging In to an MRS Management Node**.

Run the **su - root** command to switch to user **root**.

Obtain the default password by referring to ***Huawei Cloud Stack 8.3.1 Account List*** or contacting the cluster administrator.

NOTE

If **Status** of all VMs is not **Running**, contact the cluster administrator.

Step 2 Run the following command to check the container status:

kubectl get pod -n mrs -owide

Step 3 Run the following commands to access any API Gateway container and view the API Gateway container logs:

kubectl exec -ti -n mrs *API Gateway container name* **bash**

vi /opt/cloud/logs/apigateway/api-gateway.log

Step 4 Repeat **Step 2** to **Step 3** to view the logs of all API Gateway containers.

Step 5 Collect alarms, logs, configurations, and user operation logs, and contact technical support.

1. Log in to the ManageOne alarm platform to obtain the alarm information.
   a. Log in to the ManageOne Maintenance Portal and choose **Alarm Management** > **Alarms** > **Current Alarms** in the navigation pane on the top.
   b. Click **Filter** in the upper left corner and click **Location Info**. The **Location Info** dialog box is displayed.
   c. Set **Operator** to **contains** and **Value** to **CloudService=MRS**, and click **OK**. Click **OK** again to filter MRS alarms.
   d. Obtain **Location Info**, **Possible Causes**, and **Other Information**.
2. Collect system logs of the management plane. For details, see "Log Reference" > "Log Reference on the Management Plane" > "Log Collection" in ***MapReduce Service (MRS) 3.3.1-LTS Reference Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Maintenance Guide (for Huawei Cloud Stack 8.3.1)***.
3. Contact technical support engineers and provide alarm and log information for troubleshooting.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.2.34 PAAS_MRS_01011 Low Response Success Rate of MRS Job Execution Result Obtaining

Alarm Description

The system checks the response success rate of the API for querying the MRS job execution result every 60 seconds on the active node. This alarm is generated when the system detects that the response success rate has been lower than 99.99% for three consecutive times.

This alarm is cleared when the response success rate has exceeded 99.99% for three consecutive times.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
PAAS_MRS_01011	Critical	Quality of service	Management plane	MapReduce Service	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	MicroServiceInstanceName	Specifies the name of the microservice instance for which the alarm was generated.
	MicroServiceInstanceId	Specifies the ID of the microservice instance for which the alarm was generated.
	IP Address	Specifies the IP address of the microservice for which the alarm was generated.
Additional Information	ThresholdValue	Specifies the service status triggering the alarm.
	CurrentValue	Specifies the current service status.
	ThresholdRulename	Specifies the name of the threshold rule for triggering the alarm.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

Users may fail to query job execution results. Service reliability deteriorates or the service becomes unavailable.

Possible Causes

- The API Gateway service is abnormal.
- The MRS Deployer service is abnormal.

Handling Procedure

Step 1 Log in to any EICommon-Region-Master VM whose status is running as user **opsadmin**. For details, see **Logging In to an MRS Management Node**.

Run the **su - root** command to switch to user **root**.

Obtain the default password by referring to ***Huawei Cloud Stack 8.3.1 Account List*** or contacting the cluster administrator.

NOTE

If **Status** of all VMs is not **Running**, contact the cluster administrator.

Step 2 Run the following command to check the container status:

kubectl get pod -n mrs -owide

Step 3 Run the following commands to access any API Gateway container and view the API Gateway container logs:

kubectl exec -ti -n mrs *API Gateway container name* **bash**

vi /opt/cloud/logs/apigateway/api-gateway.log

Step 4 Repeat **Step 2** to **Step 4** to view the logs of all API Gateway containers.

Step 5 Collect alarms, logs, configurations, and user operation logs, and contact technical support.

1. Log in to the ManageOne alarm platform to obtain the alarm information.
   a. Log in to the ManageOne Maintenance Portal and choose **Alarm Management** > **Alarms** > **Current Alarms** in the navigation pane on the top.
   b. Click **Filter** in the upper left corner and click **Location Info**. The **Location Info** dialog box is displayed.
   c. Set **Operator** to **contains** and **Value** to **CloudService=MRS**, and click **OK**. Click **OK** again to filter MRS alarms.
   d. Obtain **Location Info**, **Possible Causes**, and **Other Information**.
2. Collect system logs of the management plane. For details, see "Log Reference" > "Log Reference on the Management Plane" > "Log Collection" in ***MapReduce Service (MRS) 3.3.1-LTS Reference Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Maintenance Guide (for Huawei Cloud Stack 8.3.1)***.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

3. Contact technical support engineers and provide alarm and log information for troubleshooting.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.2.35 PAAS_MRS_01012 Low Response Success Rate of MRS Query Job List

Alarm Description

The system checks the response success rate of the API for querying the MRS job list every 60 seconds on the active node. This alarm is generated when the system detects that the response success rate has been lower than 99.99% for three consecutive times.

This alarm is cleared when the response success rate has exceeded 99.99% for three consecutive times.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
PAAS_MRS_01012	Critical	Quality of service	Management plane	MapReduce Service	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	MicroServiceInstanceName	Specifies the name of the microservice instance for which the alarm was generated.
	MicroServiceInstanceId	Specifies the ID of the microservice instance for which the alarm was generated.
	IP Address	Specifies the IP address of the microservice for which the alarm was generated.
Additional Information	ThresholdValue	Specifies the service status triggering the alarm.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	CurrentValue	Specifies the current service status.
	ThresholdRule name	Specifies the name of the threshold rule for triggering the alarm.

Impact on the System

Users may fail to query jobs. Service reliability deteriorates or the service becomes unavailable.

Possible Causes

- The API Gateway service is abnormal.
- The MRS Deployer service is abnormal.

Handling Procedure

Step 1 Log in to any EICommon-Region-Master VM whose status is running as user **opsadmin**. For details, see **Logging In to an MRS Management Node**.

Run the **su - root** command to switch to user **root**.

Obtain the default password by referring to ***Huawei Cloud Stack 8.3.1 Account List*** or contacting the cluster administrator.

NOTE

If **Status** of all VMs is not **Running**, contact the cluster administrator.

Step 2 Run the following command to check the container status:

kubectl get pod -n mrs -owide

Step 3 Run the following commands to access any API Gateway container and view the API Gateway container logs:

kubectl exec -ti -n mrs *API Gateway container name* **bash**

vi /opt/cloud/logs/apigateway/api-gateway.log

Step 4 Repeat **Step 2** to **Step 3** to view the logs of all API Gateway containers.

Step 5 Collect alarms, logs, configurations, and user operation logs, and contact technical support.

1. Log in to the ManageOne alarm platform to obtain the alarm information.
   a. Log in to the ManageOne Maintenance Portal and choose **Alarm Management** > **Alarms** > **Current Alarms** in the navigation pane on the top.
   b. Click **Filter** in the upper left corner and click **Location Info**. The **Location Info** dialog box is displayed.
   c. Set **Operator** to **contains** and **Value** to **CloudService=MRS**, and click **OK**. Click **OK** again to filter MRS alarms.

d. Obtain **Location Info**, **Possible Causes**, and **Other Information**.

2. Collect system logs of the management plane. For details, see "Log Reference" > "Log Reference on the Management Plane" > "Log Collection" in ***MapReduce Service (MRS) 3.3.1-LTS Reference Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Maintenance Guide (for Huawei Cloud Stack 8.3.1)***.
3. Contact technical support engineers and provide alarm and log information for troubleshooting.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.2.36 PAAS_MRS_01013 Low Response Success Rate of MRS Job Stopping

Alarm Description

The system checks the response success rate of the API for stopping an MRS job every 60 seconds on the active node. This alarm is generated when the system detects that the response success rate has been lower than 99.99% for three consecutive times.

This alarm is cleared when the response success rate has exceeded 99.99% for three consecutive times.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
PAAS_MRS_01013	Critical	Quality of service	Management plane	MapReduce Service	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	MicroService InstanceName	Specifies the name of the microservice instance for which the alarm was generated.

Type	Parameter	Description
	MicroService InstanceId	Specifies the ID of the microservice instance for which the alarm was generated.
	IP Address	Specifies the IP address of the microservice for which the alarm was generated.
Additional Information	ThresholdValue	Specifies the service status triggering the alarm.
	CurrentValue	Specifies the current service status.
	ThresholdRule name	Specifies the name of the threshold rule for triggering the alarm.

Impact on the System

User jobs may fail to be stopped. Service reliability deteriorates or the service becomes unavailable.

Possible Causes

- The API Gateway service is abnormal.
- The MRS Deployer service is abnormal.

Handling Procedure

Step 1 Log in to any EICommon-Region-Master VM whose status is running as user **opsadmin**. For details, see **Logging In to an MRS Management Node**.

Run the **su - root** command to switch to user **root**.

Obtain the default password by referring to ***Huawei Cloud Stack 8.3.1 Account List*** or contacting the cluster administrator.

NOTE

If **Status** of all VMs is not **Running**, contact the cluster administrator.

Step 2 Run the following command to check the container status:

kubectl get pod -n mrs -owide

Step 3 Run the following commands to access any API Gateway container and view the API Gateway container logs:

kubectl exec -ti -n mrs *API Gateway container name* **bash**

vi /opt/cloud/logs/apigateway/api-gateway.log

Step 4 Repeat **Step 2** to **Step 3** to view the logs of all API Gateway containers.

Step 5 Collect alarms, logs, configurations, and user operation logs, and contact technical support.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

1. Log in to the ManageOne alarm platform to obtain the alarm information.
   a. Log in to the ManageOne Maintenance Portal and choose **Alarm Management** > **Alarms** > **Current Alarms** in the navigation pane on the top.
   b. Click **Filter** in the upper left corner and click **Location Info**. The **Location Info** dialog box is displayed.
   c. Set **Operator** to **contains** and **Value** to **CloudService=MRS**, and click **OK**. Click **OK** again to filter MRS alarms.
   d. Obtain **Location Info**, **Possible Causes**, and **Other Information**.
2. Collect system logs of the management plane. For details, see "Log Reference" > "Log Reference on the Management Plane" > "Log Collection" in ***MapReduce Service (MRS) 3.3.1-LTS Reference Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Maintenance Guide (for Huawei Cloud Stack 8.3.1)***.
3. Contact technical support engineers and provide alarm and log information for troubleshooting.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.2.37 PAAS_MRS_01014 Low Response Success Rate of Batch MRS Job Deletion

Alarm Description

The system checks the response success rate of the API for batch deleting MRS jobs every 60 seconds on the active node. This alarm is generated when the system detects that the response success rate has been lower than 99.99% for three consecutive times.

This alarm is cleared when the response success rate has exceeded 99.99% for three consecutive times.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
PAAS_MRS_0114	Critical	Quality of service	Management plane	MapReduce Service	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	MicroService InstanceName	Specifies the name of the microservice instance for which the alarm was generated.
	MicroService InstanceId	Specifies the ID of the microservice instance for which the alarm was generated.
	IP Address	Specifies the IP address of the microservice for which the alarm was generated.
Additional Information	ThresholdValue	Specifies the service status triggering the alarm.
	CurrentValue	Specifies the current service status.
	ThresholdRule name	Specifies the name of the threshold rule for triggering the alarm.

Impact on the System

User jobs may fail to be stopped. Service reliability deteriorates or the service becomes unavailable.

Possible Causes

- The API Gateway service is abnormal.
- The MRS Deployer service is abnormal.

Handling Procedure

Step 1 Log in to any EICommon-Region-Master VM whose status is running as user **opsadmin**. For details, see **Logging In to an MRS Management Node**.

Run the **su - root** command to switch to user **root**.

Obtain the default password by referring to ***Huawei Cloud Stack 8.3.1 Account List*** or contacting the cluster administrator.

NOTE

If **Status** of all VMs is not **Running**, contact the cluster administrator.

Step 2 Run the following command to check the container status:

kubectl get pod -n mrs -owide

Step 3 Run the following commands to access any API Gateway container and view the API Gateway container logs:

kubectl exec -ti -n mrs *API Gateway container name* **bash**

vi /opt/cloud/logs/apigateway/api-gateway.log

Step 4 Repeat **Step 2** to **Step 3** to view the logs of all API Gateway containers.

Step 5 Collect alarms, logs, configurations, and user operation logs, and contact technical support.

1. Log in to the ManageOne alarm platform to obtain the alarm information.
   a. Log in to the ManageOne Maintenance Portal and choose **Alarm Management** > **Alarms** > **Current Alarms** in the navigation pane on the top.
   b. Click **Filter** in the upper left corner and click **Location Info**. The **Location Info** dialog box is displayed.
   c. Set **Operator** to **contains** and **Value** to **CloudService=MRS**, and click **OK**. Click **OK** again to filter MRS alarms.
   d. Obtain **Location Info**, **Possible Causes**, and **Other Information**.
2. Collect system logs of the management plane. For details, see "Log Reference" > "Log Reference on the Management Plane" > "Log Collection" in ***MapReduce Service (MRS) 3.3.1-LTS Reference Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Maintenance Guide (for Huawei Cloud Stack 8.3.1)***.
3. Contact technical support engineers and provide alarm and log information for troubleshooting.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.2.38 PAAS_MRS_01015 Low Response Success Rate of MRS SQL Result Obtaining

Alarm Description

The system checks the response success rate of the API for obtaining the MRS SQL execution result every 60 seconds on the active node. This alarm is generated when the system detects that the response success rate has been lower than 99.99% for three consecutive times.

This alarm is cleared when the response success rate has exceeded 99.99% for three consecutive times.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
PAAS_MRS_01015	Critical	Quality of service	Management plane	MapReduce Service	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	MicroServiceInstanceName	Specifies the name of the microservice instance for which the alarm was generated.
	MicroServiceInstanceId	Specifies the ID of the microservice instance for which the alarm was generated.
	IP Address	Specifies the IP address of the microservice for which the alarm was generated.
Additional Information	ThresholdValue	Specifies the service status triggering the alarm.
	CurrentValue	Specifies the current service status.
	ThresholdRulename	Specifies the name of the threshold rule for triggering the alarm.

Impact on the System

User operations may fail. Service reliability deteriorates or the service becomes unavailable.

Possible Causes

- The API Gateway service is abnormal.
- The MRS Deployer service is abnormal.

Handling Procedure

Step 1 Log in to any EICommon-Region-Master VM whose status is running as user **opsadmin**. For details, see **Logging In to an MRS Management Node**.

Run the **su - root** command to switch to user **root**.

Obtain the default password by referring to ***Huawei Cloud Stack 8.3.1 Account List*** or contacting the cluster administrator.

NOTE

If **Status** of all VMs is not **Running**, contact the cluster administrator.

Step 2 Run the following command to check the container status:

kubectl get pod -n mrs -owide

Step 3 Run the following commands to access any API Gateway container and view the API Gateway container logs:

kubectl exec -ti -n mrs *API Gateway container name* **bash**

vi /opt/cloud/logs/apigateway/api-gateway.log

Step 4 Repeat **Step 2** to **Step 3** to view the logs of all API Gateway containers.

Step 5 Collect alarms, logs, configurations, and user operation logs, and contact technical support.

1. Log in to the ManageOne alarm platform to obtain the alarm information.
   a. Log in to the ManageOne Maintenance Portal and choose **Alarm Management** > **Alarms** > **Current Alarms** in the navigation pane on the top.
   b. Click **Filter** in the upper left corner and click **Location Info**. The **Location Info** dialog box is displayed.
   c. Set **Operator** to **contains** and **Value** to **CloudService=MRS**, and click **OK**. Click **OK** again to filter MRS alarms.
   d. Obtain **Location Info**, **Possible Causes**, and **Other Information**.
2. Collect system logs of the management plane. For details, see "Log Reference" > "Log Reference on the Management Plane" > "Log Collection" in ***MapReduce Service (MRS) 3.3.1-LTS Reference Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Maintenance Guide (for Huawei Cloud Stack 8.3.1)***.
3. Contact technical support engineers and provide alarm and log information for troubleshooting.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.3 Alarms of the MRS Tenant Plane

1.3.1 ALM-12001 Audit Log Dumping Failure

Alarm Description

Cluster audit logs need to be dumped on a third-party server due to the local historical data backup policy. The system starts to check the dump server at 3 a.m. every day. If the dump server meets the configuration conditions, audit logs can be successfully dumped. This alarm is generated when the audit log dump fails if the disk space of the dump directory on the third-party server is insufficient or a user changes the username, password, or dump directory of the dump server.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12001	Minor	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

System can store a maximum of only 50 dump files locally. If the fault persists on the dump server, the local audit logs may be lost, and the first 50 audit logs that exceed the current time cannot be queried.

Possible Causes

- The network connection is abnormal.
- The username, password, or dump directory of the dump server does not meet the configuration conditions.
- The disk space of the dump directory is insufficient.

Handling Procedure

Check whether the network connection is normal.

Step 1 On the FusionInsight Manager home page, choose **Audit > Configurations**.

Step 2 Check whether the SFTP IP on the dump configuration page is valid.

Log in to the node where Manager is located as user **root** and run the **ping** command to check whether the network connection between the SFTP server and the cluster is normal.

- If yes, go to **Step 5**.
- If no, go to **Step 3**.

Step 3 Repair the network connection, reset the SFTP password, and click **OK**.

Step 4 Wait for 2 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check whether the username, password, or dump directory are correct.

Step 5 On the dump configuration page, check whether the username, password, and dump directory of the third-party server are correct.

- If yes, go to **Step 8**.
- If no, go to **Step 6**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 6 Change the username, password, or dump directory, reset the SFTP password and click **OK**.

Step 7 Wait for 2 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Check whether the disk space of the dump directory is sufficient.

Step 8 Log in to the third-party server as user **root** and run the **df** command to check whether the disk space of the dump directory of the third-party server exceeds 100 MB.

- If yes, go to **Step 11**.
- If no, go to **Step 9**.

Step 9 Expand disk space capacity for the third-party server, Reset the SFTP password and click **OK**

Step 10 Wait for 2 minutes, view real-time alarms and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 11**.

Reset the dump rule.

Step 11 On the FusionInsight Manager home page, choose **Audit** > **Configurations**.

Step 12 Reset dump rules, set the parameters properly, and click **OK**.

Step 13 Wait for 2 minutes, view real-time alarms and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 14**.

Collect fault information.

Step 14 On the FusionInsight Manager, choose **O&M**>**Log** > **Download**.

Step 15 Select **OmmServer** from the **Service** and click **OK**.

Step 16 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 17 Contact the technical support and send the collected log information.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.2 ALM-12004 Manager OLdap Resource Abnormal

Alarm Description

The system checks LDAP resources every 60 seconds. This alarm is generated when the system detects that the LDAP resources in Manager are abnormal for six consecutive times.

This alarm is cleared when the Ldap resource in the Manager recovers and the alarm handling is complete.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12004	Major	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
Modify	3.3.1	Alarm Name: changed from "OLdap Resource Abnormal" to "Manager OLdap Resource Abnormal".	Alarm Name: Standardized

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

Manager active/standby switchover may occur. The Manager and WebUI authentication service of components is unavailable. Security authentication and user management functions cannot be provided for upper-layer web services. As a result, you may fail to log in to the Manager and WebUI of components.

Possible Causes

The LdapServer process in the Manager is abnormal.

Handling Procedure

Check whether the LdapServer process in the Manager is normal.

Step 1 Log in the Manager node in the cluster as user **omm**.

Log in to FusionInsight Manager using the floating IP address, and run the **sh ${BIGDATA_HOME}/om-server/om/sbin/status-oms.sh** command to check the information about the current Manager two-node cluster.

Step 2 Run **ps -ef | grep slapd**command to check whether the LdapServer resource process in the**${BIGDATA_HOME}/om-server/om/** in the process configuration file is running properly.

NOTE

You can determine that the resource is normal by checking the following information:

1. After the **sh ${BIGDATA_HOME}/om-server/om/sbin/status-oms.sh**command runs,**ResHAStatus**of the OLdap is**Normal**.
2. After the **ps -ef | grep slapd** command runs, the slapd process of port 21750 can be viewed.
   - If yes, go to **Step 3**.
   - If no, go to **Step 4**.

Step 3 Run the **kill -2***ldap pid* command to restart the LdapServer process and wait for 20 seconds. The HA starts the OLdap process automatically. Check whether the current OLdap resource is in normal state.

- If yes, the operation is complete.
- If no, go to **Step 4**.

Collect fault information.

Step 4 On the FusionInsight Manager home page, choose **O&M**>**Log > Download**.

Step 5 Select **OmsLdapServer**and**OmmServer**from the**Service** and click **OK**.

Step 6 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 7 Contact the technical support and send the collected log information.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.3 ALM-12005 Manager OKerberos Resource Abnormal

Alarm Description

The alarm module checks the status of the Kerberos resource in Manager every 80 seconds. This alarm is generated when the alarm module detects that the Kerberos resources are abnormal for six consecutive times.

This alarm is cleared when the Kerberos resource recovers and the alarm handling is complete.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12005	Major	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
Modify	3.3.1	Alarm Name: changed from "OKerberos Resource Abnormal" to "Manager OKerberos Resource Abnormal".	Alarm Name: Standardized

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

The component WebUI authentication services are unavailable and cannot provide security authentication functions for web upper-layer services. Users may be unable to log in to FusionInsight Manager and the WebUIs of components.

Possible Causes

The OLdap resource on which the Okerberos depends is abnormal.

Handling Procedure

Check whether the OLdap resource on which the Okerberos depends is abnormal in the Manager.

Step 1 Log in the Manager node in the cluster as user **omm**.

Log in to FusionInsight Manager using the floating IP address, and run the **sh ${BIGDATA_HOME}/om-server/om/sbin/status-oms.sh** command to check the information about the current Manager two-node cluster.

Step 2 Run the **sh ${BIGDATA_HOME}/om-server/OMS/workspace0/ha/module/hacom/script/status_ha.sh** command to check whether the OLdap resource status managed by HA is normal. (In single-node mode, the OLdap resource is in the Active_normal state; in the two-node mode, the OLdap resource is in the Active_normal state on the active node and in the Standby_normal state on the standby node.)

- If yes, go to **Step 4**.
- If no, go to **Step 3**.

Step 3 See the procedure in **ALM-12004 Manager OLdap Resource Abnormal** to resolve the problem. After the OLdap resource status recovers, check whether the OKerberos resource status is normal.

- If yes, the operation is complete.
- If no, go to **Step 4**.

Collect fault information.

Step 4 On the FusionInsight Manager home page, choose **O&M**>**Log > Download**.

Step 5 Select **OmsKerberos**and**OmmServer**from the**Service** and click **OK**.

Step 6 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 7 Contact the technical support and send the collected log information.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.4 ALM-12006 NodeAgent Process Is Abnormal

Alarm Description

Controller checks the NodeAgent heartbeat every 30 seconds. If Controller does not receive heartbeat messages from a NodeAgent, it attempts to restart the NodeAgent process. This alarm is generated if the NodeAgent fails to be restarted for three consecutive times.

This alarm is cleared when Controller can properly receive the status report of the NodeAgent.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12006	Major	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.

Type	Parameter	Description
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the details for which the alarm is generated.

Impact on the System

NodeAgent process is abnormal, heartbeat messages cannot be reported to the platform. If the problem is caused by network faults, hardware faults, or SSH mutual trust, component services cannot be normal.

Possible Causes

- The network is disconnected, the hardware is faulty, or the operating system runs slowly.
- The memory of the NodeAgent process is insufficient.
- The NodeAgent process is faulty.
- If the current cluster is a physical machine cluster, the SSH port number of the faulty host is different from that of the active node.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Handling Procedure

Check whether the network is disconnected, whether the hardware is faulty, or whether the operating system runs commands slowly.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. On the page that is displayed, click ⌄ in the row containing the alarm, click the host name, and view the IP address of the host for which the alarm is generated.

Step 2 Log in to the active management node as user **root**.

NOTE

If the faulty node is the active management node and fails login, the network of the active management node may be faulty. In this case, go to **Step 4**.

Step 3 Run the **ping** *IP address of the faulty host* command to check whether the faulty node is reachable.

- If yes, go to **Step 12**.
- If no, go to **Step 4**.

Step 4 Contact the network administrator to check whether the network is faulty.

- If yes, go to **Step 5**.
- If no, go to **Step 6**.

Step 5 Rectify the network fault and check whether the alarm is cleared from the alarm list.

- If yes, no further action is required.
- If no, go to **Step 6**.

Step 6 Contact the hardware administrator to check whether the hardware (CPU or memory) of the node is faulty.

- If yes, go to **Step 7**.
- If no, go to **Step 12**.

Step 7 Repair or replace faulty components and restart the node. Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Step 8 If a large number of node faults are reported in the cluster, the floating IP addresses may be abnormal. As a result, Controller cannot detect the NodeAgent heartbeat.

Log in to any management node and view the **/var/log/Bigdata/omm/oms/ha/scriptlog/floatip.log** log to check whether the logs generated one to two minutes before and after the faults occur are complete.

For example, a complete log is in the following format:

```
2017-12-09 04:10:51,000 INFO (floatip) Read from ${BIGDATA_HOME}/om-server_8.3.1/om/etc/om/
routeSetConf.ini,value is : yes
2017-12-09 04:10:51,000 INFO (floatip) check wsNetExport : eth0 is up.
2017-12-09 04:10:51,000 INFO (floatip) check omNetExport : eth0 is up.
2017-12-09 04:10:51,000 INFO (floatip) check wsInterface : eRth0:oms, wsFloatIp: XXX.XXX.XXX.XXX.
2017-12-09 04:10:51,000 INFO (floatip) check omInterface : eth0:oms, omFloatIp: XXX.XXX.XXX.XXX.
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
2017-12-09 04:10:51,000 INFO (floatip) check  wsFloatIp : XXX.XXX.XXX.XXX is reachable.
2017-12-09 04:10:52,000 INFO (floatip) check  omFloatIp : XXX.XXX.XXX.XXX is reachable.
```

- If yes, go to **Step 12**.
- If no, go to **Step 9**.

Step 9 Check whether the omNetExport log is printed after the wsNetExport is detected or whether the interval for printing two logs exceeds 10 seconds or longer.

- If yes, go to **Step 10**.
- If no, go to **Step 12**.

Step 10 View the **/var/log/message** file of the OS to check whether sssd frequently restarts or nscd exception information is displayed when the fault occurs. For Red Hat, check sssd information. For SUSE, check nscd information.

sssd restart example

```
Feb  7 11:38:16 10-132-190-105 sssd[pam]: Shutting down
Feb  7 11:38:16 10-132-190-105 sssd[nss]: Shutting down
Feb  7 11:38:16 10-132-190-105 sssd[nss]: Shutting down
Feb  7 11:38:16 10-132-190-105 sssd[be[default]]: Shutting down
Feb  7 11:38:16 10-132-190-105 sssd: Starting up
Feb  7 11:38:16 10-132-190-105 sssd[be[default]]: Starting up
Feb  7 11:38:16 10-132-190-105 sssd[nss]: Starting up
Feb  7 11:38:16 10-132-190-105 sssd[pam]: Starting up
```

Example nscd exception information

```
Feb 11 11:44:42 10-120-205-33 nscd: nss_ldap: failed to bind to LDAP server ldaps://10.120.205.55:21780:
Can't contact LDAP server
Feb 11 11:44:43 10-120-205-33 ntpq: nss_ldap: failed to bind to LDAP server ldaps://10.120.205.55:21780:
Can't contact LDAP server
Feb 11 11:44:44 10-120-205-33 ntpq: nss_ldap: failed to bind to LDAP server ldaps://10.120.205.92:21780:
Can't contact LDAP server
```

- If yes, go to **Step 11**.
- If no, go to **Step 12**.

Step 11 Check whether the LdapServer node is faulty, for example, the service IP address is unreachable or the network latency is too high. If the fault occurs periodically, locate and eliminate it and run the **top** command to check whether abnormal software exists.

Check whether the memory of the NodeAgent process is insufficient.

Step 12 Log in to the faulty node as user **root** and run the following command to view the NodeAgent process logs:

vi /var/log/Bigdata/nodeagent/scriptlog/agent_gc.log.*.current

Step 13 Check whether the log file contains an error indicating that the metaspace size or heap memory size is insufficient.

- If yes, go to **Step 14**.
- If no, go to **Step 24**.

Step 14 Run the **su - omm** command to switch to user **omm**, increase the values of **nodeagent.Xms** (initial heap memory) and **nodeagent.Xmx** (maximum heap memory) in the **$NODE_AGENT_HOME/etc/agent/nodeagent.properties** file, and save the modification.

Step 15 Run the following commands to restart the NodeAgent service:

sh ${BIGDATA_HOME}/om-agent/nodeagent/bin/stop-agent.sh

sh ${BIGDATA_HOME}/om-agent/nodeagent/bin/start-agent.sh

Step 16 Wait a moment and check whether this alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 17**.

Check whether the NodeAgent process is faulty.

Step 17 Log in to the faulty node as user **omm** and run the following command:

ps -ef | grep "Dprocess.name=nodeagent" | grep -v grep

Step 18 Check whether the command output is empty.

- If yes, go to **Step 19**.
- If no, go to **Step 21**.

Step 19 View the NodeAgent startup and run logs to locate the fault. After the fault is rectified, go to **Step 20**.

- NodeAgent run logs: **/var/log/Bigdata/nodeagent/agentlog/agent.log**
- NodeAgent start and stop logs: **/var/log/Bigdata/nodeagent/scriptlog/nodeagent_ctl.log**

Step 20 Run the following commands to restart the NodeAgent service:

sh ${BIGDATA_HOME}/om-agent/nodeagent/bin/stop-agent.sh

sh ${BIGDATA_HOME}/om-agent/nodeagent/bin/start-agent.sh

Check whether the SSH port number of the physical machine cluster is inconsistent with that of the active node.

Step 21 Run the **ssh** *host2 IP address* command and check whether the following information is displayed:

```
ssh: connect to host <host2> port <Port number>:Connection refused
```

- If yes, go to **Step 22**.
- If no, go to **Step 24**.

Step 22 Check whether the settings of **Port** in the **/etc/ssh/sshd_config** and **/etc/ssh/ssh_config** files on host2 are the same. Make sure that the settings are the same as those on the active node.

- If yes, go to **Step 24**.
- If no, change the values of **Port** in the **/etc/ssh/sshd_config** and **/etc/ssh/ssh_config** files of host2 to be the same as the value on the active node, and run the following command to restart the sshd process of the faulty host:

  service sshd restart

Step 23 Wait a moment and check whether this alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 24**.

Collect fault information.

Step 24 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 25 Select the following nodes from **Services** and click **OK**.

- NodeAgent
- Controller
- OS

Step 26 Click the edit button in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 27 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.5 ALM-12007 Process Fault

Alarm Description

The process health check module checks the process status every 5 seconds. This alarm is generated when the process health check module detects that the process connection is faulty for three consecutive times.

This alarm is cleared when the process can be connected.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12007	Major	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.

Type	Parameter	Description
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Details	Specifies alarm details.

Impact on the System

The impact varies depending on the instance that is faulty.

For example, if an HDFS instance is faulty, the impacts are as follows:

- If a DataNode instance is faulty, read and write operations cannot be performed on data blocks stored on the DataNode, which may cause data loss or unavailability. However, data in HDFS is redundant. Therefore, the client can access data from other DataNodes.
- If an HttpFS instance is faulty, the client cannot access files in HDFS over HTTP. However, the client can use other methods (such as shell commands) to access files in HDFS.

- If a JournalNode instance is faulty, namespaces and data logs cannot be stored to disks, which may cause data loss or unavailability. However, HDFS stores backups on other JournalNodes. Therefore, the faulty JournalNode can be recovered and data can be rebalanced.
- If a NameNode deployed in active/standby mode is faulty, an active/standby switchover occurs. If only one NameNode is deployed, the client cannot read or write any HDFS data. On MRS, NameNodes must be deployed in two-node mode.
- If a Router instance is faulty, the client cannot access data on the router. However, the client can use other Routers or directly access data on the backend NameNode.
- If a ZKFC instance is faulty, the NameNode does not continuously and automatically fail over. As a result, data cannot be read from or write to HDFS by the client. In this case, you need to enable automatic failover on other available ZKFC instances to restore the HDFS cluster.

Possible Causes

- The instance process is abnormal.
- The drive space is insufficient.

NOTE

If a large number of process fault alarms are reported in the same period, files in the installation directory may be deleted by mistake or the permission may be modified.

Handling Procedure

Check whether the instance process is abnormal.

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**, click ⌄ in the row that contains the target alarm, and record the service name in **Location** Information. Click the hostname to view the IP address of the host for which the alarm is generated.

Step 2 On the **Alarms** page, check whether the "ALM-12006 Abnormal NodeAgent Process" alarm is reported.

- If yes, go to **Step 3**.
- If no, go to **Step 4**.

Step 3 Handle the alarm by following the procedure provided in "ALM-12006 Abnormal NodeAgent Process".

Step 4 Log in to the host for which the alarm is generated as user **root**. Check whether the user, user group, and permission of the installation directory where the alarm role is deployed are correct. The correct user, user group, and the permission are **omm**, **ficommon**, and **750**, respectively.

For example, the NameNode installation directory is **${BIGDATA_HOME}/FusionInsight_Current/1_8_NameNode/etc**.

- If yes, go to **Step 6**.
- If no, go to **Step 5**.

Step 5 Run the following commands to set the permission to **750** and **User:Group** to **omm:ficommon**:

chmod 750 *<folder_name>*

chown omm:ficommon *<folder_name>*

Step 6 Wait 5 minutes and check whether this alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Step 7 Log in to the active OMS node as user **root** and run the following command to view the **configurations.xml** file. In the command, *Service name* indicates the service name queried in **Step 1**.

vi $BIGDATA_HOME/components/current/*Service name***/configurations.xml**

Search for **healthMonitor.properties**, locate the health check configuration of the instance for which the alarm is generated, and record the interface or script path specified by **monitor.info**.

View the logs recorded in the interface or script and rectify the fault.

```
<config category="healthMonitor.properties" format="propertyfileconfigurer">
    <property type="hidden" scope="setup" classification="System">
        <name>monitor.type</name>
        <value>SCRIPT</value>
    </property>
    <property type="hidden" scope="setup" classification="System">
        <name>monitor.preInitDelay</name>
        <value>120000</value>
        <!-- 2min -->
    </property>
    <property type="hidden" scope="setup" classification="System">
        <name>monitor.recheckTimes</name>
        <value>90</value>
        </property>
    <property type="hidden" scope="setup" classification="System">
        <name>monitor.checkIntervals</name>
        <value>10000</value>
    </property>
    <property type="hidden" scope="setup" classification="System">
        <name>monitor.info</name>
        <value>#{install_home}/sbin/dbservice_mon.sh</value>
    </property>
    <property type="hidden" scope="setup" classification="System">
        <name>monitor.metric.connector</name>
        <value>#{install_home}/sbin/dbservice_ha.sh</value>
    </property>
</config>
```

Step 8 Wait for 5 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Check whether the disk space is insufficient.

Step 9 On FusionInsight Manager, check whether the alarm list contains "ALM-12017 Insufficient Disk Capacity".

- If yes, go to **Step 10**.
- If no, go to **Step 13**.

Step 10 Rectify the fault by following the steps provided in "ALM-12017 Insufficient Disk Capacity".

Step 11 Wait 5 minutes and check whether the "ALM-12017 Insufficient Disk Capacity" alarm is cleared.

- If yes, go to **Step 12**.
- If no, go to **Step 13**.

Step 12 Wait for 5 minutes and check whether this alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 13**.

Collect fault information.

Step 13 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 14 Based on the service name obtained in **Step 1**, select the corresponding component and **NodeAgent** in the service list, and click **OK**.

Step 15 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 16 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.6 ALM-12010 Manager Heartbeat Interruption Between the Active and Standby Nodes

Alarm Description

This alarm is generated when the active Mager does not receive the heartbeat signal from the standby Manager within 7 seconds.

This alarm is cleared when the active Manager receives heartbeat signals from the standby Manager.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12010	Major	Heartbeat	Tenant plane	FusionInsight Manager	Yes

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Local Manager HA Name	Specifies a local Manager HA.
	Peer Manager HA Name	Specifies a peer Manager HA.

Impact on the System

When the active Manager process is abnormal, the active/standby switchover cannot be performed, affecting basic O&M functions.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Possible Causes

- The link between the active and standby Manager is abnormal.
- The node name configuration is incorrect.
- The port is disabled by the firewall.

Handling Procedure

Check whether the network between the active and standby Manager server is normal.

Step 1 In the FusionInsight Manager portal, click **O&M > Alarm > Alarms**, click ⌄ in the row containing the alarm and view the IP address of the standby Manager (Peer Manager) server in the alarm details.

Step 2 Log in to the active Manager server as user **root**.

Step 3 Run the **ping** *standby Manager heartbeat IP address* command to check whether the standby Manager server is reachable.

- If yes, go to **Step 6**.
- If no, go to **Step 4**.

Step 4 Contact the network administrator to check whether the network is faulty.

- If yes, go to **Step 5**.
- If no, go to **Step 6**.

Step 5 Rectify the network fault and check whether the alarm is cleared from the alarm list.

- If yes, no further action is required.
- If no, go to **Step 6**.

Step 6 Run the following command to go to the software installation directory:

cd /opt

Step 7 Run the following command to find the configuration file directory of the active and standby nodes.

find -name hacom_local.xml

Step 8 Run the following command to go to the **workspace** directory:

cd${BIGDATA_HOME}/om-server/OMS/workspace0/ha/local/hacom/conf/

Step 9 Run the **vim** command to open the **hacom_local.xml** file. Check whether the local and peer nodes are correctly configured. The local node is configured as the active node, and the peer node is configured as the standby node.

- If yes, go to **Step 12**.
- If no, go to **Step 10**.

Step 10 Modify the configuration of the active and standby nodes in the **hacom_local.xml** file and press **Esc** to return to the command mode. Run the **:wq** command to save the modification and exit.

Step 11 Check whether the alarm is cleared automatically.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If yes, no further action is required.
- If no, go to **Step 12**.

Check whether the port is disabled by the firewall.

Step 12 Run the **lsof -i :20012** command to check whether the heartbeat ports of the active and standby nodes are enabled. If the command output is displayed, the ports are enabled. Otherwise, the ports are disabled by the firewall.

- If yes, go to **Step 13**.
- If no, go to **Step 16**.

Step 13 Run the **iptables -P INPUT ACCEPT** command to avoid the server disconnection.

Step 14 Run the following command to clear the firewall:

iptables -F

Step 15 Check whether the alarm is cleared from the alarm list.

- If yes, no further action is required.
- If no, go to **Step 16**.

Collect fault information.

Step 16 On the FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 17 Select the following nodes from the **Service** and click **OK**:

- OmmServer
- Controller
- NodeAgent

Step 18 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 19 Contact the technical support and send the collected log information.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.7 ALM-12011 Manager Data Synchronization Exception Between the Active and Standby Nodes

Alarm Description

The system checks data synchronization between the active and standby Manager nodes every 60 seconds. This alarm is generated when the standby Manager fails to synchronize files with the active Manager.

This alarm is cleared when the standby Manager synchronizes files with the active Manager.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12011	Critical	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Local Manager HA Name	Specifies a local Manager HA.
	Peer Manager HA Name	Specifies a peer Manager HA.

Impact on the System

The configuration file of the standby Manager is not updated. When an active/standby switchover occurs, the configuration file that fails to be synchronized may be lost. Manager and some components may not run properly.

Possible Causes

- The link between the active and standby Managers is interrupted or The storage space of the **/srv/BigData/LocalBackup** directory is full.
- The synchronization file does not exist or the file permission is incorrect.

Handling Procedure

Check whether the network between the active Manager server and the standby Manager server is normal.

Step 1 In the FusionInsight Manager portal, click **O&M > Alarm > Alarms**, click ⌄ in the row where the alarm is located and obtain the standby Manager server IP address (Peer Manager IP address) in the alarm details.

Step 2 Log in to the active Manager server as user **root**.

Step 3 Run the **ping** *standby Manager IP address* command to check whether the standby Manager server is reachable.

- If yes, go to **Step 6**.
- If no, go to **Step 4**.

Step 4 Contact the network administrator to check whether the network is faulty.

- If yes, go to **Step 5**.
- If no, go to **Step 6**.

Step 5 Rectify the network fault and check whether the alarm is cleared from the alarm list.

- If yes, no further action is required.
- If no, go to **Step 6**.

Check whether the storage space of the /srv/BigData/LocalBackup directory is full.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 6 Run the following command to check whether the storage space of the **/srv/BigData/LocalBackup** directory is full:

df -hl /srv/BigData/LocalBackup

- If yes, go to **Step 7**.
- If no, go to **Step 10**.

Step 7 Run the following command to clear unnecessary backup files:

rm -rf *Directory to be cleared*

Example:

rm -rf /srv/BigData/LocalBackup/0/default-oms_20191211143443

Step 8 On FusionInsight Manager, choose **O&M** > **Backup and Restoration** > **Backup Management**.

In the **Operation** column of the backup task to be performed, click **Configure** and change the value of **Maximum Number of Backup Copies** to reduce the number of backup file sets.

Step 9 Wait about 1 minute and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 10**.

Check whether the synchronization file exists and whether the file permission is normal.

Step 10 Run the following command to check whether the synchronization file exists.

find /srv/BigData/ -name "sed*"

find /opt -name "sed*"

- If yes, go to **Step 11**.
- If no, go to **Step 12**.

Step 11 Run the following command to view the synchronization file information and permission obtained in **Step 10**.

ll *path of the file to be found*

- If the size of the file is 0 and the permission column is **-**, the file is a junk file. Run the following command to delete it.

  rm -rf *files to be deleted*

  Wait for several minutes and check whether the alarm is cleared. If the alarm persists, go to **Step 12**.
- If the file size is not 0, go to **Step 12**.

Step 12 View the log files generated when the alarm is generated.

1. Run the following command to switch to the HA run log file path.

   cd /var/log/Bigdata/omm/oms/ha/runlog/
2. Decompress and view the log files generated when the alarm is generated.

   For example, if the name of the file to be viewed is **ha.log.2021-03-22_12-00-07.gz**, run the following command:

gunzip *ha.log.2021-03-22_12-00-07.gz*

vi *ha.log.2021-03-22_12-00-07*

Check whether error information is reported before and after the alarm generation time.

– If yes, rectify the fault based on the error information. Then go to **Step 13**.

  For example, if the following error information is displayed, the directory permission is insufficient. In this case, change the directory permission to be the same as that on the normal node.

```
[2021-03-22 14:03:35,339][10195489349][0][  INFO][add task((null)) to list successful.][HA][sync_module.c:__SYNC_ActiveTask,1151][ha.bin,26572,35]
[2021-03-22 14:03:35,339][10195489349][0][  INFO][Start Task All_Sync][HA][sync_core_inf.c:SYNC_StartTask,183][ha.bin,26572,35]
[2021-03-22 14:03:35,339][10195489349][0][NOTICE][send sync task(alltask) to component successful][HA][sync_module.c:__SYNC_SendSyncTask,832][ha.bin,26572,35
[2021-03-22 14:03:35,344][10195489353][0][  INFO][open lstat failed:(/opt/Bigdata/apache-tomcat-7.0.78/conf/security/tomcat_om.crt ). Permission denied.][HA]
gt.c:__Create_TravelFname_Open,482][ha.bin,26572,41]
[2021-03-22 14:03:35,344][10195489353][0][ ERROR][Travel stack failed.][HA][sync_filemgt.c:__Create_TravelFname,613][ha.bin,26572,41]
[2021-03-22 14:03:35,344][10195489353][0][ ERROR][mgtcreatelistfail][HA][sync_filemgt.c:_SYNC_CreateFileList,855][ha.bin,26572,41]
[2021-03-22 14:03:35,344][10195489353][0][ ERROR][CreateFileList failed][HA][sync_core.c:__SYNC_Task_SendEnd,1866][ha.bin,26572,41]
[2021-03-22 14:03:35,344][10195489353][0][ ERROR][[41][SendEnd][Task]Failed][HA][sync_core.c:_SYNC_DbgMsgErr,202][ha.bin,26572,41]
[2021-03-22 14:03:35,344][10195489353][0][ ERROR][TaskEnd Failed][HA][sync_core.c:__SYNC_Err_TaskEnd,2720][ha.bin,26572,41]
[2021-03-22 14:03:35,344][10195489353][0][NOTICE][hasendalarm_info: id=1,category=0,cause=0,locainfo=(),addinfo=(),lochost=(node-master1qnFC),locha=(192-168-
```

– If no, go to **Step 14**.

Step 13 Wait about 10 minute and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 14**.

Collect fault information.

Step 14 On the FusionInsight Manager, choose **O&M** > **Log > Download**.

Step 15 Select the following nodes from the **Service** and click **OK**:

- OmmServer
- Controller
- NodeAgent

Step 16 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 17 Contact the technical support and send the collected log information.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.8 ALM-12012 NTP Service Is Abnormal

Alarm Description

The system checks whether the NTP service on a node synchronizes time with the NTP service on the active OMS node every 60 seconds. This alarm is generated when the NTP service fails to synchronize time for two consecutive times.

This alarm is generated when the time difference between the NTP service on a node and the NTP service on the active OMS node is greater than or equal to 20s for two consecutive times. This alarm is cleared when the time difference is less than 20s.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12012	Major	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Details	Specifies alarm details.

Impact on the System

The time on the node is inconsistent with that on other nodes in the cluster. Therefore, some FusionInsight applications on the node may not run properly. If the time difference between the node and other Kerberos service instances keeps increasing, Kerberos authentication on the node may fail and service exceptions occur.

Possible Causes

- The NTP service on the current node cannot start properly.
- The current node fails to synchronize time with the NTP service on the active OMS node.
- The key value authenticated by the NTP service on the current node is inconsistent with that on the active OMS node.
- The time offset between the node and the NTP service on the active OMS node is large.

Handling Procedure

Check the NTP service mode of the node.

Step 1 Log in to the active management node as user **root**, run the **su - omm** command to switch to user **omm**, and run the following command to check the resource status on the active and standby nodes:

sh ${BIGDATA_HOME}/om-server/om/sbin/status-oms.sh

- If "chrony" is displayed in the **ResName** column of the command output, go to **Step 2**.
- If "ntp" is displayed in the **ResName** column, go to **Step 20**.

NOTE

If both "chrony" and "ntp" are displayed in the **ResName** column of the command output, the NTP service mode is being switched. Wait for 10 minutes and go to **Step 1** again. If both "chrony" and "ntp" persist, contact technical support.

Check whether the chrony service on the node is started properly.

Step 2 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. On the page that is displayed, click ⌄ in the row containing the alarm, and view the name of the host for which the alarm is generated in **Location**.

Step 3 Check whether the chronyd process is running on the node where the alarm is generated. Log in to the node for which the alarm is generated as user **root** and

run the **ps -ef | grep chronyd | grep -v grep** command to check whether the command output contains the chronyd process.

- If yes, go to **Step 6**.
- If no, go to **Step 4**.

Step 4 Start the NTP service by running the **systemctl chronyd start** command (supported only by CentOS and Red Hat Enterprise Linux 7.0 or later currently).

Step 5 Check whether the alarm is cleared 10 minutes later.

- If yes, no further action is required.
- If no, go to **Step 6**.

Check whether the current node can synchronize time properly with the chrony service on the active OMS node.

Step 6 Check whether the node can synchronize time with the NTP service on the active OMS node based on additional information of the alarm.

- If yes, go to **Step 7**.
- If no, go to **Step 17**.

Step 7 Check whether the synchronization with the chrony service on the active OMS node is faulty.

Log in to the node for which the alarm is generated as user **root** and run the **chronyc sources** command.

In the command output, if there is an asterisk (*) before the IP address of the chrony service on the active OMS node, the synchronization is normal. The command output is as follows:

```
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================================
^* 10.10.10.162            10  10   377   626    +16us[  +15us] +/-  308us
```

In the command output, if there is no asterisk (*) before the IP address of the NTP service on the active OMS node, and the value of **Reach** is **0**, the synchronization is abnormal.

```
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================================
^? 10.1.1.1                   0  10     0     -     +0ns[   +0ns] +/-    0ns
```

- If yes, go to **Step 8**.
- If no, go to **Step 38**.

Step 8 The chrony synchronization failure is typically caused by the system firewall. If the firewall can be disabled, disable it. If the firewall cannot be disabled, check the firewall configuration policy and ensure that UDP ports 123 and 323 are not disabled. (For details, see the firewall configuration policy of each system.)

Step 9 Check whether the alarm is cleared 10 minutes later.

- If yes, no further action is required.
- If no, go to **Step 10**.

Step 10 Log in to the active OMS node as user **root** and run the following command to view the authentication code whose key value index is **1 SHA256**:

cat ${BIGDATA_HOME}/om-server/OMS/workspace/conf/chrony.keys

Step 11 Run the following command to check whether the key value is the same as that queried in **Step 10**:

diff ${BIGDATA_HOME}/om-server/OMS/workspace/conf/chrony.keys /etc/chrony.keys

NOTE

If the key values are the same, no result is returned after the command is executed. For example:

```
host01:~ # cat ${BIGDATA_HOME}/om-server/OMS/workspace/conf/chrony.keys
1 SHA256 HEX:1991BD2C51403AD3A3BB32601ADA1750
host01:~ # diff ${BIGDATA_HOME}/om-server/OMS/workspace/conf/chrony.keys /etc/chrony.keys
host01:~ #
```

- If yes, go to **Step 12**.
- If no, go to **Step 38**.

Step 12 Run the **cat ${BIGDATA_HOME}/om-server/om/packaged-distributables/chronykeyfile** command to check whether the key value is the same as that queried in **Step 10**. (Compare the key with that of the authentication key index **1 SHA256** queried in **Step 10**.)

- If yes, go to **Step 13**.
- If no, go to **Step 15**.

Step 13 Log in to the faulty node as user **root** and run the **cat /etc/chrony.keys** command to check whether the key is the same as that queried in **Step 12** (compare it with that of the authentication key index **1 SHA256**).

- If yes, go to **Step 38**.
- If no, go to **Step 14**.

Step 14 Run the **su - omm** command to switch to user **omm**, change the key of the authentication key index **1 SHA256** in **${NODE_AGENT_HOME}/chrony.keys** to the key of **chronykeyfile** in **Step 12**, and go to **Step 16**.

Step 15 Run the following commands as user **root** or **omm** to change the NTP key value of the active OMS node (change **ntp.keys** to **ntpkeys** in Red Hat Enterprise Linux):

cd ${BIGDATA_HOME}/om-server/OMS/workspace/conf

sed -i "`cat chrony.keys | grep -n '1 SHA256'|awk -F ':' '{print $1}'`d" chrony.keys

echo "`cat ${BIGDATA_HOME}/om-server/om/packaged-distributables/chronykeyfile`" >> chrony.keys

Check whether the key of the authentication key index **1 SHA256** in **chrony.keys** is the same as that of **chronykeyfile**.

- If yes, go to **Step 16**.
- If no, change the key of the authentication key index **1 SHA256** in **chrony.keys** to the key of **chronykeyfile** and go to **Step 16**.

Step 16 After 5 minutes, run the **service restart chronyd** command to restart the chrony service on the active OMS node. After 15 minutes, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 38**.

Check whether the time deviation between the node and the chrony service on the active OMS node is large.

Step 17 Check whether the time deviation is large in additional information of the alarm.

- If yes, go to **Step 18**.
- If no, go to **Step 38**.

Step 18 On the **Hosts** tab page, select the host for which the alarm is generated, and choose **More** > **Stop All Instances** to stop all the services on the node.

If the time on the alarm node is later than that on the chrony service of the active OMS node, adjust the time of the alarm node. After adjusting the time, choose **More** > **Start All Instances** to start the services on the node.

If the time on the alarm node is earlier than that on the chrony service of the active OMS node, wait until the time deviation is due and adjust the time of the alarm node. After adjusting the time, choose **More** > **Start All Instances** to start the services on the node.

NOTE

If you do not wait, data loss may occur.

Step 19 After 10 minutes, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 38**.

Check whether the NTP service on the node is started properly.

Step 20 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. On the page that is displayed, click ⌄ in the row containing the alarm, and view the name of the host for which the alarm is generated in **Location**.

Step 21 Check whether the ntpd process is running on the node using the following method. Log in to the alarm node as user **root** and run the **ps -ef | grep ntpd | grep -v grep** command to check whether the command output contains the ntpd process.

- If yes, go to **Step 24**.
- If no, go to **Step 22**.

Step 22 Run the **service ntp start** command (or the **service ntpd start** command in Red Hat Enterprise Linux) to start the NTP service.

Step 23 After 10 minutes, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 24**.

Check whether the node can synchronize time properly with the NTP service on the active OMS node.

Step 24 Check whether the node can synchronize time with the NTP service on the active OMS node based on additional information of the alarm.

- If yes, go to **Step 25**.
- If no, go to **Step 35**.

Step 25 Check whether the synchronization with the NTP service on the active OMS node is faulty.

Log in to the alarm node as user **root** and run the **ntpq -np** command.

If an asterisk (*) exists before the IP address of the NTP service on the active OMS node in the command output, the synchronization is in normal state. The command output is as follows:

```
remote refid st t when poll reach delay offset jitter
==============================================================================
*10.10.10.162 .LOCL. 1 u 1 16 377 0.270 -1.562 0.014
```

If there is no asterisk (*) before the IP address of the NTP service on the active OMS node, as shown in the following command output, and the value of **refid** is **.INIT.**, the synchronization is abnormal.

```
remote refid st t when poll reach delay offset jitter
==============================================================================
10.10.10.162 .INIT. 1 u 1 16 377 0.270 -1.562 0.014
```

- If yes, go to **Step 26**.
- If no, go to **Step 38**.

Step 26 The NTP synchronization failure is typically caused by the system firewall. If the firewall can be disabled, run the **iptables -F** command to disable it. If the firewall cannot be disabled, run the **iptables -L** command to check the firewall configuration policy and ensure that the UDP port 123 is not disabled. (For details, see the firewall configuration policy of each system.)

Step 27 After 10 minutes, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 28**.

Step 28 Log in to the active OMS node as user **root** and run the following command to view the authentication key index field **1M**:

In SUSE Linux, run the **cat ${BIGDATA_HOME}/om-server/OMS/workspace/conf/ntp.keys** command.

In Red Hat Enterprise Linux or EulerOS, run the **cat ${BIGDATA_HOME}/om-server/OMS/workspace/conf/ntpkeys** command.

Step 29 Run the following command to check whether the key value is the same as that queried in **Step 28**:

In SUSE Linux, run the **diff ${BIGDATA_HOME}/om-server/OMS/workspace/conf/ntp.keys /etc/ntp.keys** command.

In Red Hat Enterprise Linux or EulerOS, run the **diff ${BIGDATA_HOME}/om-server/OMS/workspace/conf/ntpkeys /etc/ntp/ntpkeys** command.

NOTE

If the key values are the same, no result is returned after the command is executed. For example:

```
host01:~ # cat ${BIGDATA_HOME}/om-server/OMS/workspace/conf/ntp.keys
1 M sdYbq;o^CzEAWo<U=Tw5
host01:~ # diff ${BIGDATA_HOME}/om-server/OMS/workspace/conf/ntp.keys /etc/ntp.keys
host01:~ #
```

- If yes, go to **Step 30**.
- If no, go to **Step 38**.

Step 30 Run the **cat ${BIGDATA_HOME}/om-server/om/packaged-distributables/ntpKeyFile** command to check whether the key value is the same as that queried in **Step 28**. (Compare the key value with that of the authentication key index field **1M** queried in **Step 28**.)

- If yes, go to **Step 31**.
- If no, go to **Step 33**.

Step 31 Log in to the faulty node as user **root** and run the **cat /etc/ntp.keys** command in SUSE Linux (or the **cat /etc/ntp/ntpkeys** command in Red Hat Enterprise Linux) to check whether the key value is the same as the value queried in **Step 30** (use the key value of the authentication key index field **1M** for comparison).

- If yes, go to **Step 38**.
- If no, go to **Step 32**.

Step 32 Run the **su - omm** command to switch to user **omm**, change the key of the authentication key index **1M** in **${NODE_AGENT_HOME}/ntp.keys** (**${NODE_AGENT_HOME}/ntpkeys** in Red Hat Enterprise Linux) to the key of **ntpKeyFile** in **Step 30**, and go to **Step 34**.

Step 33 Run the following commands as user **root** or **omm** to change the NTP key value of the active OMS node (change **ntp.keys** to **ntpkeys** in Red Hat Enterprise Linux):

cd ${BIGDATA_HOME}/om-server/OMS/workspace/conf

sed -i "`cat ntp.keys | grep -n '1 M'|awk -F ':' '{print $1}'`d" ntp.keys

echo "1 M `cat ${BIGDATA_HOME}/om-server/om/packaged-distributables/ntpKeyFile`" >>ntp.keys

Check whether the key value of the authentication key index field **1M** in **ntp.keys** is the same as that of **ntpKeyFile**.

- If yes, go to **Step 34**.
- If no, change the key value of the authentication key index field **1M** in **ntp.keys** to the key value of **ntpKeyFile** and go to **Step 34**.

Step 34 After 5 minutes, run the **service ntpd restart** command to restart the NTP service on the active OMS node. After 15 minutes, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 38**.

Check whether the time deviation between the node and the NTP service on the active OMS node is large.

Step 35 Check whether the time deviation is large in additional information of the alarm.

- If yes, go to **Step 36**.
- If no, go to **Step 38**.

Step 36 On the **Hosts** tab page, select the host for which the alarm is generated, and choose **More** > **Stop All Instances** to stop all the services on the node.

If the time on the alarm node is later than that on the NTP service of the active OMS node, adjust the time of the alarm node. After adjusting the time, choose **More** > **Start All Instances** to start the services on the node.

If the time on the alarm node is earlier than that on the NTP service of the active OMS node, wait until the time deviation is due and adjust the time of the alarm node. After adjusting the time, choose **More** > **Start All Instances** to start the services on the node.

NOTE

If you do not wait, data loss may occur.

Step 37 After 10 minutes, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 38**.

Collect the fault information.

Step 38 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 39 In the **Services** area, select **NodeAgent** and **OmmServer**, and click **OK**. Expand the **Hosts** dialog box and select the alarm node and the active OMS node.

Step 40 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time respectively. Then, click **Download**.

Step 41 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.9 ALM-12014 Device Partition Lost

Alarm Description

This alarm is generated when the system detects that a partition to which service directories are mounted is lost (because the device is removed or offline, or the partition is deleted). The system checks the partition status every 60 seconds.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12014	Major	Physical resource	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	MountDirectoryName	Specifies the directory for which the alarm was generated.
	PartitionName	Specifies the device partition for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Details	Specifies alarm details.
	Disk ESN	Specifies the serial number of the disk in the device partition for which the alarm was generated.

Impact on the System

- Data loss: The device partition is lost and the data stored in the partition is lost.
- System breakdown: If the system disk is lost, the system deployed on the node cannot run properly. In some cases, the system may break down and cannot be started.
- Service failure: Read and write jobs on the lost device partition fail to run or run slowly.
- Service interruption: Customers may need time to restore data and systems, and services cannot be provided.
- Security risk: Important data may be stolen or disclosed, which severely affects customer services.

Possible Causes

- The disk is removed.
- The disk is offline, or a bad sector exists on the disk.

Handling Procedure

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**, and click ⌄ in the row that contains the alarm.

Step 2 Obtain the **HostName**, **PartitionName**, and **DirName** from the **Location** area.

Step 3 Check whether the disk of **PartitionName** on **HostName** is inserted to the correct server slot.

- If yes, go to **Step 4**.
- If no, go to **Step 5**.

Step 4 Contact hardware engineers to remove the faulty disk.

Step 5 Log in to the host for which the alarm is generated as user **root** and check whether the **/etc/fstab** file has a row containing the directory name.

- If yes, go to **Step 6**.
- If no, go to **Step 7**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 6 Run the **vi /etc/fstab** command to edit the file and delete the line containing the mounting directory name.

Step 7 Contact hardware engineers to insert a new disk. For details, see the hardware product document of the relevant model. If the faulty disk is in a RAID group, configure the RAID group. For details, see the configuration methods of the relevant RAID controller card.

Step 8 Wait 20 to 30 minutes (The disk size determines the waiting time), and run the **mount** command to check whether the disk has been mounted to the specified directory.

- If yes, perform **Step 9**.
- If no, go to **Step 10**.

Step 9 Wait 2 minutes and check whether the alarm is automatically cleared.

- If yes, no further action is required.
- If no, go to **Step 10**.

Collect fault information.

Step 10 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 11 Expand the **Service** drop-down list, select **OmmServer** for the target cluster, and click **OK**.

Step 12 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 13 Contact technical support and provide the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears the alarm.

Related Information

None.

1.3.10 ALM-12015 Partition Filesystem Readonly

Alarm Description

The system checks the partition status every 60 seconds. This alarm is generated when the system detects that a partition to which service directories are mounted enters the read-only mode (due to a bad sector or a faulty file system). The system checks the partition status periodically.

This alarm is cleared when the system detects that the partition to which service directories are mounted exits from the read-only mode (because the file system is restored to read/write mode, the device is removed, or the device is formatted).

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12015	Major	Physical resource	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	DirName	Specifies the directory for which the alarm is generated.
	PartitionName	Specifies the device partition for which the alarm is generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the details for which the alarm is generated.
	Disk serial number	Specifies the serial number of the disk of the device partition for which the alarm is generated.

Impact on the System

- Service failure: If a job needs to modify the data on the read-only device partition, the job may fail to run.
- Latency: If some components need to synchronize data to the read-only device partition, data synchronization may fail or time out, causing service delay.

Possible Causes

The hard disk is faulty, for example, a bad sector exists.

Handling Procedure

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**, click ⌄ in the row where the alarm is located.

Step 2 Obtain **HostName** and **PartitionName** from **Location**. **HostName** is the node where the alarm is reported, and **PartitionName** is the partition of the faulty disk.

Step 3 Contact hardware engineers to check whether the disk is faulty. If the disk is faulty, remove it from the server.

Step 4 After the disk is removed, alarm **ALM-12014 Partition Lost** is reported. Handle the alarm. For details, see **ALM-12014 Device Partition Lost**. After the alarm **ALM-12014 Partition Lost** is cleared, alarm **ALM-12015 Partition Filesystem Readonly** is automatically cleared.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

1.3.11 ALM-12016 CPU Usage Exceeds the Threshold

Alarm Description

The system checks the CPU usage every 30 seconds and compares the actual CPU usage with the threshold. The CPU usage has a default threshold. This alarm is generated when the CPU usage exceeds the threshold for several times (configurable, 10 times by default) consecutively.

The alarm is cleared in the following two scenarios: The value of **Trigger Count** is 1 and the CPU usage is smaller than or equal to the threshold; the value of **Trigger Count** is greater than 1 and the CPU usage is smaller than or equal to 90% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12016	Major	Physical resource	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the triggering condition for which the alarm is generated.

Impact on the System

- Latency: If the CPU usage of a host is too high, service processes may run slowly and services may be delayed.
- Service failure: If the host CPU usage is too high, service processing may slow down, time out, or fail. As a result, jobs may fail to run.

Possible Causes

- The alarm threshold or alarm smoothing times are incorrect.
- The CPU configuration cannot meet service requirements, and the CPU usage reaches the upper limit. Or the service is in peak hours. As a result, the CPU usage reaches the upper limit in a short period of time.

Handling Procedure

Check whether the alarm threshold or alarm Trigger Count are correct.

Step 1 Change the alarm threshold and alarm **Trigger Count** based on CPU usage.

On FusionInsight Manager, choose **O&M** > **Alarm** > **Thresholds >** *Name of the desired cluster* > **Host** > **CPU** > **Host CPU Usage** and change the alarm smoothing times based on CPU usage.

NOTE

This option defines the alarm check phase. **Trigger Count** indicates the alarm check threshold. An alarm is generated when the number of check times exceeds the threshold.

On **Host CPU Usage** page and click **Modify** in the **Operation** column to change the alarm threshold, as shown in **Figure 1-3**.

Figure 1-3 Setting an alarm threshold

Step 2 After 2 minutes, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 3**.

Check whether the CPU usage reaches the upper limit.

Step 3 In the alarm list on FusionInsight Manager, click ∨ in the row where the alarm is located to view the alarm host address in the alarm details.

Step 4 On the **Hosts** page, click the node on which the alarm is reported.

Step 5 View the CPU usage for 5 minutes. If the CPU usage exceeds the threshold for multiple times, contact the system administrator to add more CPUs.

Step 6 Check whether the current traffic is in peak hours. If the alarm is generated during peak hours, you are advised to expand the capacity of the node or contact the system administrator to add more CPUs.

Step 7 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Collect fault information.

Step 8 On the FusionInsight Manager in the active cluster, choose **O&M** > **Log** > **Download**.

Step 9 Select **OmmServer** from the **Service** and click **OK**.

Step 10 Set **Start Date** for log collection to 10 minutes ahead of the alarm generation time and **End Date** to 10 minutes behind the alarm generation time in **Time Range** and click **Download**.

Step 11 Contact the technical support and send the collected log information.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.12 ALM-12017 Insufficient Disk Capacity

Alarm Description

The system checks the host disk usage of the system every 30 seconds and compares the actual disk usage with the threshold. The disk usage has a default threshold, this alarm is generated when the host disk usage exceeds the specified threshold.

When the **Trigger Count** is 1, this alarm is cleared when the usage of a host disk partition is less than or equal to the threshold. When the **Trigger Count** is greater than 1, this alarm is cleared when the usage of a host disk partition is less than or equal to 90% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12017	Critical (default threshold: 95%) Major (default threshold: 85%)	Physical resource	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	PartitionName	Specifies the device partition for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the triggering condition for which the alarm is generated.

Impact on the System

Service failure: If you need to modify or use data on the disk when the disk capacity is insufficient, the job may fail.

Possible Causes

- The alarm threshold is incorrect.
- Disk configuration of the server cannot meet service requirements.

Handling Procedure

Check whether the alarm threshold is appropriate.

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Disk** > **Disk Usage** and check whether the threshold (configurable, 90% by default) is appropriate.

- If yes, go to **Step 2**.
- If no, go to **Step 4**.

Step 2 Choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Disk** > **Disk Usage** and click **Modify** in the **Operation** column to change the alarm threshold based on site requirements.

Step 3 After 2 minutes, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 4**.

Check whether the disk usage reaches the upper limit.

Step 4 In the alarm list on FusionInsight Manager, click ⌄ in the row where the alarm is located to view the alarm host name and disk partition information in the alarm details.

Step 5 Log in to the node where the alarm is generated as user **root**.

Step 6 Run the **df -lmPT | awk '$2 != "iso9660"' | grep '^/dev/' | awk '{"readlink -m "$1 | getline real }{$1=real; print $0}' | sort -u -k 1,1** command to check the system disk partition usage. Check whether the disk is mounted to the following directories based on the disk partition name obtained in **Step 4**: **/**, **/opt**, **/tmp**, **/var**, **/var/log**, and **/srv/BigData**(can be customized).

- If yes, the disk is a system disk. Then go to **Step 10**.
- If no, the disk is not a system disk. Then go to **Step 7**.

Step 7 Run the **df -lmPT | awk '$2 != "iso9660"' | grep '^/dev/' | awk '{"readlink -m "$1 | getline real }{$1=real; print $0}' | sort -u -k 1,1** command to check the system disk partition usage. Determine the role of the disk based on the disk partition name obtained in **Step 4**.

Step 8 Check the disk service.

In MRS, check whether the disk service is HDFS, Yarn, Solr, Kafka, or Redis.

- If yes, adjust the capacity. For details, see the *MapReduce Service (MRS) 3.3.1-LTS Physical Machine Cluster Component Migration Guide (for Huawei Cloud Stack 8.3.1)*. Then go to **Step 9**.
- If no, go to **Step 12**.

Step 9 After 2 minutes, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 12**.

Step 10 Run the **find / -xdev -size +500M -execls -l {} \;** command to check whether a file larger than 500 MB exists on the node and disk.

- If yes, go to **Step 11**.

- If no, go to **Step 12**.

Step 11 Handle the large file and check whether the alarm is cleared 2 minutes later.

- If yes, no further action is required.
- If no, go to **Step 12**.

Step 12 Contact the system administrator to expand the disk capacity.

Step 13 After 2 minutes, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 14**.

Collect fault information.

Step 14 On FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 15 Select **OMS** from the **Service** and click **OK**.

Step 16 Click the edit button in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 17 Contact the technical support and send the collected log information.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.13 ALM-12018 Memory Usage Exceeds the Threshold

Alarm Description

The system checks the memory usage of the system every 30 seconds and compares the actual memory usage with the threshold. The memory usage has a default threshold, this alarm is generated when the value of the memory usage exceeds the threshold.

When the **Trigger Count** is 1, this alarm is cleared when the host memory usage is less than or equal to the threshold. When the **Trigger Count** is greater than 1, this alarm is cleared when the host memory usage is less than or equal to 90% of the threshold.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12018	Critical (default threshold: 95%) Major (default threshold: 90%)	Physical resource	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the triggering condition for which the alarm is generated.

Impact on the System

- Latency: If the host memory usage is too high, service processes may run slowly and services may be delayed.
- Service failure: If the host memory usage is too high, memory overflow may occur in service processes and jobs may fail.

Possible Causes

Memory configuration cannot meet service requirements. The memory usage reaches the upper limit.

The SUSE 12.X OS has an earlier **free** command. The calculated memory usage cannot reflect the real-world memory usage.

Handling Procedure

Perform the following operations if SUSE 12.X is used.

Step 1 Log in to any node in the cluster as user **root**, and run the **cat /etc/*-release** command to check whether the OS is SUSE 12.X as user **root**.

- If yes, go to **Step 2**.
- If no, go to **Step 4**.

Step 2 Run the **cat /proc/meminfo | grep Mem** command to check the real-world memory usage of the OS.

```
MemTotal: 263576192 kB
MemFree: 198283116 kB
MemAvailable: 227641452 kB
```

Step 3 Calculate the real-world memory usage: Memory usage = 1 - (Memory available/Memory total)

- If the memory usage is lower than 90%, manually disable transferring from monitoring indicators to alarms. For details, see "Threshold Configuration" in *MapReduce Service (MRS) 3.3.1-LTS User Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Usage Guide (for Huawei Cloud Stack 8.3.1)*.
- If the memory usage is higher than 90%, go to **Step 4**.

Expand the system.

Step 4 In the alarm list on FusionInsight Manager, click ⌄ in the row where the alarm is located to view the alarm host address in the alarm details.

Step 5 Log in to the host where the alarm is generated as user **root**.

Step 6 If the memory usage exceeds the threshold, perform memory capacity expansion. For details, see the *MapReduce Service (MRS) 3.3.1-LTS Physical Machine Cluster Component Migration Guide (for Huawei Cloud Stack 8.3.1) Capacity Expansion Guide (Physical Machine Cluster)*.

Step 7 Run the command **free -m | grep Mem\: | awk '{printf("%s,", $3 * 100 / $2)}'** to check the system memory usage.

Step 8 Wait for 5 minutes, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Collect fault information.

Step 9 On the FusionInsight Manager in the active cluster, choose **O&M** > **Log** > **Download**.

Step 10 Select **OmmServer** from the **Servic**e and click **OK**.

Step 11 Click the edit button in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact the technical support and send the collected log information.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.14 ALM-12027 Host PID Usage Exceeds the Threshold

Alarm Description

The system checks the PID usage every 30 seconds and compares the actual PID usage with the default PID usage threshold. This alarm is generated when the system detects that the PID usage exceeds the threshold.

When the **Trigger Count** is 1, this alarm is cleared when the PID usage is less than or equal to the threshold. When the **Trigger Count** is greater than 1, this alarm is cleared when the PID usage is less than or equal to 90% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12027	Critical (default threshold: 95%) Major (default threshold: 90%)	Environment	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the triggering condition for which the alarm is generated.

Impact on the System

Service failure: If the PID usage of the host is too high, PIDs cannot be allocated to new service processes. As a result, jobs may fail to be executed.

Possible Causes

Too many processes are running on the node. You need to increase the value of **pid_max**.

Handling Procedure

Increase the value of pid_max.

Step 1 In the alarm list on FusionInsight Manager, click ⌄ in the row where the alarm is located to view the alarm host address in the alarm details.

Step 2 Log in to the host where the alarm is generated as user **root**.

Step 3 Run the **cat /proc/sys/kernel/pid_max**command to check the value of **pid_max**.

Step 4 If the PID usage exceeds the threshold, run the command **echo** *new value* **> /proc/sys/kernel/pid_max** to enlarge the value of **pid_max**.

Example: **echo 65536 > /proc/sys/kernel/pid_max**

NOTE

The maximum value of **pid_max** is as follows:

- On 32-bit systems: 32768
- On 64-bit systems: 4194304 (2^22)

Step 5 Wait for 5 minutes, and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On the FusionInsight Manager home page of the active cluster, choose **O&M** > **Log** > **Download**.

Step 7 Select all services from the **Service** and click **OK**.

Step 8 Click the edit button in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact the technical support and send the collected log information.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.15 ALM-12028 Number of Processes in the D State and Z State on a Host Exceeds the Threshold

Alarm Description

The system checks the number of processes in the D state and Z state of user **omm** on the host every 30 seconds and compares the actual number with the threshold. The number of processes in the D state and Z state on the host has a default threshold range. This alarm is generated when the number of processes exceeds the threshold.

This alarm is cleared when the **Trigger Count** is **1** and the total number of processes in the D state and Z state of user **omm** on the host does not exceed the threshold. This alarm is cleared when the **Trigger Count** is greater than **1** and the total number of processes in the D state and Z state of user **omm** on the host is less than or equal to 90% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12028	Major	Environment	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.

Type	Parameter	Description
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger condition	Specifies the alarm triggering condition.

Impact on the System

- Latency: New service processes cannot be created. Concurrent task processing may be slow and services may be delayed.
- Service failure: New service processes cannot be created, which may cause job failures.

Possible Causes

The host responds slowly to I/O (disk I/O and network I/O) requests and some processes are in the D state and Z state.

Handling Procedure

Check the processes in the D state and Z state.

Step 1 In the alarm list on FusionInsight Manager, locate the row that contains the alarm, and click ⌄ to view the IP address of the host for which the alarm is generated.

Step 2 Log in to the host for which the alarm is generated as user **root**. () Then run the **su - omm** command to switch to user **omm**.

Step 3 Run the following command as user **omm** to view the PID of the process that is in the D state and Z state:

ps -elf | grep -v "\[thread_checkio\]" | awk 'NR!=1 {print $2, $3, $4}' | grep omm | awk -F' ' '{print $1, $3}' | grep -E "Z|D" | awk '{print $2}'

Step 4 Check whether the command output is empty.

- If yes, the service process is running properly. Then go to **Step 6**.
- If no, go to **Step 5**.

Step 5 Switch to user **root** and run the **reboot** command to restart the host for which the alarm is generated. (Restarting a host is risky. Ensure that the service process is normal after the restart.)

Step 6 Check whether the alarm is cleared 5 minutes later.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect the fault information.

Step 7 On FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 8 Select **OMS** for **Service** and click **OK**.

Step 9 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.16 ALM-12033 Slow Disk Fault

Alarm Description

- For HDDs, the alarm is triggered when any of the following conditions is met:
  - By default, the system collects data every 3 seconds. The svctm latency reaches 1000 ms within 30 seconds in at least seven collection periods.
  - By default, the system collects data every 3 seconds. At least 50% of detected svctm take no less than 150 ms within 300 seconds.

- For SSDs, the alarm is triggered when any of the following conditions is met:
  - By default, the system collects data every 3 seconds. The svctm latency reaches 1000 ms within 30 seconds in at least seven collection periods.
  - By default, the system collects data every 3 seconds. At least 50% of detected svctm take no less than 20 ms within 300 seconds.

The collection period is 3 seconds, and the detection period is 30 or 300 seconds. This alarm is automatically cleared when none of the preceding conditions are met for three consecutive detection periods (30 or 300 seconds).

NOTE

The **svctm** value can be obtained as follows:

svctm = (tot_ticks_new - tot_ticks_old) / (rd_ios_new + wr_ios_new - rd_ios_old - wr_ios_old)

When the detection period is 30 seconds, if **rd_ios_new + wr_ios_new - rd_ios_old - wr_ios_old = 0**, then **svctm = 0**.

When the detection period is 300 seconds and **rd_ios_new + wr_ios_new - rd_ios_old - wr_ios_old = 0**, if **tot_ticks_new - tot_ticks_old = 0**, then **svctm = 0**; otherwise, the value of **svctm** is infinite.

The parameters can be obtained as follows:

The system runs the **cat /proc/diskstats** command every 3 seconds to collect data.

```
[omm@                    g]$ cat /proc/diskstats
 253       0 vda 1101553 35446 83439787 3338546 28744856 48314024 1054257652 52667332 0 19569526 40342913 0 0 0 0
 253       1 vda1 596970 25494 54533791 2565698 5446004 8749340 215777628 12114542 0 6473883 11339691 0 0 0 0
 253       2 vda2 15 0 108 136 0 0 0 0 0 150 129 0 0 0 0
 253       5 vda5 22373 1364 2525122 79502 4212374 4104759 161597984 8145606 0 3598808 6239095 0 0 0 0
 253       6 vda6 11145 314 529002 85050 259201 70368 4412408 321454 0 189336 259725 0 0 0 0
 253       7 vda7 157987 105 3477434 149542 6507077 1028968 140666992 14349866 0 1679035 11116587 0 0 0 0
 253       8 vda8 312935 8169 22369722 458354 12179958 34360589 531802640 17724858 0 9060731 11385470 0 0 0 0
 253      16 vdb 275920 21939 15977738 2171665 39472291 28236575 2653825040 482230505 0 30580346 465962048 0 0 0 0
 253      17 vdb1 275439 21939 15948866 2171472 31290400 28236555 2653824832 481837775 0 30036724 465855080 0 0 0 0
   7       0 loop0 356 0 17442 150 0 0 0 0 0 149 105 0 0 0 0
[omm@                    ]$ cat /proc/diskstats
 253       0 vda 1101553 35446 83439787 3338546 28747977 48319338 1054352084 52672715 0 19571460 40346640 0 0 0 0
 253       1 vda1 596970 25494 54533791 2565698 5446015 8750402 215791076 12115169 0 6474429 11339985 0 0 0 0
 253       2 vda2 15 0 108 136 0 0 0 0 0 150 129 0 0 0 0
 253       5 vda5 22373 1364 2525122 79502 4212822 4105244 161614088 8146153 0 3599216 6239432 0 0 0 0
 253       6 vda6 11145 314 529002 85050 259245 70433 4413368 321489 0 189389 259730 0 0 0 0
 253       7 vda7 157987 105 3477434 149542 6507759 1029060 140677872 14351373 0 1679157 11117724 0 0 0 0
 253       8 vda8 312935 8169 22369722 458354 12181277 34364199 531855680 17727525 0 9061647 11387424 0 0 0 0
 253      16 vdb 275920 21939 15977738 2171665 39477604 28238831 2653881640 482234435 0 30581946 465964144 0 0 0 0
 253      17 vdb1 275439 21939 15948866 2171472 31293358 28238811 2653881432 481841639 0 30038274 465857164 0 0 0 0
   7       0 loop0 356 0 17442 150 0 0 0 0 0 149 105 0 0 0 0
```

In the data collected for the first time, the number in the fourth column is the **rd_ios_old** value, the number in the eighth column is the **wr_ios_old** value, and the number in the thirteenth column is the **tot_ticks_old** value.

In the data collected for the second time, the number in the fourth column is the **rd_ios_new** value, the number in the eighth column is the **wr_ios_new** value, and the number in the thirteenth column is the **tot_ticks_new** value.

In this case, the value of **svctm** is as follows:

(19571460 - 19569526) / (1101553 + 28747977 - 1101553 - 28744856) = 0.6197

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12033	Minor	Physical resource	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	DiskName	Specifies the disk for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Disk ESN	Specified the serial number of the disk for which the alarm was generated.

Impact on the System

- The system I/O performance deteriorates, which means slow response and low throughput. For example, job submission is slow, page responds slowly, interface response times out, and the system is in error or even crash.

- System fault: Customer services may be interrupted. The system may break down and the key information stored on the faulty disk may be lost.

Possible Causes

The disk is aged or has bad sectors.

Handling Procedure

Check the disk status.

Step 1 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**.

Step 2 View the detailed information about the alarm. Check the values of **HostName** and **DiskName** in the location information to obtain the information about the faulty disk for which the alarm is generated.

Step 3 Check whether the node for which the alarm is generated is in a virtualization environment.

- If yes, go to **Step 4**.
- If no, go to **Step 7**.

Step 4 Check whether the storage performance provided by the virtualization environment meets the hardware requirements. Then, go to **Step 5**.

Step 5 Log in to the alarm node as user **root**, run the **df -h** command, and check whether the command output contains the value of the **DiskName** field.

- If yes, go to **Step 7**.
- If no, go to **Step 6**.

Step 6 Run the **lsblk** command to check whether the mapping between the value of **DiskName** and the disk has been created.

```
sda                    8:0    0 27810G 0
├─sda1                 8:1    0   509M 0 /boot
└─sda2                 8:2    0 278.4G 0
  ├─system-opt (dm-0)  253:0  0    50G 0 /opt
  ├─system-root (dm-1) 253:1  0    50G 0 /
  ├─system-swap (dm-2) 253:2  0    50G 0
  └─system-var (dm-3)  253:3  0    50G 0 /var
```

- If yes, go to **Step 7**. .
- If no, go to **Step 25**.

Step 7 Log in to the alarm node as user **root**, run the **lsscsi | grep "/dev/sd[x]"** command to view the disk information, and check whether RAID has been set up.

NOTE

In the command, **/dev/sd[x]** indicates the disk name obtained in **Step 2**.

Example:

lsscsi | grep "/dev/sda"

In the command output, if **ATA**, **SATA**, or **SAS** is displayed in the third line, the disk has not been organized into a RAID group. If other information is displayed, RAID has been set up.

- If yes, go to **Step 12**.
- If no, go to **Step 8**.

Step 8 Run the **smartctl -i /dev/sd[x]** command to check whether the hardware supports the SMART tool.

Example:

smartctl -i /dev/sda

In the command output, if "SMART support is: Enabled" is displayed, the hardware supports SMART. If "Device does not support SMART" or other information is displayed, the hardware does not support SMART.

- If yes, go to **Step 9**.
- If no, go to **Step 16**.

Step 9 Run the **smartctl -H --all /dev/sd[x]** command to check basic SMART information and determine whether the disk is working properly.

Example:

smartctl -H --all /dev/sda

Check the value of **SMART overall-health self-assessment test result** in the command output. If the value is **FAILED**, the disk is faulty and needs to be replaced. If the value is **PASSED**, check the value of **Reallocated_Sector_Ct** or **Elements in grown defect list**. If the value is greater than 100, the disk is faulty and needs to be replaced.

- If yes, go to **Step 10**.
- If no, go to **Step 18**.

Step 10 Run the **smartctl -l error -H /dev/sd[x]** command to check the Glist of the disk and determine whether the disk is normal.

Example:

smartctl -l error -H /dev/sda

Check the **Command/Feature_name** column in the command output. If **READ SECTOR(S)** or **WRITE SECTOR(S)** is displayed, the disk has bad sectors. If other errors occur, the disk circuit board is faulty. Both errors indicate that the disk is abnormal and needs to be replaced.

If "No Errors Logged" is displayed, no error log exists. You can perform step 9 to trigger the disk SMART self-check.

- If yes, go to **Step 11**.
- If no, go to **Step 18**.

Step 11 Run the **smartctl -t long /dev/sd[x]** command to trigger the disk SMART self-check. After the command is executed, the time when the self-check is to be completed is displayed. After the self-check is completed, repeat **Step 9** and **Step 10** to check whether the disk is working properly.

Example:

smartctl -t long /dev/sda

- If yes, go to **Step 17**.
- If no, go to **Step 18**.

Step 12 Run the **smartctl -d [sat|scsi]+megaraid,[DID] -H --all /dev/sd[x]** command to check whether the hardware supports SMART.

NOTE

- In the command, **[sat|scsi]** indicates the disk type. Both types need to be used.
- **[DID]** indicates the slot information. Slots 0 to 15 need to be used.

For example, run the following commands in sequence:

smartctl -d sat+megaraid,0 -H --all /dev/sda

smartctl -d sat+megaraid,1 -H --all /dev/sda

smartctl -d sat+megaraid,2 -H --all /dev/sda

...

Try the command combinations of different disk types and slot information. If "SMART support is: Enabled" is displayed in the command output, the disk supports SMART. Record the parameters of the disk type and slot information when a command is successfully executed. If "SMART support is: Enabled" is not displayed in the command output, the disk does not support SMART.

- If yes, go to **Step 13**.
- If no, go to **Step 16**.

Step 13 Run the **smartctl -d [sat|scsi]+megaraid,[DID] -H --all /dev/sd[x]** command recorded in **Step 12** to check basic SMART information and determine whether the disk is normal.

Example:

smartctl -d sat+megaraid,2 -H --all /dev/sda

Check the value of **SMART overall-health self-assessment test result** in the command output. If the value is **FAILED**, the disk is faulty and needs to be replaced. If the value is **PASSED**, check the value of **Reallocated_Sector_Ct** or **Elements in grown defect list**. If the value is greater than 100, the disk is faulty and needs to be replaced.

- If yes, go to **Step 14**.
- If no, go to **Step 18**.

Step 14 Run the **smartctl -d [sat|scsi]+megaraid,[DID] -l error -H /dev/sd[x]** command to check the Glist of the disk and determine whether the hard disk is working properly.

Example:

smartctl -d sat+megaraid,2 -l error -H /dev/sda

Check the **Command/Feature_name** column in the command output. If **READ SECTOR(S)** or **WRITE SECTOR(S)** is displayed, the disk has bad sectors. If other

errors occur, the disk circuit board is faulty. Both errors indicate that the disk is abnormal and needs to be replaced.

If "No Errors Logged" is displayed, no error log exists. You can trigger the disk SMART self-check.

- If yes, go to **Step 15**.
- If no, go to **Step 18**.

Step 15 Run the **smartctl -d [sat|scsi]+megaraid,[DID] -t long /dev/sd[x]** command to trigger the disk SMART self-check. After the command is executed, the time when the self-check is to be completed is displayed. After the self-check is completed, repeat **Step 13** and **Step 14** to check whether the disk is working properly.

Example:

smartctl -d sat+megaraid,2 -t long /dev/sda

- If yes, go to **Step 17**.
- If no, go to **Step 18**.

Step 16 If the configured RAID controller card does not support SMART, the disk does not support SMART. In this case, use the check tool provided by the corresponding RAID controller card vendor to rectify the fault. Then go to **Step 17**.

For example, LSI is a MegaCLI tool.

Step 17 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**, click **Clear** in the **Operation** column of the alarm, and check whether the alarm is reported on the same disk again.

If the alarm is reported for three times, replace the disk.

- If yes, go to **Step 18**.
- If no, no further action is required.

Replace the disk.

Step 18 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**.

Step 19 View the detailed information about the alarm. Check the values of **HostName** and **DiskName** in the location information to obtain the information about the faulty disk for which the alarm is reported.

Step 20 Check whether the host for which the alarm is generated is the active OMS node or the active node of the instance in active/standby mode.

- If yes, go to **Step 21**.
- If no, go to **Step 23**.

Step 21 Log in to the node for which the alarm is generated as the **root** user and run the following command to check the mount point of the faulty disk:

df -h | grep "*Name of the faulty disk*"

Check whether the mount point partition of the faulty disk is the cluster software installation directory (**${BIGDATA_HOME}**) or data disk directory (**${BIGDATA_DATA_HOME}** by default).

- If yes, go to **Step 22**.
- If no, go to **Step 23**.

Step 22 Trigger an active/standby switchover to rectify the fault.

- Active OMS node

  If O&M operations cannot be performed due to slow disk faults, such as system freezing, delayed page refreshing, or slow API response, and the alarm is generated for the active OMS node, perform the following operations to trigger an active/standby switchover to restore services:

  a. Log in to the active OMS node as user **omm**.

  b. Run the following command to perform an active/standby switchover:

     - For the IPv4 network: **${OMS_RUN_PATH}/workspace/ha/module/hacom/tools/ha_client_tool --ip=127.0.0.1 --port=20013 --switchover --name=product**
     - For the IPv6 network: **${OMS_RUN_PATH}/workspace/ha/module/hacom/tools/ha_client_tool --ip=::1 --port=20013 --switchover --name=product**

  c. After the active/standby switchover is successful, the system recovers. Perform **Step 23** to replace the faulty disk.

- Active node of an active/standby instance

  If the alarm is generated for the active node of an instance in active/standby mode and the slow disk fault affects the running of the instance, trigger an active/standby switchover on FusionInsight Manager to restore services.

  a. Log in to FusionInsight Manager and choose **Cluster** > **Services** > *Name of the desired service*.

  b. On the service details page, expand the **More** drop-down list and select **Perform** *xxx* **Switchover**.

  c. In the displayed dialog box, enter the password of the current login user and click **OK**.

  d. In the displayed dialog box, click **OK** to perform active/standby switchover.

  e. After the active/standby switchover is successful, the system recovers. Perform **Step 23** to replace the faulty disk.

Step 23 Replace the disk.

Step 24 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 25**.

Collect the fault information.

Step 25 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 26 Select **OMS** for **Service** and click **OK**.

Step 27 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 28 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.17 ALM-12034 Periodical Backup Failure

Alarm Description

The system executes the periodic backup task every 60 minutes. This alarm is generated when a periodical backup task fails to be executed. This alarm is cleared when the next backup task is executed successfully.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12034	Major	Backup status	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	TaskName	Specifies the task.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the details for which the alarm is generated.

Impact on the System

The periodic backup task failed, resulting in no available backup packages during the time period when the backup failed. When a system exception occurs and you need to use the backup package to restore data, no backup package is available during the failure period. As a result, data during the failure period cannot be restored.

Possible Causes

The alarm cause depends on the task details. Handle the alarm according to the logs and alarm details.

Handling Procedure

Check whether the disk space is sufficient.

Step 1 In the FusionInsight Manager portal, click **O&M** > **Alarm** > **Alarms**.

Step 2 In the alarm list, click ⌄ in the row where the alarm is located and obtain **TaskName** from **Location**.

Step 3 Log in to the active node of the cluster as the **root** user and check whether information similar to the following is recorded in backup and restoration logs in **/var/log/Bigdata/controller/backup/**.

```
Upload backup files to *** file failed, error info: ***
```

- If yes, go to **Step 4**.
- If no, go to **Step 7**.

Step 4 On FusionInsight Manager, choose **O&M** > **Backup and Restoration > Backup Management**. Locate the backup task based on **TaskName**, click **Configure** in the **Operation** column, and check whether all configuration items are correctly configured.

- If yes, go to **Step 7**.
- If no, modify the configuration, save the modification, and go to **Step 5**.

Step 5 Choose **More > Back Up Now** to start the backup task and check whether the backup task is successfully executed.

- If yes, go to **Step 6**.
- If no, go to **Step 7**.

Step 6 After 2 minutes, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Step 7 Choose **More > View History** in the **Operation** column. In the displayed dialog box view the task details.

Step 8 In the displayed dialog box and click ⌄ to check whether the following message is displayed: Failed to backup xx due to insufficient disk space, move the data in the xx directory to other directories.

- If yes, go to **Step 9**.
- If no, go to **Step 16**.

Step 9 Choose **Backup Path** > **View** and obtain the **Backup Path**.

Step 10 Log in to the node as user **root** and run the following command to check the node mounting details:

```
df -h
```

Step 11 Check whether the available space of the node to which the backup path is mounted is less than 20 GB.

- If yes, go to **9**.
- If no, go to **Step 16**.

Step 12 Check whether there are many backup packages in the backup directory.

- If yes, go to **Step 13**.
- If no, go to **Step 16**.

Step 13 Enable the available space of the node to which the backup directory is mounted to be greater than 20 GB by moving backup packages out of the backup directory or delete the backup packages.

Step 14 After the problem is resolved, perform the backup task again and check whether the backup task execution is successful.

- If yes, go to **Step 15**.
- If no, go to **Step 16**.

Step 15 After 2 minutes, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 16**.

Collect fault information.

Step 16 On the FusionInsight Manager portal, choose **O&M** > **Log** > **Download**.

Step 17 Select **Controller** from the **Service** and click **OK**.

Step 18 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 19 Contact the technical support and send the collected log information.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.18 ALM-12035 Unknown Data Status After Recovery Task Failure

Alarm Description

After the recovery task fails, the system automatically rolls back every 60 minutes. If the rollback fails, data may be lost. If this occurs, an alarm is reported. This alarm is cleared when the next recovery task execution is successful.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12035	Critical	Backup status	Tenant plane	FusionInsight Manager	Yes

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	TaskName	Specifies the task.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

After the recovery task fails, the system automatically rolls back. If the rollback fails, data may be lost or the data status may be unknown, which may affect services.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Possible Causes

The alarm cause depends on the task details. Handle the alarm according to the logs and alarm details.

Handling Procedure

Collect fault information.

Step 1 In the FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services**, and check whether the running status of the component meets the requirements. (The OMS and DBService must be in the normal state, and other components must be stopped.)

- If yes, go to **Step 9**.
- If no, go to **Step 2**.

Step 2 Restore the component status as required and start the recovery task again.

Step 3 Log in to the FusionInsight Manager portal and click **O&M** > **Alarm** > **Alarms**.

Step 4 In the alarm list, click ⌄ in the row where the alarm is located to obtain **TaskName**from**Location**.

Step 5 Choose **O&M**>**Backup and Restoration** > **Restoration Management**.

Step 6 Find the restoration task by **Task Name** and view the task details.

Step 7 Perform the recovery task again and check whether the recovery task execution is successful.

- If yes, go to **8**.
- If no, go to **9**.

Step 8 After 2 minutes, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **9**.

Collect fault information.

Step 9 On the FusionInsight Manager portal, choose **O&M**>**Log** > **Download**.

Step 10 Select **Controller**from the**Service** and click **OK**.

Step 11 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact the technical support and send the collected log information.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.19 ALM-12037 NTP Server Abnormal

Alarm Description

The system checks the NTP server status every 60 seconds. This alarm is generated when the NTP service mode is **ntp** and the NTP server is abnormal for 10 consecutive times. When the NTP service mode is **chrony**, this alarm is generated when the NTP server is abnormal for 20 consecutive times.

This alarm is cleared when the NTP server recovers.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12037	Major	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the details for which the alarm is generated.

Impact on the System

- The NTP server configured on the active OMS node is abnormal. In this case, the active OMS node cannot synchronize time with the NTP server and a time offset may be generated in the cluster.
- If the time difference exceeds 5 minutes, the client outside the cluster fails to authenticate the client inside the cluster. As a result, the job may fail to run.

Possible Causes

- The NTP server network is abnormal.
- The NTP server authentication fails.
- The NTP server time cannot be obtained.
- The time obtained from the NTP server is not continuously updated.

Handling Procedure

Check the NTP server network.

Step 1 On the FusionInsight Manager portal, click **O&M** > **Alarm** > **Alarms** and click ⌄ in the row where the alarm is located.

Step 2 View the alarm additional information to check whether the NTP server fails to be pinged.

- If yes, go to **Step 3**.
- If no, go to **Step 4**.

Step 3 Contact the network administrator to check the network configuration and ensure that the network between the NTP server and the active OMS node is normal. Then, check whether the alarm is cleared.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If yes, no further action is required.
- If no, go to **Step 4**.

Check whether the NTP server authentication fails.

Step 4 Log in to the active OMS node as user **root**.

Step 5 Run the following command to check the status of the resources on the active and standby nodes:

su - omm

sh ${BIGDATA_HOME}/om-server/om/sbin/status-oms.sh

- If "chrony" is displayed in the **ResName** column of the command output, go to **Step 6**.
- If "ntp" is displayed in the **ResName** column, go to **Step 7**.

NOTE

If both "chrony" and "ntp" are displayed in the **ResName** column of the command output, the NTP service mode is being switched. Wait for 10 minutes and perform **Step 5** again. If both "chrony" and "ntp" still exist in the **ResName** column, contact technical support.

Step 6 Run the command **chronyc sources** to check whether the NTP server authentication fails.

If the value of **Reach** for chrony is **0**, the connection or authentication fails.

- If yes, go to **Step 12**.
- If no, go to **Step 8**.

Step 7 Run the command **ntpq -np** to check whether the NTP server authentication fails.

If **refid** of the NTP server is **.AUTH.**, the authentication fails.

- If yes, go to **Step 12**.
- If no, go to **Step 8**.

Check whether the time can be obtained from the NTP server.

Step 8 View the alarm additional information to check whether the time can be obtained from the NTP server.

- If yes, go to **Step 9**.
- If no, go to **Step 10**.

Step 9 Contact the provider of the NTP server to rectify the NTP server fault. After the NTP server is normal, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 10**.

Check whether the time obtained from the NTP server is not continuously updated.

Step 10 View the alarm additional information to check whether the time obtained from the NTP server is not continuously updated.

- If yes, go to **Step 11**.

- If no, go to **Step 12**.

Step 11 Contact the provider of the NTP server to rectify the NTP server fault. After the NTP server is normal, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 12**.

Collect fault information.

Step 12 On the FusionInsight Manager, choose **O&M**>**Log** > **Download**.

Step 13 Select **NodeAgent**and**OmmServer**from the**Service** and click **OK**.

Step 14 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 15 Contact the technical support and send the collected log information.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.20 ALM-12038 Monitoring Indicator Dumping Failure

Alarm Description

After monitoring indicator dumping is configured on FusionInsight Manager, the system checks the monitoring indicator dumping result at the dumping interval (60 seconds by default). This alarm is generated when the dumping fails.

This alarm is cleared when dumping is successful.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12038	Major	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

The upper-layer management system cannot obtain monitoring indicators from the FusionInsight Manager system.

Possible Causes

- The server cannot be connected.
- The save path on the server cannot be accessed.
- The monitoring indicator file fails to be uploaded.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Handling Procedure

Check whether the server connection is normal.

Step 1 Check whether the network between the FusionInsight Manager system and the server is normal.

- If yes, go to **Step 3**.
- If no, go to **Step 2**.

Step 2 Contact the network administrator to recover the network and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 3**.

Step 3 Choose **System** > **Interconnection** > **Upload Performance Data** and check whether the FTP username, password, port, dump mode, and public key configured on the upload performance data page are consistent with the configuration on the server.

- If yes, go to **Step 5**.
- If no, go to **Step 4**.

Step 4 Enter the correct configuration information, click **OK**, and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check the permission of the save path on the server is correct.

Step 5 Choose **System** > **Interconnection** > **Upload Performance Data** and check the configuration items **FTP Username**, **Save Path**, and **Dump Mode**.

- If the dump mode is FTP, go to **Step 6**.
- If the dump mode is SFTP, go to **Step 7**.

Step 6 Log in to the server in FTP mode. In the default path, check whether **FTP Username** has the read and write permission of the relative path **Save Path**.

- If yes, go to **Step 9**.
- If no, go to **Step 8**.

Step 7 Log in to the server in SFTP mode and check whether **FTP Username** has the read and write permission of the absolute path **Save Path**.

- If yes, go to **Step 9**.
- If no, go to **Step 8**.

Step 8 Add the read and write permission and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Check whether the save path on the server has sufficient disk space.

Step 9 Log in to the server and check whether the save path has sufficient disk space.

- If yes, go to **Step 11**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If no, go to **Step 10**.

Step 10 Delete unnecessary files or go to the monitoring indicator dumping configuration page to change the save path. Then, check whether the save path has sufficient disk space.

- If yes, no further action is required.
- If no, go to **Step 11**.

Collect fault information.

Step 11 On the FusionInsight Manager portal, choose **O&M** > **Log** > **Download**.

Step 12 Select **OMS** from the **Service** and click **OK**.

Step 13 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 14 Contact the technical support and send the collected log information.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.21 ALM-12039 Active/Standby OMS Databases Not Synchronized

Alarm Description

The system checks the data synchronization status between the active and standby OMS Databases every 10 seconds. This alarm is generated when the synchronization status cannot be queried for 30 consecutive times or when the synchronization status is abnormal.

This alarm is cleared when the data synchronization status becomes normal.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12039	Major	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
Modify	3.3.1	Alarm Severity: changed from Critical to Major.	Alarm Severity: Accuracy optimized

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	Local GaussDB HA IP	Specifies the HA IP address of the local GaussDB.
	Peer GaussDB HA IP	Specifies the HA IP address of the peer GaussDB.
	SYNC_PERCENT	Specifies the synchronization percentage.

Impact on the System

If the active/standby of the OMS database is not synchronized, data in the active database cannot be synchronized to the standby database. If the active instance is abnormal during the alarm reporting period, service data may be lost or data on the FusionInsight Manager may be abnormal.

Possible Causes

- The network between the active and standby nodes is unstable.
- The standby OMS Database is abnormal.
- The standby node disk space is full.

Handling Procedure

Check whether the network between the active and standby nodes is normal.

Step 1 Log in to FusionInsight Manager, click **O&M > Alarm > Alarms**, click ⌄ in the row where the alarm is located, and query the standby OMS Database IP address.

Step 2 Log in to the active OMS Database node as user **root**.

Step 3 Run the **ping** *Standby OMS Database heartbeat IP address* command to check whether the standby OMS Database node is reachable.

- If yes, go to **Step 6**.
- If no, go to **Step 4**.

Step 4 Contact the network administrator to check whether the network is faulty.

- If yes, go to **Step 5**.
- If no, go to **Step 6**.

Step 5 Rectify the network fault and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Check whether the standby OMS Database is normal.

Step 6 Log in to the standby OMS Database node as user **root**.

Step 7 Run the **su - omm** command to switch to user **omm**.

Step 8 Go to the **${BIGDATA_HOME}/om-server/om/sbin/** directory and run the **./status-oms.sh** command to check whether the OMS Database resource status of the standby DBService is normal. In the command output, check whether the following information is displayed in the row where **ResName** is **gaussDB**:

For example:

```
10_10_10_231 gaussDB Standby_normal Normal Active_standby
```

- If yes, go to **Step 9**.
- If no, go to **Step 16**.

Check whether the standby node disk space is full.

Step 9 Log in to the standby OMS Database node as user **root**.

Step 10 Run the **su - omm** command to switch to user **omm**.

Step 11 Run the **echo ${BIGDATA_DATA_HOME}/dbdata_om** command to obtain the OMS Database data directory.

Step 12 Run the **df -h** command to view the system disk partition usage information.

Step 13 Check whether the disk where the OMS Database data directory is mounted is full.

- If yes, go to **Step 14**.
- If no, go to **Step 16**.

Step 14 Expand the disk capacity. For details, see the *MapReduce Service (MRS) 3.3.1-LTS Physical Machine Cluster Component Migration Guide (for Huawei Cloud Stack 8.3.1)*.

Step 15 After the disk capacity is expanded, wait 2 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 16**.

Collect fault information.

Step 16 On the FusionInsight Manager portal, choose **O&M** > **Log** > **Download**.

Step 17 Select **OMMServer** from the **Service** and click **OK**.

Step 18 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 19 Contact the technical support and send the collected log information.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.22 ALM-12040 Insufficient OS Entropy

Alarm Description

The system checks whether the rng-tools or haveged tool has been enabled and correctly configured every 5 minutes. If neither tool is configured, this alarm is generated. If either is configured, the system continues to check the entropy. If the entropy is less than 100 for five consecutive times, this alarm is generated.

This alarm is cleared when rng-tools or haveged has been installed and enabled on the target node and the entropy of the OS is greater than or equal to 100 in at least one of five entropy checks.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12040	Critical	Environment	Tenant plane	FusionInsight Manager	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
Modify	3.3.1	Alarm Name: changed from "Insufficient System Entropy" to "Insufficient OS Entropy".	Alarm Name: Standardized

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the details for which the alarm is generated.

Impact on the System

The entropy of the operating system of the node is insufficient. As a result, commands such as encryption and decryption are executed slowly on the node. As a result, the service processing performance of each instance deteriorates, and even service processes cannot be executed properly.

Possible Causes

- rng-tools or haveged has not been installed or started.
- The entropy of the OS is smaller than 100 for multiple consecutive times.

Handling Procedure

Check whether haveged or rng-tools has been installed or started.

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Alarms**.

Step 2 Check the value of **HostName** in the **Location** area to obtain the name of the host for which the alarm is generated.

Step 3 Log in to the node for which the alarm is generated as user **root**.

Step 4 Run the **/bin/rpm -qa | grep -w "haveged"** command to check the haveged installation status and check whether the command output is empty.

- If yes, go to **Step 6**.
- If no, go to **Step 5**.

Step 5 Run the **/sbin/service haveged status |grep "running"** command and check the command output.

- If the command is executed successfully, haveged has been installed and configured correctly and is running properly. Go to **Step 8**.
- If the command fails to execute, haveged is not running properly. Run the following command to manually restart haveged and go to **Step 9**:

  systemctl restart haveged.service

Step 6 Run the **/bin/rpm -qa | grep -w "rng-tools"** command to check the rng-tools installation and check whether the command output is empty.

- If yes, contact the OS vendor to install and start haveged or rng-tools. Then go to **Step 9**.
- If no, go to **Step 7**.

Step 7 Run the **ps -ef | grep -v "grep" | grep rngd | tr -d " " | grep "\-r/dev/urandom"** command and check the command output.

- If the command is executed successfully, rngd has been installed and configured correctly and is running properly. Go to **Step 8**.
- If the command fails to execute, rngd is not running properly. Run the following command to manually restart rngd and go to **Step 9**:

  systemctl restart rngd.service

Check the entropy of the OS.

Step 8 Manually check the entropy of the OS.

Log in to the target node as user **root** and run the **cat /proc/sys/kernel/random/entropy_avail** command to check whether the entropy of the OS meets cluster installation requirements (no less than 100).

- If yes, the entropy of the OS is not less than 100. Go to **Step 9**.
- If no, the entropy of the OS is less than 100. Use either of the following methods and go to **Step 9**.
  - Method 1: Use haveged (true random number mode). Contact the OS vendor to install and start haveged.

    In Kylin, run the following command:

    vi /usr/lib/systemd/system/haveged.service

    Configure **Type**, **ExecStart**, **SuccessExitStatus**, and **Restart** in **[Service]** as follows:

    ```
    Type=simple
    ExecStart=/usr/sbin/haveged -w 1024 -v 1 --Foreground
    SuccessExitStatus=137 143
    Restart=always
    ```

  - Method 2: Use rng-tools (pseudo-random number mode). Contact the OS vendor to install and start rng-tools and configure it based on the OS type.

    - In Red Hat Linux or CentOS, run the following commands:

sed -i 's|EXTRAOPTIONS=.*|EXTRAOPTIONS="-r \/dev\/urandom -o \/dev\/random -t 1 -i"|g' /etc/sysconfig/rngd

vi /usr/lib/systemd/system/rngd.service

Change the value of **ExecStart** in **[Service]** as follows:

```
ExecStart=/sbin/rngd -f -r /dev/urandom -s 2048
```

Run the following command to reload the configuration:

systemctl daemon-reload

Run the following commands to restart the rngd service:

systemctl stop rngd.service

systemctl start rngd.service

Run the following command to enable automatic startup:

chkconfig rngd on

- In SUSE, run the following commands:

  rngd -r /dev/urandom -o /dev/random

  echo "rngd -r /dev/urandom -o /dev/random" >> /etc/rc.d/after.local

- In Kylin, run the following command as user **root** on the node where the alarm is reported:

  vi /usr/lib/systemd/system/rngd.service

  Change the value of **ExecStart** in **[Service]** as follows:

  ```
  ExecStart=/sbin/rngd -f -r /dev/urandom -s 2048
  ```

  Run the following commands to restart the rngd service:

  systemctl stop rngd.service

  systemctl start rngd.service

Step 9 Wait until the system to check the entropy 5 minutes later and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 10**.

Collect fault information.

Step 10 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 11 Expand the **Service** drop-down list, select **NodeAgent** for the target cluster, and click **OK**.

Step 12 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 13 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.23 ALM-12041 Incorrect Permission on Key Files

Alarm Description

The system checks whether the permission, user, and user group information about critical directories or files is normal every 5 minutes. This alarm is generated when the information is abnormal.

This alarm is cleared when the information becomes normal.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12041	Major	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	PathName	Specifies the path or name of the abnormal file.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the details for which the alarm is generated.

Impact on the System

System functions are unavailable.

- If the permission on the okerberos and oldap key files is abnormal, authentication fails and jobs may fail.
- If the permission on the controller and pms key files is abnormal, the process may be faulty, which may affect the elastic scaling performance.
- If the permission on key Tomcat files is abnormal, the login and viewing functions of FusionInsight Manager are affected.

Possible Causes

The file permission is abnormal or the file is lost due to a user manually modified information such as the file permission, user, and user group, or the system is powered off unexpectedly.

Handling Procedure

Check whether the abnormal file exists and whether the permission on the abnormal file is correct.

Step 1 On the FusionInsight Manager portal, choose **O&M > Alarm > Alarms**.

Step 2 Check the value of **HostName** to obtain the host name involved in this alarm. Check the value of **PathName** to obtain the path or name of the abnormal file.

Step 3 Log in to the node for which the alarm is generated as user **root**.

Step 4 Run the **ll** *pathName* command, where *pathName* indicates the name of the abnormal file to obtain the user, permission, and user group information about the file or directory.

Step 5 Go to **${BIGDATA_HOME}/om-agent/nodeagent/etc/agent/autocheck** directory. Then run the **vi keyfile** command and search for the name of the abnormal file and check the due permission of the file.

NOTE

To ensure proper configuration synchronization between the active and standby OMS servers, files, directories, and files and sub-directories in the directories configured in **$OMS_RUN_PATH/workspace/ha/module/hasync/plugin/conf/filesync.xml** will also be monitored except files and directories in **keyfile**. User **omm** must have read and write permissions of files and read and execute permissions of directories.

Step 6 Compare the real-world permission of the file with the due permission obtained in **Step 5** and correct the permission, user, and user group information for the file.

Step 7 Wait a hour and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

NOTE

If the disk partition where the cluster installation directory resides is used up, some temporary files will be generated in the program installation directory when running the **sed** command fails. Users do not have the read, write, and execute permissions of these temporary files. The system reports an alarm indicating that permissions of temporary files are abnormal if these files are within the monitoring range of the alarm. Perform the preceding alarm handling processes to clear the alarm. Alternatively, you can directly delete the temporary files after confirming that files with abnormal permissions are temporary. The temporary file generated after a **sed** command execution failure is similar to the following.

```
-rwx------. 1 omm wheel   347 Jan 26 13:11 REALM_RESET_CONFIG
-rwx------. 1 omm wheel   351 Jan 22 09:07 REALM_RESET_CONFIG_KRB
----------. 1 omm wheel     0 Jan 26 13:15 sedbT8Cs4
-rwx------. 1 omm wheel  7457 Jan 22 03:20 unlockuser.sh
```

Collect fault information.

Step 8 On the FusionInsight Manager portal, choose **O&M** > **Log** > **Download**.

Step 9 Select **NodeAgent** from the **Service** and click **OK**.

Step 10 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 11 Contact the technical support and send the collected log information.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.24 ALM-12042 Incorrect Configuration of Key Files

Alarm Description

The system checks whether critical configurations are correct every 5 minutes. This alarm is generated when the configurations are abnormal.

This alarm is cleared when the configurations become normal.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12042	Major	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	HostName	Specifies the host for which the alarm was generated.
	PathName	Specifies the path or name of the abnormal file.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

Functions related to the file are abnormal.

- If the permission on the okerberos and oldap key files is abnormal, authentication fails and jobs may fail.
- If the permission on the controller and pms key files is abnormal, the process may be faulty, which may affect the elastic scaling performance.
- If the permission on key Tomcat files is abnormal, the login and viewing functions of FusionInsight Manager are affected.

Possible Causes

The file configuration is modified manually or the system is powered off unexpectedly.

Handling Procedure

Check abnormal file configuration.

Step 1 On the FusionInsight Manager portal, choose **O&M > Alarm > Alarms**.

Step 2 Check the value of **HostName** to obtain the host name involved in this alarm. Check the value of **PathName** to obtain the path or name of the abnormal file.

Step 3 Log in to the node for which the alarm is generated as user **root**.

Step 4 View the **${BIGDATA_LOG_HOME}/nodeagent/scriptlog/checkfileconfig.log** file and analyze the cause based on the error log. Locate the check standards of the file in the **Related Information** and manually check and modify the file based on the standards.

Run the **vi** *file name* command to enter the editing mode, and then press **Insert** to start editing.

After the modification is complete, press **Esc** to exit the editing mode and enter **:wq** to save the settings and exit.

For example:

vi /etc/ssh/sshd_config

Step 5 Wait a hour and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On the FusionInsight Manager portal, choose **O&M** > **Log** > **Download**.

Step 7 Select **NodeAgent** from the **Service** and click **OK**.

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact the technical support and send the collected log information.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

- **Check standards of /etc/fstab**

  Check whether the partitions configured in the **/etc/fstab** file can be found in **/proc/mounts**.

  Check whether the swap partitions configured in fstab correspond to those in /proc/swaps.

- **Check the /etc/hosts configuration file.**

  Run **cat /ect/hosts**. If any of the following situations occurs, the **/etc/hosts** configuration file is abnormal:

  a. The **/etc/hosts** file does not exist.

  b. The host name is not configured in the file.

  c. The host name maps to multiple IP addresses in the file.

  d. The IP address corresponding to the host name does not exist in the command output of the **ifconfig** command.

  e. One IP address maps to multiple host names in the file.

- **Check standards of /etc/ssh/sshd_config**

  Run the **vi /etc/ssh/sshd_config** command to check whether configuration items are configured as follows:

  a. The value of **UseDNS** must be set to **no**.

  b. The value of **MaxStartups** must be greater than or equal to 1000.

  c. At least one of the **PasswordAuthentication** and **ChallengeResponseAuthentication** parameters must be left blank or at least one of the parameters be set to **yes**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

1.3.25 ALM-12045 Read Packet Dropped Rate Exceeds the Threshold

Alarm Description

The system checks the read packet dropped rate every 30 seconds. This alarm is generated when the read packet dropped rate exceeds the threshold for multiple times (the default value is **5**).

To change the threshold, choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Network Reading** > **Read Packet Dropped Rate**.

This alarm is cleared when **Trigger Count** is 1 and the read packet dropped rate is less than or equal to the threshold. This alarm is cleared when **Trigger Count** is greater than 1 and the read packet dropped rate is less than or equal to 90% of the threshold.

The alarm detection is disabled by default. If you want to enable this function, check whether this function can be enabled based on Checking System Environments.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12045	Critical (default threshold: 5%) Major (default threshold: 0.5%)	Communications	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	NetworkCard Name	Specifies the network port for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold for triggering the alarm.

Impact on the System

- Latency: When the read packet loss rate of the host network exceeds the threshold, request response is slowed down and services are delayed.
- Service failure: When the read packet loss rate of the host network exceeds the threshold, requests cannot be properly responded or times out, which may cause job running failures.

Risk warning: In SUSE kernel 3.0 or later or Red Hat 7.2, the system kernel modifies the mechanism for counting the number of dropped read packets. In this case, this alarm may be generated even if the network is running properly, but services are not affected. You are advised to check the system environment first.

Possible Causes

- An OS exception occurs.
- The NICs are bonded in active/standby mode.

- The alarm threshold is improperly configured.
- The network quality is poor.

Handling Procedure

View the network packet dropped rate.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. On the page that is displayed, click ⌄ in the row containing the alarm, and view the name of the host for which the alarm is generated and the NIC name.

Step 2 Log in to the alarm node as user **omm**, and run the **/sbin/ifconfig** *NIC name* command to check whether packet loss occurs on the network.

```
omm@          :~> /sbin/ifconfig eth2
eth2      Link encap:Ethernet  HWaddr E4:35:C8:7B:B5:48
          inet addr:192.168        Bcast:192.168        Mask:255.255.0.0
          inet6 addr: fe80::e635:c8ff:fe7b:b548/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5254854 errors:0 dropped:214676 overruns:0 frame:0
          TX packets:329443 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:354839633 (338.4 Mb)  TX bytes:25083094 (23.9 Mb)
```

NOTE

- *IP address of the node for which the alarm is generated*: Query the IP address of the node for which the alarm is generated on the **Hosts** page of FusionInsight Manager based on the value of **HostName** in the alarm location information. Check both the IP addresses of the management plane and service plane.
- Packet loss rate = (Number of dropped packets/Total number of received packets) x 100%. If the packet loss rate is greater than the system threshold, read packets are dropped.

- If yes, go to **Step 11**.
- If no, go to **Step 3**.

Check the system environment.

Step 3 Log in to the active OMS node or the alarm node as user **omm**.

Step 4 Run the **cat /etc/*-release** command to check the OS type.

- For Red Hat Enterprise Linux, go to **Step 5**.
```
# cat /etc/*-release
Red Hat Enterprise Linux Server release 7.2 (Santiago)
```
- For SUSE Linux, go to **Step 6**.
```
# cat /etc/*-release
SUSE Linux Enterprise Server 11 (x86_64)
VERSION = 11
PATCHLEVEL = 3
```
- For other OS types, go to **Step 11**.

Step 5 Run the **cat /etc/redhat-release** command to check whether the OS version is **Red Hat 7.2 (x86)** or **Red Hat 7.4 (KunPeng)**.

```
# cat /etc/redhat-release
Red Hat Enterprise Linux Server release 7.2 (Santiago)
```

- If yes, the alarm sending function cannot be enabled. Go to **Step 7**.
- If no, go to **Step 11**.

Step 6 Run the **cat /proc/version** command to check whether the SUSE kernel version is 3.0 or later.

```
# cat /proc/version
Linux version 3.0.101-63-default (geeko@buildhost) (gcc version 4.3.4 [gcc-4_3-branch revision 152973]
(SUSE Linux) ) #1 SMP Tue Jun 23 16:02:31 UTC 2015 (4b89d0c)
```

- If yes, the alarm sending function cannot be enabled. Go to **Step 7**.
- If no, go to **Step 11**.

Step 7 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Threshold Configuration**.

Step 8 In the navigation tree of the **Thresholds** page, choose *Name of the desired cluster* > **Host** > **Network Reading** > **Read Packet Dropped Rate**. In the area on the right, check whether the **Switch** is toggled on.

- If yes, the alarm sending function is enabled. Go to **Step 9**.
- If no, the alarm sending function is disabled. Go to **Step 10**.

Step 9 In the area on the right, toggle **Switch** off to disable the checking of **Network Read Packet Dropped Rate Exceeds the Threshold**.

Step 10 On the **Alarm** page of FusionInsight Manager, search for alarm **12045** and manually clear the alarm if it is not automatically cleared. No further action is required.

NOTE

ID of the Network Read Packet Dropped Rate Exceeds the Threshold alarm is **12045**.

Check whether the NICs are bonded in active/standby mode.

Step 11 Log in to the alarm node as user **omm** and run the **ls -l /proc/net/bonding** command to check whether the **/proc/net/bonding** directory exists on the node.

- If yes, the bond mode is configured for the node. Go to **Step 12**.

```
# ls -l /proc/net/bonding/
total 0
-r--r--r-- 1 root root 0 Oct 11 17:35 bond0
```

- If no, the bond mode is not configured for the node. Go to **Step 14**.

```
# ls -l /proc/net/bonding/
ls: cannot access /proc/net/bonding/: No such file or directory
```

Step 12 Run the **cat /proc/net/bonding/***bond0* command to check whether the value of **Bonding Mode** in the configuration file is **fault-tolerance**.

NOTE

In the command, **bond0** indicates the name of the bond configuration file. Use the file name obtained in **Step 11**.

```
# cat /proc/net/bonding/bond0
Ethernet Channel Bonding Driver: v3.7.1 (April 27, 2011)

Bonding Mode: fault-tolerance (active-backup)
Primary Slave: eth1 (primary_reselect always)
Currently Active Slave: eth1
MII Status: up
MII Polling Interval (ms): 100
Up Delay (ms): 0
Down Delay (ms): 0

Slave Interface: eth0
MII Status: up
Speed: 1000 Mbps
Duplex: full
Link Failure Count: 1
Slave queue ID: 0

Slave Interface: eth1
MII Status: up
Speed: 1000 Mbps
Duplex: full
Link Failure Count: 1
Slave queue ID: 0
```

- If yes, the NICs are bonded in active/standby mode. Go to **Step 13**.
- If no, go to **Step 14**.

Step 13 Check whether the NIC specified by **NetworkCardName** in the alarm is the standby NIC.

- If yes, the alarm of the standby NIC cannot be automatically cleared. Manually clear the alarm on the alarm management page. No further action is required.
- If no, go to **Step 14**.

NOTE

To determine the standby NIC, check the **/proc/net/bonding/bond0** configuration file. If the NIC name corresponding to **NetworkCardName** is **Slave Interface** but not **Currently Active Slave** (the current active NIC), the NIC is the standby one.

Check whether the threshold is set properly.

Step 14 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Network Reading** > **Read Packet Dropped Rate**, and check whether the alarm threshold is configured properly. The default value is **0.5%**. You can adjust the threshold as needed.

- If yes, go to **Step 17**.
- If no, go to **Step 15**.

Step 15 Choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Network Reading** > **Read Packet Dropped Rate**. Click **Modify** in the **Operation** column to change the threshold.

Step 16 After 5 minutes, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 17**.

Check whether the network connection is normal.

Step 17 Contact the network administrator to check whether the network is normal.

- If yes, rectify the fault and go to **Step 18**.
- If no, go to **Step 19**.

Step 18 After 5 minutes, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 19**.

Collect the fault information.

Step 19 On FusionInsight Manager of the active cluster, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 20 Select **OMS** for **Service** and click **OK**.

Step 21 Expand the **Hosts** dialog box and select the alarm node and the active OMS node.

Step 22 Click the edit button in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time respectively. Then, click **Download**.

Step 23 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.26 ALM-12046 Write Packet Dropped Rate Exceeds the Threshold

Alarm Description

The system checks the write packet dropped rate every 30 seconds. This alarm is generated when the write packet dropped rate exceeds the threshold for multiple times (the default value is **5**).

To change the threshold, choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Network Writing** > **Write Packet Dropped Rate**.

If **Trigger Count** is **1**, this alarm is cleared when the network write packet dropped rate is less than or equal to the threshold. If **Trigger Count** is greater than **1**, this alarm is cleared when the network write packet dropped rate is less than or equal to 90% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12046	Critical (default threshold: 5%) Major (default threshold: 0.5%)	Communications	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	Port Name	Specifies the network port for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger condition	Specifies the alarm triggering condition.

Impact on the System

- Latency: Requests are responded slowly and services are delayed.
- Service failure: Requests cannot be responded or time out. Jobs may fail to run.

Possible Causes

- The alarm threshold is improperly configured.
- The network quality is poor.

Handling Procedure

Check whether the threshold is set properly.

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Network Writing** > **Write Packet Dropped Rate**, and check whether the alarm threshold is configured properly. The default value is **0.5%**. You can adjust the threshold as needed.

- If yes, go to **Step 4**.
- If no, go to **Step 2**.

Step 2 Choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Network Writing** > **Write Packet Dropped Rate**. Click **Modify** in the **Operation** column to change the threshold.

Step 3 After 5 minutes, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 4**.

Check whether the network connection is normal.

Step 4 Contact the network administrator to check whether the network is normal.

- If yes, rectify the fault and go to **Step 5**.
- If no, go to **Step 6**.

Step 5 After 5 minutes, check whether the alarm is cleared.

- If yes, no further action is required.

- If no, go to **Step 6**.

Collect the fault information.

Step 6 On FusionInsight Manager of the active cluster, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Select **OMS** for **Service** and click **OK**.

Step 8 Expand the **Hosts** dialog box and select the alarm node and the active OMS node.

Step 9 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.27 ALM-12047 Read Packet Error Rate Exceeds the Threshold

Alarm Description

The system checks the read packet error rate every 30 seconds. This alarm is generated when the read packet error rate exceeds the threshold for multiple times (the default value is **5**).

To change the threshold, choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Network Reading** > **Read Packet Error Rate**.

If **Trigger Count** is **1**, this alarm is cleared when the read packet error rate is less than or equal to the threshold. If **Trigger Count** is greater than **1**, this alarm is cleared when the read packet error rate is less than or equal to 90% of the threshold.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12047	Critical (default threshold: 5%) Major (default threshold: 0.5%)	Communications	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	Port Name	Specifies the network port for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger condition	Specifies the alarm triggering condition.

Impact on the System

- Latency: Requests are responded slowly and services are delayed.
- Service failure: Requests cannot be responded or time out. Jobs may fail to run.

Possible Causes

- The alarm threshold is improperly configured.
- The network quality is poor.

Handling Procedure

Check whether the threshold is set properly.

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Network Reading** > **Read Packet Error Rate**, and check whether the alarm threshold is configured properly. The default value is **0.5%**. You can adjust the threshold as needed.

- If yes, go to **Step 4**.
- If no, go to **Step 2**.

Step 2 Choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Network Reading** > **Read Packet Error Rate**. Click **Modify** in the **Operation** column to change the threshold.

Step 3 After 5 minutes, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 4**.

Check whether the network connection is normal.

Step 4 Contact the network administrator to check whether the network is normal.

- If yes, rectify the fault and go to **Step 5**.
- If no, go to **Step 6**.

Step 5 After 5 minutes, check whether the alarm is cleared.

- If yes, no further action is required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If no, go to **Step 6**.

Collect the fault information.

Step 6 On FusionInsight Manager of the active cluster, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Select **OMS** for **Service** and click **OK**.

Step 8 Expand the **Hosts** dialog box and select the alarm node and the active OMS node.

Step 9 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.28 ALM-12048 Write Packet Error Rate Exceeds the Threshold

Alarm Description

The system checks the write packet error rate every 30 seconds. This alarm is generated when the write packet error rate exceeds the threshold for multiple times (the default value is **5**).

To change the threshold, choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Network Writing** > **Write Packet Error Rate**.

If **Trigger Count** is **1**, this alarm is cleared when the write packet error rate is less than or equal to the threshold. If **Trigger Count** is greater than **1**, this alarm is cleared when the write packet error rate is less than or equal to 90% of the threshold.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12048	Critical (default threshold: 5%) Major (default threshold: 0.5%)	Communications	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	Port Name	Specifies the network port for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger condition	Specifies the alarm triggering condition.

Impact on the System

- Latency: Requests are responded slowly and services are delayed.
- Service failure: Requests cannot be responded or time out. Jobs may fail to run.

Possible Causes

- The alarm threshold is improperly configured.
- The network quality is poor.

Handling Procedure

Check whether the threshold is set properly.

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Network Writing** > **Write Packet Error Rate**, and check whether the alarm threshold is configured properly. The default value is **0.5%**. You can adjust the threshold as needed.

- If yes, go to **Step 4**.
- If no, go to **Step 2**.

Step 2 Choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Network Writing** > **Write Packet Error Rate**. Click **Modify** in the **Operation** column to change the threshold.

Step 3 After 5 minutes, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 4**.

Check whether the network connection is normal.

Step 4 Contact the network administrator to check whether the network is normal.

- If yes, rectify the fault and go to **Step 5**.
- If no, go to **Step 6**.

Step 5 After 5 minutes, check whether the alarm is cleared.

- If yes, no further action is required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If no, go to **Step 6**.

Collect the fault information.

Step 6 On FusionInsight Manager of the active cluster, choose **O&M** > **Log** > **Download**.

Step 7 Select **OMS** for **Service** and click **OK**.

Step 8 Expand the **Hosts** dialog box and select the alarm node and the active OMS node.

Step 9 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.29 ALM-12049 Network Read Throughput Rate Exceeds the Threshold

Alarm Description

The system checks the network read throughput rate every 30 seconds and compares the actual throughput rate with the threshold (the default threshold is 80%). This alarm is generated when the system detects that the network read throughput rate exceeds the threshold for several times (5 times by default) consecutively.

To change the threshold, choose **O&M > Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Network Reading** > **Read Throughput Rate**.

When the **Trigger Count** is 1, this alarm is cleared when the network read throughput rate is less than or equal to the threshold. When the **Trigger Count** is greater than 1, this alarm is cleared when the network read throughput rate is less than or equal to 90% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12049	Major	Communications	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	NetworkCardName	Specifies the network port for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold for triggering the alarm.

Impact on the System

- Latency: When the host network read throughput exceeds the threshold, the request response slows down, causing service delay.

- Service failure: When the host network read throughput exceeds the threshold, requests cannot be properly responded or timed out, which may cause job execution failures.

Possible Causes

- The alarm threshold is set improperly.
- The network port rate cannot meet the current service requirements.

Handling Procedure

Check whether the threshold is set properly.

Step 1 On the FusionInsight Manager, choose **O&M > Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Network Reading** > **Read Throughput Rate** and check whether the alarm threshold is set properly. (By default, 80% is a proper value. However, users can configure the value as required.)

- If yes, go to **Step 2**.
- If no, go to **Step 4**.

Step 2 Based on actual usage condition, choose **O&M > Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Network Reading** > **Read Throughput Rate** and click **Modify** in the **Operation** column to modify the alarm threshold.

Step 3 Wait for 5 minutes, and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 4**.

Check whether the network port rate can meet the service requirements.

Step 4 On FusionInsight Manager, click ⌄ in the row where the alarm is located in the real-time alarm list and obtain the IP address of the host and the network port name for which the alarm is generated.

Step 5 Log in to the host for which the alarm is generated as user **root**.

Step 6 Run the **ethtool** *network port name* command to check the maximum speed of the current network port.

NOTE

In the VM environment, you cannot run a command to query the network port rate. It is recommended that you contact the system administrator to confirm whether the network port rate meets the requirements.

Step 7 If the network read throughput rate exceeds the threshold, contact the system administrator to increase the network port rate.

Step 8 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Collect fault information.

Step 9 On the FusionInsight Manager home page of the active cluster, choose **O&M** > **Log > Download**.

Step 10 Select **OMS** from the **Service** and click **OK**.

Step 11 Set **Host** to the node for which the alarm is generated and the active OMS node.

Step 12 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 13 Contact the technical support and send the collected log information.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.30 ALM-12050 Network Write Throughput Rate Exceeds the Threshold

Alarm Description

The system checks the network write throughput rate every 30 seconds and compares the actual throughput rate with the threshold (the default threshold is 80%). This alarm is generated when the system detects that the network write throughput rate exceeds the threshold for several times (5 times by default) consecutively.

To change the threshold, choose **O&M > Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Network Writing** > **Write Throughput Rate**.

When the **Trigger Count** is 1, this alarm is cleared when the network write throughput rate is less than or equal to the threshold. When the **Trigger Count** is greater than 1, this alarm is cleared when the network write throughput rate is less than or equal to 90% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12050	Major	Communications	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	NetworkCardName	Specifies the network port for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold for triggering the alarm.

Impact on the System

- Latency: When the host network write throughput exceeds the threshold, the request response is slowed down and services are delayed.

- Service failure: When the host network write throughput exceeds the threshold, requests cannot be responded or times out, which may cause job running failures.

Possible Causes

- The alarm threshold is set improperly.
- The network port rate cannot meet the current service requirements.

Handling Procedure

Check whether the threshold is set properly.

Step 1 On the FusionInsight Manager, choose **O&M > Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Network Writing** > **Write Throughput Rate** and check whether the alarm threshold is set properly. (By default, 80% is a proper value. However, users can configure the value as required.)

- If yes, go to **Step 4**.
- If no, go to **Step 2**.

Step 2 Based on actual usage condition, choose **O&M > Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Network Writing** > **Write Throughput Rate** and click **Modify** in the **Operation** column to modify the alarm threshold.

Step 3 Wait for 5 minutes, and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 4**.

Check whether the network port rate can meet the service requirements.

Step 4 On FusionInsight Manager, click ⌄ in the row where the alarm is located in the real-time alarm list and obtain the IP address of the host and the network port name for which the alarm is generated.

Step 5 Log in to the host for which the alarm is generated as user **root**.

Step 6 Run the **ethtool***network port name* command to check the maximum speed of the current network port.

NOTE

In the VM environment, you cannot run a command to query the network port rate. It is recommended that you contact the system administrator to confirm whether the network port rate meets the requirements.

Step 7 If the network write throughput rate exceeds the threshold, contact the system administrator to increase the network port rate.

Step 8 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Collect fault information.

Step 9 On the FusionInsight Manager home page of the active cluster, choose **O&M** > **Log > Download**.

Step 10 Select **OMS** from the **Service** and click **OK**.

Step 11 Set **Host** to the node for which the alarm is generated and the active OMS node.

Step 12 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 13 Contact the technical support and send the collected log information.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.31 ALM-12051 Disk Inode Usage Exceeds the Threshold

Alarm Description

The system checks the disk Inode usage every 30 seconds and compares the actual Inode usage with the threshold. This alarm is generated when the Inode usage exceeds the threshold for several times (5 times by default) consecutively.

To change the threshold, choose **O&M > Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Disk** > **Disk Inode Usage**.

When the **Trigger Count** is 1, this alarm is cleared when the disk Inode usage is less than or equal to the threshold. When the **Trigger Count** is greater than 1, this alarm is cleared when the disk Inode usage is less than or equal to 90% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12051	Critical (default threshold: 95%) Major (default threshold: 80%)	Physical resource	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	PartitionName	Specifies the disk partition for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold for triggering the alarm.

Impact on the System

Service failure: If you need to modify or use data on the disk when data cannot be written to the file system, the job may fail.

Possible Causes

Massive small files are stored in the disk.

Handling Procedure

Massive small files are stored in the disk.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** and click ⌄ in the row where the alarm is located in the real-time alarm list and obtain the IP address of the host and the disk partition for which the alarm is generated.

Step 2 Log in to the host for which the alarm is generated as user **root**.

Step 3 Run the **df -i | grep -iE "***partition name***|**Filesystem" command to check the current disk Inode usage.

```
# df -i | grep -iE "xvda2|Filesystem"
Filesystem          Inodes   IUsed   IFree IUse% Mounted on
/dev/xvda2          2359296  207420 2151876    9% /
```

Step 4 If the Inode usage exceeds the threshold, manually check small files stored in the disk partition and confirm whether these small files can be deleted.

NOTE

Run the **for i in /*; do echo $i; find $i|wc -l; done** command to query the number of files in a partition. Replace **/*** with the specified partition.

```
# for i in /srv/*; do echo $i; find $i|wc -l; done
/srv/BigData
4284
/srv/ftp
1
/srv/www
13
```

- If yes, run the **rm -rf** *Path of the file or folder* to be deleted command to delete the file or folder and go to **Step 5**.

  NOTE

  Deleting a file or folder is a high-risk operation. Ensure that the file or folder is no longer required before performing this operation.

- If no, expand the capacity by following the instructions of step 1 to step 4 in section **Adding New Disks to an Existing Node** of the *MapReduce Service (MRS) 3.3.1-LTS Physical Machine Cluster Component Migration Guide (for Huawei Cloud Stack 8.3.1)*. Then, perform **Step 5**.

Step 5 Wait for 5 minutes, and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On the FusionInsight Manager home page of the active cluster, choose **O&M** > **Log** > **Download**.

Step 7 Select **OMS** from the **Service** and click **OK**.

Step 8 Set **Host** to the node for which the alarm is generated and the active OMS node.

Step 9 Click the edit button in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact the technical support and send the collected log information.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.32 ALM-12052 TCP Temporary Port Usage Exceeds the Threshold

Alarm Description

The system checks the TCP temporary port usage every 30 seconds and compares the actual usage with the threshold. This alarm is generated when the TCP temporary port usage exceeds the threshold for several times (5 times by default) consecutively.

To change the threshold, choose **O&M > Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Network Status** > **TCP Ephemeral Port Usage**.

When the **Trigger Count** is 1, this alarm is cleared when the TCP temporary port usage is less than or equal to the threshold. When the **Trigger Count** is greater than 1, this alarm is cleared when the TCP temporary port usage is less than or equal to 90% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12052	Critical (default threshold: 95%) Major (default threshold: 80%)	Environment	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold for triggering the alarm.

Impact on the System

Services on the host cannot establish external connections, and therefore they are interrupted.

Possible Causes

- The temporary port cannot meet the current service requirements.

- The system is abnormal.

Handling Procedure

Expand the temporary port number range.

Step 1 On FusionInsight Manager, click ⌄ in the row where the alarm is located in the real-time alarm list and obtain the IP address of the host for which the alarm is generated.

Step 2 Log in to the host for which the alarm is generated as user **omm**.

Step 3 Run the **cat /proc/sys/net/ipv4/ip_local_port_range |cut -f 1** command to obtain the value of the start port and run the **cat /proc/sys/net/ipv4/ip_local_port_range |cut -f 2** command to obtain the value of the end port. The total number of temporary ports is the value of the end port minus the value of the start port. If the total number of temporary ports is smaller than 28,232, the random port range of the OS is narrow. Contact the system administrator to increase the port range.

Step 4 Run the following command to calculate the number of used temporary ports.

ss -ant 2>/dev/null | grep -v LISTEN | awk 'NR > 2 {print $4}'| awk -F':' '{print $NF}' | awk '$1 >"*Value of the start port***" {print $1}' | sort -u | wc -l**

Step 5 The formula for calculating the usage of the temporary ports is: Usage of the temporary ports = (Number of used temporary ports/Total number of temporary ports) x 100%. Check whether the temporary port usage exceeds the threshold.

- If yes, go to **Step 7**.
- If no, go to **Step 6**.

Step 6 Wait for 5 minutes, and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Check whether the system environment is abnormal.

Step 7 Run the following command to import the temporary file and view the frequently used ports in the **port_result.txt file**:

netstat -tnp|sort > $BIGDATA_HOME/tmp/port_result.txt

```
netstat -tnp|sort

Active Internet connections (w/o servers)

Proto Recv Send LocalAddress ForeignAddress State PID/ProgramName tcp   0   0 10-120-85-154:45433
10-120-85-154:25009 CLOSE_WAIT 94237/java
tcp   0   0 10-120-85-154:45434  10-120-85-154:25009 CLOSE_WAIT 94237/java
tcp   0   0 10-120-85-154:45435  10-120-85-154:25009 CLOSE_WAIT 94237/java
...
```

Step 8 Run the following command to view the processes that occupy a large number of ports:

ps -ef |grep *PID*

NOTE

- PID is the processes ID queried in **Step 7**.
- Run the following command to collect information about all processes and check the processes that occupy a large number of ports:

  ps -ef > $BIGDATA_HOME/tmp/ps_result.txt

Step 9 After obtaining the administrator's approval, clear the processes that occupy a large number of ports. Wait for 5 minutes, and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 10**.

Collect fault information.

Step 10 On the FusionInsight Manager home page of the active cluster, choose **O&M** > **Log** > **Download**.

Step 11 Select **OMS** from the **Service** and click **OK**.

Step 12 Set **Host** to the node for which the alarm is generated and the active OMS node.

Step 13 Click the edit button in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 14 Contact the technical support and send the collected log information and files **port_result.txt** and **ps_result.txt**. Then, delete the two residual temporary files from the environment.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.33 ALM-12053 Host File Handle Usage Exceeds the Threshold

Alarm Description

The system checks the file handle usage every 30 seconds and compares the actual usage with the threshold. This alarm is generated when the host file handle usage exceeds the threshold for several times (5 times by default) consecutively.

To change the threshold, choose **O&M > Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Host Status** > **Host File Handle Usage**.

When the **Trigger Count** is 1, this alarm is cleared when the host file handle usage is less than or equal to the threshold. When the **Trigger Count** is greater

than 1, this alarm is cleared when the host file handle usage is less than or equal to 90% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12053	Critical (default threshold: 95%) Major (default threshold: 80%)	Environment	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold for triggering the alarm.

Impact on the System

Service failure: When the host file handle usage exceeds the threshold, system applications cannot perform I/O operations such as file opening and network operations. As a result, the program is abnormal, which may cause job running failure.

Possible Causes

- The application process is abnormal. For example, the opened file or socket is not closed.
- The number of file handles cannot meet the current service requirements.
- The system is abnormal.

Handling Procedure

Check information about files opened in processes.

Step 1 On FusionInsight Manager, click ⌄ in the row where the alarm is located in the real-time alarm list and obtain the IP address of the host for which the alarm is generated.

Step 2 Log in to the host for which the alarm is generated as user **root**.

Step 3 Run the **lsof -n|awk '{print $2}'|sort|uniq -c|sort -nr|more** command to check the process that occupies excessive file handles.

Step 4 Check whether the processes in which a large number of files are opened are normal. For example, check whether there are files or sockets not closed.

- If yes, go to **Step 5**.
- If no, go to **Step 7**.

Step 5 Release the abnormal processes that occupy too many file handles.

Step 6 Five minutes later, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Increase the number of file handles.

Step 7 On FusionInsight Manager, click ⌄ in the row where the alarm is located in the real-time alarm list and obtain the IP address of the host for which the alarm is generated.

Step 8 Log in to the host for which the alarm is generated as user **root**.

Step 9 Contact the system administrator to increase the number of system file handles.

Step 10 Run the **cat /proc/sys/fs/file-nr** command to view the used handles and the maximum number of file handles. The first value is the number of used handles, the third value is the maximum number. Please check whether the usage exceeds the threshold.

- If yes, go to **Step 9**.
- If no, go to **Step 11**.

```
# cat /proc/sys/fs/file-nr
12704 0 640000
```

Step 11 Wait for 5 minutes, and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 12**.

Check whether the system environment is abnormal.

Step 12 Contact the system administrator to check whether the operating system is abnormal.

- If yes, go to **Step 13** to rectify the fault.
- If no, go to **Step 14**.

Step 13 Wait for 5 minutes, and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 14**.

Collect fault information.

Step 14 On the FusionInsight Manager home page of the active cluster, choose **O&M** > **Log** > **Download**.

Step 15 Select **OMS** from the **Service** and click **OK**.

Step 16 Set **Host** to the node for which the alarm is generated and the active OMS node.

Step 17 Click the edit button in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 18 Contact the technical support and send the collected log information.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.34 ALM-12054 Invalid Certificate File

Alarm Description

The system checks whether the certificate file is invalid (has expired or is not valid yet) at the beginning of each hour. This alarm is generated when the certificate file is invalid.

This alarm is cleared when a valid certificate is imported and the alarm detection mechanism is triggered on the next hour.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12054	Critical	Security	Tenant plane	FusionInsight Manager	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
Modify	3.3.1	Alarm Severity: changed from Major to Critical.	Alarm Severity: Accuracy optimized

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Details	Specifies alarm details.

Impact on the System

The functions of the related modules cannot be used.

Possible Causes

No certificate (CA certificate, HA root certificate, HA user certificate, GaussDB root certificate, or GaussDB user certificate) is imported to the system, the certificate fails to be imported, or the certificate file is invalid.

Handling Procedure

Locate the alarm cause.

Step 1 On FusionInsight Manager, locate the target alarm in the real-time alarm list and click ⌄.

View **Additional Information** to obtain the additional information about the alarm.

- If **CA Certificate** is displayed in the additional alarm information, log in to the active OMS management node as user **omm** and go to **Step 2**.
- If **HA root Certificate** is displayed in the additional information, view **Location** to obtain the name of the host involved in this alarm. Then, log in to the host as user **omm** and go to **Step 3**.

- If **HA server Certificate** is displayed in the additional information, view **Location** to obtain the name of the host involved in this alarm. Then, log in to the host as user **omm** and go to **Step 4**.
- If **Gaussdb root Certificate** is displayed in the additional information, view **Location** to obtain the name of the host involved in this alarm. Then, log in to the host as user **ommdba** and go to **Step 5**.
- If **Gaussdb server Certificate** is displayed in the additional information, view **Location** to obtain the name of the host involved in this alarm. Then, log in to the host as user **ommdba** and go to **Step 6**.
- If **DBService HA root Certificate** is displayed in the additional information, view **Location** to obtain the name of the host involved in this alarm. Then, log in to the host as user **omm** and go to **Step 7**.
- If **DBService HA server Certificate** is displayed in the additional information, view **Location** to obtain the name of the host involved in this alarm. Then, log in to the host as user **omm** and go to **Step 8**.
- If **DBService Gaussdb root Certificate** is displayed in the additional information, view **Location** to obtain the name of the host involved in this alarm. Then, log in to the host as user **omm** and go to **Step 9**.
- If **DBService Gaussdb server Certificate** is displayed in the additional information, view **Location** to obtain the name of the host involved in this alarm. Then, log in to the host as user **omm** and go to **Step 10**.
- If **Certificate has expired** is displayed in the additional information, view **Location** to obtain the name of the host for which the alarm is generated. Then, log in to the host as user **omm** (user **ommdba** is required for querying the GaussDB root certificate or GaussDB user certificate) and perform **Step 2** to **Step 10** in sequence to check whether the certificates have expired. If these certificates have not expired, check whether other certificates have been imported. If yes, import the certificate files again.

Check the validity period of the certificate files in the system.

Step 2 Check whether the current system time is within the validity period of the CA certificate.

Run the **bash ${CONTROLLER_HOME}/security/cert/conf/querycertvalidity.sh** command to check the effective time and due time of the CA root certificate.

- If yes, go to **Step 16**.
- If no, go to **Step 11**.

Step 3 Check whether the current system time is within the validity period of the HA root certificate.

Run the **openssl x509 -noout -text -in ${CONTROLLER_HOME}/security/certHA/root-ca.crt** command to check the effective time and due time of the HA root certificate.

- If yes, go to **Step 16**.
- If no, go to **Step 12**.

Step 4 Check whether the current system time is within the validity period of the HA user certificate.

Run the **openssl x509 -noout -text -in ${CONTROLLER_HOME}/security/certHA/server.crt** command to check the effective time and due time of the HA user certificate.

- If yes, go to **Step 16**.
- If no, go to **Step 12**.

Step 5 Check whether the current system time is within the validity period of the GaussDB root certificate.

Run the **openssl x509 -noout -text -in ${GAUSSHOME}/../db_ssl/root-ca.crt** command to check the effective time and due time of the GaussDB root certificate.

- If yes, go to **Step 16**.
- If no, go to **Step 13**.

Step 6 Check whether the current system time is within the validity period of the GaussDB user certificate.

Run the **openssl x509 -noout -text -in ${GAUSSHOME}/../db_ssl/server.crt** command to check the effective time and due time of the GaussDB user certificate.

- If yes, go to **Step 16**.
- If no, go to **Step 13**.

Step 7 Check whether the current system time is within the validity period of the DBService HA root certificate.

Run the **openssl x509 -noout -text -in ${DBSERVER_HOME}/ha/local/cert/root-ca.crt** command to check the effective time and due time of the DBService HA root certificate.

- If yes, go to **Step 16**.
- If no, go to **Step 14**.

Step 8 Check whether the current system time is within the validity period of the DBService HA user certificate.

Run the **openssl x509 -noout -text -in ${DBSERVER_HOME}/ha/local/cert/server.crt** command to check the effective time and due time of the DBService HA user certificate.

- If yes, go to **Step 16**.
- If no, go to **Step 14**.

Step 9 Check whether the current system time is within the validity period of the DBService GaussDB root certificate.

Run the **openssl x509 -noout -text -in ${DBSERVER_HOME}/security/db-root-ca.crt** command to check the effective time and due time of the DBService GaussDB root certificate.

- If yes, go to **Step 16**.
- If no, go to **Step 15**.

Step 10 Check whether the current system time is within the validity period of the DBService GaussDB user certificate.

Run the **openssl x509 -noout -text -in ${DBSERVER_HOME}/security/db-server.crt** command to check the effective time and due time of the DBService GaussDB user certificate.

- If yes, go to **Step 16**.
- If no, go to **Step 15**.

The following is an example of the effective time and due time of a CA or HA certificate:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            97:d5:0e:84:af:ec:34:d8
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=CN, ST=xxx, L=yyy, O=zzz, OU=IT, CN=HADOOP.COM
        Validity
            Not Before: Dec 13 06:38:26 2016 GMT            // Effective time
            Not After : Dec 11 06:38:26 2026 GMT            // Due time
```

Import certificate files.

Step 11 Import a new CA certificate file.

Apply for or generate a new CA certificate file and import it to the system. For details, see "Replacing the CA Certificate" in MapReduce Service (MRS) 3.3.1-LTS User Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Usage Guide (for Huawei Cloud Stack 8.3.1). The alarm is automatically cleared after the CA certificate is imported. Check whether this alarm is reported again during periodic check.

- If yes, go to **Step 16**.
- If no, no further action is required.

Step 12 Import a new HA certificate file.

Apply for or generate a new HA certificate file and import it to the system. For details, see "Replacing HA Certificates" in MapReduce Service (MRS) 3.3.1-LTS User Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Usage Guide (for Huawei Cloud Stack 8.3.1). The alarm is automatically cleared after the certificate is imported. Check whether this alarm is reported again during periodic check.

- If yes, go to **Step 16**.
- If no, no further action is required.

Step 13 Import a new GaussDB certificate file.

Apply for or generate a new GaussDB certificate file and import it to the system. For details, see "Replacing the OMS GaussDB Certificate" in MapReduce Service (MRS) 3.3.1-LTS User Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Usage Guide (for Huawei Cloud Stack 8.3.1). The alarm is automatically cleared after the GaussDB certificate is imported. Check whether this alarm is reported again during periodic check.

- If yes, go to **Step 16**.

- If no, no further action is required.

Step 14 Import a new DBService HA certificate file.

Apply for or generate a new DBService HA certificate file and import it to the system. For details, see "Replacing the DBService HA Certificate" in MapReduce Service (MRS) 3.3.1-LTS User Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Usage Guide (for Huawei Cloud Stack 8.3.1). The alarm is automatically cleared after the DBService HA certificate is imported. Check whether this alarm is reported again during periodic check.

- If yes, go to **Step 16**.
- If no, no further action is required.

Step 15 Import a new DBService GaussDB certificate file.

Apply for or generate a new DBService GaussDB certificate file and import it to the system. For details, see "Replacing the DBService GaussDB Certificate" in MapReduce Service (MRS) 3.3.1-LTS User Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Usage Guide (for Huawei Cloud Stack 8.3.1). The alarm is automatically cleared after the DBService GaussDB certificate is imported. Check whether this alarm is reported again during periodic check.

- If yes, go to **Step 16**.
- If no, no further action is required.

Collect fault information.

Step 16 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 17 In the **Services** area, select **Controller**, **OmmServer**, **OmmCore**, and **Tomcat**, and click **OK**.

Step 18 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 19 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.3.35 ALM-12055 The Certificate File Is About to Expire

Alarm Description

The system checks the certificate file at the beginning of each hour. This alarm is generated if the certificate file is about to expire within 30 days.

This alarm is cleared when a certificate that is not about to expire is imported and the alarm detection mechanism is triggered on the next hour.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12055	Major	Security	Tenant plane	FusionInsight Manager	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
Modify	3.3.1	Alarm Severity: changed from Minor to Major.	Alarm Severity: Accuracy optimized

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Details	Specifies alarm details.

Impact on the System

Some functions will be unavailable if the certificate expires.

Possible Causes

The remaining validity period of a system certificate (CA certificate, HA root certificate, HA user certificate, GaussDB root certificate, or GaussDB user certificate) is less than 30 days.

Handling Procedure

Locate the alarm cause.

Step 1 On FusionInsight Manager, locate the target alarm in the real-time alarm list and click ∨.

View **Additional Information** to obtain the additional information about the alarm.

- If **CA Certificate** is displayed in the additional alarm information, log in to the active OMS management node as user **omm** and go to **Step 2**.
- If **HA root Certificate** is displayed in the additional information, view **Location** to obtain the name of the host involved in this alarm. Then, log in to the host as user **omm** and go to **Step 3**.
- If **HA server Certificate** is displayed in the additional information, view **Location** to obtain the name of the host involved in this alarm. Then, log in to the host as user **omm** and go to **Step 4**.
- If **Gaussdb root Certificate** is displayed in the additional information, view **Location** to obtain the name of the host involved in this alarm. Then, log in to the host as user **ommdba** and go to **Step 5**.
- If **Gaussdb server Certificate** is displayed in the additional information, view **Location** to obtain the name of the host involved in this alarm. Then, log in to the host as user **ommdba** and go to **Step 6**.

- If **DBService HA root Certificate** is displayed in the additional information, view **Location** to obtain the name of the host involved in this alarm. Then, log in to the host as user **omm** and go to **Step 7**.
- If **DBService HA server Certificate** is displayed in the additional information, view **Location** to obtain the name of the host involved in this alarm. Then, log in to the host as user **omm** and go to **Step 8**.
- If **DBService Gaussdb root Certificate** is displayed in the additional information, view **Location** to obtain the name of the host involved in this alarm. Then, log in to the host as user **omm** and go to **Step 9**.
- If **DBService Gaussdb server Certificate** is displayed in the additional information, view **Location** to obtain the name of the host involved in this alarm. Then, log in to the host as user **omm** and go to **Step 10**.

Check the validity period of the certificate files in the system.

Step 2 Check whether the remaining validity period of the CA certificate is smaller than the alarm threshold.

Run the **bash ${CONTROLLER_HOME}/security/cert/conf/querycertvalidity.sh** command to check the effective time and due time of the CA root certificate.

- If yes, go to **Step 11**.
- If no, go to **Step 16**.

Step 3 Check whether the remaining validity period of the HA root certificate is smaller than the alarm threshold.

Run the **openssl x509 -noout -text -in ${CONTROLLER_HOME}/security/certHA/root-ca.crt** command to check the effective time and due time of the HA root certificate.

- If yes, go to **Step 12**.
- If no, go to **Step 16**.

Step 4 Check whether the remaining validity period of the HA user certificate is smaller than the alarm threshold.

Run the **openssl x509 -noout -text -in ${CONTROLLER_HOME}/security/certHA/server.crt** command to check the effective time and due time of the HA user certificate.

- If yes, go to **Step 12**.
- If no, go to **Step 16**.

Step 5 Check whether the remaining validity period of the GaussDB root certificate is smaller than the alarm threshold.

Run the **openssl x509 -noout -text -in ${GAUSSHOME}/../db_ssl/root-ca.crt** command to check the effective time and due time of the GaussDB root certificate.

- If yes, go to **Step 13**.
- If no, go to **Step 16**.

Step 6 Check whether the remaining validity period of the GaussDB user certificate is smaller than the alarm threshold.

Run the **openssl x509 -noout -text -in ${GAUSSHOME}/../db_ssl/server.crt** command to check the effective time and due time of the GaussDB user certificate.

- If yes, go to **Step 13**.
- If no, go to **Step 16**.

Step 7 Check whether the remaining validity period of the DBService HA root certificate is smaller than the alarm threshold.

Run the **openssl x509 -noout -text -in ${DBSERVER_HOME}/ha/local/cert/root-ca.crt** command to check the effective time and due time of the DBService HA root certificate.

- If yes, go to **Step 14**.
- If no, go to **Step 16**.

Step 8 Check whether the remaining validity period of the DBService HA root certificate is smaller than the alarm threshold.

Run the **openssl x509 -noout -text -in ${DBSERVER_HOME}/ha/local/cert/server.crt** command to check the effective time and due time of the DBService HA user certificate.

- If yes, go to **Step 14**.
- If no, go to **Step 16**.

Step 9 Check whether the remaining validity period of the DBService GaussDB root certificate is smaller than the alarm threshold.

Run the **openssl x509 -noout -text -in ${DBSERVER_HOME}/security/db-root-ca.crt** command to check the effective time and due time of the DBService GaussDB root certificate.

- If yes, go to **Step 15**.
- If no, go to **Step 16**.

Step 10 Check whether the remaining validity period of the DBService GaussDB user certificate is smaller than the alarm threshold.

Run the **openssl x509 -noout -text -in ${DBSERVER_HOME}/security/db-server.crt** command to check the effective time and due time of the DBService GaussDB user certificate.

- If yes, go to **Step 15**.
- If no, go to **Step 16**.

The following is an example of the effective time and due time of a CA or HA certificate:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            97:d5:0e:84:af:ec:34:d8
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=CN, ST=xxx, L=yyy, O=zzz, OU=IT, CN=HADOOP.COM
        Validity
            Not Before: Dec 13 06:38:26 2016 GMT          // Effective time
            Not After : Dec 11 06:38:26 2026 GMT          // Due time
```

Import certificate files.

Step 11 Import a new CA certificate file.

Apply for or generate a new CA certificate file and import it to the system. For details, see "Replacing the CA Certificate" in MapReduce Service (MRS) 3.3.1-LTS User Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Usage Guide (for Huawei Cloud Stack 8.3.1). Manually clear the alarm and check whether this alarm is generated again during periodic check.

- If yes, go to **Step 16**.
- If no, no further action is required.

Step 12 Import a new HA certificate file.

Apply for or generate a new HA certificate file and import it to the system. For details, see "Replacing HA Certificates" in MapReduce Service (MRS) 3.3.1-LTS User Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Usage Guide (for Huawei Cloud Stack 8.3.1). Manually clear the alarm and check whether this alarm is generated again during periodic check.

- If yes, go to **Step 16**.
- If no, no further action is required.

Step 13 Import a new GaussDB certificate file.

Apply for or generate a new HA certificate file and import it to the system.For details, see "Replacing the OMS GaussDB Certificate" in MapReduce Service (MRS) 3.3.1-LTS User Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Usage Guide (for Huawei Cloud Stack 8.3.1). Manually clear the alarm and check whether this alarm is generated again during periodic check.

- If yes, go to **Step 16**.
- If no, no further action is required.

Step 14 Import a new DBService HA certificate file.

Apply for or generate a new HA certificate file and import it to the system. For details, see "Replacing the DBService HA Certificate" in MapReduce Service (MRS) 3.3.1-LTS User Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Usage Guide (for Huawei Cloud Stack 8.3.1). Manually clear the alarm and check whether this alarm is generated again during periodic check.

- If yes, go to **Step 16**.
- If no, no further action is required.

Step 15 Import a new DBService GaussDB certificate file.

Apply for or generate a new HA certificate file and import it to the system. For details, see "Replacing the DBService GaussDB Certificate" in MapReduce Service (MRS) 3.3.1-LTS User Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Usage Guide (for Huawei Cloud Stack 8.3.1). Manually clear the alarm and check whether this alarm is generated again during periodic check.

- If yes, go to **Step 16**.
- If no, no further action is required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Collect fault information.

Step 16 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 17 In the **Services** area, select **Controller**, **OmmServer**, **OmmCore**, and **Tomcat**, and click **OK**.

Step 18 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 19 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.36 ALM-12057 Metadata Not Configured with the Task to Periodically Back Up Data to a Third-Party Server

Alarm Description

After the system is installed, it checks whether the task for periodically backing up metadata to the third-party server, and then performs the check hourly. If the task for periodically backing up metadata to a third-party server is not configured, a critical alarm is generated.

This alarm is cleared when a user creates such a backup task.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12057	Major	Backup status	Tenant plane	FusionInsight Manager	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
Modify	3.3.1	Alarm Severity: changed from Major to Minor.	Alarm Severity: Accuracy optimized

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the details for which the alarm is generated.

Impact on the System

If the metadata is not backed up to a third-party server, when the active/standby management nodes in the cluster are faulty and the local backup data is lost, if you want to use the backup package to restore the cluster metadata, no backup package is available.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Possible Causes

Metadata is not configured with the task to periodically back up data to a third-party server.

Handling Procedure

Step 1 On the FusionInsight Manager portal choose **O&M > Alarm > Alarms**.

Step 2 In the alarm list, click ⌄ in the row where the alarm is located and identify the data module from which the alarm is generated based on **Additional Information**.

Step 3 Choose **O&M** > **Backup and Restoration > Backup Management** > **Create**.

Step 4 Configure a backup task. The backup data to be configured is consistent with the data in Additional Information of the alarm.

In MRS, configure a backup task by referring to section **Backing Up Data** in *MapReduce Service (MRS) 3.3.1-LTS User Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Usage Guide (for Huawei Cloud Stack 8.3.1)*.

Step 5 After the backup task is created successfully, wait for two minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information

Step 6 On FusionInsight Manager, choose **O&M** > **Log > Download**.

Step 7 In the **Service** area, select **Controller** and click **OK**.

Step 8 Click ✎ in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact the technical support and send the collected log information.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.37 ALM-12061 Process Usage Exceeds the Threshold

Alarm Description

The system checks the usage of the omm process every 30 seconds. Users can run the **ps -o nlwp, pid, args, -u omm | awk '{sum+=$1} END {print "", sum}'**

command to obtain the number of concurrent processes of user **omm**. Run the **ulimit -u**command to obtain the maximum number of processes that can be simultaneously opened by user **omm**. Divide the number of concurrent processes by the maximum number to obtain the process usage of user **omm**. The process usage has a default threshold. This alarm is generated when the process usage exceeds the threshold.

If **Trigger Count** is **3** and the process usage is less than or equal to the threshold, this alarm is cleared. If **Trigger Count** is greater than **1**and the process usage is less than or equal to 90% of the threshold, this alarm is cleared.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12061	Critical (default threshold: 95) Major (default threshold: 90)	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the details for which the alarm is generated.

Impact on the System

Service failure: When the process usage exceeds the threshold, you cannot switch to user **omm**. A new **omm** thread cannot be created. As a result, the job may fail to run.

Possible Causes

- The alarm threshold is improperly configured.
- The maximum number of processes (including threads) that can be concurrently opened by user **omm** is inappropriate.
- An excessive number of threads are opened at the same time.

Handling Procedure

Check whether the alarm threshold or alarm hit number is properly configured.

Step 1 On the FusionInsight Manager, change the alarm threshold and **Trigger Count** based on the actual CPU usage.

Specifically, choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Host**> **Process** > **omm Process Usage** to change Trigger Count, as shown in **Figure 1-4**.

NOTE

The alarm is generated when the process usage exceeds the threshold for the times specified by **Trigger Count**.

Figure 1-4 Setting Trigger Count

Set the alarm threshold based on the actual process usage. To check the process usage, choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Host**> **Process** > **omm Process Usage**.

Step 2 2 minutes later, check whether the alarm is cleared.

- If it is, no further action is required.
- If it is not, go to **Step 3**.

Check whether the maximum number of processes (including threads) opened by user omm is appropriate.

Step 3 In the alarm list on FusionInsight Manager, locate the row that contains the alarm, and view the IP address of the host for which the alarm is generated.

Step 4 Log in to the host where the alarm is generated as user **root**.

Step 5 Run the **su - omm** command to switch to user **omm**.

Step 6 Run the **ulimit -u** command to obtain the maximum number of threads that can be concurrently opened by user **omm** and check whether the number is greater than or equal to 60000.

- If it is, go to **Step 8**.
- If it is not, go to **Step 7**.

Step 7 Run the **ulimit -u 60000** command to change the maximum number to 60000. Two minutes later, check whether the alarm is cleared.

- If it is, no further action is required.
- If it is not, go to **Step 12**.

Check whether an excessive number of processes are opened at the same time.

Step 8 In the alarm list on FusionInsight Manager, locate the row that contains the alarm, and view the IP address of the host for which the alarm is generated.

Step 9 Log in to the host where the alarm is generated as user **root**.

Step 10 Run the **ps -o nlwp, pid, lwp, args, -u omm|sort -n** command to check the numbers of threads used by the system. The result is sorted based on the thread number. Analyze the top 5 thread numbers and check whether the threads are

incorrectly used. If they are, contact maintenance personnel to rectify the fault. If they are not, run the **ulimit -u** command to change the maximum number to be greater than 60000.

Step 11 Five minutes later, check whether the alarm is cleared.

- If it is, no further action is required.
- If it is not, go to **Step 12**.

Collect fault information.

Step 12 On the FusionInsight Manager home page of the active clusters, choose **O&M** > **Log** > **Download**.

Step 13 Select **OmmServer** and **NodeAgent** from the **Service** and click **OK**.

Step 14 Click the edit button in the upper right corner. In the displayed dialog box, set **Start Date** and **End Date** to 10 minutes before and after the alarm generation time respectively and click **OK**. Then, click **Download**.

Step 15 Contact the technical support and send the collected log information.

----End

Alarm Clearance

This alarm will be automatically cleared after the fault is rectified.

Related Information

None.

1.3.38 ALM-12062 OMS Parameter Configurations Mismatch with the Cluster Scale

Alarm Description

The system checks whether the OMS parameter configurations match with the cluster scale at each top hour. If the OMS parameter configurations do not meet the cluster scale requirements, the system generates this alarm. This alarm is automatically cleared when the OMS parameter configurations are modified.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12062	Major	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

If the parameters configured for the current cluster are smaller than the configuration standard required by the cluster scale, problems such as job running delay and slow service page response may occur. In severe cases, the Agent or OMS process on the cluster node is abnormal. As a result, component jobs fail to be submitted and OMS data fails to be synchronized.

Possible Causes

The OMS parameter configurations mismatch with the cluster scale.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Handling Procedure

Check whether the OMS parameter configurations match with the cluster scale.

Step 1 Log in to the active Manager node as user **omm**.

Step 2 Run the **vi ${BIGDATA_LOG_HOME}/controller/scriptlog/modify_manager_param.log** command to open the log file and search for the log file containing the following information: Current oms configurations cannot support *xx* nodes. In the information, *xx* indicates the number of nodes in the cluster.

Step 3 Optimize the current cluster configuration by following the instructions in **Related Information**.

Step 4 One hour later, check whether the alarm is cleared.

- If it is, no further action is required.
- If it is not, go to **Step 5**.

Collect fault information.

Step 5 On FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 6 Select **Controller** from the **Service** and click **OK**.

Step 7 Click the edit button in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 8 Contact the technical support and send the collected log information.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

Optimizing Manager Configurations Based on the Number of Cluster Nodes

Step 1 Log in to the active Manager node as user **omm**.

Step 2 Run the following command to switch the directory:

cd ${BIGDATA_HOME}/om-server/om/sbin

Step 3 Run the following command to view the current Manager configurations.

sh oms_config_info.sh -q

Step 4 Run the following command to specify the number of nodes in the current cluster.

Command format: **sh oms_config_info.sh -s** *number of nodes*

Example:

sh oms_config_info.sh -s 1000

Enter **y** as prompted.

```
The following configurations will be modified:
    Module       Parameter          Current          Target
    Controller   controller.Xmx     4096m        =>  16384m
    Controller   controller.Xms     1024m        =>  8192m
    Controller   controller.node.heartbeat.error.threshold     30000                    =>   60000
    Pms          pms.mem            8192m        =>  10240m
Do you really want to do this operation? (y/n):
```

The configurations are updated successfully if the following information is displayed:

```
...
Operation has been completed. Now restarting OMS server.                [done]
Restarted oms server successfully.
```

NOTE

- OMS is automatically restarted during the configuration update process.
- Clusters with similar quantities of nodes have same Manager configurations. For example, when the number of nodes is changed from 100 to 101, no configuration item needs to be updated.

----End

1.3.39 ALM-12063 Unavailable Disk

Alarm Description

The system checks whether the data disk of the current host is available every five minutes. The system creates files, writes files, and deletes files in the mount directory of the disk. If the operations fail, the alarm is generated. If the operations succeed, the disk is available, and the alarm is cleared.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12063	Major	Physical resource	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.

Type	Parameter	Description
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	Partition mount point	Specifies the disk partition for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Disk serial number	Specifies the serial number of the disk for which the alarm is generated.

Impact on the System

Service failure: If you need to modify or use data on a disk that is unwritable or unreadable, the job may fail.

Possible Causes

- The permission of the disk mount directory is abnormal.
- There are disk bad sectors.

Handling Procedure

Check whether the permission of the disk mount directory is normal.

Step 1 In the alarm list on FusionInsight Manager, locate the row that contains the alarm, and view the IP address of the host and **DiskName** for the disk for which the alarm is generated.

Step 2 Log in to the host where the alarm is generated as user **root**.

Step 3 Run the **df -h |grep DiskName** command to obtain the mount point and check whether the permission of the mount directory is unwritable or unreadable.

- If it is, go to **Step 4**.
- If it is not, go to **Step 8**.

NOTE

If the permission of the mount directory is 000 or the owner is **root**, the mount directory is unreadable and unwritable.

Step 4 Modify the directory permission.

Step 5 One hour later, check whether this alarm is cleared.

- If it is, no further action is required.
- If it is not, go to **Step 6**.

Step 6 Contact hardware engineers to rectify the disk.

Step 7 One hour later, check whether this alarm is cleared.

- If it is, no further action is required.
- If it is not, go to **Step 8**.

Collect fault information.

Step 8 On FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 9 Select **NodeAgent** from the **Service** and click **OK**.

Step 10 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 11 Contact the technical support and send the collected log information.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.40 ALM-12064 Host Random Port Range Conflicts with Cluster Used Port

Alarm Description

The system checks whether the random port range of the host conflicts with the range of ports used by the Cluster system every hour. The alarm is generated if they conflict. The alarm is automatically cleared when the random port range of the host is changed to the normal range.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12064	Major	Environment	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

- If ports such as okerberos and oldap are occupied, authentication fails and jobs may fail.
- If the controller and pms ports are occupied, the process is faulty, which may affect the elastic scaling performance.
- If the Tomcat port is occupied, the login and query functions of FusionInsight Manager are affected.

Possible Causes

The random port range configuration is modified.

Handling Procedure

Check the random port range of the system.

Step 1 In the alarm list on FusionInsight Manager, locate the row that contains the alarm, and view the IP address of the host for which the alarm is generated.

Step 2 Log in to the host where the alarm is generated as user **root**.

Step 3 Run the **cat /proc/sys/net/ipv4/ip_local_port_range** command to obtain the random port range of the host and check whether the minimum value is smaller than 32768.

- If it is, go to **Step 4**.
- If it is not, goto **Step 7**.

Step 4 Run the **vim /etc/sysctl.conf** command to change the value of **net.ipv4.ip_local_port_range** to **32768 61000**. If this parameter does not exist, add the following configuration: **net.ipv4.ip_local_port_range = 32768 61000**.

Step 5 Run the **sysctl -p /etc/sysctl.conf** command for the modification to take effect.

Step 6 One hour later, check whether the alarm is cleared.

- If it is, no further action is required.
- If it is not, go to **Step 7**.

Collect fault information.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 7 On FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 8 Select **NodeAgent** for **Service** and click **OK**.

Step 9 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact the technical support and send the collected log information.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.41 ALM-12066 Trust Relationships Between Nodes Become Invalid

Alarm Description

The system checks whether the trust relationship between the active OMS node and other Agent nodes is normal every hour. The alarm is generated if the mutual trust fails. This alarm is automatically cleared after the fault is rectified.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12066	Major	Communications	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.

Type	Parameter	Description
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	Alarm Severity	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Failed hosts	Specifies hosts that fail to be trusted.

Impact on the System

Some operations (such as restart, configuration synchronization, and instance status query) that need to connect to the node may fail. If the trust relationships between nodes are invalid, services may be affected.

Possible Causes

- The **/etc/ssh/sshd_config** configuration file is damaged.
- The password of user **omm** has expired.
- If the current cluster is a physical machine cluster, the SSH port number of the faulty host is different from that of the active node.

Handling Procedure

Check the status of the /etc/ssh/sshd_config configuration file.

Step 1 In the alarm list on FusionInsight Manager, locate the row that contains the alarm and click ⌄ to view the host list in the alarm details.

Step 2 Log in to the active OMS node as user **omm**.

Step 3 Run the **ssh** command, for example, **ssh *host2***, on each node in the alarm details to check whether the connection fails. (***host2*** is a node other than the OMS node in the alarm details.)

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 Open the **/etc/ssh/sshd_config** configuration file on host2 and check whether **AllowUsers** or **DenyUsers** is configured for other nodes.

- If yes, go to **Step 5**.
- If no, contact OS experts.

Step 5 Modify the whitelist or blacklist to ensure that user **omm** is in the whitelist or not in the blacklist. Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Check the status of the password of user omm.

Step 6 Check the interaction information of the **ssh** command.

- If the password of user **omm** is required, go to **Step 7**.
- If message "Enter passphrase for key '/home/omm/.ssh/id_rsa':" is displayed, go to **Step 9**.
- If the SSH server can be connected, run the following command to restart **ssh-agent** and then go to **Step 3**:

  ps -ef|grep ssh-agent |grep -v grep |awk '{print $2}' | xargs kill -9

Step 7 Check the trust list (**/home/omm/.ssh/authorized_keys**) of user **omm** on the OMS node and host2 node. Check whether the trust list contains the public key file (**/home/omm/.ssh/id_rsa.pub**) of user **omm** on the peer host.

- If yes, contact OS experts.
- If no, add the public key of user **omm** of the peer host to the trust list of the local host.

Step 8 Add the public key of user **omm** of the peer host to the trust list of the local host. Run the **ssh** command, for example, **ssh host2**, on each node in the alarm details to check whether the connection fails. (***host2*** is a node other than the OMS node in the alarm details.)

- If yes, go to **Step 9**.
- If no, check whether the alarm is cleared. If the alarm is cleared, no further action is required; otherwise, go to **Step 9**.

Check whether the SSH port number of the physical machine cluster is inconsistent with that of the active node.

Step 9 Run the **ssh** *host2 IP address* command and check whether the following information is displayed:

```
ssh: connect to host <host2> port <Port number >:Connection refused
```

- If yes, go to **Step 10**.
- If no, go to **Step 12**.

Step 10 Check whether the settings of **Port** in the **/etc/ssh/sshd_config** and **/etc/ssh/ssh_config** files on host2 are the same. Make sure that the settings are the same as those on the active node.

- If yes, go to **Step 12**.
- If no, change the values of **Port** in the **/etc/ssh/sshd_config** and **/etc/ssh/ssh_config** files of host2 to be the same as the value on the active node, and run the following command to restart the sshd process of the faulty host:

  service sshd restart

Step 11 Wait a moment and check whether this alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 12**.

Collect the fault information.

Step 12 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 13 Select **Controller** for **Service** and click **OK**.

Step 14 Click in the upper right corner to set the log collection time range. Generally, the time range is 10 minutes before and after the alarm generation time. Click **Download**.

Step 15 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.3.42 ALM-12067 Abnormal Tomcat Resources of Manager

Alarm Description

HA checks the Tomcat resources of Manager every 85 seconds. This alarm is generated when HA detects that the Tomcat resources are abnormal for two consecutive times.

This alarm is cleared when HA detects that the Tomcat resources become normal.

Resource Type of Tomcat is **Single-active**. Active/standby will be triggered upon resource exceptions. When this alarm is generated, the active/standby switchover is complete and new Tomcat resources have been enabled on the new active Manager. In this case, this alarm is cleared. This alarm is used to notify users of the cause of the active/standby Manager switchover.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12067	Major	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
Modify	3.3.1	Alarm Name: changed from "Tomcat Resource Is Abnormal" to "Abnormal Tomcat Resources of Manager".	Alarm Name: Standardized

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

An active/standby Manager switchover may occur. The Manager and component web UIs are unavailable. The cluster management function cannot be provided for upper-layer web applications, and users may fail to log in to the Manager and component web UIs.

Possible Causes

The Tomcat directory permission is abnormal, and the Tomcat process is abnormal.

Handling Procedure

Check whether the permission on the Tomcat directory is normal.

Step 1 In the alarm list on FusionInsight Manager, locate the row that contains the alarm, and click ⌄ to view the IP address of the host for which the alarm is generated.

Step 2 Log in to the alarm host as user **root**.

Step 3 Run the **su - omm** command to switch to user **omm**.

Step 4 Run the **vi ${BIGDATA_LOG_HOME}/omm/oms/ha/scriptlog/tomcat.log** command to check whether the Tomcat resource log contains keyword **Cannot find *XXX*** and rectify the file permission based on the keyword.

Step 5 After 5 minutes, check whether the alarm is automatically cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect the fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 In the **Services** area, select **OmmServer** and **Tomcat**, and click **OK**.

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.43 ALM-12068 Abnormal ACS Resources of Manager

Alarm Description

HA checks the ACS resources of Manager every 80 seconds. This alarm is generated when HA detects that the ACS resources are abnormal for two consecutive times.

This alarm is cleared when HA detects that the ACS resources are normal.

Resource Type of ACS is **Single-active**. Active/standby will be triggered upon resource exceptions. When this alarm is generated, the active/standby switchover is complete and new ACS resources have been enabled on the new active Manager. In this case, this alarm is cleared. This alarm is used to notify users of the cause of the active/standby Manager switchover.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12068	Major	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
Modify	3.3.1	Alarm Name: changed from "ACS Resource Is Abnormal" to "Abnormal ACS Resources of Manager".	Alarm Name: Standardized

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

An active/standby Manager switchover may occur. The security authentication and user management functions cannot be provided for ACS upper-layer applications. As a result, you may fail to log in to Manager and component web UIs.

Possible Causes

The ACS process is abnormal.

Handling Procedure

Check whether the ACS process is normal.

Step 1 In the alarm list on FusionInsight Manager, locate the row that contains the alarm, and click ⌄ to view the name of the host for which the alarm is generated.

Step 2 Log in to the host for which the alarm is generated as user **root**.

Step 3 Run the **su - omm** command and then **sh ${BIGDATA_HOME}/om-server/OMS/workspace0/ha/module/hacom/script/status_ha.sh** to check whether the status of the ACS resources managed by the HA is normal. In the single-node system, the ACS resource is in the normal state. In the dual-node system, the ACS resource is in the normal state on the active node and in the stopped state on the standby node.

- If yes, go to **Step 6**.
- If no, go to **Step 4**.

Step 4 Run the **vi ${BIGDATA_LOG_HOME}/omm/oms/ha/scriptlog/acs.log** command to check whether the ACS resource log of HA contains the keyword **ERROR**. If yes, analyze the logs to locate the resource exception cause and fix the exception.

Step 5 After 5 minutes, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect the fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 In the **Services** area, select **Controller** and **OmmServer**, and click **OK**.

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.44 ALM-12069 Abnormal AOS Resources of Manager

Alarm Description

HA checks the AOS resources of Manager every 81 seconds. This alarm is generated when HA detects that the AOS resources are abnormal for two consecutive times.

This alarm is cleared when HA detects that the AOS resources become normal.

Resource Type of AOS is **Single-active**. Active/standby will be triggered upon resource exceptions. When this alarm is generated, the active/standby switchover is complete and new AOS resources have been enabled on the new active Manager. In this case, this alarm is cleared. This alarm is used to notify users of the cause of the active/standby Manager switchover.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12069	Major	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
Modify	3.3.1	Alarm Name: changed from "AOS Resource Exception" to "Abnormal AOS Resources of Manager".	Alarm Name: Standardized

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

An active/standby Manager switchover may occur. Tenant and role management cannot be provided for AOS upper-layer applications. As a result, you may fail to log in to Manager and component web UIs.

Possible Causes

The AOS process is abnormal.

Handling Procedure

Check whether the AOS process is normal.

Step 1 In the alarm list on FusionInsight Manager, locate the row that contains the alarm, and click ⌄ to view the name of the host for which the alarm is generated.

Step 2 Log in to the host for which the alarm is generated as user **root**.

Step 3 Run **su - omm** and then **sh ${BIGDATA_HOME}/om-server/OMS/workspace0/ha/module/hacom/script/status_ha.sh** to check whether the status of the AOS resources managed by the HA is normal. In the single-node system, the AOS resource is in the normal state. In the dual-node system, the AOS resource is in the normal state on the active node and in the stopped state on the standby node.

- If yes, go to **Step 6**.
- If no, go to **Step 4**.

Step 4 Run the **vi ${BIGDATA_LOG_HOME}/omm/oms/ha/scriptlog/aos.log** command to check whether the AOS resource log of HA contains the keyword **ERROR**. If yes, analyze the logs to locate the resource exception cause and fix the exception.

Step 5 After 5 minutes, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect the fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 In the **Services** area, select **Controller** and **OmmServer**, and click **OK**.

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.45 ALM-12070 Controller Resource Is Abnormal

Alarm Description

HA checks the controller resources of Manager every 80 seconds. This alarm is generated when HA detects that the controller resources are abnormal for 2 consecutive times.

This alarm is cleared when the Controller resource is normal.

Resource Type of Controller is **Single-active**. Active/standby will be triggered upon resource exceptions. When this alarm is generated, the active/standby switchover is complete and new Controller resources have been enabled on the new active FusionInsight Manager. In this case, this alarm is cleared. This alarm is used to notify users of the cause of the active/standby switchover.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12070	Major	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

- The alarm persists for a long time, causing frequent active/standby switchovers of FusionInsight Manager. As a result, users cannot log in to FusionInsight Manager and perform O&M operations.
- The Controller process repeatedly restarts, which may cause the native UI of the service login failure.

Possible Causes

The Controller process is abnormal.

Handling Procedure

Check whether the controller process is normal.

Step 1 In the alarm list on FusionInsight Manager, locate the row that contains the alarm, and view the name of the host for which the alarm is generated.

Step 2 Log in to the host for which the alarm is generated as user **root**.

Step 3 Run the **su - omm** command to switch to user **omm**.Run the **sh $ {BIGDATA_HOME}/om-server/OMS/workspace0/ha/module/hacom/script/status_ha.sh** command to check whether the status of the Controller resources managed by the HA is normal. In the single-node system, the Controller resource is in the normal state. In the dual-node system, the Controller resource is in the normal state on the active node and in the stopped state on the standby node.

- If it is, go to **Step 6**.
- If it is not, go to **Step 4**.

Step 4 Run the **vi ${BIGDATA_LOG_HOME}/omm/oms/ha/scriptlog/controller.log** command to view the Controller resource logs, and run the **vi $ {BIGDATA_LOG_HOME}/controller/controller.log** command to view the Controller running logs, check whether the keyword **ERROR** exists. Analyze the logs to locate and rectify the fault.

Step 5 Five minutes later, check whether this alarm is cleared.

- If it is, no further action is required.
- If it is not, go to **Step 6**.

Collect fault information.

Step 6 On FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 7 Select **Controller** and **OmmServe** for **Service** and click **OK**.

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour before and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact the technical support and send the collected log information.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.46 ALM-12071 Httpd Resource Is Abnormal

Alarm Description

HA checks the httpd resources of Manager every 120 seconds. This alarm is generated when HA detects that the httpd resources are abnormal for 10 consecutive times.

This alarm is cleared when the httpd resource is normal.

Resource Type of httpd is **Single-active**. Active/standby will be triggered upon resource exceptions. When this alarm is generated, the active/standby switchover is complete and new httpd resources have been enabled on the new active FusionInsight Manager. In this case, this alarm is cleared. This alarm is used to notify users of the cause of the active/standby switchover.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12071	Major	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

- The alarm persists for a long time, causing frequent active/standby switchovers of FusionInsight Manager. As a result, users cannot log in to FusionInsight Manager and perform O&M operations.
- The httpd process is repeatedly restarts, which may lead to the failure to visit the native service UI.

Possible Causes

The httpd process is abnormal.

Handling Procedure

Check whether the httpd process is abnormal.

Step 1 In the alarm list on FusionInsight Manager, locate the row that contains the alarm, and view the name of the host for which the alarm is generated.

Step 2 Log in to the host for which the alarm is generated as user **root**.

Step 3 Run the **su - omm** command to switch to user **omm**.

Step 4 Run the **sh ${BIGDATA_HOME}/om-server/OMS/workspace0/ha/module/hacom/script/status_ha.sh** command to check whether the status of the httpd resources managed by the HA is normal. In the single-node system, the httpd

resource is in the normal state. In the dual-node system, the httpd resource is in the normal state on the active node and in the stopped state on the standby node.

- If it is, go to **Step 7**.
- If it is not, go to **Step 5**.

Step 5 Run the **vi ${BIGDATA_LOG_HOME}/omm/oms/ha/scriptlog/httpd.log** command to view the httpd resource logs, check whether the keyword **ERROR** exists. Analyze the logs to locate and rectify the fault.

Step 6 Five minutes later, check whether this alarm is cleared.

- If it is, no further action is required.
- If it is not, go to **Step 7**.

Collect fault information.

Step 7 On FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 8 Select **Controller** and **OmmServer** for **Service** and click **OK**.

Step 9 Click in the upper right corner. In the displayed dialog box, set **Start Date** and **End Date** to 1 hour before and after the alarm generation time respectively and click **OK**. Then, click **Download**.

Step 10 Contact the technical support and send the collected log information.

----End

Alarm Clearance

This alarm will be automatically cleared after the fault is rectified.

Related Information

None.

1.3.47 ALM-12072 FloatIP Resource Is Abnormal

Alarm Description

HA checks the floatip resources of Manager every 9 seconds. This alarm is generated when HA detects that the floatip resources are abnormal for 3 consecutive times.

This alarm is cleared when the FloatIP resource is normal.

Resource Type of FloatIP is **Single-active**. Active/standby will be triggered upon resource exceptions. When this alarm is generated, the active/standby switchover is complete and new FloatIP resources have been enabled on the new active FusionInsight Manager. In this case, this alarm is cleared. This alarm is used to notify users of the cause of the active/standby switchover.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12072	Major	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

- The alarm persists for a long time, causing frequent active/standby switchovers of FusionInsight Manager. As a result, users cannot log in to FusionInsight Manager and perform O&M operations.
- The FloatIP process is repeatedly restarts, which may lead to the failure to visit the native service UI.

Possible Causes

- The floating IP address is abnormal.

Handling Procedure

Check the floating IP address status of the active management node.

Step 1 In the alarm list on FusionInsight Manager, locate the row that contains the alarm, and view the address of the host for which the alarm is generated and the resource name.

Step 2 Log in to the active management node as user **root**.

Step 3 Run the following command, go to the **${BIGDATA_HOME}/om-server/om/sbin/** directory.

su - omm

cd ${BIGDATA_HOME}/om-server/om/sbin/

Step 4 Run the **sh status-oms.sh** command, and execute the **status-oms.sh** script to check whether the floating IP address of the active FusionInsight Manager is normal. View the command output, locate the row where **ResName** is **floatip**, and check whether the following information is displayed.

For example:

```
10-10-10-160 floatip Normal Normal Single_active
```

- If it is, go to **Step 8**.
- If it is not, go to **Step 5**.

Step 5 Run the **ifconfig** command to check whether the NIC with the floating IP address exists.

- If it does, go to **Step 8**.
- If it does not, go to **Step 6**.

Step 6 Run the **ifconfig** *NIC name Floating IPaddress* netmask *Subnet mask* command to reconfigure the NIC with the floating IP address. (For example, **ifconfig eth0 10.10.10.102 netmask 255.255.255.0**).

Step 7 Five minutes later, check whether the alarm is cleared.

- If it is, no further action is required.
- If it is not, go to **Step 8**.

Collect fault information.

Step 8 On FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 9 Select **Controller** and **OmmServer** for **Service** and click **OK**.

Step 10 Click in the upper right corner. In the displayed dialog box, set **Start Date** and **End Date** to 1 hour before and after the alarm generation time respectively and click **OK**. Then, click **Download**.

Step 11 Contact the technical support and send the collected log information.

----End

Alarm Clearance

This alarm will be automatically cleared after the fault is rectified.

Related Information

None.

1.3.48 ALM-12074 FMS Resource Is Abnormal

Alarm Description

HA checks the fms resources of Manager every 60 seconds. This alarm is generated when HA detects that the fms resources are abnormal for 2 consecutive times.

This alarm is cleared when the FMS resource is normal.

Resource Type of FMS is **Single-active**. Active/standby will be triggered upon resource exceptions. When this alarm is generated, the active/standby switchover is complete and new FMS resources have been enabled on the new active FusionInsight Manager. In this case, this alarm is cleared. This alarm is used to notify users of the cause of the active/standby switchover.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12074	Major	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.

Type	Parameter	Description
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

- The alarm persists for a long time, causing frequent active/standby switchovers of FusionInsight Manager. As a result, users cannot log in to FusionInsight Manager and perform O&M operations.
- The FMS process repeatedly restarts. As a result, the alarm data reported during the alarm reporting period is abnormal. In severe cases, the alarm data reported during the alarm reporting period may fail to be reported and cleared.

Possible Causes

The FMS process is abnormal.

Handling Procedure

Check whether the FMS process is abnormal.

Step 1 In the alarm list on FusionInsight Manager, locate the row that contains the alarm, and view the name of the host for which the alarm is generated.

Step 2 Log in to the host for which the alarm is generated as user **root**.

Step 3 Run the **su -omm** command and then the **sh ${BIGDATA_HOME}/om-server/OMS/workspace0/ha/module/hacom/script/status_ha.sh** command to check whether the status of the FMS resources managed by the HA is normal. In the single-node system, the FMS resource is in the normal state. In the dual-node system, the FMS resource is in the normal state on the active node and in the stopped state on the standby node.

- If it is, go to **Step 6**.
- If it is not, go to **Step 4**.

Step 4 Run the **vi ${BIGDATA_LOG_HOME}/omm/oms/fms/fms.log** and **vi ${BIGDATA_LOG_HOME}/omm/oms/fms/scriptlog/fms_ha.log** commands to view the FMS resource logs, check whether the keyword **ERROR** exists. Analyze the logs to locate and rectify the fault.

Step 5 5 minutes later, check whether this alarm is cleared.

- If it is, no further action is required.
- If it is not, go to **Step 6**.

Collect fault information.

Step 6 On FusionInsight Manager, choose **O&M**> **Log** > **Download**.

Step 7 Select **Controller** and **OmmServer** for **Service** and click **OK**.

Step 8 Click in the upper right corner. In the displayed dialog box, set **Start Date** and **End Date** to 1 hour before and after the alarm generation time respectively and click **OK**. Then, click **Download**.

Step 9 Contact the technical support and send the collected log information.

----End

Alarm Clearance

This alarm will be automatically cleared after the fault is rectified.

Related Information

None.

1.3.49 ALM-12075 PMS Resource Is Abnormal

Alarm Description

HA checks the pms resources of Manager every 55 seconds. This alarm is generated when HA detects that the pms resources are abnormal for three consecutive times.

This alarm is cleared when the PMS resource is normal.

Resource Type of PMS is **Single-active**. Active/standby will be triggered upon resource exceptions. When this alarm is generated, the active/standby switchover is complete and new PMS resources have been enabled on the new active FusionInsight Manager. In this case, this alarm is cleared. This alarm is used to notify users of the cause of the active/standby switchover.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12075	Major	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

- The alarm persists for a long time, causing frequent active/standby switchovers of FusionInsight Manager. As a result, users cannot log in to FusionInsight Manager and perform O&M operations.
- The PMS process repeatedly restarts. As a result, monitoring data collection fails during the alarm reporting period. In severe cases, monitoring data may be lost during the alarm reporting period.

Possible Causes

The PMS process is abnormal.

Handling Procedure

Check whether the PMS process is abnormal.

Step 1 In the alarm list on FusionInsight Manager, locate the row that contains the alarm, and view the name of the host for which the alarm is generated.

Step 2 Log in to the host for which the alarm is generated as user **root**.

Step 3 Run the **su -omm** command and then the **sh ${BIGDATA_HOME}/om-server/OMS/workspace0/ha/module/hacom/script/status_ha.sh** command to check whether the status of the PMS resources managed by the HA is normal. In the single-node system, the PMS resource is in the normal state. In the dual-node system, the PMS resource is in the normal state on the active node and in the stopped state on the standby node.

- If it is, go to **Step 6**.
- If it is not, go to **Step 4**.

Step 4 Run the **vi ${BIGDATA_LOG_HOME}/omm/oms/pms/pms.log** and **vi ${BIGDATA_LOG_HOME}/omm/oms/pms/scriptlog/pms_ha.log** commands to view the PMS resource logs, check whether the keyword **ERROR** exists. Analyze the logs to locate and rectify the fault.

Step 5 Five minutes later, check whether this alarm is cleared.

- If it is, no further action is required.
- If it is not, go to **Step 6**.

Collect fault information.

Step 6 On FusionInsight Manager, choose **O&M**> **Log** > **Download**.

Step 7 Select **Controller** and **OmmServer** for **Service** and click **OK**.

Step 8 Click in the upper right corner. In the displayed dialog box, set **Start Date** and **End Date** to 1 hour before and after the alarm generation time respectively and click **OK**. Then, click **Download**.

Step 9 Contact the technical support and send the collected log information.

----End

Alarm Clearance

This alarm will be automatically cleared after the fault is rectified.

Related Information

None.

1.3.50 ALM-12076 GaussDB Resource Is Abnormal

Alarm Description

HA checks the Manager database every 10 seconds. This alarm is generated when HA detects that the database is abnormal for 3 consecutive times.

This alarm is cleared when the database is normal.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12076	Major	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

If the database is abnormal, all core services and related service processes of Manager, such as the alarm, monitoring, and query functions, are affected.

Possible Causes

An exception occurs in the database.

Handling Procedure

Check the database status of the active and standby management nodes.

Step 1 Log in to the active and standby management nodes respectively as user **root**. Run the **su - ommdba** command to switch to user **ommdba**, and then run the **gs_ctl query** command to check whether the following information is displayed in the command output.

Command output of the active management node:

```
Ha state:
        LOCAL_ROLE: Primary
        STATIC_CONNECTIONS          : 1
        DB_STATE                    : Normal
        DETAIL_INFORMATION          : user/password invalid
Senders info:
        No information
Receiver info:
        No information
```

Command output of the standby management node:

```
Ha state:
    LOCAL_ROLE: Standby
    STATIC_CONNECTIONS          : 1
    DB_STATE                    : Normal
    DETAIL_INFORMATION          : user/password invalid
Senders info:
    No information
Receiver info:
    No information
```

- If it is, go to **Step 3**.
- If it is not, go to **Step 2**.

Step 2 Contact the network administrator to check whether the network is faulty.

- If it is, go to **Step 3**.
- If it is not, go to **Step 5**.

Step 3 Five minutes later, check whether the alarm is cleared.

- If it is, no further action is required.
- If it is not, go to **Step 4**.

Step 4 Log in to the active and standby management nodes, run the **su -omm** command to switch to user **omm**, go to the **${BIGDATA_HOME} /om-server/om/sbin/** directory, and run the **status-oms.sh** script to check whether the floating IP addresses and GaussDB resources of the active and standby FusionInsight Managers are in the status shown in the following figure.

```
acs                     Normal          Normal          Single_active
aos                     Normal          Normal          Single_active
cep                     Normal          Normal          Single_active
controller              Normal          Normal          Single_active
feed_watchdog           Normal          Normal          Double_active
floatip                 Normal          Normal          Single_active
fms                     Normal          Normal          Single_active
gaussDB                 Active_normal   Normal          Active_standby
heartBeatCheck          Normal          Normal          Single_active
httpd                   Normal          Normal          Single_active
iam                     Normal          Normal          Single_active
ntp                     Active_normal   Normal          Active_standby
okerberos               Normal          Normal          Double_active
oldap                   Active_normal   Normal          Active_standby
pms                     Normal          Normal          Single_active
tomcat                  Normal          Normal          Single_active
acs                     Stopped         Normal          Single_active
aos                     Stopped         Normal          Single_active
cep                     Stopped         Normal          Single_active
controller              Stopped         Normal          Single_active
feed_watchdog           Normal          Normal          Double_active
floatip                 Stopped         Normal          Single_active
fms                     Stopped         Normal          Single_active
gaussDB                 Standby_normal  Normal          Active_standby
heartBeatCheck          Stopped         Normal          Single_active
httpd                   Stopped         Normal          Single_active
```

- If they are, find the alarm in the alarm list and manually clear the alarm.
- If they are not, go to **Step 5**.

Collect fault information.

Step 5 On FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 6 Select **OmmServer** for **Service** and click **OK**.

Step 7 Click in the upper right corner. In the displayed dialog box, set **Start Date** and **End Date** to 10 minutes before and after the alarm generation time respectively and click **OK**. Then, click **Download**.

Step 8 Contact the technical support and send the collected log information.

----End

Alarm Clearance

This alarm will be automatically cleared after the fault is rectified.

Related Information

None.

1.3.51 ALM-12077 User omm Expired

Alarm Description

The system starts at 00:00 every day to check whether user **omm** has expired every eight hours. This alarm is generated if the user account has expired.

This alarm is cleared when the expiration time of user **omm** is changed and the user account status becomes normal.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12077	Major	Security	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.

Type	Parameter	Description
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the details for which the alarm is generated.

Impact on the System

User **omm** has expired. The node trust relationship is unavailable, and FusionInsight Manager cannot manage the services.

Possible Causes

User **omm** has expired.

Handling Procedure

Check whether user omm in the system has expired.

Step 1 Log in to the faulty node as user **root**.

Run the **chage -l omm**command to view the information about the password of user **omm**.

Step 2 View the value of **Account expires** to check whether the user configurations have expired.

NOTE

If the parameter value is **never**, the user configurations never expire.

- If they do, go to **Step 3**.
- If they do not, go to **Step 4**.

Step 3 Run the **chage -E 'yyyy-MM-dd' omm** command to set the expiration time of user **omm**. Eight hours later, check whether the alarm is automatically cleared.

- If it is, no further action is required.
- If it is not, go to **Step 4**.

Collect fault information.

Step 4 On FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 5 Select **NodeAgent** for **Service** and click **OK**.

Step 6 Click in the upper right corner. In the displayed dialog box, set **Start Date** and **End Date** to 10 minutes before and after the alarm generation time respectively and click **OK**. Then, click **Download**.

Step 7 Contact the technical support and send the collected log information.

----End

Alarm Clearance

This alarm will be automatically cleared after the fault is rectified.

Related Information

None.

1.3.52 ALM-12078 Password of User omm Expired

Alarm Description

The system starts at 00:00 every day to check whether the password of user **omm** has expired every 8 hours. This alarm is generated if the password has expired.

This alarm is cleared when the expiration time of user **omm** password is changed and the user password status becomes normal.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12078	Critical	Security	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the details for which the alarm is generated.

Impact on the System

The password of user **omm** has expired. The node trust relationship is unavailable, and FusionInsight Manager cannot manage the services. The **crontab** scheduled task cannot be executed, affecting the ClickHouse service.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Possible Causes

The password of user **omm** has expired.

Handling Procedure

Check whether the password of user omm in the system has expired.

Step 1 Log in to the faulty node as user **root**.

Run the **chage -l omm**command to view the information about the password of user **omm**.

Step 2 View the value of **Password expires** to check whether the user configurations have expired.

NOTE

If the parameter value is **never**, the user configurations never expire.

- If they do, go to **Step 3**.
- If they do not, go to **Step 4**.

Step 3 Run the **chage -M '***days***' omm** command to set the validity period of the password for user **omm**. Eight hours later, check whether the alarm is automatically cleared.

If *days* is set to **99999**, it indicates that the password never expires.

- If it is, no further action is required.
- If it is not, go to **Step 4**.

Collect fault information.

Step 4 On FusionInsight Manager, choose **O&M**> **Log** > **Download**.

Step 5 Select **NodeAgent** for **Service** and click **OK**.

Step 6 Click edit icon in the upper right corner. In the displayed dialog box, set **Start Date** and **End Date** to 10 minutes before and after the alarm generation time respectively and click **OK**. Then, click **Download**.

Step 7 Contact the technical support and send the collected log information.

----End

Alarm Clearance

This alarm will be automatically cleared after the fault is rectified.

Related Information

None.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

1.3.53 ALM-12079 User omm Is About to Expire

Alarm Description

The system starts at 00:00 every day to check whether user **omm** is about to expire every 8 hours. This alarm is generated if the user account will expire no less than 15 days later.

This alarm is cleared when the expiration time of user **omm** is changed and the user account status becomes normal.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12079	Minor	Security	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the details for which the alarm is generated.

Impact on the System

User **omm** has expired. The node trust relationship is unavailable, and FusionInsight Manager cannot manage the services.

Possible Causes

The account of user **omm** is about to expire.

Handling Procedure

Check whether user omm is about to expire.

Step 1 Log in to the faulty node as user **root**.

Run the **chage -l omm** command to view the information about the password of user **omm**.

Step 2 View the value of **Account expires** to check whether the user configurations are about to expire.

NOTE

If the parameter value is **never**, the user and password are valid permanently; if the value is a date, check whether the user and password are about to expire within 15 days.

- If they are, go to **Step 3**.
- If they are not, go to **Step 4**.

Step 3 Run the **chage -E** *'yyyy-MM-dd'* **omm** command to set the validity period of user **omm**. Eight hours later, check whether the alarm is automatically cleared.

- If it is, no further action is required.
- If it is not, go to **Step 4**.

Collect fault information.

Step 4 On FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 5 Select **NodeAgent** for **Service** and click **OK**.

Step 6 Click in the upper right corner. In the displayed dialog box, set **Start Date** and **End Date** to 10 minutes before and after the alarm generation time respectively and click **OK**. Then, click **Download**.

Step 7 Contact the technical support and send the collected log information.

----End

Alarm Clearance

This alarm will be automatically cleared after the fault is rectified.

Related Information

None.

1.3.54 ALM-12080 Password of User omm Is About to Expire

Alarm Description

The system starts at 00:00 every day to check whether the password of user **omm** is about to expire every 8 hours. This alarm is generated if the password will expire no less than 15 days later.

This alarm is cleared when the expiration time of user **omm** password is reset and the user password status becomes normal.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12080	Major	Security	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.

Type	Parameter	Description
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the details for which the alarm is generated.

Impact on the System

The password of user **omm** has expired. The node trust relationship is unavailable, and FusionInsight Manager cannot manage the services. The **crontab** scheduled task cannot be executed, affecting the ClickHouse service.

Possible Causes

The password of user **omm** is about to expire.

Handling Procedure

Check whether the password of user omm in the system is about to expire.

Step 1 Log in to the faulty node as user **root**.

Run the **chage -l omm**command to view the information about the password of user **omm**.

Step 2 View the value of **Password expires** to check whether the user configurations are about to expire.

NOTE

If the parameter value is **never**, the user and password are valid permanently; if the value is a date, check whether the user and password are about to expire within 15 days.

- If they are, go to **Step 3**.
- If they are not, go to **Step 4**.

Step 3 Run the **chage -M '***days***' omm** command to set the validity period of the password for user **omm**. Eight hours later, check whether the alarm is automatically cleared.

- If it is, no further action is required.
- If it is not, go to **Step 4**.

Collect fault information.

Step 4 On FusionInsight Manager, choose **O&M**> **Log** > **Download**.

Step 5 Select **NodeAgent** for **Service** and click **OK**.

Step 6 Click edit icon in the upper right corner. In the displayed dialog box, set **Start Date** and **End Date** to 10 minutes before and after the alarm generation time respectively and click **OK**. Then, click **Download**.

Step 7 Contact the technical support and send the collected log information.

----End

Alarm Clearance

This alarm will be automatically cleared after the fault is rectified.

Related Information

None.

1.3.55 ALM-12081 User ommdba Expired

Alarm Description

The system starts at 00:00 every day to check whether user **ommdba** has expired every 8 hours. This alarm is generated if the user account has expired.

This alarm is cleared when the expiration time of user **ommdba** is reset and the user account status becomes normal.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12081	Major	Security	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the details for which the alarm is generated.

Impact on the System

The OMS database cannot be managed and data cannot be accessed.

Possible Causes

The account of user **ommdba** for the host has expired.

Handling Procedure

Check whether user ommdba has expired.

Step 1 Log in to the faulty node as user **root**.

Run the **chage -l ommdba** command to view the information about the password of user **ommdba**.

Step 2 View the value of **Account expires** to check whether the user configurations have expired.

NOTE

If the parameter value is **never**, the user and password are valid permanently; if the value is a date, check whether the user and password have expired.

- If they do, go to **Step 3**.
- If they do not, go to **Step 4**.

Step 3 Run the **chage -E** *'yyyy-MM-dd'* **omm** command to set the validity period of user **ommdba**. Eight hours later, check whether the alarm is automatically cleared.

- If it is, no further action is required.
- If it is not, go to **Step 4**.

Collect fault information.

Step 4 On FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 5 Select **NodeAgent** for **Service** and click **OK**.

Step 6 Click in the upper right corner. In the displayed dialog box, set **Start Date** and **End Date** to 10 minutes before and after the alarm generation time respectively and click **OK**. Then, click **Download**.

Step 7 Contact the technical support and send the collected log information.

----End

Alarm Clearance

This alarm will be automatically cleared after the fault is rectified.

Related Information

None.

1.3.56 ALM-12082 User ommdba Is About to Expire

Alarm Description

The system starts at 00:00 every day to check whether user **ommdba** is about to expire every 8 hours. This alarm is generated if the user account will expire no less than 15 days later.

This alarm is cleared when the expiration time of user **ommdba** is reset and the user account status becomes normal.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12082	Minor	Security	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	Detail	Specifies the details for which the alarm is generated.

Impact on the System

The OMS database cannot be managed and data cannot be accessed.

Possible Causes

The account of user **ommdba** for the host is about to expire.

Handling Procedure

Check whether user ommdba is about to expire.

Step 1 Log in to the faulty node as user **root**.

Run the **chage -l ommdba** command to view the information about user **ommdba**.

Step 2 View the value of **Account expires** to check whether the user configurations are about to expire.

NOTE

If the parameter value is **never**, the user and password are valid permanently; if the value is a date, check whether the user and password are about to expire within 15 days.

- If they are, go to **Step 3**.
- If they are not, go to **Step 4**.

Step 3 Run the **chage -E** *'yyyy-MM-dd'* **ommdba** command to set the validity period of user **ommdba**. Eight hours later, check whether the alarm is automatically cleared.

- If it is, no further action is required.
- If it is not, go to **Step 4**.

Collect fault information.

Step 4 On FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 5 Select **NodeAgent** for **Service** and click **OK**.

Step 6 Click in the upper right corner. In the displayed dialog box, set **Start Date** and **End Date** to 10 minutes before and after the alarm generation time respectively and click **OK**. Then, click **Download**.

Step 7 Contact the technical support and send the collected log information.

----End

Alarm Clearance

This alarm will be automatically cleared after the fault is rectified.

Related Information

None.

1.3.57 ALM-12083 Password of User ommdba Is About to Expire

Alarm Description

The system starts at 00:00 every day to check whether the password of user **ommdba** is about to expire every 8 hours. This alarm is generated if the password is about to expire no less than 15 days later.

This alarm is cleared when the expiration time of user **ommdba** password is reset and the user password status becomes normal.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12083	Minor	Security	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the details for which the alarm is generated.

Impact on the System

The OMS database cannot be managed and data cannot be accessed.

Possible Causes

The password of user **ommdba** is about to expire.

Handling Procedure

Check whether the password of user ommdba in the system is about to expire.

Step 1 Log in to the faulty node as user **root**.

Run the **chage -l ommdba** command to view the information about the password of user **ommdba**.

Step 2 View the value of **Password expires** to check whether the user configurations are about to expire.

NOTE

If the parameter value is **never**, the user and password are valid permanently; if the value is a date, check whether the user and password are about to expire within 15 days.

- If they are, go to **Step 3**.
- If they are not, go to **Step 4**.

Step 3 Run the **chage -M** *'days'* **ommdba** command to set the validity period of the password for user **ommdba**. Eight hours later, check whether the alarm is automatically cleared.

- If it is, no further action is required.

- If it is not, go to **Step 4**.

Collect fault information.

Step 4 On FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 5 Select **NodeAgent** for **Service** and click **OK**.

Step 6 Click in the upper right corner. In the displayed dialog box, set **Start Date** and **End Date** to 10 minutes before and after the alarm generation time respectively and click **OK**. Then, click **Download**.

Step 7 Contact the technical support and send the collected log information.

----End

Alarm Clearance

This alarm will be automatically cleared after the fault is rectified.

Related Information

None.

1.3.58 ALM-12084 Password of User ommdba Expired

Alarm Description

The system starts at 00:00 every day to check whether the password of user **ommdba** has expired every 8 hours. This alarm is generated if the password has expired.

This alarm is cleared when the expiration time of user **ommdba** password is reset and the user password status becomes normal.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12084	Major	Security	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the details for which the alarm is generated.

Impact on the System

The password of user **ommdba** has expired. The node trust relationship is unavailable, and FusionInsight Manager cannot manage the services.

Possible Causes

The password of user **ommdba** for the host has expired.

Handling Procedure

Check whether the password of user ommdba in the system has expired.

Step 1 Log in to the faulty node as user **root**.

Run the **chage -l ommdba** command to view the information about the password of user **ommdba**.

Step 2 View the value of **Password expires** to check whether the user configurations have expired.

NOTE

If the parameter value is **never**, the user and password are valid permanently; if the value is a date, check whether the user and password have expired.

- If they do, go to **Step 3**.
- If they do not, go to **Step 4**.

Step 3 Run the **chage -M** *'days'* **ommdba** command to set the validity period of the password for user **ommdba**. Eight hours later, check whether the alarm is automatically cleared.

If *days* is set to **99999**, it indicates that the password never expires.

- If it is, no further action is required.
- If it is not, go to **Step 4**.

Collect fault information.

Step 4 On FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 5 Select **NodeAgent** for **Service** and click **OK**.

Step 6 Click in the upper right corner. In the displayed dialog box, set **Start Date** and **End Date** to 10 minutes before and after the alarm generation time respectively and click **OK**. Then, click **Download**.

Step 7 Contact the technical support and send the collected log information.

----End

Alarm Clearance

This alarm will be automatically cleared after the fault is rectified.

Related Information

None.

1.3.59 ALM-12085 Service Audit Log Dump Failure

Alarm Description

The system dumps service audit logs at 03:00 every day and stores them on the OMS node. This alarm is generated when the dump fails. This alarm is cleared when the next dump succeeds.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12085	Minor	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	Detail	Specifies the details for which the alarm is generated.

Impact on the System

If the audit logs of a component fail to be dumped, the audit logs cannot be retrieved if they are aged locally. This affects service analysis and troubleshooting of the component.

Possible Causes

- The service audit logs are oversized.
- The OMS backup storage space is insufficient.
- The storage space of a host where the service is located is insufficient.

Handling Procedure

Check whether the service audit logs are oversized.

Step 1 In the alarm list on FusionInsight Manager, locate the row that contains the alarm, and view the IP address of the host and additional information for which the alarm is generated.

Step 2 Log in to the host where the alarm is generated as user **root**.

Step 3 Run the **vi ${BIGDATA_LOG_HOME}/controller/scriptlog/getLogs.log** command to check whether the keyword "LOG SIZE is more than 5000MB" can be searched.

- If it can, go to **Step 4**.
- If it cannot, go to **Step 5**.

Step 4 Check whether the oversized service audit logs are caused by exceptions.

The OMS backup storage space is insufficient.

Step 5 Run the **vi ${BIGDATA_LOG_HOME}/controller/scriptlog/getLogs.log** command to check whether the keyword "Collect log failed, too many logs on" can be searched.

- If it can, obtain the host IP address following the keyword "Collect log failed, too many logs on", and go to **Step 6**.
- If it cannot, go to **Step 11**.

Step 6 Log in to the host with the IP address obtained in **Step 5** as user **root**.

Step 7 Run the **vi {BIGDATA_LOG_HOME}/nodeagent/scriptlog/collectLog.log** command to check whether the keyword "log size exceeds" can be searched.

- If it can, go to **Step 9**.
- If it cannot, go to **Step 8**.

Step 8 Check whether the alarm additional information contains the keyword "no enough space".

- If yes, go to **Step 9**.
- If no, go to**Step 11**.

Step 9 Perform the following operations to expand the disk capacity or reduce the maximum number of audit log backups:

- Expand the capacity of the OMS node by following the instructions in section **Adding New Disks to an Existing Node** of *MapReduce Service (MRS) 3.3.1-LTS Physical Machine Cluster Component Migration Guide (for Huawei Cloud Stack 8.3.1)*.
- Run the following command to edit the file and decrease the value of **MAX_NUM_BK_AUDITLOG**.

  vi ${CONTROLLER_HOME}/etc/om/componentsauditlog.properties

Step 10 In the next execution period, 03:00, check whether the alarm is cleared.

- If it is, no further action is required.
- If it is not, go to **Step 11**.

Check whether the space of the host where the service is located is insufficient.

Step 11 Run the **vi ${BIGDATA_LOG_HOME}/controller/scriptlog/getLogs.log** command to check whether the keyword "Collect log failed, no enough space on *hostIp*" can be searched.

- If it can, obtain the IP address of the abnormal host and go to **Step 12**.
- If it cannot, go to **Step 15**.

Step 12 Log in to the host with the IP address obtained as user **root**, and run the **df "$BIGDATA_HOME/tmp" -lP | tail -1 | awk '{print ($4/1024)}'** command to obtain the remaining space of the host log directory. Check whether the value is less than 1000 MB.

- If it is, go to **Step 13**.
- If it is not, go to **Step 15**.

Step 13 Expand the capacity of the node by following the instructions in section **Adding New Disks to an Existing Node** of *MapReduce Service (MRS) 3.3.1-LTS Physical Machine Cluster Capacity Expansion Guide (for Huawei Cloud Stack 8.3.1)*.

Step 14 In the next execution period, 03:00, check whether the alarm is cleared.

- If it is, no further action is required.
- If it is not, go to **Step 15**.

Collect fault information.

Step 15 On FusionInsight Manager, choose **O&M**> **Log** > **Download**.

Step 16 Select **Controller** for **Service** and click **OK**.

Step 17 Click in the upper right corner. In the displayed dialog box, set **Start Date** and **End Date** to 10 minutes before and after the alarm generation time respectively and click **OK**. Then, click **Download**.

Step 18 Contact the technical support and send the collected log information.

----End

Alarm Clearance

This alarm will be automatically cleared after the fault is rectified.

Related Information

None.

1.3.60 ALM-12087 System Is in the Upgrade Observation Period

Alarm Description

The system checks whether it is in the upgrade observation period at 00:00 every day and checks whether the duration that it has been in the upgrade observation state exceeds the preset upgrade observation period, 10 days by default. This alarm is generated when the system is in the upgrade observation period and the duration that the system has been in the upgrade observation state exceeds the preset period (10 days by default). This alarm is automatically cleared if the system exits the upgrade observation period after the user performs a rollback or submission.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12087	Major	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the details for which the alarm is generated.

Impact on the System

During the upgrade observation period, do not add or delete users, instances, roles, services, hosts, or resource pools that affect the management topology.

Possible Causes

The upgrade task is not submitted a specified period of time (10 days by default) after the system upgrade.

Handling Procedure

Check whether the system is in the upgrade observation period.

Step 1 Log in to the active management node as user **root**.

Step 2 Run the following commands to switch to user **omm** and log in to the **omm** database:

su - omm

gsql -U omm -W *omm database password* **-p 20015**

Step 3 Run the **select * from OM_CLUSTERS** command to view cluster information.

Step 4 Check whether the value of **upgradObservationPeriod isON** is **true**, as shown in **Figure 1-5**.

- If it is, the system is in the upgrade observation period. Use the UpdateTool to submit the upgrade task. For details, see the upgrade guide of the corresponding version.
- If it is not, go to **Step 6**.

Figure 1-5 Cluster information

```
CLUSTER_ID | CLUSTER_NAME | CLUSTER_DESCRIPTION |  STACK_NAME   |  STACK_TIME   | PRESTACK_NAME | PRESTACK_TIME | STACK_MODEL | CURRENT_PATCH_VERSION | IS_DETACHED | UPDATE_MODE |
                          | OBSERVATION_PERIOD                                                                                  | EXTERN_PARAM
-----------+--------------+---------------------+---------------+---------------+---------------+---------------+-------------+-----------------------+-------------+-------------+-----------------------------------------------------------------------------------------------------------------------------------------------------
-----------+--------------+---------------------+---------------+---------------+---------------+---------------+-------------+-----------------------+-------------+-------------+-----------------------------------------------------------------------------------------------------------------------------------------------------
cluster_1  | Test_1       |                     | DEFAULT_STACK | 1552290738986 |               |               | Sec         |                       |           0 |             | {"upgradeObservationPeriod":{"isOn":true, proje
":"1903180931467010l0","type":"UPGRADE"},"updateEndTime":1552881484884},"patchObservationPeriod":{"isOn":false,"updateEndTime":0}} | {}
```

Step 5 In the early morning of the next day, check whether this alarm is cleared.

- If it is, no further action is required.
- If it is not, go to **Step 6**.

Collect fault information.

Step 6 On the FusionInsight Manager portal, choose **O&M** > **Log** > **Download**.

Step 7 Select **Controller** from the **Service** and click **OK**.

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact the technical support and send the collected log information.

----End

Alarm Clearance

This alarm will be automatically cleared after the fault is rectified.

Related Information

None.

1.3.61 ALM-12089 Network Connections Between Nodes Are Abnormal

Alarm Description

The alarm module checks the network health status of nodes in the cluster every 10 seconds. This alarm is generated when the network between two nodes is unreachable or the network status is unstable.

This alarm is cleared when the network recovers.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12089	Major	Communications	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	Trigger condition	Specifies the trigger condition of the alarm.

Impact on the System

- Data transmission becomes slow or interrupted. Data may be lost or incomplete.
- Task scheduling is affected. For example, Yarn tasks cannot be executed properly or fail to be executed due to timeout.
- Data processing is affected. For example, HDFS data synchronization fails or the data is inaccurate.
- System performance deteriorates. The efficiency and quality of data processing is low.

Possible Causes

- A node breaks down.
- The network is faulty.

Handling Procedure

Check the network health status.

Step 1 In the alarm list on FusionInsight Manager, locate the row that contains the alarm, click ⌄, and view the description in additional information. Record the source IP address and destination IP address of the node for which the alarm is reported.

Step 2 Log in to the node for which the alarm is reported . On the node, ping the target node to check whether the network between the two nodes is normal.

- If yes, go to **6**.
- If no, go to **3**.

Check the node status.

Step 3 On FusionInsight Manager, click **Host** and check whether the host list contains the faulty node to determine whether the faulty node has been removed from the cluster.

- If yes, go to **5**.
- If no, go to **4**.

Step 4 Check whether the faulty node is powered off.

- If yes, start the node and go to **Step 2**.
- If no, contact the engineer in charge to locate the fault. If you need to remove the faulty node from the cluster, go to **5**. If you do not need, go to **6**.

Step 5 Remove the faulty node from the **$NODE_AGENT_HOME/etc/agent/hosts.ini** file on all nodes in the cluster, clear the **/var/log/Bigdata/unreachable/unreachable_ip_info.log** file, and clear the alarm.

Step 6 Wait 30 seconds, check whether the alarm is automatically cleared.

- If yes, no further action is required.
- If no, go to 7.

Collect fault information.

Step 7 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 8 Expand the **Service** drop-down list, select **OmmAgent** for the target cluster, and click **OK**.

Step 9 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.62 ALM-12091 Abnormal disaster Resources

Alarm Description

HA checks the disaster resources of Manager every 86 seconds. This alarm is generated when HA detects that the disaster resources have been abnormal for 10 consecutive times.

This alarm is cleared when HA detects that the disaster resources become normal.

Resource Type of disaster is **Single-active**. Active/Standby switchover will be triggered upon resource exceptions. When this alarm is generated, the active/standby switchover is complete and new disaster resources have been enabled on the new active Manager. In this case, this alarm is cleared. This alarm is used to notify users of the cause of the active/standby Manager switchover.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12091	Major	Quality of service	Tenant plane	FusionInsight Manager	Yes

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

- An active/standby Manager switchover is triggered.
- If the disaster process is still abnormal after the switchover, switchover will be performed repeatedly. The DR function may be unavailable or the FusionInsight Manager page cannot be accessed.

Possible Causes

The disaster process is abnormal.

Handling Procedure

Check whether the disaster process is normal.

Step 1 In the alarm list on FusionInsight Manager, locate the row that contains the alarm, and click ⌄ to view the name of the host for which the alarm is generated.

Step 2 Log in to the host for which the alarm is generated as user **root**.

Step 3 Run the **su - omm** command to switch to user **omm**.

Step 4 Run the **sh ${BIGDATA_HOME}/om-server/OMS/workspace0/ha/module/hacom/script/status_ha.sh** command to check whether the status of the disaster resources managed by the HA is normal. In the single-node system, the disaster resource is in the normal state. In the dual-node system, the disaster resource is in the normal state on the active node and in the stopped state on the standby node.

- If yes, go to **Step 7**.
- If no, go to **Step 5**.

Step 5 Run the **vi ${BIGDATA_LOG_HOME}/disaster/disaster.log** command to check whether the disaster resource log of HA contains the keyword **ERROR**. If yes, analyze the logs to locate the resource exception cause and fix the exception.

Step 6 Wait 5 minutes and check whether the alarm is automatically cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect fault information.

Step 7 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 8 Expand the **Service** drop-down list, select **Disaster** for the target cluster, and click **OK**.

Step 9 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

1.3.63 ALM-12099 Core Dump for Cluster Processes

Alarm Description

Core files generated when applications crash are centrally managed on a cluster. This alarm is generated when a new core file is detected.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12099	Minor	Quality of service	Tenant plane	FusionInsight Manager	No

Alarm Changes

Change Type	Version	Description	Reason for Change
Modify	3.3.1	–Alarm Name: changed from "Core Dump Occurred" to "Core Dump for Cluster Processes".	Alarm Name: Standardized

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	Viewing the timestamp	Timestamp
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Details	Specifies alarm details.

Impact on the System

If a key process crashes, the cluster may be unavailable for a short period of time.

Possible Causes

Processes crash.

Handling Procedure

CAUTION

- The following operations for parsing and viewing core file stack information may involve sensitive user data. Developers or technical support can perform these operations only after being authorized by users.
- By default, the system keeps the core files the alarm is generated for for 72 hours. The system automatically clears the files upon expiration or if the files are too large. If this alarm is report, contact technical support as soon as possible.

Step 1 In the alarm list on FusionInsight Manager, locate the row that contains the alarm, view the host address for which the alarm is generated in the alarm details, and view the path for storing the core files specified by the **DumpedFilePath** attribute in the additional information.

Step 2 Log in to the host for which the alarm is generated as user **omm** and run the **gdb --version** command to check whether the gdb tool is installed on the host.

- If no, install the gdb tool and then go to **Step 3**.
- If yes, go to **Step 3**.

Step 3 Use the gdb tool to view the detailed stack information about the core files.

1. Go to the **DumpedFilePath** directory and find the core files.
2. Run the following command to obtain the symbol table of the core files:

   source $BIGDATA_HOME/mppdb/.mppdbgs_profile

   cd ${BIGDATA_HOME}/FusionInsight_MPPDB_*XXX*/install/FusionInsight-MPPDB-*XXX*/package/MPPDB_ALL_PACKAGE

   tar -xzvf GaussDB-Kernel-V300R002C00- *Operating system*-**64bit-symbol.tar.gz**

   cd symbols/bin/

   Find the symbol table file whose name is the same as the process name in the alarm. For example, the symbol table of **cm_agent** is **cm_agent.symbol**.

   Copy the symbol table to the **${GAUSSHOME}/bin** directory.
3. Run the **gdb --batch -n -ex thread -ex bt** *Core file name* command to view the detailed stack information about the core file.

Step 4 Contact technical support and provide the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system does not automatically clear this alarm and you need to manually clear the alarm.

Related Information

None.

1.3.64 ALM-12100 AD Service Connection Failed

Alarm Description

After a third-party active directory (AD) is interconnected, the third-party AD domain user can be synchronized using the synchronization period (60 minutes by default) or manually. During data synchronization, the AD service status will be checked. This alarm is generated when AD service unavailability is detected for three consecutive times. This alarm is cleared when AD service recovers.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12100	Major	Communications	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

When the alarm is generated, the AD service is unavailable, and AD domain user synchronization fails. An AD domain user cannot log in to FusionInsight Manager and execute services.

Possible Causes

- The configuration item for interconnecting with the third-party AD is incorrect.
- The network connection between FusionInsight and the third-party AD service is faulty.
- AD server fault
- AD service fault

Handling Procedure

Check the third-party AD configuration.

Step 1 On the **FusionInsight Manager** page, choose **System** > **Permission** > **Third-Party AD**. The third-party AD configuration page is displayed.

Step 2 Check whether the **AD IP Address**, **LDAP Port**, **Bind DN**, and **Bind DN Password** parameters are correctly set. For details, see section "Third-Party AD Management" in *MapReduce Service (MRS) 3.3.1-LTS User Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Usage Guide (for Huawei Cloud Stack 8.3.1)*.

- If yes, go to **Step 5**.
- If no, go to **Step 3**.

Step 3 Modify the incorrect parameters, and then click **OK**.

Step 4 Choose **System** > **Permission** > **User** > **AD Domain User**, click **Manual Synchronization**, and check whether the message "Manual synchronization successfully." is displayed in the upper right corner of the page.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check the third-party AD server and the network.

Step 5 Log in to the active management node as user **root**.

Step 6 On the host you have logged in to, ping the IP address of the third-party AD server to check whether the third-party AD server can be pinged.

- If yes, go to **Step 7**.
- If no, go to **Step 8**.

Step 7 Run the following command to check whether the third-party AD service can be connected:

telnet *IP port*

IP indicates the IP address of the third-party AD server, and *port* indicates the port used by the third-party AD server.

- If yes, go to **Step 8**.
- If no, contact technical support to check the network.

Step 8 Contact the third-party AD service administrator to check whether the AD service is normal.

- If yes, go to **Step 9**.
- If no, contact the third-party AD service administrator to rectify the AD server fault.

Collect the fault information.

Step 9 On the **FusionInsight Manager** page, choose **O&M** > **Log** > **Download**.

Step 10 In the **Service** area, select **Controller** under **OMS** and click **OK**.

Step 11 Click in the upper right corner to set **Start Date** and **End Date** to 10 minutes before and after the time when the alarm is generated, and click **Download**.

Step 12 Contact the technical support and send the collected log information.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm. You do not need to manually clear it.

Related Information

None.

1.3.65 ALM-12101 AZ Unhealthy

Alarm Description

After the AZ DR function is enabled, the system checks the AZ health status every 5 minutes. This alarm is generated when the system detects that the AZ is subhealthy or unhealthy. This alarm is cleared when the AZ becomes healthy.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12101	Critical	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	AZName	Specifies the AZ for which the alarm is generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the details for which the alarm is generated.

Impact on the System

The health status of an AZ is determined by whether the health status of storage resources (HDFS), computing resources (Yarn), and key roles in the AZ exceeds the configured threshold.

An AZ is subhealthy when:

- The computing resources (Yarn) are unhealthy, but the storage resources (HDFS) are healthy. Tasks cannot be submitted to the local AZ, but data can still be read and written in the local AZ.
- The computing resources (Yarn) are healthy, but some storage resources (HDFS) are unhealthy. Tasks can be submitted to the local AZ, and some data can be read and written in the local AZ. This depends on the locality of data detected by Spark/Hive scheduling.

An AZ is unhealthy when:

- The computing resources (Yarn) are healthy, but the storage resources (HDFS) are unhealthy. Although tasks can be submitted to the local AZ, data cannot be read or written in the local AZ. As a result, the tasks submitted to the local AZ are invalid.
- The computing resources (Yarn) and storage resources (HDFS) are unhealthy. Tasks cannot be submitted to the local AZ, and data cannot be read or written in the local AZ.
- The health status of key roles except Yarn and HDFS is lower than the configured threshold.

Possible Causes

- The computing resources (Yarn) are unhealthy.
- The storage resources (HDFS) are unhealthy.
- Some storage resources (HDFS) are unhealthy.
- Key roles except Yarn and HDFS are unhealthy.

Handling Procedure

Disable the DR drill.

Step 1 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Cross-AZ HA**. The Cross-AZ HA page is displayed.

Step 2 In the AZ DR list, check whether **Perform DR Drill** in the **Operation** column of the AZ whose health status is **Unhealthy** is gray.

- If yes, go to **Step 4**.
- If no, go to **Step 3**.

Step 3 Click **Restore** in the **Operation** column of the target AZ. Wait 2 minutes and refresh the page to view the health status of the AZ. Check whether the health status is normal.

- If yes, no further action is required.
- If no, go to **Step 4**.

Collect the fault information.

Step 4 Log in to the active management node as user **root**.

Step 5 View logs of unhealthy services.

- HDFS log files are stored in **/var/log/Bigdata/hdfs/nn/hdfs-az-state.log**.
- Yarn log files are stored in **/var/log/Bigdata/yarn/rm/yarn-az-state.log**.

- For other services, view the service health check logs in the corresponding service log directory.

Step 6 Contact technical support and provide detailed log file information.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.66 ALM-12102 AZ HA Component Is Not Deployed Based on DR Requirements

Alarm Description

The alarm module checks the deployment status of AZ HA components every 5 minutes. This alarm is generated when the components that support DR are not deployed based on DR requirements after AZ is enabled. This alarm is cleared when the components are deployed based on DR requirements.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12102	Major	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Details	Specifies alarm details.

Impact on the System

The cross-AZ HA capability of a single cluster is affected.

Possible Causes

The roles of the components that support DR are not deployed based on DR requirements.

Handling Procedure

Obtain alarm information.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**.

Step 2 In the alarm list, click ⌄ in the row that contains the alarm and view the roles that are not deployed based on DR requirements in **Additional Information**.

Redeploy the role instance.

Step 3 Choose **Cluster** > **Services** > *Name of the desired service* > **Instance**. On the instance page, redeploy or adjust the role instance.

Step 4 Wait 10 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, contact technical support.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.67 ALM-12103 Executor Resource Exception

Alarm Description

HA checks the Executor resources of Manager every 30 seconds. This alarm is generated when HA detects that the Executor resources are abnormal for two consecutive times.

This alarm is cleared when the Executor resources are normal.

Resource Type of Executor is **Single-active**. Active/standby will be triggered upon resource exceptions. When this alarm is generated, the active/standby switchover is complete and new Executor resources have been enabled on the new active Manager. In this case, this alarm is cleared. This alarm is used to notify users of the cause of the active/standby Manager switchover.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12103	Major	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Details	Specifies alarm details.

Impact on the System

- The active/standby Manager switchover occurs.
- The Executor process keeps restarting. As a result, the cluster page may fail to be accessed.

Possible Causes

The Executor process is abnormal.

Handling Procedure

Check whether the Executor process is abnormal.

Step 1 In the alarm list on FusionInsight Manager, locate the row that contains the alarm, and click ⌄ to view the name of the host for which the alarm is generated.

Step 2 Log in to the host for which the alarm is generated as user **root**.

Step 3 Run the **su - omm** command to switch to user **omm**.

Step 4 Run the **sh ${BIGDATA_HOME}/om-server/OMS/workspace0/ha/module/hacom/script/status_ha.sh** command to check whether the status of the Executor resources managed by the HA is normal. In the single-node system, the Executor resource is in the normal state. In the dual-node system, the Executor resource is

in the normal state on the active node and in the stopped state on the standby node.

- If yes, go to **Step 7**.
- If no, go to **Step 5**.

Step 5 Run the **vi ${BIGDATA_LOG_HOME}/omm/oms/ha/scriptlog/executor.log** command to check whether the Executor resource log of HA contains the keyword **ERROR**. If yes, analyze the log to locate the resource exception cause and fix the exception.

Step 6 After 5 minutes, check whether this alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect the fault information.

Step 7 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 8 In the **Services** area, select **Controller** and **OmmServer**, and click **OK**.

Step 9 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.68 ALM-12104 Abnormal Knox Resources

Alarm Description

HA checks the Knox resources of Manager every 70 seconds. This alarm is generated when HA detects that the Knox resources are abnormal for three consecutive times.

This alarm is cleared when HA detects that the Knox resources are normal.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12104	Major	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Details	Specifies alarm details.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

Requests sent by upper-layer services by using Knox cannot be properly processed.

Possible Causes

The Knox process is abnormal.

Handling Procedure

Check whether the Knox process is normal.

Step 1 Log in to FusionInsight Manager. In the alarm list, locate the row that contains the alarm and view the name of the host for which the alarm is generated.

Step 2 Use PuTTY to log in to the host for which the alarm is generated as user **root**.

Step 3 Run the **su - omm** command to switch to user **omm**.

Step 4 Run the **sh ${BIGDATA_HOME}/om-server/om/sbin/status-oms.sh** command to check whether the status of the Knox resources managed by HA is normal. If the status is normal, the Knox resources are normal. Otherwise, the Knox resources are abnormal.

- If yes, go to **Step 7**.
- If no, go to **Step 5**.

Step 5 Run the **vi ${BIGDATA_LOG_HOME}/omm/oms/ha/scriptlog/knox.log** command to check whether the Knox resource log of HA contains the keyword **ERROR**. If yes, analyze the log to locate the resource exception cause and fix the exception.

Step 6 After 5 minutes, check whether this alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect the fault information.

Step 7 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 8 In the **Services** area, select **Controller** and **OmmServer**, and click **OK**.

Step 9 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

1.3.69 ALM-12110 Failed to get ECS temporary AK/SK

Alarm Description

Meta calls the ECS API to obtain the AK/SK information every 5 minutes and caches the information. Before the AK/SK expires, Meta calls the API again to update it. This alarm is generated when Meta fails to call the API for three consecutive times.

This alarm is cleared when Meta successfully calls the ECS API.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12110	Major	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	RoleName	Specifies the role for which the alarm is generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the details for which the alarm is generated.

Impact on the System

The cluster cannot obtain the latest temporary AK/SK. In the storage and compute separation scenario, OBS may fail to be accessed. As a result, component services cannot be properly processed.

Possible Causes

- The meta role of the MRS cluster is abnormal.
- The cluster has been bound to an agency and accessed OBS but has been unbound from the agency. As a result, the cluster has not been bound to any agency.

Handling Procedure

Check the status of the meta role.

Step 1 On FusionInsight Manager of the cluster, choose **O&M** > **Alarm** > **Alarms**. On the page that is displayed, click ⌄ in the row containing the alarm, and determine the IP address of the host for which the alarm is generated.

Step 2 On FusionInsight Manager of the cluster, choose **Cluster** > **Services** > **meta**. On the page that is displayed, click the **Instance** tab, and check whether the meta role corresponding to the host for which the alarm is generated is normal.

- If yes, go to **Step 5**.
- If no, go to **Step 3**.

Step 3 Select the abnormal role, click **More**, and select **Restart Instance** to restart the abnormal meta role.

Step 4 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Step 5 Log in to the host obtained in **Step 1** and check whether the **/var/log/Bigdata/meta/mrs-meta.log** file contains error information. If yes, rectify the fault based on the log information.

Step 6 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Rebind the cluster to an agency.

Step 7 Log in to the MRS management console.

Step 8 In the navigation pane on the left, choose **Active Clusters**. On the page that is displayed, click the cluster name to go to its overview page. Then, check whether the cluster is bound to an agency in the O&M management area.

- If yes, go to **Step 10**.
- If no, go to **Step 9**.

Step 9 Click **Manage Agency**. On the page that is displayed, rebind the cluster to an agency. Then check whether the alarm is cleared a few minutes later.

- If yes, no further action is required.
- If no, go to **Step 10**.

Collect fault information.

Step 10 On FusionInsight Manager of the active cluster, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 11 Expand the **Service** drop-down list, select **meta** for the target cluster, and click **OK**.

Step 12 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 13 Contact technical support and provide the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.70 ALM-12150 Disconnection Between the Active and DR Clusters

Alarm Description

The system performs a periodic heartbeat detection task every 30 seconds. This alarm is generated when the periodic heartbeat detection task fails. This alarm is cleared when the next heartbeat detection task is performed successfully.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12150	Critical	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Details	Specifies alarm details.

Impact on the System

Some DR operations are restricted and real-time synchronization is affected.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Possible Causes

- The network between the active and DR clusters is disconnected.
- The DR services of the active and DR clusters are abnormal.

Handling Procedure

Check the network status of the active and DR clusters.

Step 1 On FusionInsight Manager of the active cluster, choose **O&M > Alarm > Alarms**, click ⌄ in the row where the alarm is located, and determine the IP address of the host for which the alarm is generated.

Step 2 Log in to the active management node of the active cluster as user **omm** and run the **ping** *IP address of the DR cluster* command to check whether the faulty node is reachable.

- If yes, go to **Step 5**.
- If no, go to **Step 3**.

Step 3 Rectify the network fault between the active and DR clusters.

Step 4 Choose **O&M** > **Alarm** > **Alarms** and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check the DR service status in the active and standby clusters.

Step 5 Log in to the active management node of the active cluster by using PuTTY as user **omm** and run the **sh ${BIGDATA_HOME}/om-server/om/sbin/status-oms.sh** command to check whether the **Disaster** status of the Manager DR service is **Normal**.

- If yes, go to **Step 7**.
- If no, go to **Step 6**.

Step 6 View the **/var/log/Bigdata/disaster/heartbeat.log** file and check whether the logs generated before and after the alarm is generated contain the keyword **ERROR**. Analyze the logs to check the cause of the resource exception and rectify the fault. Then, check whether the alarm is cleared 5 minutes later.

- If yes, no further action is required.
- If no, go to **Step 7**.

Step 7 Log in to the active management node of the DR cluster by using PuTTY as user **omm** and run the **sh ${BIGDATA_HOME}/om-server/om/sbin/status-oms.sh** command to check whether the **Disaster** status of the Manager DR service is **Normal**.

- If yes, go to **Step 9**.
- If no, go to **Step 8**.

Step 8 View the **/var/log/Bigdata/disaster/heartbeat.log** file and check whether the logs generated before and after the alarm is generated contain the keyword **ERROR**. Analyze the logs to check the cause of the resource exception and rectify the fault. Then, check whether the alarm is cleared 5 minutes later.

- If yes, no further action is required.
- If no, go to **Step 9**.

Collect the fault information.

Step 9 On FusionInsight Manager of the active cluster, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 10 In the **Service** dialog box, choose **OMS > Disaster**, select the active node from the **Host** drop-down list, and click **OK**.

Step 11 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.71 ALM-12151 Failed to Synchronize Ranger Permission Information for Cluster DR

Alarm Description

The system synchronizes Ranger permission information every 10 minutes. This alarm is generated when the synchronization fails. This alarm is cleared when the synchronization is successful.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12151	Critical	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.

Type	Parameter	Description
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	Synchronization Information Type	Specifies the type of Ranger information that fails to synchronize.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Details	Specifies alarm details.

Impact on the System

An exception occurs when the Ranger authentication component performs authentication.

Possible Causes

- The network between the active and DR clusters is disconnected.
- The DR service of the active cluster is abnormal.

Handling Procedure

Check the network status of the active and DR clusters.

Step 1 On FusionInsight Manager of the active cluster, choose **O&M > Alarm > Alarms**, click ⌄ in the row where the alarm is located, and determine the IP address of the host for which the alarm is generated.

Step 2 Log in to the active management node of the active cluster as user **omm** and run the **ping** *IP address of the DR cluster* command to check whether the faulty node is reachable.

- If yes, go to **Step 5**.
- If no, go to **Step 3**.

Step 3 Rectify the network fault between the active and DR clusters.

Step 4 Choose **O&M** > **Alarm** > **Alarms** and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check the DR service status in the active cluster.

Step 5 Log in to the active management node of the active cluster as user **omm** and run the **sh ${BIGDATA_HOME}/om-server/om/sbin/status-oms.sh** command to check whether the **Disaster** status of the Manager DR service is **Normal**.

- If yes, go to **Step 7**.
- If no, go to **Step 6**.

Step 6 View the **/var/log/Bigdata/disaster/disaster.log** file and check whether the logs generated before and after the alarm was generated contain the keyword **ERROR**. Analyze the logs to check the cause of the resource exception and rectify the fault. Then, check whether the alarm is cleared 5 minutes later.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect the fault information.

Step 7 On FusionInsight Manager of the active cluster, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 8 In the **Service** dialog box, choose **OMS** > **Disaster**, select the active node from the **Host** drop-down list, and click **OK**.

Step 9 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.72 ALM-12160 RPO of Streaming Data Synchronization of the Cluster DR Protection Group Exceeds the Threshold

Alarm Description

This alarm is generated when the recovery point objective (RPO) exceeds the preset value during data synchronization of a streaming protection group.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12160	Major	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	Protection Group	Specifies the protection group for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

Data may not be completely synchronized between the active and standby DR clusters. If a fault occurs, service data may be lost.

Possible Causes

- The connection between the active and standby DR clusters is interrupted.
- Services in the active and standby DR clusters are abnormal.

Handling Procedure

Check the network status of the active and DR clusters.

Step 1 On FusionInsight Manager of the active cluster, choose **O&M > Alarm > Alarms**, click ⌄ in the row where the alarm is located, and determine the IP address of the host for which the alarm is generated.

Step 2 Log in to the active management node of the active cluster as user **omm** and run the **ping** *IP address of the DR cluster* command to check whether the faulty node is reachable.

- If yes, go to **Step 5**.
- If no, go to **Step 3**.

Step 3 Rectify the network fault between the active and DR clusters.

Step 4 After the protection group runs for 10 minutes, choose **O&M > Alarm > Alarms** and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check the service status in the active and DR clusters.

Step 5 Log in to FusionInsight Manager of the active and DR clusters, choose **Cluster > Services**, and check whether any faulty service exists.

- If yes, go to **Step 6**.
- If no, go to **Step 8**.

Step 6 Choose **O&M > Alarm > Alarms** to view the alarm indicating that the service is unavailable. Click **View Help** in the **Operation** column to restore the faulty service in the active and DR clusters, and check whether the service is running properly.

- If yes, go to **Step 7**.
- If no, go to **Step 8**.

Step 7 After the protection group runs for 10 minutes, choose **O&M > Alarm > Alarms** and check whether the alarm is cleared.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If yes, no further action is required.
- If no, go to **Step 8**.

Collect the fault information.

Step 8 On FusionInsight Manager of the active cluster, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 9 In the **Service** dialog box, choose **OMS** > **Disaster**, select the active node from the **Host** drop-down list, and click **OK**.

Step 10 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 11 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.73 ALM-12161 Periodic Synchronization Duration of Cluster DR Data Exceeds the Threshold

Alarm Description

This alarm is generated when the data synchronization duration of a periodic protection group exceeds the preset value.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12161	Major	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.

Type	Parameter	Description
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	Protection Group	Specifies the protection group for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

Data may not be completely synchronized between the active and standby DR clusters. If a fault occurs, service data may be lost.

Possible Causes

- The connection between the active and standby DR clusters is interrupted.
- Services in the active and standby DR clusters are abnormal.

Handling Procedure

Check the network status of the active and DR clusters.

Step 1 On FusionInsight Manager of the active cluster, choose **O&M** > **Alarm** > **Alarms**, click ⌄ in the row where the alarm is located, and determine the IP address of the host for which the alarm is generated.

Step 2 Log in to the active management node of the active cluster as user **omm** and run the **ping** *IP address of the DR cluster* command to check whether the faulty node is reachable.

- If yes, go to **Step 5**.
- If no, go to **Step 3**.

Step 3 Rectify the network fault between the active and DR clusters.

Step 4 After the protection group runs for 10 minutes, choose **O&M > Alarm > Alarms** and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check the service status in the active and DR clusters.

Step 5 Log in to FusionInsight Manager of the active and DR clusters, choose **Cluster > Services**, and check whether any faulty service exists.

- If yes, go to **Step 6**.
- If no, go to **Step 8**.

Step 6 Choose **O&M > Alarm > Alarms** to view the alarm indicating that the service is unavailable. Click **View Help** in the **Operation** column to restore the faulty service in the active and DR clusters, and check whether the service is running properly.

- If yes, go to **Step 7**.
- If no, go to **Step 8**.

Step 7 After the protection group runs for 10 minutes, choose **O&M > Alarm > Alarms** and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Collect the fault information.

Step 8 On FusionInsight Manager of the active cluster, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 9 In the **Service** dialog box, choose **OMS** > **Disaster**, select the active node from the **Host** drop-down list, and click **OK**.

Step 10 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 11 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

1.3.74 ALM-12162 Streaming Data Synchronization Failed During Cluster DR

Alarm Description

This alarm is generated when data synchronization of a streaming protection group fails.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12162	Critical	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	Protection Group	Specifies the protection group for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

Data may not be completely synchronized between the active and standby DR clusters. If a fault occurs, service data may be lost.

Possible Causes

- The connection between the active and standby DR clusters is interrupted.
- Services in the active and standby DR clusters are abnormal.

Handling Procedure

Check the network status of the active and DR clusters.

Step 1 On FusionInsight Manager of the active cluster, choose **O&M > Alarm > Alarms**, click ⌄ in the row where the alarm is located, and determine the IP address of the host for which the alarm is generated.

Step 2 Log in to the active management node of the active cluster as user **omm** and run the **ping** *IP address of the DR cluster* command to check whether the faulty node is reachable.

- If yes, go to **Step 5**.
- If no, go to **Step 3**.

Step 3 Rectify the network fault between the active and DR clusters.

Step 4 After the protection group runs for 10 minutes, choose **O&M > Alarm > Alarms** and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check the service status in the active and DR clusters.

Step 5 Log in to FusionInsight Manager of the active and DR clusters, choose **Cluster > Services**, and check whether any faulty service exists.

- If yes, go to **Step 6**.
- If no, go to **Step 8**.

Step 6 Choose **O&M > Alarm > Alarms** to view the alarm indicating that the service is unavailable. Click **View Help** in the **Operation** column to restore the faulty service in the active and DR clusters, and check whether the service is running properly.

- If yes, go to **Step 7**.
- If no, go to **Step 8**.

Step 7 After the protection group runs for 10 minutes, choose **O&M > Alarm > Alarms** and check whether the alarm is cleared.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If yes, no further action is required.
- If no, go to **Step 8**.

Collect the fault information.

Step 8 On FusionInsight Manager of the active cluster, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 9 In the **Service** dialog box, choose **OMS** > **Disaster**, select the active node from the **Host** drop-down list, and click **OK**.

Step 10 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 11 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.75 ALM-12163 Periodical Data Synchronization Failed During Cluster DR

Alarm Description

This alarm is generated when data synchronization of a periodical protection group fails.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12163	Critical	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.

Type	Parameter	Description
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	Protection Group	Specifies the protection group for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

Data may not be completely synchronized between the active and standby DR clusters. If a fault occurs, service data may be lost.

Possible Causes

- The connection between the active and standby DR clusters is interrupted.
- Services in the active and standby DR clusters are abnormal.

Handling Procedure

Check the network status of the active and DR clusters.

Step 1 On FusionInsight Manager of the active cluster, choose **O&M** > **Alarm** > **Alarms**, click ⌄ in the row where the alarm is located, and determine the IP address of the host for which the alarm is generated.

Step 2 Log in to the active management node of the active cluster as user **omm** and run the **ping** *IP address of the DR cluster* command to check whether the faulty node is reachable.

- If yes, go to **Step 5**.
- If no, go to **Step 3**.

Step 3 Rectify the network fault between the active and DR clusters.

Step 4 After the protection group runs for 10 minutes, choose **O&M > Alarm > Alarms** and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check the service status in the active and DR clusters.

Step 5 Log in to FusionInsight Manager of the active and DR clusters, choose **Cluster > Services**, and check whether any faulty service exists.

- If yes, go to **Step 6**.
- If no, go to **Step 8**.

Step 6 Choose **O&M > Alarm > Alarms** to view the alarm indicating that the service is unavailable. Click **View Help** in the **Operation** column to restore the faulty service in the active and DR clusters, and check whether the service is running properly.

- If yes, go to **Step 7**.
- If no, go to **Step 8**.

Step 7 After the protection group runs for 10 minutes, choose **O&M > Alarm > Alarms** and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Collect the fault information.

Step 8 On FusionInsight Manager of the active cluster, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 9 In the **Service** dialog box, choose **OMS** > **Disaster**, select the active node from the **Host** drop-down list, and click **OK**.

Step 10 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 11 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.76 ALM-12164 Cluster DR Data Verification Failed

Alarm Description

This alarm is generated when the data verification of a protection group fails.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12164	Critical	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	Protection Group	Specifies the protection group for which the alarm was generated.
	Alarm Severity	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	Details	Specifies alarm details.

Impact on the System

Data may not be completely synchronized between the active and standby DR clusters. If a fault occurs, service data may be lost.

Possible Causes

- Data in the DR cluster is mis-deleted or lost due to cluster exceptions.
- The connection between the active and standby DR clusters is interrupted.
- Services in the active and standby DR clusters are abnormal.

Handling Procedure

Restore the lost Hive, Spark, or Hudi data in the DR cluster.

NOTE

- Hive, Spark, and Hudi tables use Hive DR for data replication.
- Snapshot-based file systems are supported. For Hive DR, full replication is required only for the first time, and data is replicated incrementally based on data changes in the active cluster. If incremental data in the standby cluster is lost, it cannot be automatically restored. You need to perform full copy again.

Step 1 On the FusionInsight Manager of the active cluster, choose **O&M** > **Alarm** > **Alarms**, click ⌄ in the row that contains the alarm, and check whether the Hive, Spark, or Hudi protection group fails the verification in **Location Information**.

- If yes, go to **Step 2**.
- If no, go to **Step 7**.

Step 2 Contact service engineers to check whether the table data in the DR cluster contained in the protection group for which the alarm is generated is deleted by mistake or whether the table data of the protection group is lost due to DR cluster exceptions.

- If yes, go to **Step 3**.
- If no, go to **Step 7**.

Step 3 Determine whether to perform full replication for the entire protection group based on service requirements.

- If yes, go to **Step 4**.
- If no, go to **Step 5**.

Step 4 Log in to the FusionInsight Manager of the active cluster, choose **Cluster** > **Active/Standby Cluster DR**, stop the protection group for which the alarm is generated, and choose **More** > **Start Replication**. In the displayed dialog box, select **Start full replication** and click **OK**. After the task is complete and data is consistent, enable the protection group again and go to **Step 6**.

Step 5 Log in to the node where the DR cluster client is deployed, run the following command to delete the table whose data is lost, and wait for the automatic full copy in the next period:

cd *Client installation directory*

source bigdata_env

kinit *Component service user* (skip this step if Kerberos authentication is disabled for the cluster (the cluster is in normal mode))

beeline

DROP TABLE *TBL*;

Step 6 After the protection group runs for 10 minutes, choose **O&M** > **Alarm** > **Alarms** and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Check the network status of the active and DR clusters.

Step 7 On FusionInsight Manager of the active cluster, choose **O&M** > **Alarm** > **Alarms**, click ⌄ in the row where the alarm is located, and determine the IP address of the host for which the alarm is generated.

Step 8 Log in to the active management node of the active cluster as user **omm** and run the **ping** *IP address of the DR cluster* command to check whether the faulty node is reachable.

- If yes, go to **Step 11**.
- If no, go to **Step 9**.

Step 9 Rectify the network fault between the active and DR clusters.

Step 10 After the protection group runs for 10 minutes, choose **O&M** > **Alarm** > **Alarms** and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 11**.

Check the service status in the active and DR clusters.

Step 11 Log in to FusionInsight Manager of the active and DR clusters, choose **Cluster** > **Services**, and check whether any faulty service exists.

- If yes, go to **Step 12**.
- If no, go to **Step 14**.

Step 12 Choose **O&M** > **Alarm** > **Alarms** to view the alarm indicating that the service is unavailable. Click **View Help** in the **Operation** column to restore the faulty service in the active and DR clusters, and check whether the service is running properly.

- If yes, go to **Step 13**.
- If no, go to **Step 14**.

Step 13 After the protection group runs for 10 minutes, choose **O&M** > **Alarm** > **Alarms** and check whether the alarm is cleared.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If yes, no further action is required.
- If no, go to **Step 14**.

Collect the fault information.

Step 14 On FusionInsight Manager of the active cluster, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 15 In the **Service** dialog box, choose **OMS** > **Disaster**, select the active node from the **Host** drop-down list, and click **OK**.

Step 16 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 17 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.77 ALM-12165 Cluster DR User Information Synchronization Failure

Alarm Description

The system synchronizes DR user information every 30 seconds. This alarm is generated when the synchronization fails. This alarm is cleared when the synchronization is successful.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12165	Critical	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.

Type	Parameter	Description
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	Synchronization Information Type	Specifies the type of the synchronized user information for which the alarm was generated.
	Synchronization Information Name	Specifies the synchronized user information for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

If user information fails to be synchronized, no user can access the data synchronized to the DR cluster.

Possible Causes

- The network between the active and DR clusters is disconnected.
- The DR service of the active cluster is abnormal.

Handling Procedure

Check the network status of the active and DR clusters.

Step 1 On FusionInsight Manager of the active cluster, choose **O&M > Alarm > Alarms**, click ⌄ in the row where the alarm is located, and determine the IP address of the host for which the alarm is generated.

Step 2 Log in to the active management node of the active cluster as user **omm** and run the **ping** *IP address of the DR cluster* command to check whether the faulty node is reachable.

- If yes, go to **Step 5**.
- If no, go to **Step 3**.

Step 3 Rectify the network fault between the active and DR clusters.

Step 4 Choose **O&M** > **Alarm** > **Alarms** and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check the DR service status in the active cluster.

Step 5 Log in to the active management node of the active cluster as user **omm** and run the **sh ${BIGDATA_HOME}/om-server/om/sbin/status-oms.sh** command to check whether the **Disaster** status of the Manager DR service is **Normal**.

- If yes, go to **Step 7**.
- If no, go to **Step 6**.

Step 6 View the **/var/log/Bigdata/disaster/disaster.log** file and check whether the logs generated before and after the alarm is generated contain the keyword **ERROR**. Analyze the logs to check the cause of the resource exception and rectify the fault. Then, check whether the alarm is cleared 5 minutes later.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect the fault information.

Step 7 On FusionInsight Manager of the active cluster, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 8 In the **Service** dialog box, choose **OMS** > **Disaster**, select the active node from the **Host** drop-down list, and click **OK**.

Step 9 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.78 ALM-12166 Cluster DR Protection Group Disabled for a Long Time

Alarm Description

The system checks the status of the cluster DR protection group every 5 minutes. This alarm is generated when the protection group is not enabled for a long time. This alarm is cleared when the protection group is enabled.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12166	Major	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	Protection Group	Specifies the protection group for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

If the protection group is not enabled, data cannot be synchronized between the active cluster and the DR cluster, causing data loss during planned migration.

Possible Causes

- The initial status of a protection group is disabled and the protection group has not been enabled.
- The protection group is not enabled after being disabled.
- The cluster DR data verification fails.

Handling Procedure

Check the data verification status of the protection group.

Step 1 On FusionInsight Manager of the active cluster, choose **Cluster > Active/Standby Cluster DR**. In the protection group list, check whether the data verification status of the protection group is passed.

- If yes, go to **Step 2**.
- If no, go to **Step 3**.

Enable the protection group.

Step 2 Locate the protection group and click **Enable** in the **Operation** column. Then check whether the protection group is enabled.

- If yes, go to **Step 4**.
- If no, go to **Step 5**.

Modify the cluster DR data verification status.

Step 3 Modify the cluster DR data verification status by referring to **ALM-12164 Cluster DR Data Verification Failed**.

Step 4 Wait for 5 minutes, choose **O&M > Alarm > Alarms**, and check whether the alarm is cleared.

If yes, no further action is required.

If no, go to **Step 5**.

Collect the fault information.

Step 5 On FusionInsight Manager of the active cluster, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 6 In the **Service** dialog box, choose **OMS** > **Disaster**, select the active node from the **Host** drop-down list, and click **OK**.

Step 7 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 8 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.79 ALM-12167 Cluster DR Configuration Check Failed

Alarm Description

This alarm is generated when the DR service pairing configuration check fails. This check may fail due to the modification of the active or DR cluster configuration, capacity expansion or reduction, or logical cluster addition or deletion. This alarm is cleared when the check is passed.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12167	Major	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the service for which the alarm was generated.
	NameService	Specifies the federation for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Details	Specifies alarm details.

Impact on the System

Data may not be synchronized or completely synchronized between the active and standby DR clusters. If a fault occurs, service data may be lost.

Possible Causes

- The network between the active and DR clusters is disconnected.
- DR-related configuration items may have been modified in the active and standby clusters. For details about key check items of cluster DR configurations, see **Related Information**.
- Operations, such as scaling in/out, logical cluster addition or deletion, may have been performed on the active and standby clusters. As a result, the pairing relationship is damaged.

Handling Procedure

Check the network status of the active and DR clusters.

Step 1 On FusionInsight Manager of the active cluster, choose **O&M > Alarm > Alarms**, click ⌄ in the row where the alarm is located, and determine the IP address of the host for which the alarm is generated.

Step 2 Log in to the active management node of the active cluster as user **omm** and run the **ping** *IP address of the DR cluster* command to check whether the faulty node is reachable.

- If yes, go to **Step 5**.
- If no, go to **Step 3**.

Step 3 Rectify the network fault between the active and DR clusters.

Step 4 After the system runs for 10 minutes, choose **O&M > Alarm > Alarms** and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Rectify the fault based on the alarm cause.

Step 5 On FusionInsight Manager of the active cluster, choose **O&M > Alarm > Alarms**, click ⌄ in the row where the alarm is located, and determine the additional alarm information.

Step 6 Check whether the alarm is caused by misoperations based on the additional alarm information.

- If yes, go to **Step 7**.
- If no, go to **Step 8**.

Step 7 It is found that the alarm is caused by a rollback. After the system runs for 10 minutes, choose **O&M > Alarm > Alarms** and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Step 8 Choose **Cluster** > **Active/Standby Cluster DR** > **Details**, click **Update DR Configurations** in the **Operation** column of the corresponding service to update the DR service pairing configuration. After the configuration is successful, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Collect the fault information.

Step 9 On FusionInsight Manager of the active cluster, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 10 In the **Service** dialog box, choose **OMS** > **Disaster**, select the active node from the **Host** drop-down list, and click **OK**.

Step 11 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Related Information

The following table describes the impact and description of key service configurations for cluster DR.

Service	Key Configuration	Description
Kafka	**log.message.format.version**: The configurations of the two clusters must be the same.	Different message versions affect service usage and performance overhead.
	log.retention.hours: The configurations of the two clusters must be the same.	Ensure that data is stored for a sufficient period of time.
	log.retention.bytes: The configurations of the two clusters must be the same.	Ensure that valid data is stored.
	offsets.retention.minutes: The configurations of the two clusters must be the same.	Ensure that offsets are stored for a sufficient period of time.
	log.dirs: The configurations of the two clusters must match with each other.	Ensure that the disk configurations of the active and standby clusters match with each other to support the volume of protected data.
	metrics.reporter.security.protocol: The configurations of the two clusters must be the same.	Ensure that the service protocols of the active and standby clusters match with each other. Otherwise, the synchronization may be abnormal.
	allow.everyone.if.no.acl.found: The configurations of the two clusters must be the same.	Ensure that the access control permissions of the active and standby clusters are consistent. Otherwise, services may fail to be accessed after an active/standby switchover.
	auto.create.topics.enable: The configurations of the two clusters must be the same.	Ensure that the topic management policies of the active and standby clusters are consistent.
	min.insync.replicas: The configurations of the two clusters must be the same.	Ensure consistent reliability when data is written.
	message.max.bytes: The configurations of the two clusters must be the same.	Ensure that the maximum message sizes supported by the active and standby clusters are the same. Otherwise, services may fail.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Service	Key Configuration	Description
	num.io.threads: The configurations of the two clusters must match with each other.	Ensure that the DR cluster can handle the load of synchronizing services.
	num.network.threads: The configurations of the two clusters must match with each other.	Ensure that the DR cluster can handle the load of synchronizing requests.
	ssl.mode.enable: The configurations of the two clusters must be the same.	Ensure that the encryption capabilities of the active and standby clusters are consistent. Otherwise, services may be affected.
	unclean.leader.election.enable: The configurations of the two clusters must be the same.	Ensure that the policies for electing partition leaders are the same. Otherwise, services may be affected.
	compression.type: The configurations of the two clusters must be the same.	Ensure that the data storage modes are the same. Otherwise, the disk space may be used up and a fault occurs.
	zookeeper.set.acl: The configurations of the two clusters must be the same.	Ensure that the ZooKeeper access policies are the same. Otherwise, services may be affected.
Hive	**hive.server2.enable.doAs**: The configurations of the two clusters must be the same.	This parameter specifies whether the proxy user is one of the users who has permissions on data directories. If the configurations are inconsistent, data in the standby cluster may fail to be read.
	hive.cbo.enable: The configurations of the two clusters must be the same.	This parameter specifies the data read logic during the execution of service SQL statements. If the configurations are inconsistent, service execution is affected.
	hive.security.whitelist.switch: The configurations of the two clusters must be the same.	These parameters specify whether the parameters of a SQL statement (SET statement) can be correctly set. If the configurations are inconsistent, service execution is affected.
	hive.security.authorization.sqlstd.confwhitelist: The configurations of the two clusters must be the same.	

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Service	Key Configuration	Description
	hive.security.authorization.sqlstd.confwhitelist.append: The configurations of the two clusters must be the same.	
Elasticsearch	**index.routing.allocation.total_shards_per_node**: Set this parameter based on the site requirements.	This parameter specifies the number of shards of the same index that can be allocated to each instance (index-level configuration). You need to modify the parameter based on the site requirements to ensure that shards can be allocated.
HBase	**hbase.rpc.protection**: The configurations of the two clusters must be the same.	The configurations must be the same. Otherwise, synchronization between the active and standby clusters is affected, and services cannot be accessed after switchover.
	HBASE_ZK_SSL_ENABLED: The configurations of the two clusters must be the same.	The configurations must be the same. Otherwise, synchronization between the active and standby clusters is affected, and services cannot be accessed after switchover.

1.3.80 ALM-12168 Key Service Configuration Check for Cluster DR Failed

Alarm Description

The system checks the key service configuration of the cluster DR every 10 minutes. This alarm is generated when the key configuration of the service protected by the active cluster does not match that of the DR cluster and the key configuration check is enabled for the service. This alarm is cleared when the check is passed.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12168	Major	Quality of service	Tenant plane	FusionInsight Manager	Yes

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the service for which the alarm was generated.
	NameService	Specifies the federation for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Details	Specifies alarm details.

Impact on the System

Service migration may be affected.

Possible Causes

Related configurations may have been modified in the active or standby cluster. For details about key check items of cluster DR configurations, see **Related Information**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Handling Procedure

Check related configuration items.

Step 1 On FusionInsight Manager of the active cluster, choose **O&M > Alarm > Alarms**, click ⌄ in the row where the alarm is located, and confirm the corresponding service and additional information of the alarm.

Step 2 Check whether the configuration of the active cluster is the same as that of the DR cluster based on the additional information.

If yes, no further action is required.

If no, go to **Step 3**.

Step 3 Modify the configuration of the DR cluster based on the configuration of the active cluster and synchronize the configuration.

Step 4 After the system runs for 10 minutes, choose **O&M > Alarm > Alarms** and check whether the alarm is cleared.

If yes, no further action is required.

If no, go to **Step 5**.

Collect the fault information.

Step 5 On FusionInsight Manager of the active cluster, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 6 In the **Service** dialog box, choose **OMS** > **Disaster**, select the active node from the **Host** drop-down list, and click **OK**.

Step 7 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 8 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

The following table describes the impact and description of key service configurations for cluster DR.

Service	Key Configuration	Description
Kafka	**log.message.format.version**: The configurations of the two clusters must be the same.	Different message versions affect service usage and performance overhead.

Service	Key Configuration	Description
	log.retention.hours: The configurations of the two clusters must be the same.	Ensure that data is stored for a sufficient period of time.
	log.retention.bytes: The configurations of the two clusters must be the same.	Ensure that valid data is stored.
	offsets.retention.minutes: The configurations of the two clusters must be the same.	Ensure that offsets are stored for a sufficient period of time.
	log.dirs: The configurations of the two clusters must match with each other.	Ensure that the disk configurations of the active and standby clusters match with each other to support the volume of protected data.
	metrics.reporter.security.protocol: The configurations of the two clusters must be the same.	Ensure that the service protocols of the active and standby clusters match with each other. Otherwise, the synchronization may be abnormal.
	allow.everyone.if.no.acl.found: The configurations of the two clusters must be the same.	Ensure that the access control permissions of the active and standby clusters are consistent. Otherwise, services may fail to be accessed after an active/standby switchover.
	auto.create.topics.enable: The configurations of the two clusters must be the same.	Ensure that the topic management policies of the active and standby clusters are consistent.
	min.insync.replicas: The configurations of the two clusters must be the same.	Ensure consistent reliability when data is written.
	message.max.bytes: The configurations of the two clusters must be the same.	Ensure that the maximum message sizes supported by the active and standby clusters are the same. Otherwise, services may fail.
	num.io.threads: The configurations of the two clusters must match with each other.	Ensure that the DR cluster can handle the load of synchronizing services.
	num.network.threads: The configurations of the two clusters must match with each other.	Ensure that the DR cluster can handle the load of synchronizing requests.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Service	Key Configuration	Description
	ssl.mode.enable: The configurations of the two clusters must be the same.	Ensure that the encryption capabilities of the active and standby clusters are consistent. Otherwise, services may be affected.
	unclean.leader.election.enable: The configurations of the two clusters must be the same.	Ensure that the policies for electing partition leaders are the same. Otherwise, services may be affected.
	compression.type: The configurations of the two clusters must be the same.	Ensure that the data storage modes are the same. Otherwise, the disk space may be used up and a fault occurs.
	zookeeper.set.acl: The configurations of the two clusters must be the same.	Ensure that the ZooKeeper access policies are the same. Otherwise, services may be affected.
Hive	**hive.server2.enable.doAs**: The configurations of the two clusters must be the same.	This parameter specifies whether the proxy user is one of the users who has permissions on data directories. If the configurations are inconsistent, data in the standby cluster may fail to be read.
	hive.cbo.enable: The configurations of the two clusters must be the same.	This parameter specifies the data read logic during the execution of service SQL statements. If the configurations are inconsistent, service execution is affected.
	hive.security.whitelist.switch: The configurations of the two clusters must be the same.	These parameters specify whether the parameters of a SQL statement (SET statement) can be correctly set. If the configurations are inconsistent, service execution is affected.
	hive.security.authorization.sqlstd.confwhitelist: The configurations of the two clusters must be the same.	
	hive.security.authorization.sqlstd.confwhitelist.append: The configurations of the two clusters must be the same.	

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Service	Key Configuration	Description
Elasticsearch	**index.routing.allocation.total_shards_per_node**: Set this parameter based on the site requirements.	This parameter specifies the number of shards of the same index that can be allocated to each instance (index-level configuration). You need to modify the parameter based on the site requirements to ensure that shards can be allocated.
HBase	**hbase.rpc.protection**: The configurations of the two clusters must be the same.	The configurations must be the same. Otherwise, synchronization between the active and standby clusters is affected, and services cannot be accessed after switchover.
	HBASE_ZK_SSL_ENABLED: The configurations of the two clusters must be the same.	The configurations must be the same. Otherwise, synchronization between the active and standby clusters is affected, and services cannot be accessed after switchover.

1.3.81 ALM-12169 Historical Data Synchronization Failed During Cluster DR

Alarm Description

This alarm is generated when the historical data in a protection group fails to be synchronized.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12169	Critical	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.

Type	Parameter	Description
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	Protection Group	Specifies the protection group for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

Data may not be completely synchronized between the active and standby DR clusters. If a fault occurs, service data may be lost.

Possible Causes

- The connection between the active and standby DR clusters is interrupted.
- Services in the active and standby DR clusters are abnormal.

Handling Procedure

Check the network status of the active and DR clusters.

Step 1 On FusionInsight Manager of the active cluster, choose **O&M** > **Alarm** > **Alarms**, click ⌄ in the row where the alarm is located, and determine the IP address of the host for which the alarm is generated.

Step 2 Log in to the active management node of the active cluster as user **omm** and run the **ping** *IP address of the DR cluster* command to check whether the faulty node is reachable.

- If yes, go to **Step 5**.
- If no, go to **Step 3**.

Step 3 Rectify the network fault between the active and DR clusters.

Step 4 After the protection group runs for 10 minutes, choose **O&M > Alarm > Alarms** and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check the service status in the active and DR clusters.

Step 5 Log in to FusionInsight Manager of the active and DR clusters, choose **Cluster > Services**, and check whether any faulty service exists.

- If yes, go to **Step 6**.
- If no, go to **Step 8**.

Step 6 Choose **O&M > Alarm > Alarms** to view the alarm indicating that the service is unavailable. Click **View Help** in the **Operation** column to restore the faulty service in the active and DR clusters, and check whether the service is running properly.

- If yes, go to **Step 7**.
- If no, go to **Step 8**.

Step 7 After the protection group runs for 10 minutes, choose **O&M > Alarm > Alarms** and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Collect the fault information.

Step 8 On FusionInsight Manager of the active cluster, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 9 In the **Service** dialog box, choose **OMS > Disaster**, select the active node from the **Host** drop-down list, and click **OK**.

Step 10 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 11 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.82 ALM-12180 Suspended Disk I/O

Alarm Description

- For HDDs, the alarm is triggered when any of the following conditions is met:
  - By default, the system collects data every 3 seconds. The svctm latency reaches 6 seconds within 30 seconds in at least seven collection periods.
  - By default, the system collects data every 3 seconds. Disk queue depth (**avgqu-sz**) > 0 and IOPS = 0, or bandwidth = 0 and **ioutil** > 99% in at least 10 collection periods within 30 seconds.
  - By default, the system collects data every 3 seconds. At least 50% of detected svctm take no less than 1000 ms within 300 seconds.
- For SSDs, the alarm is triggered when any of the following conditions is met:
  - By default, the system collects data every 3 seconds. The svctm latency reaches 3 seconds within 30 seconds in at least seven collection periods.
  - By default, the system collects data every 3 seconds. Disk queue depth (**avgqu-sz**) > 0 and IOPS = 0, or bandwidth = 0 and **ioutil** > 99% in at least 10 collection periods within 30 seconds.
  - By default, the system collects data every 3 seconds. At least 50% of detected svctm take no less than 500 ms within 300 seconds.

The collection period is 3 seconds, and the detection period is 30 or 300 seconds. This alarm is automatically cleared when none of the conditions are met for three consecutive detection periods (30 or 300 seconds).

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

NOTE

- Run the following command in the OS to collect data:

  iostat -x -t 1 1

```
[root@[redacted]~]# iostat -x -t 1 1
Linux 4.18.0-147.5.2.10.h933.eulerosv2r10.x86_64 (node-master1Ceyv)     10/12/2022     _x86_64_       (8 CPU)

10/12/2022 05:24:09 PM
avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           24.49    0.00   13.82    0.11    0.00   61.58

Device            r/s     rkB/s   rrqm/s  %rrqm r_await rareq-sz     w/s     wkB/s   wrqm/s  %wrqm w_await wareq-sz     d/s     dkB/s   drqm/s  %drqm d_await dareq-sz  aqu-sz  %util
dm-0             1.59     57.23     0.00   0.00    1.22    35.94   15.80    124.80     0.00   0.00    2.39     7.90    0.00      0.00     0.00   0.00    0.00     0.00    0.04   0.79
dm-1             0.07      0.30     0.00   0.00    0.67     4.41    0.00      0.00     0.00   0.00    0.00     0.00    0.00      0.00     0.00   0.00    0.00     0.00    0.00   0.01
vda              1.90     61.59     0.02   0.96    1.65    32.43   22.16    403.26    33.50  60.19    1.80    18.20    0.00      0.00     0.00   0.00    0.00     0.00    0.03   1.80
vdb              0.11      2.51     0.00   0.01    0.68    22.22   24.05    351.18    16.74  41.03    1.02    14.60    0.00      0.00     0.00   0.00    0.00     0.00    0.01   1.59
```

  Parameters in the command output are as follows:

  avgqu-sz indicates the disk queue depth.

  The sum of **r/s** and **w/s** is the IOPS.

  The sum of **rkB/s** and **wkB/s** is the bandwidth.

  %util is the **ioutil** value.

- Calculate **svctm** as follows:

  svctm = (tot_ticks_new - tot_ticks_old) / (rd_ios_new + wr_ios_new - rd_ios_old - wr_ios_old)

  When the detection period is 30 seconds, if **rd_ios_new + wr_ios_new - rd_ios_old - wr_ios_old = 0**, then **svctm = 0**.

  When the detection period is 300 seconds and **rd_ios_new + wr_ios_new - rd_ios_old - wr_ios_old = 0**, if **tot_ticks_new - tot_ticks_old = 0**, then **svctm = 0**; otherwise, the value of **svctm** is infinite.

  The parameters can be obtained as follows:

  The system runs the **cat /proc/diskstats** command every 3 seconds to collect data.

```
[omm@[redacted]g]$ cat /proc/diskstats
 253       0 vda 1101553 35446 83439787 3338546 28744856 48314024 1054257652 52667332 0 19569526 40342913 0 0 0 0
 253       1 vda1 596970 25494 54533791 2565698 5446604 8749340 215777628 12114542 0 6473803 11339691 0 0 0 0
 253       2 vda2 15 0 108 136 0 0 0 0 0 150 129 0 0 0 0
 253       5 vda5 22373 1364 2525122 79502 4212374 4104759 161597984 8145606 0 3598808 6239095 0 0 0 0
 253       6 vda6 11145 314 529002 85050 259201 70368 4412408 321454 0 189336 259725 0 0 0 0
 253       7 vda7 157987 105 3477434 149542 6507077 1028968 140666992 14349866 0 1679035 11116587 0 0 0 0
 253       8 vda8 312935 8169 22369722 458354 12179958 34360589 531802640 17724858 0 9060731 11385470 0 0 0 0
 253      16 vdb 275920 21939 15977738 2171665 39472291 28236575 2653825040 482230505 0 30580346 465962048 0 0 0 0
 253      17 vdb1 275439 21939 15948866 2171472 31290400 28236555 2653824832 481837775 0 30036724 465855080 0 0 0 0
   7       0 loop0 356 0 17442 150 0 0 0 0 0 149 105 0 0 0 0
[omm@[redacted]]$ cat /proc/diskstats
 253       0 vda 1101553 35446 83439787 3338546 28747977 48319338 1054352084 52672715 0 19571460 40346640 0 0 0 0
 253       1 vda1 596970 25494 54533791 2565698 5446613 8750402 215791076 12115169 0 6474429 11339985 0 0 0 0
 253       2 vda2 15 0 108 136 0 0 0 0 0 150 129 0 0 0 0
 253       5 vda5 22373 1364 2525122 79502 4212822 4105244 161614088 8146153 0 3599216 6239432 0 0 0 0
 253       6 vda6 11145 314 529002 85050 259245 70433 4413368 321489 0 189389 259730 0 0 0 0
 253       7 vda7 157987 105 3477434 149542 6507759 1029060 140677872 14351373 0 1679157 11117724 0 0 0 0
 253       8 vda8 312935 8169 22369722 458354 12181277 34364199 531855680 17727525 0 9061647 11387424 0 0 0 0
 253      16 vdb 275920 21939 15977738 2171665 39477604 28238831 2653881640 482234435 0 30581946 465964144 0 0 0 0
 253      17 vdb1 275439 21939 15948866 2171472 31293358 28238811 2653881432 481841639 0 30038274 465857164 0 0 0 0
   7       0 loop0 356 0 17442 150 0 0 0 0 0 149 105 0 0 0 0
```

  In the data collected for the first time, the number in the fourth column is the **rd_ios_old** value, the number in the eighth column is the **wr_ios_old** value, and the number in the thirteenth column is the **tot_ticks_old** value.

  In the data collected for the second time, the number in the fourth column is the **rd_ios_new** value, the number in the eighth column is the **wr_ios_new** value, and the number in the thirteenth column is the **tot_ticks_new** value.

  In this case, the value of **svctm** is as follows:

  (19571460 - 19569526) / (1101553 + 28747977 - 1101553 - 28744856) = 0.6197

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12180	Major	Physical resource	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	DiskName	Specifies the disk for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Disk ESN	Specifies the serial number of the disk for which the alarm was generated.

Impact on the System

If the I/O usage keeps increasing, operations will be affected and services will be interrupted. The possible impacts are as follows:

- The system I/O performance deteriorates, which means slow response and low throughput. For example, job submission is slow, page responds slowly, interface response times out, and the system is in error or even crash.
- Customer services may be interrupted. The system may break down and the key information stored on the faulty disk may be lost.

Possible Causes

The disk is aged.

Handling Procedure

Replace the disk.

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Alarms**.

Step 2 View the detailed information about the alarm. Check the values of **HostName** and **DiskName** in the location information to obtain the information about the faulty disk for which the alarm is reported.

Step 3 Check whether the host for which the alarm is generated is the active OMS node or the active node of the instance in active/standby mode.

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 Log in to the node for which the alarm is generated as the **root** user and run the following command to check the mount point of the faulty disk:

df -h | grep "*Name of the faulty disk*"

Check whether the mount point partition of the faulty disk is the cluster software installation directory (**${BIGDATA_HOME}**) or data disk directory (**${BIGDATA_DATA_HOME}** by default).

- If yes, go to **Step 5**.
- If no, go to **Step 6**.

Step 5 Trigger an active/standby switchover to rectify the fault.

- Active OMS node

  If O&M operations cannot be performed due to slow disk faults, such as system freezing, delayed page refreshing, or slow API response, and the alarm

is generated for the active OMS node, perform the following operations to trigger an active/standby switchover to restore services:

a. Log in to the active OMS node as user **omm**.

b. Run the following command to perform an active/standby switchover:

- For the IPv4 network: **${OMS_RUN_PATH}/workspace/ha/module/hacom/tools/ha_client_tool --ip=127.0.0.1 --port=20013 --switchover --name=product**
- For the IPv6 network: **${OMS_RUN_PATH}/workspace/ha/module/hacom/tools/ha_client_tool --ip=::1 --port=20013 --switchover --name=product**

c. After the active/standby switchover is successful, the system recovers. Perform **Step 6** to replace the faulty disk.

- Active node of an active/standby instance

  If the alarm is generated for the active node of an instance in active/standby mode and the slow disk fault affects the running of the instance, trigger an active/standby switchover on FusionInsight Manager to restore services.

  a. Log in to FusionInsight Manager and choose **Cluster** > **Services** > *Name of the desired service*.

  b. On the service details page, expand the **More** drop-down list and select **Perform** *xxx* **Switchover**.

  c. In the displayed dialog box, enter the password of the current login user and click **OK**.

  d. In the displayed dialog box, click **OK** to perform active/standby switchover.

  e. After the active/standby switchover is successful, the system recovers. Perform **Step 6** to replace the faulty disk.

Step 6 Replace the hard disk.

Step 7 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Collect fault information.

Step 8 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 9 Select **OMS** for **Service** and click **OK**.

Step 10 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 11 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.83 ALM-12186 CGroup Task Usage Exceeds the Threshold

Alarm Description

The system checks the CGroup task usage of user **omm** every 5 minutes. This alarm is generated when the CGroup task usage exceeds 90%. This alarm is cleared when the CGroup task usage is less than or equal to 90%.

CGroup task usage = Number of used CGroup tasks/Maximum number of CGroup tasks

You can run the **systemctl status user-$(id -u).slice | grep limit | awk -F ' ' '{print $2}'** command as user **omm** to obtain the number of used CGroup tasks of this user and run the **echo $(systemctl status user-$(id -u).slice | grep limit | awk -F ' ' '{print $4}') | sed -e 's/)//g'** command to obtain the maximum number of CGroup tasks allowed for this user.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12186	Major	Environment	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Details	Specifies alarm details.

Impact on the System

- Failed to switch to user **omm**.
- Failed to create new **omm** processes.
- A faulty service or process cannot be restarted.

Possible Causes

The CGroup task usage exceeds 90%.

Handling Procedure

Check the maximum number of threads that can be concurrently opened by user omm is properly set.

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Alarms**. On the page that is displayed, click ⌄ in the row containing the alarm, and view the name of the host for which the alarm is generated in **Location**. Click the host name to view its IP address.

Step 2 Log in to the host for which the alarm is generated as user **omm**.

Step 3 Run the following command to obtain the maximum number of threads that can be concurrently opened by user **omm** and check whether this number is greater than or equal to **60000**:

systemctl status user-$(id -u).slice | grep limit

- If yes, go to **Step 6**.
- If no, go to **Step 4**.

Step 4 Switch to user **root** and run the following command to change the value for user **omm** to **60000**:

systemctl set-property user-2000.slice TasksMax=60000

Step 5 Change the value of **UserTasksMax** in the **/etc/systemd/logind.conf** file to **60000**. (If the parameter is commented out, uncomment it.) Save the file, wait 5 minutes, and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On FusionInsight Manager of the cluster, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, select **OmmServer** and **NodeAgent** for the target cluster, and click **OK**.

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.84 ALM-12187 Failed to Expand Disk Partition Capacity

Alarm Description

The system checks the disk space every 60 seconds. When detecting that the disk space is expanded, the system expands disk partition. This alarm is generated when the disk partition fails to be expanded.

This alarm is cleared when the system detects that the disk partition is successfully expanded.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12187	Minor	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	MountDirectoryName	Specifies the directory for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Disk ESN	Specifies the serial number of the disk for which the alarm was generated.

Impact on the System

A disk partition scale-out failure may have the following impacts on the system:

- Data may be lost. (It is important to back up key information before scale-out.)
- The system may be unstable or cannot be started because the system files may be damaged.
- The disk may be unavailable. In this case, you need to format the disk and partition it again.
- The system performance may deteriorate because the disk partition space is not enough. The performance remains low until the disk partition is scaled out successfully.

Possible Causes

- The growpart scale-out tool is not installed.
- The system fails to execute the command for expanding disk partition.

Handling Procedure

Check whether growpart is installed.

Step 1 Log in to FusionInsight Manager, click **O&M**, and choose **Alarm** > **Alarms** to view the alarm details. In the **Location** column, check the name of the host and mount directory for which the alarm is generated. Click the host name to view its IP address.

Step 2 Log in to the node for which the alarm is generated as user **root**.

Step 3 Run the following command to check whether growpart is installed:

which growpart

If information similar to the following is displayed, the growpart tool is installed. Otherwise, contact technical support to install the growpart tool.

```
[root@xxx ~]#which growpart
/usr/bin/growpart
```

Step 4 Wait for 5 minutes, then choose **O&M**, and choose **Alarm** > **Alarms** on FusionInsight Manager. Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Run the disk partition expansion command.

Step 5 Run the following command to view the disk and partition information:

lsblk

Search for the partition and the disk based on the mount directory name in the alarm location information, and check the disk and partition sizes.

In the following example, the mount directory is **/srv/BigData/data1**, the used disk is **/dev/vdb**, and the disk partition is **/dev/vdb1**.

```
[root@[redacted] ~]# lsblk
NAME    MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
loop0     7:0    0  1.5G  0 loop /media
vda     253:0    0  500G  0 disk
├─vda1 253:1    0  220G  0 part /
├─vda2 253:2    0    1K  0 part
├─vda5 253:5    0   10G  0 part /tmp
├─vda6 253:6    0   10G  0 part /var
├─vda7 253:7    0   60G  0 part /srv/BigData
└─vda8 253:8    0  180G  0 part /var/log
vdb     253:16   0  650G  0 disk
└─vdb1 253:17   0  600G  0 part /srv/BigData/data1
```

Step 6 Run the following command to expand the partition using growpart:

growpart *Data disk Partition number*

Run the following command:

growpart /dev/vdb 1

If information similar to the following is displayed, the execution is successful. If the execution fails, contact technical support.

```
[root@host-[redacted] ~]# growpart /dev/vdb 1
CHANGED: partition=1 start=2048 old: size=1258287104 end=1258289152 new: size=1363146719 end=1363148767
```

Step 7 Run the following command to expand the file system size of the disk partition:

resize2fs *Disk partition*

Run the following command:

resize2fs /dev/vdb1

If information similar to the following is displayed, the execution is successful:

```
[root@host-[redacted] ~]# resize2fs /dev/vdb1
resize2fs 1.46.4 (18-Aug-2021)
Filesystem at /dev/vdb1 is mounted on /srv/BigData/data1; on-line resizing required
old_desc_blocks = 75, new_desc_blocks = 82
The filesystem on /dev/vdb1 is now 170393339 (4k) blocks long.
```

Step 8 Wait for 5 minutes, click **O&M**, and choose **Alarm** > **Alarms** on FusionInsight Manager. Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, contact technical support.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.85 ALM-12188 diskmgt Disk Monitoring Unavailable

Alarm Description

NodeAgent checks the status of the diskmgt disk monitoring service every 5 minutes. This alarm is generated when diskmgt disk monitoring is unavailable.

This alarm is cleared when the diskmgt disk monitoring service recovers.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12188	Minor	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

When diskmgt disk monitoring is unavailable, the read-only detection of the device partition file system, device partition loss detection, and disk partition scale-out detection cannot be performed.

Possible Causes

- The diskmgt disk monitoring service does not exist.
- The diskmgt disk monitoring service is not started.

Handling Procedure

Check whether the diskmgt disk monitoring service exists.

Step 1 Log in to FusionInsight Manager, click **O&M**, and choose **Alarm** > **Alarms** to view the alarm details. In the **Location** column, check the name of the host for which the alarm is generated. Click the host name to view its IP address.

Step 2 Log in to the node for which the alarm is generated as user **root**.

Step 3 Run the following command to check whether the core service file exists:

stat /usr/local/diskmgt/inner/diskmgtd

If the file does not exist, contact technical support.

Start the diskmgt disk monitoring service.

Step 4 Run the following command to start the diskmgt disk monitoring service:

systemctl restart diskmgt

Step 5 Run the following command to check whether the diskmgt disk monitoring service is started:

systemctl status diskmgt

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If information similar to the following is displayed, the service is started successfully. Go to **Step 6**.

```
[root@host-                    ~]# systemctl status diskmgt
● diskmgt.service - Disk monitor service
     Loaded: loaded (/usr/lib/systemd/system/diskmgt.service; enabled; vendor preset: disabled)
     Active: active (running) since Thu 2023-08-10 09:29:18 CST; 5 days ago
   Main PID: 33996 (diskmgtd)
      Tasks: 2 (limit: 407663)
     Memory: 5.6M
     CGroup: /system.slice/diskmgt.service
             ├─   33996 /bin/bash /usr/local/diskmgt/inner/diskmgtd
             └─ 1974506 sleep 8

Notice: journal has been rotated since unit was started, output may be incomplete.
```

- If no, contact technical support.

Step 6 Wait for 5 minutes, click **O&M**, and choose **Alarm** > **Alarms** on FusionInsight Manager. Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, contact technical support.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.86 ALM-12190 Number of Knox Connections Exceeds the Threshold

Alarm Description

The system periodically checks the number of connections in all Knox topologies. This alarm is generated when the number of connections in a topology exceeds the threshold (90% by default). This alarm is automatically cleared when the number falls below the threshold.

NOTE

This alarm is used for ECS/BMS clusters only.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12190	Major	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	Topology	Specifies the Knox topology for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

The topology may reach the upper limit of connections and fail to forward requests, adversely affecting the MRS functions.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Possible Causes

Hue or Manager is too frequently used, but the default maximum number of Knox connections is small.

Handling Procedure

Step 1 Log in to active and standby OMS nodes as user **root**, respectively.

Step 2 Add the following configuration to the **gateway-site.xml** file on the active and standby OMS nodes to increase the number of thread pools:

vi /opt/knox/conf/gateway-site.xml

```
<property>
<name>gateway.httpclient.maxConnections</name>
<value>64</value>
</property>
```

Step 3 Log in to the active OMS node as user **omm** and run the following command to restart the Knox process:

sh /opt/knox/bin/restart-knox.sh

Step 4 After 5 minutes, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Step 5 Contact technical support to rectify the fault.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.87 ALM-12191 Disk I/O Usage Exceeds the Threshold

Alarm Description

The system checks the disk I/O usage every 30 seconds and compares the actual disk I/O usage with the threshold. This alarm is generated when the disk I/O usage exceeds the threshold for multiple consecutive times (**3** by default).

If the **hit number** is **1**, this alarm is cleared when the disk I/O usage is less than or equal to the threshold. If the **hit number** is greater than **1**, this alarm is cleared when the disk I/O usage is less than or equal to 90% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12191	Major	Physical resource	Tenant plane	FusionInsight Manager	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
New	3.3.1	New alarm	New alarm

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

- Latency: Service processes may run slowly and there is a latency.
- Service failure: Service processing may be slow, time out, or fail. As a result, jobs may fail to run.

Possible Causes

- The alarm threshold or alarm trigger count is improperly configured.
- The disk configuration cannot meet service requirements. The disk I/O usage reaches the upper limit. Alternatively, services are in peak hours. The disk I/O usage reaches the upper limit in a short period.

Handling Procedure

Check whether the alarm threshold or alarm trigger count is properly configured.

Step 1 Modify the alarm threshold and alarm trigger count based on the actual disk I/O usage.

1. Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Thresholds**, click the name of the desired cluster, and choose **Host** > **Disk** > **Disk IO Utilization**.
2. Click the edit button next to **Trigger Count** to change it to a proper value based on the actual service usage.

   NOTE

   Trigger Count indicates how many consecutive times the threshold is reached when the alarm is triggered.
3. Click **Modify** in the **Operation** column of the row that contains the rule and change the alarm threshold.

Step 2 Wait 2 minutes and check whether the alarm is automatically cleared.

- If yes, no further action is required.
- If no, go to **Step 3**.

Check whether the disk I/O usage reaches the upper limit.

Step 3 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. In the alarm list, expand the alarm details and click the name of the host for which the alarm is generated in **Location** area.

Step 4 On the overview page of the host, observe the real-time data of the disk I/O usage for about 5 minutes. If the disk I/O usage exceeds the threshold for multiple times, contact the MRS cluster administrator to improve the disk specification.

If **Disk IO Utilization** chart is not displayed, click the drop-down arrow on the right, select **Customize**, select the desired item, and click **OK**.

Step 5 Check whether it was the peak hour. If this alarm was generated during peak hours, expand the node capacity or contact the MRS cluster administrator to improve the disk specification.

Step 6 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect fault information.

Step 7 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 8 Expand the **Service** drop-down list, select **NodeAgent** for the target cluster, and click **OK**.

Step 9 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.88 ALM-12192 Host Load Exceeds the Threshold

Alarm Description

The system checks the average load every 30 seconds and compares the actual average load with the threshold. This alarm is generated when the average load exceeds the threshold for multiple consecutive times (10 by default).

This alarm is cleared when **Trigger Count** is **1** and the average load is less than or equal to the threshold. This alarm is cleared when **Trigger Count** is greater than 1 and the average load is less than or equal to 90% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12192	Major	Physical resource	Tenant plane	FusionInsight Manager	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
New	3.3.1	New alarm	New alarm

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

- Latency: Service processes may run slowly and there is a latency.
- Service failure: Service processing may be slow, time out, or fail. As a result, jobs may fail to run.

Possible Causes

- The alarm threshold or alarm trigger count is improperly configured.
- The host cannot meet service requirements. The average load reaches the upper limit. Alternatively, requirements surged during peak hours, and the average load reaches the upper limit in a short period.

Handling Procedure

Check whether the alarm threshold or alarm trigger count is properly configured.

Step 1 Modify the alarm threshold and alarm trigger count based on the actual CPU usage.

1. To change the threshold, log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Thresholds**, click the name of the desired cluster, and choose **Host** > **Host Status** > **Average Host Load Information**.
2. Click the edit button next to **Trigger Count** to set it a proper value based on the actual service usage.

   NOTE

   Trigger Count indicates how many consecutive times the threshold is reached when the alarm is triggered.
3. Click **Modify** in the **Operation** column of the row that contains the rule and change the alarm threshold.

Step 2 Wait 2 minutes and check whether the alarm is automatically cleared.

- If yes, no further action is required.
- If no, go to **Step 3**.

Check whether the average load reaches the upper limit.

Step 3 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. In the alarm list, expand the alarm details and click the name of the host for which the alarm is generated in **Location** area.

Step 4 On the overview page of the host, observe the real-time data of average host load for about 5 minutes. If the average load exceeds the threshold for multiple times, contact the MRS cluster administrator to improve the host specification.

If **Average Host Load Information** chart is not displayed, click the drop-down arrow on the right, select **Customize**, select the desired item, and click **OK**.

Step 5 Check whether it was the peak hour. If this alarm was generated during peak hours, expand the node capacity or contact the MRS cluster administrator to improve the host specification.

Step 6 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect fault information.

Step 7 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 8 Expand the **Service** drop-down list, select **NodeAgent** for the target cluster, and click **OK**.

Step 9 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.89 ALM-12200 Password Is About to Expire

Alarm Description

The system checks whether a user password is about to expire at 1:00 a.m. every day. This alarm is generated when a user password is about to expire in less than 5 days by default.

This alarm is cleared when the password is about to expire in at least five days by default.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12200	Major	Security	Tenant plane	FusionInsight Manager	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
New	3.3.1	New alarm	New alarm

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	Alarm Severity	Specifies the alarm severity.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Details	Specifies that the username of password that is about to expire.

Impact on the System

The account cannot be used.

Possible Causes

The password is about to expire.

Handling Procedure

Change the user password.

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Alarms**. In the alarm list, expand the alarm details, and view and record the name of the user whose password is about to expire in additional information.

Step 2 Change the password.

For details, see "Account Management" in MapReduce Service (MRS) 3.3.1-LTS User Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Usage Guide (for Huawei Cloud Stack 8.3.1).

Step 3 If the DataArts Studio service is interconnected, check whether DataArts Studio jobs uses a password that is about to expire. If yes, go to the DataArts Studio management center to change the password. Otherwise, a large number of jobs may fail.

Step 4 Check whether the alarm is automatically cleared after 1:00 a.m. the next day.

- If yes, no further action is required.
- If no, go to **Step 5**.

Collect fault information.

Step 5 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 6 Select **Controller** for **Service** and click **OK**.

Step 7 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 8 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.90 ALM-12201 Process CPU Usage Exceeds the Threshold

Alarm Description

The system checks the CPU usage every 30 seconds and compares the check result with the default threshold. This alarm is generated when the CPU usage exceeds the threshold for multiple consecutive times (**10** by default).

This alarm is cleared when **Trigger Count** is **1** and the CPU usage is less than or equal to the threshold. This alarm is cleared when **Trigger Count** is greater than 1 and the CPU usage is less than or equal to 90% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12201	Major	Physical resource	Tenant plane	FusionInsight Manager	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
New	3.3.1	New alarm	New alarm

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

- Latency: Service processes may run slowly and there is a latency.
- Service failure: Service processing may be slow, time out, or fail. As a result, jobs may fail to run.

Possible Causes

- The alarm threshold or alarm trigger count is improperly configured.
- The CPU configuration cannot meet service requirements, and the CPU usage reaches the upper limit. Alternatively, services are in peak hours. The CPU usage reaches the upper limit in a short period.

Handling Procedure

Check whether the alarm threshold or alarm trigger count is properly configured.

Step 1 Modify the alarm threshold and alarm trigger count based on the actual CPU usage.

1. Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Thresholds** > **OMS** > **OMSServices** > **CPU** > **Process Used CPU (OMS)**.
2. Click the edit button next to **Trigger Count** to set it a proper value based on the actual service usage.

   NOTE

   Trigger Count indicates how many consecutive times the threshold is reached when the alarm is triggered.
3. Click **Modify** in the **Operation** column of the row that contains the rule and change the alarm threshold.

Step 2 Wait 2 minutes and check whether the alarm is automatically cleared.

- If yes, no further action is required.
- If no, go to **Step 3**.

Check whether the CPU usage reaches the upper limit.

Step 3 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. In the alarm list, expand the alarm details and click the name of the host for which the alarm is generated in **Location** area.

Step 4 On the overview page of the host, observe the real-time data of the host CPU usage for about 5 minutes. If the CPU usage exceeds the threshold for multiple times, contact the MRS cluster administrator to increase the CPU.

If no chart is available, click the drop-down arrow on the right, select **Customize**, select the desired item, and click **OK**.

Step 5 Check whether it was the peak hour. If this alarm was generated during peak hours, expand the node capacity or contact the MRS cluster administrator to improve the CPU specification.

Step 6 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect fault information.

Step 7 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 8 Expand the **Service** drop-down list, select **OmmServer** for the target cluster, and click **OK**.

Step 9 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.91 ALM-12202 Process Memory Usage Exceeds the Threshold

Alarm Description

The system checks the memory usage of main OMS processes every 30 seconds. This alarm is generated when the memory usage of main OMS processes is greater than 90% (default value) of the maximum memory.

This alarm is cleared when the memory usage of main OMS processes is less than or equal to 90% of the maximum memory.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12202	Major	Quality of service	Tenant plane	OMS	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
New	3.3.1	New alarm	New alarm

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

If the memory usage of main OMS processes is too high, the performance of these processes deteriorates, and even memory overflow occurs. As a result, main OMS processes are unavailable, and OMS tasks are slow or fail to run.

Possible Causes

The memory usage of main OMS processes is too high or the memory is inappropriately allocated.

Handling Procedure

Check the memory usage of main OMS processes.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. In the alarm list, expand the alarm details, record the process name in **Location**, click the reported host name, and record the service IP address of the host.

Step 2 Choose **System** > **OMS** to view the **OMS Process Memory Usage Ratio** chart. Check whether the memory usage of the processes reaches the threshold (90% by default) at the time when the alarm is generated.

If no chart is available, click the drop-down arrow on the right, select **Customize**, select the desired item, and click **OK**.

- If yes, go to **Step 3**.
- If the threshold is not reached, go to **Step 6**.

Step 3 Contact technical support to modify the memory configurations of the processes.

Step 4 Restart the processes for which the alarm is generated.

Step 5 Check whether the alarm is cleared in 10 minutes.

- If yes, no further action is required.
- If the threshold is not reached, go to **Step 6**.

Collect fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **OmmServer** for the target cluster.

Step 8 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.92 ALM-12203 Process Full GC Duration Exceeds the Threshold

Alarm Description

The system checks the GC duration of main OMS processes every 30 seconds. If the GC duration of an OMS process exceeds the threshold for three consecutive times, this alarm is generated. You can choose **O&M** > **Alarm** > **Thresholds** > **OMS** > **OMSServices** to change the threshold.

This alarm is cleared when the GC duration of the OMS process is shorter than or equal to the threshold.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12203	Major	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
New	3.3.1	New alarm	New alarm

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

Read and write performance deteriorates. As a result, the task execution may slow down and even the service may restart unexpectedly.

Possible Causes

The memory of main OMS processes is too high or inappropriately allocated, causing frequent occurrence of the full GC.

Handling Procedure

Check the GC duration.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. In the alarm list, expand the alarm details, record the process name in **Location**, click the reported host name, and record the service IP address of the host.

Step 2 Choose **System** > **OMS**, view the Full GC Times of OMS Process chart, and check whether the GC time is longer than 12 seconds (default value).

If no chart is available, click the drop-down arrow on the right, select **Customize**, select the desired item, and click **OK**.

- If yes, go to **Step 3**.
- If no, go to **Step 6**.

Step 3 Contact technical support to modify the memory configurations of the processes.

Step 4 Restart the process.

Step 5 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **OmmServer** for the target cluster.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 8 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.93 ALM-12204 Wait Duration of a Disk Read Exceeds the Threshold

Alarm Description

The system checks the wait duration of a disk read every 30 seconds and compares the actual wait duration with the threshold. This alarm is generated when the wait duration exceeds the threshold (10s by default) for multiple consecutive times.

This alarm is cleared when the wait duration is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12204	Major	Physical resource	Tenant plane	FusionInsight Manager	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
New	3.3.1	New alarm	New alarm

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.

Type	Parameter	Description
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

- Latency: Service processes may run slowly and there is a latency.
- Service failure: Service processing may be slow, time out, or fail. As a result, jobs may fail to run.

Possible Causes

- The alarm threshold or alarm trigger count is improperly configured.
- The disk configuration cannot meet service requirements. The disk I/O performance reaches the upper limit. Alternatively, services are in peak hours. The wait duration of a disk read reaches the upper limit in a short period.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Handling Procedure

Check whether the alarm threshold or alarm trigger count is properly configured.

Step 1 Modify the alarm threshold and alarm trigger count based on the actual disk I/O usage.

1. Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Disk** > **Average Time Required for Each Read operation**.
2. Click the edit button next to **Trigger Count** to set it a proper value based on the actual service usage.

   NOTE

   Trigger Count indicates how many consecutive times the threshold is reached when the alarm is triggered.
3. Click **Modify** in the **Operation** column of the row that contains the rule and change the alarm threshold.

Step 2 Wait 2 minutes and check whether the alarm is automatically cleared.

- If yes, no further action is required.
- If no, go to **Step 3**.

Check whether the average time required for each read operation reaches the upper limit.

Step 3 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. In the alarm list, expand the alarm details and click the name of the host for which the alarm is generated in **Location** area.

Step 4 On the overview page of the host, observe the real-time data of average time required for each read operation for about 5 minutes. If the wait duration exceeds the threshold for multiple times, contact the MRS cluster administrator to improve the disk specification.

If the **Average Time Required for Each Read Operation** chart is unavailable, click the drop-down arrow on the right, select **Customize**, select the corresponding item, and click **OK**.

Step 5 Check whether it was the peak hour. If this alarm was generated during peak hours, expand the node capacity or contact the MRS cluster administrator to improve the disk specification.

Step 6 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect fault information.

Step 7 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 8 Expand the **Service** drop-down list, select **NodeAgent** for the target cluster, and click **OK**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 9 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.94 ALM-12205 Wait Duration of a Disk Write Exceeds the Threshold

Alarm Description

The system checks the wait duration of a disk write every 30 seconds and compares the actual wait duration with the threshold. This alarm is generated when the wait duration exceeds the threshold (10s by default) for multiple consecutive times.

This alarm is cleared when the wait duration is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12205	Major	Physical resource	Tenant plane	FusionInsight Manager	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
New	3.3.1	New alarm	New alarm

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.

Type	Parameter	Description
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

- Latency: Service processes may run slowly and there is a latency.
- Service failure: Service processing may be slow, time out, or fail. As a result, jobs may fail to run.

Possible Causes

- The alarm threshold or alarm trigger count is improperly configured.
- The disk configuration cannot meet service requirements. The disk I/O performance reaches the upper limit. Alternatively, services are in peak hours. The wait duration of a disk write reaches the upper limit in a short period.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Handling Procedure

Check whether the alarm threshold or alarm trigger count is properly configured.

Step 1 Modify the alarm threshold and alarm trigger count based on the actual disk I/O usage.

1. Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Disk** > **Average Time Required for Each Write Operation**.
2. Click the edit button next to **Trigger Count** to set it a proper value based on the actual service usage.

   NOTE

   Trigger Count indicates how many consecutive times the threshold is reached when the alarm is triggered.
3. Click **Modify** in the **Operation** column of the row that contains the rule and change the alarm threshold.

Step 2 Wait 2 minutes and check whether the alarm is automatically cleared.

- If yes, no further action is required.
- If no, go to **Step 3**.

Check whether the average time required for each write operation reaches the upper limit.

Step 3 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. In the alarm list, expand the alarm details and click the name of the host for which the alarm is generated in **Location** area.

Step 4 On the overview page of the host, observe the real-time data of average time required for each write operation for about 5 minutes. If the wait duration exceeds the threshold for multiple times, contact the MRS cluster administrator to improve the disk specification.

If the **Average Time Required for Each Write Operation** chart is not displayed, click the drop-down arrow on the right, select **Customize**, select the desired item, and click **OK**.

Step 5 Check whether it was the peak hour. If this alarm was generated during peak hours, expand the node capacity or contact the MRS cluster administrator to improve the disk specification.

Step 6 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect fault information.

Step 7 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 8 Expand the **Service** drop-down list, select **NodeAgent** for the target cluster, and click **OK**.

Step 9 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.95 ALM-12206 Password Has Expired

Alarm Description

The system checks whether a user password has expired at 1:00 a.m. every day. This alarm is generated when a user password has expired.

This alarm is cleared when the user password in the system is within the validity period.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
12206	Major	Security	Tenant plane	FusionInsight Manager	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
New	3.3.1	New alarm	New alarm

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	Alarm Severity	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Details	Specifies that the username of password that has expired.

Impact on the System

The account cannot be used.

Possible Causes

The user password has expired.

Handling Procedure

Change the user password.

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Alarms**. In the alarm list, expand the alarm details, and view and record the name of the user whose password has expired in additional information.

Step 2 Change the user password that has expired.

For details, see "Account Management" in MapReduce Service (MRS) 3.3.1-LTS User Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Usage Guide (for Huawei Cloud Stack 8.3.1).

Step 3 If the DataArts Studio service is interconnected, check whether DataArts Studio jobs uses an expired user password. If yes, go to the DataArts Studio management center to change the password and execute the affected jobs again.

Step 4 Check whether the alarm is automatically cleared after 1:00 a.m. the next day.

- If yes, no further action is required.
- If no, go to **Step 5**.

Collect fault information.

Step 5 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 6 Select **Controller** for **Service** and click **OK**.

Step 7 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 8 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.96 ALM-13000 ZooKeeper Service Unavailable

Alarm Description

The system checks the ZooKeeper service status every 60 seconds. This alarm is generated when the ZooKeeper service is unavailable.

This alarm is cleared when the ZooKeeper service recovers.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
13000	Critical	Quality of service	Tenant plane	ZooKeeper	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

ZooKeeper cannot provide coordination services for upper layer components and the components (such as Yarn and Flink) that depend on ZooKeeper may not run properly.

Possible Causes

- The DNS is installed on the ZooKeeper node.
- The network is faulty.

- The KrbServer service is abnormal.
- The ZooKeeper instance is abnormal.
- The disk capacity is insufficient.

Handling Procedure

Check the DNS.

Step 1 Check whether the DNS is installed on the node where the ZooKeeper instance is located. On the Linux node where the ZooKeeper instance is located, run the **cat /etc/resolv.conf** command to check whether the file is empty.

- If yes, go to **Step 2**.
- If no, go to **Step 3**.

Step 2 Run the **service named status** command to check whether the DNS is started.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 Run the **service named stop** command to stop the DNS service. If "Shutting down name server BIND waiting for named to shut down (28s)" is displayed, the DNS service is stopped successfully. Comment out the content (if any) in **/etc/resolv.conf**.

Step 4 On the **O&M** > **Alarm** > **Alarms** tab, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check the network status.

Step 5 On the Linux node where the ZooKeeper instance is located, run the **ping** command to check whether the host names of other nodes where the ZooKeeper instance is located can be pinged successfully.

- If yes, go to **Step 9**.
- If no, go to **Step 6**.

Step 6 Modify the IP addresses in **/etc/hosts** and add the host name and IP address mapping.

Step 7 Run the **ping** command again to check whether the host names of other nodes where the ZooKeeper instance is located can be pinged successfully.

- If yes, go to **Step 8**.
- If no, go to **Step 23**.

Step 8 On the **O&M** > **Alarm** > **Alarms** tab, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Check the KrbServer service status (Skip this step if the normal mode is used).

Step 9 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services**.

Step 10 Check whether the KrbServer service is normal.

- If yes, go to **Step 13**.
- If no, go to **Step 11**.

Step 11 Perform operations based on "ALM-25500 KrbServer Service Unavailable" and check whether the KrbServer service is recovered.

- If yes, go to **Step 12**.
- If no, go to **Step 23**.

Step 12 On the **O&M** > **Alarm** > **Alarms** tab, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 13**.

Check the ZooKeeper service instance status.

Step 13 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **ZooKeeper** > **quorumpeer**.

Step 14 Check whether the ZooKeeper instances are normal.

- If yes, go to **Step 18**.
- If no, go to **Step 15**.

Step 15 Select instances whose status is not good, and choose **More** > **Restart Instance**.

Step 16 Check whether the instance status is good after restart.

- If yes, go to **Step 17**.
- If no, go to **Step 18**.

Step 17 On the **O&M** > **Alarm** > **Alarms** tab, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 18**.

Check disk status.

Step 18 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Service** > **ZooKeeper** > **quorumpeer**, and check the node host information of the ZooKeeper instance.

Step 19 On FusionInsight Manager, click **Host**.

Step 20 In the **Disk** column, check whether the disk space of each node where ZooKeeper instances are located is insufficient (disk usage exceeds 80%).

- If yes, go to **Step 21**.
- If no, go to **Step 23**.

Step 21 Expand disk capacity. For details, see "ALM-12017 Insufficient Disk Capacity".

Step 22 On the **O&M** > **Alarm** > **Alarms** tab, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 23**.

Collect fault information.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 23 On the FusionInsight Manager portal, choose **O&M** > **Log** > **Download**.

Step 24 Select the following nodes in the required cluster from the **Service**: (KrbServer logs do not need to be downloaded in normal mode.)

- ZooKeeper
- KrbServer

Step 25 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 26 Contact the technical support and send the collected log information.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.97 ALM-13001 Available ZooKeeper Connections Are Insufficient

Alarm Description

The system checks ZooKeeper connections every 60 seconds. This alarm is generated when the system detects that the number of used ZooKeeper instance connections exceeds the threshold.

When the **Trigger Count** is 1, this alarm is cleared when the number of used ZooKeeper instance connections is smaller than or equal to the threshold. When the **Trigger Count** is greater than 1, this alarm is cleared when the number of used ZooKeeper instance connections is smaller than or equal to 90% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
13001	Critical (default threshold: 90%) Major (default threshold: 80%)	Quality of service	Tenant plane	ZooKeeper	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

Available ZooKeeper connections are insufficient. When the connection usage reaches 100%, the ZooKeeper cannot process external connections. As a result, upstream components (such as Yarn and Flink) cannot run properly.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Possible Causes

The number of connections to the ZooKeeper node exceeds the threshold. Connection leakage occurs on some connection processes, or the maximum number of connections does not comply with the actual scenario.

Handling Procedure

Check connection status.

Step 1 On the FusionInsight Manager portal, choose **O&M** > **Alarm** > **Alarms**. On the displayed interface, click the drop-down button of **Available ZooKeeper Connections Are Insufficient** and confirm the node IP address of the host for which the alarm is generated in the Location Information.

Step 2 Obtain the PID of the ZooKeeper process. Log in to the node involved in this alarm as user **root** and run the **pgrep -f proc_zookeeper** command.

Step 3 Check whether the PID can be correctly obtained.

- If yes, go to **Step 4**.
- If no, go to **Step 15**.

Step 4 Obtain all the IP addresses connected to the ZooKeeper instance and the number of connections and check 10 IP addresses with top connections. Run the following command based on the obtained PID: **lsof -i|grep** *$pid* **| awk '{print $9}' | cut -d : -f 2 | cut -d \>-f 2 | awk '{a[$1]++} END {for(i in a){print i,a[i] | "sort -r -g -k 2"}}' | head -10**. (The PID obtained in the preceding step is used.)

Step 5 Check whether node IP addresses and number of connections are successfully obtained.

- If yes, go to **Step 6**.
- If no, go to **Step 15**.

Step 6 Obtain the ID of the port connected to the process. Run the following command based on the obtained PID and IP address: **lsof -i|grep** *$pid* **| awk '{print $9}'|cut -d \> -f 2 |grep** *$IP*| **cut -d : -f 2**. (The PID and IP address obtained in the preceding step are used.)

Step 7 Check whether the port ID is successfully obtained.

- If yes, go to **Step 8**.
- If no, go to **Step 15**.

Step 8 Obtain the ID of the connected process. Log in to each IP address and run the following command based on the obtained port ID: **lsof -i|grep** *$port*. (The port ID obtained in the preceding step is used.)

Step 9 Check whether the process ID is successfully obtained.

- If yes, go to **Step 10**.
- If no, go to **Step 15**.

Step 10 Check whether connection leakage occurs on the process based on the obtained process ID.

- If yes, go to **Step 11**.

- If no, go to **Step 12**.

Step 11 Close the process where connection leakage occurs and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 12**.

Step 12 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **ZooKeeper** > **Configurations** > **All Configurations** > **quorumpeer** > **Performance** and increase the value of **maxCnxns** as required.

Step 13 Save the configuration and restart the ZooKeeper service.

Step 14 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 15**.

Collect fault information.

Step 15 On the FusionInsight Manager portal, choose **O&M** > **Log > Download**.

Step 16 Select **ZooKeeper** in the required cluster from the **Service**:

Step 17 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 18 Contact the technical support and send the collected log information.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.98 ALM-13002 ZooKeeper Direct Memory Usage Exceeds the Threshold

Alarm Description

The system checks the direct memory usage of the ZooKeeper service every 30 seconds. The alarm is generated when the direct memory usage of a ZooKeeper instance exceeds the threshold.

When the **Trigger Count** is 1, this alarm is cleared when the ZooKeeper Direct memory usage is less than the threshold. When the **Trigger Count** is greater than 1, this alarm is cleared when the ZooKeeper Direct memory usage is less than 80% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
13002	Critical (default threshold: 90%) Major (default threshold: 80%)	Quality of service	Tenant plane	ZooKeeper	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold for triggering the alarm.

Impact on the System

If the available memory of ZooKeeper is insufficient, memory overflow may occur and services may break down. As a result, upstream services (such as HDFS and Yarn) fail to run.

Possible Causes

The direct memory of the ZooKeeper instance is overused or the direct memory is inappropriately allocated.

Handling Procedure

Check the direct memory usage.

Step 1 On the FusionInsight Manager portal, choose **O&M** > **Alarm** > **Alarms**. On the displayed interface, click the drop-down button of **ZooKeeper Direct Memory Usage Exceeds the Threshold**. Check the IP address of the instance that reports the alarm.

Step 2 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **ZooKeeper** > **Instance** > **quorumpeer(the IP address checked)**. Click the drop-down menu in the upper right corner of **Chart**, choose **Customize** > **CPU and Memory**, and select **ZooKeeper Heap And Direct Buffer Resource Percentage**, click **OK**.

Step 3 Check whether the used direct buffer memory of ZooKeeper reaches 80% of the maximum direct buffer memory specified for ZooKeeper.

- If yes, go to **Step 4**.
- If no, go to **Step 8**.

Step 4 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **ZooKeeper** > **Configurations** > **All Configurations** > **quorumpeer** > **System** to check whether "-XX:MaxDirectMemorySize" exists in the **GC_OPTS** parameter.

- If yes, in the **GC_OPTS** parameter, delete "-XX:MaxDirectMemorySize" and go to **Step 5**.
- If no, go to **Step 6**.

Step 5 Save the configuration and restart the ZooKeeper service.

Step 6 Check whether the **ALM-13004 ZooKeeper Heap Memory Usage Exceeds the Threshold** exists.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If yes, handle the alarm by referring to **ALM-13004 ZooKeeper Heap Memory Usage Exceeds the Threshold**.
- If no, go to **Step 7**.

Step 7 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Collect fault information.

Step 8 On the FusionInsight Manager portal, choose **O&M** > **Log** > **Download**.

Step 9 Select **ZooKeeper** in the required cluster from the **Service**.

Step 10 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 11 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.99 ALM-13003 GC Duration of the ZooKeeper Process Exceeds the Threshold

Alarm Description

The system checks the garbage collection (GC) duration of the ZooKeeper process every 60 seconds. This alarm is generated when the GC duration exceeds the threshold.

This alarm is cleared when the GC duration is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
13003	Critical (default threshold: 10000 ms) Major (default threshold: 5000 ms)	Quality of service	Tenant plane	ZooKeeper	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

The ZooKeeper process may respond slowly. Services of upper-layer components (such as Yarn, Flink, and Spark) may fail.

Possible Causes

The heap memory of the ZooKeeper process is overused or inappropriately allocated, causing frequent occurrence of the GC process.

Handling Procedure

Check the GC duration.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. On the displayed page, click the drop-down list of **GC Duration of the ZooKeeper Process Exceeds the Threshold**. View the IP address of the instance for which the alarm was generated.

Step 2 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **ZooKeeper** > **Instance** > **quorumpeer**. Click the drop-down list in the upper right corner of **Chart**, choose **Customize** > **GC**, select **ZooKeeper GC Duration per Minute**, and click **OK** to check the GC duration statistics of the ZooKeeper process collected every minute.

Step 3 Check whether the GC duration of the ZooKeeper process collected every minute exceeds the threshold.

- If yes, go to **Step 4**.
- If no, go to **Step 8**.

Step 4 Check whether memory leakage occurs in the application.

Step 5 On FusionInsight Manager, choose **Cluster**, click the name of the desired cluster, and choose **Services** > **ZooKeeper** > **Configurations** > **All Configurations** > **quorumpeer** > **System**. Increase the value of the **GC_OPTS** parameter as required.

NOTE

Generally, **-Xmx** is twice of ZooKeeper data capacity. If the capacity of ZooKeeper reaches 2 GB, set **GC_OPTS** as follows:

-Xms4G -Xmx4G -XX:NewSize=512M -XX:MaxNewSize=512M -XX:MetaspaceSize=64M -XX:MaxMetaspaceSize=64M -XX:CMSFullGCsBeforeCompaction=1

Step 6 Save the configuration and restart the ZooKeeper service.

Step 7 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Collect the fault information.

Step 8 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 9 Expand the **Service** drop-down list, and select **ZooKeeper** for the target cluster.

Step 10 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 11 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.100 ALM-13004 ZooKeeper Heap Memory Usage Exceeds the Threshold

Alarm Description

The system checks the heap memory usage of the ZooKeeper service every 60 seconds. The alarm is generated when the heap memory usage of a ZooKeeper instance exceeds the threshold.

The alarm is cleared when the memory usage is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
13004	Critical (default threshold: 95%) Major (default threshold: 85%)	Quality of service	Tenant plane	ZooKeeper	Yes

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

If the available ZooKeeper heap memory is insufficient, memory overflow may cause service breakdown, and upstream components (such as Yarn, Flink, and Spark) may fail to run.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Possible Causes

The heap memory of the ZooKeeper instance is overused or the heap memory is inappropriately allocated.

Handling Procedure

Check heap memory usage.

Step 1 On the FusionInsight Manager portal, On the displayed interface, click the drop-down button of **ZooKeeper Heap Memory Usage Exceeds the Threshold** and confirm the node IP address of the host for which the alarm is generated in the Location Information.

Step 2 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **ZooKeeper** > **Instance**, click **quorumpeer** in the **Role** column of the corresponding IP address. Click the drop-down menu in the upper right corner of **Chart**, choose **Customize** > **CPU and Memory**, and select **ZooKeeper Heap And Direct Buffer Resource Percentage**, click **OK**. Check the heap memory usage.

Step 3 Check whether the used heap memory of ZooKeeper reaches 95% of the maximum heap memory specified for ZooKeeper.

- If yes, go to **Step 4**.
- If no, go to **Step 7**.

Step 4 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **ZooKeeper** > **Configurations** > **All Configurations** > **quorumpeer** > **System**. Increase the value of **-Xmx** in **GC_OPTS** as required. The details are as follows:

1. On the **Instance** tab, click **quorumpeer** in the **Role** column of the corresponding IP address. Choose **Customize** > **CPU and Memory** in the upper right corner, and select **ZooKeeper Heap And Direct Buffer Resource**, click **OK** to check the heap memory used by ZooKeeper.
2. Change the value of **-Xmx** in the **GC_OPTS** parameter based on the actual heap memory usage. Generally, the value is twice the size of the ZooKeeper data volume. For example, if 2 GB ZooKeeper heap memory is used, the following configurations are recommended: -Xms4G -Xmx4G -XX:NewSize=512M -XX:MaxNewSize=512M -XX:MetaspaceSize=64M -XX:MaxMetaspaceSize=64M -XX:CMSFullGCsBeforeCompaction=1

Step 5 Save the configuration and restart the ZooKeeper service.

Step 6 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect fault information.

Step 7 On the FusionInsight Manager portal, choose **O&M** > **Log > Download**.

Step 8 Select **ZooKeeper** in the required cluster from the **Service**.

Step 9 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.101 ALM-13005 Failed to Set the Quota of Top Directories of ZooKeeper Components

Alarm Description

The system sets quotas for each ZooKeeper top-level directory in the **customized.quota** configuration item and components every 5 hours. This alarm is generated when the system fails to set the quota for a directory.

This alarm is cleared when the setting succeeds after a failure.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
13005	Minor	Quality of service	Tenant plane	ZooKeeper	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.

Type	Parameter	Description
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	ServiceDirectory	Specifies the directory for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold for triggering the alarm.

Impact on the System

Components can write a large amount of data to the top-level directory of ZooKeeper. As a result, services or services of upstream components (such as Yarn, Flink, and Spark) that depend on the top-level directory are abnormal.

Possible Causes

The quota for the alarm directory is inappropriate.

Handling Procedure

Check whether the quota for the alarm directory is appropriate.

Step 1 Log in to FusionInsight Manager, and choose **Cluster >** *Name of the desired cluster* **> Services** > **ZooKeeper**. On the displayed page, choose **Configurations** > **All Configurations** > **Quota**. Check whether the directory for which the alarm is reported and its quota exist in the **customized.quota** configuration item.

- If yes, go to **Step 5**.
- If no, go to **Step 2**.

Step 2 Check whether the alarm directory for which the alarm is reported is in the following alarm list.

Table 1-1 Component alarm directory

Component	Alarm Directory
Solr	/solr
Hbase	/hbase
Hive	/beelinesql
Yarn	/rmstore
Kafka	/kafka
Elasticsearch	/elasticsearch

- If yes, go to **Step 3**.
- If no, go to **Step 7**.

Step 3 View the component of the alarm directory in the table, open the corresponding service page, and choose **Configurations** > **All Configurations**. On the displayed page, search for **zk.quota** in the upper right corner. The search result is the quota of the alarm directory.

Step 4 Check whether the quota of the alarm directory for which the alarm is reported is appropriate. The quota must be greater than or equal to the actual value, which can be obtained in **Trigger Condition**.

Step 5 Modify the **services.quota** value as prompted and save the configuration.

Step 6 After the time specified by **service.quotas.auto.check.cron.expression**, check whether the alarm is cleared.

The **service.quotas.auto.check.cron.expression** parameter indicates the scheduled expression used by ZooKeeper to set the directory quota. You can choose **Cluster** > **Services** > **ZooKeeper** > **Configurations** > **All Configurations** on FusionInsight Manager and set this parameter. The default value is */5 * * * *, indicating 5 minutes.

- If it is, no further action is required.
- If no, go to **Step 7**.

Collect fault information.

Step 7 On the FusionInsight Manager portal, choose **O&M** > **Log** > **Download**.

Step 8 Select **ZooKeeper** in the required cluster from the **Service**.

Step 9 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.102 ALM-13006 Znode Number or Capacity Exceeds the Threshold

Alarm Description

The system periodically detects the status of secondary Znode in the ZooKeeper service data directory every four hours. This alarm is generated when the number or capacity of secondary Znodes exceeds the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
13006	Critical (default threshold: 963718) Major (default threshold: 953718) Minor (default threshold: 943718)	Quality of service	Tenant plane	ZooKeeper	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	ServiceDirectory	Specifies the directory for which the alarm is generated.
	MetricName	Specifies the name of the indicator for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold for triggering the alarm.

Impact on the System

A large amount of data is written to the ZooKeeper data directory space. As a result, services of upstream components (such as Yarn, Flink, and Spark) that depend on this directory are abnormal. For details, see the alarm location information.

Possible Causes

A large amount of data is written to the ZooKeeper data directory. The threshold is not appropriate.

Handling Procedure

Check whether a large amount of data is written to the directory for which the alarm is generated.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. On the displayed interface, click the drop-down button of **Znode Number or Capacity Exceeds the Threshold**. Confirm the Znode for which the alarm is generated in Location Information.

Step 2 Log in to FusionInsight Manager, open the ZooKeeper service interface, and select **Resource**. In the table **Used Resources (By Second-Level Znode)**, check whether a large amount of data is written to the top-level Znode for which the alarm is reported.

- If it is, go to **Step 3**.
- If it is not, go to **Step 4**.

Step 3 Log in to the ZooKeeper client and delete the data in the top-level Znode.

Step 4 Log in to FusionInsight Manager and open the ZooKeeper service interface. On the **Resource** page, choose > **By Znode quantity** in **Used Resources (By Second-Level Znode)**. **Threshold Configuration of By Znode quantity** is displayed. Click **Modify** under **Operation**. Increase the threshold by referringto the value of **max.Znode.count** by choosing **Cluster >** *Name of the desired cluster* **> Services** > **ZooKeeper** > **Configurations > All Configurations > Quota**.

Step 5 In the **Used Resources (By Second-Level Znode)**, choose > **By capacity**. The **Threshold Settings** page of **By Capacity** is displayed. Click **Modify** under **Operation**. Increase the threshold by referring to the value of **max.data.size** by choosing **Cluster >** *Name of the desired cluster* **> Services** > **ZooKeeper** > **Configurations > All Configurations** > **Quota**.

Step 6 Check whether the alarm is cleared.

- If it is, no further action is required.
- If it is not, go to **Step 7**.

Collect fault information.

Step 7 On the FusionInsight Manager portal, choose **O&M** > **Log > Download**.

Step 8 Select **ZooKeeper** in the required cluster from the **Service**.

Step 9 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.103 ALM-13007 Available ZooKeeper Client Connections Are Insufficient

Alarm Description

The system periodically detects the number of active processes between the ZooKeeper client and the ZooKeeper server every 60 seconds. This alarm is generated when the number of connections exceeds the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
13007	Critical (default threshold: 2200) Major (default threshold: 2000) Minor (default threshold: 1800)	Quality of service	Tenant plane	ZooKeeper	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role name for which the alarm is generated.
	HostName	Specifies the host name for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	ClientIP	Specifies the client IP address.
	ServerIP	Specifies the server IP address.
	Trigger Condition	Specifies the threshold for triggering the alarm.

Impact on the System

A large number of processes are connected to ZooKeeper, and the number of ZooKeeper connections is used up. As a result, services of upstream components (such as Yarn, Flink, and Spark) are abnormal.

Possible Causes

A large number of client processes are connected to ZooKeeper. The thresholds are not appropriate.

Handling ProcedureHandling Procedure

Check whether there are a large number of client processes connected to ZooKeeper.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. On the displayed interface, click the drop-down button of **Available ZooKeeper Client Connections Are Insufficient**. Confirm the node IP address of the host for which the alarm is generated in the Location Information.

Step 2 Open the ZooKeeper service interface, click **Resource** to enter the **Resource** page, and check whether the number of connections of the client with the IP address specified by **Number of Connections (By Client IP Address)** is large.

- If it is, go to **Step 3**.

- If it is not, go to **Step 4**.

Step 3 Check whether connection leakage occurs on the client process.

Step 4 Click in the **Number of Connections (by Client IP Address)** to enter the **Thresholds** page, and click **Modify** under **Operation**. Increase the threshold by referring to the value of **maxClientCnxns** by choosing **Cluster** > *Name of the desired cluster* > **Services** > **ZooKeeper** > **Configurations** > **All Configurations** > **quorumpeer**.

Step 5 Check whether the alarm is cleared.

- If it is, no further action is required.
- If it is not, go to **Step 6**.

Collect fault information.

Step 6 On the FusionInsight Manager portal, choose **O&M** > **Log** > **Download**.

Step 7 Select **ZooKeeper** in the required cluster from the **Service**.

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.104 ALM-13008 ZooKeeper Znode Usage Exceeds the Threshold

Alarm Description

The system checks the level-2 Znode status in the ZooKeeper data directory every hour. This alarm is generated when the system detects that the level-2 Znode usage exceeds the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
13008	Critical (default threshold: 90%) Major (default threshold: 80%)	Quality of service	Tenant plane	ZooKeeper	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	ServiceDirectory	Specifies the directory for which the alarm is generated.
	RoleName	Specifies the role for which the alarm is generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold for triggering the alarm.

Impact on the System

When a large amount of data is written to the ZooKeeper data directory space, ZooKeeper cannot provide services for external systems. As a result, services of upstream components (such as Yarn, Flink, and Spark) that depend on the alarm directory are abnormal.

Possible Causes

- A large amount of data is written to the ZooKeeper data directory.
- The user-defined threshold is inappropriate.

Procedure

Check whether a large amount of data is written into the directory for which the alarm is generated.

Step 1 Log in to FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **ZooKeeper**, and click **Resource**. Click **By Znode quantity** in **Used Resources (By Second-Level Znode)**, and check whether a large amount of data is written to the top Znode.

- If yes, go to **Step 2**.
- If no, go to **Step 4**.

Step 2 Log in to FusionInsight Manager, choose **O&M > Alarm > Alarms**, select **Location** from the drop-down list box next to **ALM-13008 ZooKeeper Znode Quantity Usage Exceeds Threshold**, and obtain the Znode path in **ServiceDirectory**.

Step 3 Log in to the ZooKeeper client as a cluster user and delete unnecessary data from the Znode corresponding to the alarm.

Step 4 Log in to FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **ZooKeeper** > **Configurations** > **All Configurations**, and search for **max.znode.count**, which is the maximum number of ZooKeeper directories. The alarm threshold is 80% of this parameter. Increase the value of this parameter, click **Save**, and restart the service for the configuration to take effect.

Step 5 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 6 On the FusionInsight Manager portal, choose **O&M** > **Log** > **Download**.

Step 7 Select **ZooKeeper** in the required cluster from the **Service**.

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.105 ALM-13009 ZooKeeper Znode Capacity Usage Exceeds the Threshold

Alarm Description

The system checks the level-2 ZNode status in the ZooKeeper data directory every hour. This alarm is generated when the system detects that the capacity usage exceeds the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
13009	Critical (default threshold: 90%) Major (default threshold: 80%)	Quality of service	Tenant plane	ZooKeeper	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.

Type	Parameter	Description
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	ServiceDirectory	Specifies the directory for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

ZooKeeper cannot provide services for external systems, and the services of upstream components (such as Yarn, Flink, and Spark) that depend on the alarm directory are abnormal.

Possible Causes

- A large volume of data has been written to the ZooKeeper data directory.
- The threshold is improperly defined.

Handling Procedure

Check whether a large volume of data is written to the alarm directory.

Step 1 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**. Click the drop-down list in the row containing **ALM-13009 ZooKeeper ZNode Capacity Usage Exceeds the Threshold**, and find the ZNode for which the alarm is generated in the **Location** area.

Step 2 Choose **Cluster** > **Services** > **ZooKeeper**. On the page that is displayed, click the **Resource** tab. In the **Used Resources (By Second-Level ZNode)** area, click **By capacity** and check whether a large amount of data is written to the top-level ZNode directory.

- If yes, record the directory to which a large amount of data is written and go to **Step 3**.
- If no, go to **Step 5**.

Step 3 Check whether data in the directory can be deleted.

NOTICE

Deleting data from ZooKeeper is a high-risk operation. Exercise caution when performing this operation.

- If yes, go to **Step 4**.
- If no, go to **Step 5**.

Step 4 Log in to the ZooKeeper client and delete unnecessary data from the directory to which a large amount of data is written.

1. Log in to the ZooKeeper client installation directory, for example, **/opt/hadoopclient**, and configure environment variables.

   cd /opt/hadoopclient

   source bigdata_env

2. Run the following command to authenticate the user (skip this step for a cluster in normal mode):

   kinit *Component service user*

3. Run the following command to log in to the client tool:

   zkCli.sh -server <*Service IP address of the node where any ZooKeeper instance resides*>:<*Client port*>

4. Run the following command to delete unnecessary data:

   delete *Path of the file to be deleted*

Step 5 Log in to FusionInsight Manager and choose **Cluster** > **Services** > **ZooKeeper**. On the page that is displayed, click the **Configuration** tab then the **All Configurations** sub-tab, and search for **max.data.size**. The value of **max.data.size** is the maximum capacity quota of the ZooKeeper directory. The unit is byte. Search for the **GC_OPTS** configuration item and check the value of **Xmx**.

Step 6 Compare the values of **max.data.size** and **Xmx*0.65**. The threshold is the smaller value multiplied by 80%. You can change the values of **max.data.size** and **Xmx*0.65** to increase the threshold.

Step 7 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Collect the fault information.

Step 8 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 9 Expand the **Service** drop-down list, and select **ZooKeeper** for the target cluster.

Step 10 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 11 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.106 ALM-13010 Znode Usage of a Directory with Quota Configured Exceeds the Threshold

Alarm Description

The system checks the Znode usage of all service directories with quota configured every hour. This alarm is generated when the system detects that the level-2 Znode usage exceeds the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
13010	Critical (default threshold: 90%) Major (default threshold: 80%)	Quality of service	Tenant plane	ZooKeeper	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	ServiceDirectory	Specifies the directory for which the alarm is generated.
	RoleName	Specifies the role for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold for triggering the alarm.

Impact on the System

When a large amount of data is written to the ZooKeeper data directory space, ZooKeeper cannot provide services for external systems. As a result, services of upstream components (such as Yarn, Flink, and Spark) that depend on the alarm directory are abnormal.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Possible Causes

- A large amount of data is written to the ZooKeeper data directory.
- The user-defined threshold is inappropriate.

Handling Procedure

Check whether a large amount of data is written into the directory for which the alarm is generated.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm > Alarms**. Confirm the Znode for which the alarm is generated in **Location** of this alarm.

Step 2 Choose **Cluster** > *Name of the desired cluster* > **Services** > **ZooKeeper** and click **Resource**. In **Used Resources (By Second-Level Znode)**, check whether a large amount of data is written into the top Znode.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 Log in to FusionInsight Manager, choose **O&M > Alarm > Alarms**, select Location from the drop-down list box next to **ALM-13010 Znode Usage of a Directory with Quota Configured Exceeds the Threshold**, and obtain the Znode path in ServiceDirectory.

Step 4 Log in to the ZooKeeper client as a cluster user and delete unwanted data in the Znode for which the alarm is generated.

Step 5 Log in to FusionInsight Manager, and choose **Cluster** > *Name of the desired cluster* > **Services** > *Component of the top Znode for which the alarm isgenerated*. Choose **Configurations** > **All Configurations**, search for **zk.quota.number**, increase its value, click **Save**.

NOTICE

If the Component of the top Znode for which the alarm isgenerated is ClickHouse, change the value of **clickhouse.zookeeper.quota.node.count**.

Step 6 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect fault information.

Step 7 On the FusionInsight Manager portal, choose **O&M** > **Log > Download**.

Step 8 Select **ZooKeeper** in the required cluster from the **Service**.

Step 9 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.107 ALM-14000 HDFS Service Unavailable

Alarm Description

The system checks the NameService service status every 60 seconds. This alarm is generated when all the NameService services are abnormal and the system considers that the HDFS service is unavailable.

This alarm is cleared when at least one NameService service is normal and the system considers that the HDFS service recovers.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
14000	Critical	Quality of service	Tenant plane	HDFS	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm is generated.
	HostName	Specifies the host for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

HDFS fails to provide services for HDFS service-based upper-layer components, such as HBase and MapReduce. As a result, users cannot read or write files.

Possible Causes

- The ZooKeeper service is abnormal.
- All NameService services are abnormal.
- The number of service requests is too large, and the HDFS health check fails to read and write files.
- The health check fails due to HDFS FullGC.

Handling Procedure

Check the ZooKeeper service status.

Step 1 On the FusionInsight Manager portal, choose **O&M > Alarm > Alarms**. On the Alarm page, check whether **ALM-13000 ZooKeeper Service Unavailable** is reported.

- If yes, go to **Step 2**.
- If no, go to **Step 4**.

Step 2 See **ALM-13000 ZooKeeper Service Unavailable** to rectify the health status of ZooKeeper fault and check whether the **Running Status** of the ZooKeeper service restores to **Normal**.

- If yes, go to **Step 3**.
- If no, go to **Step 13**.

Step 3 On the **O&M > Alarm > Alarms** page, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 4**.

Handle the NameService service exception alarm.

Step 4 On the FusionInsight Manager portal, choose **O&M > Alarm > Alarms**. On the Alarms page, check whether **ALM-14010 NameService Service Unavailable** is reported.

- If yes, go to **Step 5**.
- If no, go to **Step 7**.

Step 5 See **ALM-14010 NameService Service Unavailable** to handle the abnormal NameService services and check whether each NameService service exception alarm is cleared.

- If yes, go to **Step 6**.
- If no, go to **Step 13**.

Step 6 On the **O&M > Alarm > Alarms** page, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Check whether the HDFS health check fails to read or write files due to a large number of service requests.

Step 7 On FusionInsight Manager, choose **O&M > Alarm > Alarms**, and check whether **ALM-14021 NameNode Average RPC Processing Time Exceeds the Threshold** or **ALM-14022 NameNode Average RPC Queuing Time Exceeds the Threshold** is generated.

- If yes, go to **Step 8**.
- If no, go to **Step 10**.

Step 8 Rectify the abnormal NameServices by following the handling methods of **ALM-14021 NameNode Average RPC Processing Time Exceeds the Threshold** and **ALM-14022 NameNode Average RPC Queuing Time Exceeds the Threshold**. Then, check whether the alarms are cleared.

- If yes, go to **Step 9**.
- If no, go to **Step 13**.

Step 9 On the **O&M > Alarm > Alarms** page, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 10**.

Check whether the health check fails due to HDFS FullGC.

Step 10 On the FusionInsight Manager portal, choose **O&M > Alarm > Alarms**. On the Alarms page, check whether **ALM-14014 NameNode GC Time Exceeds the Threshold** is reported.

- If yes, go to **Step 11**.
- If no, go to **Step 13**.

Step 11 See **ALM-14014 NameNode GC Time Exceeds the Threshold** to handle the abnormal NameService services and check whether each NameService service exception alarm is cleared.

- If yes, go to **Step 12**.
- If no, go to **Step 13**.

Step 12 On the **O&M > Alarm > Alarms** page, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 13**.

Collect fault information.

Step 13 On the FusionInsight Manager portal, choose **O&M** > **Log > Download**.

Step 14 Select the following nodes in the required cluster from the **Service**:

- ZooKeeper
- HDFS

Step 15 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 16 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.108 ALM-14001 HDFS Disk Usage Exceeds the Threshold

Alarm Description

The system checks the HDFS disk usage every 30 seconds and compares the actual HDFS disk usage with the threshold. The HDFS disk usage indicator has a default threshold, this alarm is generated when the value of the disk usage of a Hadoop distributed file system (HDFS) indicator exceeds the threshold.

To change the threshold, choose **O&M** > **Alarm > Thresholds** > *Name of the desired cluster* **> HDFS**.

When the **Trigger Count** is 1, this alarm is cleared when the value of the disk usage of HDFS cluster indicator is less than or equal to the threshold. When the **Trigger Count** is greater than 1, this alarm is cleared when the value of the disk usage of HDFS cluster indicator is less than or equal to 80% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
14001	Critical (default threshold: 90%) Major (default threshold: 80%)	Environment	Tenant plane	HDFS	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm is generated.
	HostName	Specifies the host for which the alarm is generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	NameService Name	Specifies the NameService for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

Writing Hadoop distributed file system (HDFS) data is affected.

Possible Causes

The disk space configured for the HDFS cluster is insufficient.

Handling Procedure

Check the disk capacity and delete unnecessary files.

Step 1 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services** > **HDFS**.

Step 2 Click the drop-down menu in the upper right corner of **Chart**, choose **Customize** > **Disk**, and select **Percentage of HDFS Capacity** to check whether the HDFS disk usage exceeds the threshold.

- If yes, go to **Step 3**.
- If no, go to **Step 11**.

Step 3 In the **Basic Information** area, click the **NameNode(Active)** of the failure NameService and the HDFS WebUI page is displayed.

NOTE

By default, the **admin** user does not have the permissions to manage other components. If the page cannot be opened or the displayed content is incomplete when you access the native UI of a component due to insufficient permissions, you can manually create a user with the permissions to manage that component.

Step 4 On the HDFS web user interface (WebUI), click **Datanodes** tab. In the **Block pool used** column, view the disk usage of all DataNodes to check whether the disk usage of any DataNode exceeds the threshold.

- If yes, go to **Step 6**.
- If no, go to **Step 11**.

Step 5 Log in to the MRS client node as user **root**.

Step 6 Run **cd /opt/hadoopclient** to switch to the client installation directory, and run **source bigdata_env**. If the cluster uses the security mode, perform security authentication. Run **kinit hdfs** and enter the password as prompted. Please obtain the password from the administrator.

Step 7 Run the **hdfs dfs -rm -r** *file or directory* command to delete unnecessary files.

Step 8 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Expand the system.

Step 9 Expand the disk capacity. For details, see the *MapReduce Service (MRS) 3.3.1-LTS Physical Machine Cluster Component Migration Guide (for Huawei Cloud Stack 8.3.1)*.

Step 10 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 11**.

Collect fault information.

Step 11 On the FusionInsight Manager portal, choose **O&M** > **Log > Download**.

Step 12 Select the following nodes in the required cluster from the **Service**:

- ZooKeeper
- HDFS

Step 13 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 14 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.109 ALM-14002 DataNode Disk Usage Exceeds the Threshold

Alarm Description

The system checks the DataNode disk usage every 30 seconds and compares the actual disk usage with the threshold. A default threshold range is provided for the DataNode disk usage. This alarm is generated when the DataNode disk usage exceeds the threshold.

To change the threshold, choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **HDFS**.

If **Trigger Count** is **1**, this alarm is cleared when the DataNode disk usage is less than or equal to the threshold. If **Trigger Count** is greater than **1**, this alarm is cleared when the DataNode disk usage is less than or equal to 80% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
14002	Critical (default threshold: 90%) Major (default threshold: 80%)	Quality of service	Tenant plane	HDFS	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

Insufficient disk space will impact data write to HDFS.

Possible Causes

- The disk space configured for the HDFS cluster is insufficient.
- Data skew occurs among DataNodes.

Handling Procedure

Check whether the cluster disk capacity is full.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**, and check whether the **ALM-14001 HDFS Disk Usage Exceeds the Threshold** alarm exists.

- If yes, go to **Step 2**.
- If no, go to **Step 4**.

Step 2 Handle the alarm by following the instructions in **ALM-14001 HDFS Disk Usage Exceeds the Threshold** and check whether the alarm is cleared.

- If yes, go to **Step 3**.
- If no, go to **Step 11**.

Step 3 Choose **O&M** > **Alarm** > **Alarms** and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 4**.

Check the balance status of DataNodes.

Step 4 On FusionInsight Manager, choose **Hosts**. Check whether the number of DataNodes on each rack is almost the same. If the difference is large, adjust the racks to which DataNodes belong to ensure that the number of DataNodes on each rack is almost the same. Restart the HDFS service for the settings to take effect.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 5 Choose **Cluster** > *Name of the desired cluster* > **Services** > **HDFS**.

Step 6 In the **Basic Information** area, click **NameNode(Active)**. The HDFS web UI is displayed.

NOTE

By default, the **admin** user does not have the permissions to manage other components. If the page cannot be opened or the displayed content is incomplete when you access the native UI of a component due to insufficient permissions, you can manually create a user with the permissions to manage that component.

Step 7 In the **Summary** area of the HDFS web UI, check whether the value of **Max** is 10% greater than that of **Median** in **DataNodes usages**.

- If yes, go to **Step 8**.
- If no, go to **Step 11**.

Step 8 Balance skewed data in the cluster. Log in to the MRSclient as user **root**. If the cluster is in normal mode, run the **su - omm** command to switch to user **omm**. Run the **cd** command to go to the client installation directory and run the **source bigdata_env** command. If the cluster uses the security mode, perform security authentication. Run **kinit hdfs** and enter the password as prompted. Obtain the password from the MRS cluster administrator.

Step 9 Run the following command to balance data distribution:

hdfs balancer -threshold 10

Step 10 Wait several minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 11**.

Collect the fault information.

Step 11 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 12 Expand the drop-down list next to the **Service** field. In the **Services** dialog box that is displayed, select **HDFS** for the target cluster.

Step 13 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 14 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.110 ALM-14003 Number of Lost HDFS Blocks Exceeds the Threshold

Alarm Description

The system checks the lost blocks every 30 seconds and compares the actual lost blocks with the threshold. The lost blocks indicator has a default threshold. This alarm is generated when the number of lost HDFS blocks exceeds the threshold.

To change the threshold, choose **O&M** > **Alarm > Thresholds** > *Name of the desired cluster* **> HDFS**.

If **Trigger Count** is **1**, this alarm is cleared when the value of lost HDFS blocks is less than or equal to the threshold. If **Trigger Count** is greater than **1**, this alarm is cleared when the value of lost HDFS blocks is less than or equal the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
14003	Critical (default threshold: 1000) Major (default threshold: 0)	Quality of service	Tenant plane	HDFS	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	NameService Name	Specifies the NameService for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

Data stored in HDFS is lost. HDFS may enter the safe mode and cannot provide write services. Lost block data cannot be restored.

Possible Causes

- The DataNode instance is abnormal.
- Data is deleted.

Handling Procedure

Check the DataNode instance.

Step 1 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **HDFS** > **Instance**.

Step 2 Check whether the **Running Status** of all DataNode instance is **Normal**.

- If yes, go to **Step 11**.
- If no, go to **Step 3**.

Step 3 Restart the DataNode instance and check whether the DataNode instance restarts successfully.

- If yes, go to **Step 4**.
- If no, go to **Step 5**.

Step 4 Choose **O&M** > **Alarm** > **Alarms** and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Delete the damaged file.

Step 5 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **HDFS** > **NameNode(Active)**. On the WebUI page of the HDFS, view the information about lost blocks.

NOTE

- If a block is lost, a line in red is displayed on the WebUI.
- By default, the **admin** user does not have the permissions to manage other components. If the page cannot be opened or the displayed content is incomplete when you access the native UI of a component due to insufficient permissions, you can manually create a user with the permissions to manage that component.

Step 6 The user checks whether the file containing the lost data block is useful.

NOTE

Files generated in directories **/mr-history**, **/tmp/hadoop-yarn**, and **/tmp/logs** during MapReduce task execution are unnecessary.

- If yes, go to **Step 7**.
- If no, go to **Step 8**.

Step 7 The user checks whether the file containing the lost data block is backed up.

- If yes, go to **Step 8**.
- If no, go to **Step 11**.

Step 8 Log in to the HDFS client as user **root**. The user password is defined by the user before the installation. Contact the MRS cluster administrator to obtain the password. Run the following commands:

- Security mode:

  cd *Client installation directory*

  source bigdata_env

  kinit hdfs

- Normal mode:

  su - omm

  cd *Client installation directory*

  source bigdata_env

Step 9 On the node client, run **hdfs fsck / -delete** to delete the lost file. If the file where the lost block is located is a useful file, you need to write the file again to restore the data.

NOTE

Deleting a file or folder is a high-risk operation. Ensure that the file or folder is no longer required before performing this operation.

Step 10 Choose **O&M** > **Alarm** > **Alarms** and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 11**.

Collect the fault information.

Step 11 On FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 12 Expand the drop-down list next to the **Service** field. In the **Services** dialog box that is displayed, select **HDFS** for the target cluster.

Step 13 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 14 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.111 ALM-14006 Number of HDFS Files Exceeds the Threshold

Alarm Description

The system periodically checks the number of HDFS files every 30 seconds and compares the number of HDFS files with the threshold. This alarm is generated when the system detects that the number of HDFS files exceeds the threshold.

If **Trigger Count** is **1**, this alarm is cleared when the number of HDFS files is less than or equal to the threshold. If **Trigger Count** is greater than **1**, this alarm is cleared when the number of HDFS files is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
14006	Major	Quality of service	Tenant plane	HDFS	Yes

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Changes

Change Type	Version	Description	Reason for Change
Modify	3.3.1	Alarm Severity: changed from minor to major.	Alarm Severity: Accuracy optimized

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	NameServiceName	Specifies the NameService for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

If there are too many HDFS files, the HDFS system may respond slowly or the disk space may be used up.

Possible Causes

The number of HDFS files exceeds the threshold.

Handling Procedure

Check the number of files in the system.

Step 1 On FusionInsight Manager, check the number of HDFS files. Specifically, choose **Cluster** > *Name of the desired cluster* > **Services** > **HDFS**. Click the drop-down menu in the upper right corner of **Chart**, choose **Customize** > **File and Block**, and select **HDFS File** and **Total Blocks**.

Step 2 Choose **Cluster** > *Name of the desired cluster* > **Services** > **HDFS** > **Configurations** > **All Configurations**, and search for the **GC_OPTS** parameter under **NameNode**.

Step 3 Configure the threshold of the number of configuration file objects. Specifically, change the value of **Xmx** (GB) in the **GC_OPTS** parameter. The threshold (specified by y) is calculated as follows: y = 0.2007 x Xmx - 0.6312, where x indicates the memory capacity Xmx (GB) and y indicates the number of files (unit: kW). Adjust the memory size as required.

Step 4 Confirm that the value of **GC_PROFILE** is **custom** so that the **GC_OPTS** configuration takes effect. Click **Save** and choose **More** > **Restart Instance** to restart the service.

Step 5 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Check whether needless files exist in the system.

Step 6 Log in to the HDFS client as user **root**. Run **cd** to switch to the client installation directory, and run **source bigdata_env** to configure the environment variables.

If the cluster uses the security mode, perform security authentication.

Run the **kinit hdfs** command and enter the password as prompted. Obtain the password from the MRS cluster administrator.

Step 7 Run **hdfs dfs -ls** *file or directory* to check whether the files in the directory can be deleted.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If yes, go to **Step 8**.
- If no, go to **Step 9**.

Step 8 Run the **hdfs dfs -rm -r** *file or directory path* command. After deleting unnecessary files, wait until the files are retained in the recycle bin for a period longer than the value of **fs.trash.interval** on the NameNode. Then check whether the alarm is cleared.

NOTE

Deleting a file or folder is a high-risk operation. Ensure that the file or folder is no longer required before performing this operation.

- If yes, no further action is required.
- If no, go to **Step 9**.

Collect the fault information.

Step 9 On FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 10 Expand the drop-down list next to the **Service** field. In the **Services** dialog box that is displayed, select **HDFS** for the target cluster.

Step 11 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

Configuration rules of the NameNode JVM parameter

Default value of the NameNode JVM parameter **GC_OPTS**:

-Xms2G -Xmx4G -XX:NewSize=128M -XX:MaxNewSize=256M -XX:MetaspaceSize=128M -XX:MaxMetaspaceSize=128M -XX:+UseConcMarkSweepGC -XX:+CMSParallelRemarkEnabled -XX:CMSInitiatingOccupancyFraction=65 -XX:+PrintGCDetails -Dsun.rmi.dgc.client.gcInterval=0x7FFFFFFFFFFFFE -Dsun.rmi.dgc.server.gcInterval=0x7FFFFFFFFFFFFE -XX:-OmitStackTraceInFastThrow -XX:+PrintGCDateStamps -XX:+UseGCLogFileRotation -XX:NumberOfGCLogFiles=10 -XX:GCLogFileSize=1M -Djdk.tls.ephemeralDHKeySize=3072 -Djdk.tls.rejectClientInitiatedRenegotiation=true -Djava.io.tmpdir=${Bigdata_tmp_dir}

The number of NameNode files is proportional to the used memory size of the NameNode. When file objects change, you need to change **-Xms2G -Xmx4G -XX:NewSize=128M -XX:MaxNewSize=256M** in the default value. The following table lists the reference values.

Table 1-2 NameNode JVM configuration

Number of File Objects	Reference Value
10,000,000	-Xms6G -Xmx6G -XX:NewSize=512M -XX:MaxNewSize=512M
20,000,000	-Xms12G -Xmx12G -XX:NewSize=1G -XX:MaxNewSize=1G
50,000,000	-Xms32G -Xmx32G -XX:NewSize=3G -XX:MaxNewSize=3G
100,000,000	-Xms64G -Xmx64G -XX:NewSize=6G -XX:MaxNewSize=6G
200,000,000	-Xms96G -Xmx96G -XX:NewSize=9G -XX:MaxNewSize=9G
300,000,000	-Xms164G -Xmx164G -XX:NewSize=12G -XX:MaxNewSize=12G

1.3.112 ALM-14007 NameNode Heap Memory Usage Exceeds the Threshold

Alarm Description

The system checks the HDFS NameNode Heap Memory usage every 30 seconds and compares the actual Heap memory usage with the threshold. The HDFS NameNode Heap Memory usage has a default threshold. This alarm is generated when the HDFS NameNode Heap Memory usage exceeds the threshold.

You can change the threshold in **O&M** > **Alarm > Thresholds** > *Name of the desired cluster* **> HDFS**.

When the **Trigger Count** is 1, this alarm is cleared when the HDFS NameNode Heap memory usage is less than or equal to the threshold. When the **Trigger Count** is greater than 1, this alarm is cleared when the HDFS NameNode Heap memory usage is less than or equal to 95% of the threshold.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
14007	Critical (default threshold: 98%) Major (default threshold: 95%)	Quality of service	Tenant plane	HDFS	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm is generated.
	HostName	Specifies the host for which the alarm is generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

The HDFS NameNode Heap Memory usage is too high, which affects the data read/write performance of the HDFS.

Possible Causes

The HDFS NameNode Heap Memory is insufficient.

Handling Procedure

Delete unnecessary files.

Step 1 Log in to the HDFS client as user **root**. Run **cd** to switch to the client installation directory, and run **source bigdata_env**.

If the cluster uses the security mode, perform security authentication.

Run the **kinit hdfs** command and enter the password as prompted. Obtain the password from the administrator.

Step 2 Run the **hdfs dfs -rm -r** *file or directory* command to delete unnecessary files.

Step 3 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 4**.

Check the NameNode JVM memory usage and configuration.

Step 4 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services** > **HDFS**.

Step 5 In the **Basic Information** area, click **NameNode(Active)** to go to the HDFS WebUI.

NOTE

By default, the **admin** user does not have the permissions to manage other components. If the page cannot be opened or the displayed content is incomplete when you access the native UI of a component due to insufficient permissions, you can manually create a user with the permissions to manage that component.

Step 6 On the HDFS WebUI, click the **Overview** tab. In **Summary**, check the numbers of files, directories, and blocks in the HDFS.

Step 7 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **HDFS** > **Configurations** > **All Configurations**. In **Search**, enter **GC_OPTS** to check the **GC_OPTS** memory parameter of **HDFS->NameNode**.

Adjust the configuration in the system.

Step 8 Check whether the memory is configured properly based on the number of files in **Step 6** and the NameNode Heap Memory parameters in **Step 7**.

- If yes, go to **Step 9**.
- If no, go to **Step 11**.

NOTE

The recommended mapping between the number of HDFS file objects (filesystem objects = files + blocks) and the JVM parameters configured for NameNode is as follows:

- If the number of file objects reaches 10,000,000, you are advised to set the JVM parameters as follows: -Xms6G -Xmx6G -XX:NewSize=512M -XX:MaxNewSize=512M
- If the number of file objects reaches 20,000,000, you are advised to set the JVM parameters as follows: -Xms12G -Xmx12G -XX:NewSize=1G -XX:MaxNewSize=1G
- If the number of file objects reaches 50,000,000, you are advised to set the JVM parameters as follows: -Xms32G -Xmx32G -XX:NewSize=3G -XX:MaxNewSize=3G
- If the number of file objects reaches 100,000,000, you are advised to set the JVM parameters as follows: -Xms64G -Xmx64G -XX:NewSize=6G -XX:MaxNewSize=6G
- If the number of file objects reaches 200,000,000, you are advised to set the JVM parameters as follows: -Xms96G -Xmx96G -XX:NewSize=9G -XX:MaxNewSize=9G
- If the number of file objects reaches 300,000,000, you are advised to set the JVM parameters as follows: -Xms164G -Xmx164G -XX:NewSize=12G -XX:MaxNewSize=12G

Step 9 Modify the heap memory parameters of the NameNode based on the mapping between the number of file objects and the memory. Click **Save** and choose **Dashboard** > **More** > **Restart Service**.

Step 10 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 11**.

Collect fault information.

Step 11 On the FusionInsight Manager portal, choose **O&M** > **Log > Download**.

Step 12 Select the following nodes in the required cluster from the **Service**:

- ZooKeeper
- HDFS

Step 13 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 14 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.113 ALM-14008 DataNode Heap Memory Usage Exceeds the Threshold

Alarm Description

The system checks the HDFS DataNode Heap Memory usage every 30 seconds and compares the actual Heap Memory usage with the threshold. The HDFS DataNode Heap Memory usage has a default threshold. This alarm is generated when the HDFS DataNode Heap Memory usage exceeds the threshold.

You can change the threshold in **O&M** > **Alarm > Thresholds** > *Name of the desired cluster* **> HDFS**.

When the **Trigger Count** is 1, this alarm is cleared when the HDFS DataNode Heap Memory usage is less than or equal to the threshold. When the **Trigger Count** is greater than 1, this alarm is cleared when the HDFS DataNode Heap Memory usage is less than or equal to 95% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
14008	Critical (default threshold: 98%) Major (default threshold: 95%)	Quality of service	Tenant plane	HDFS	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.

Type	Parameter	Description
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm is generated.
	HostName	Specifies the host for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

The HDFS DataNode Heap Memory usage is too high, which affects the data read/write performance of the HDFS.

Possible Causes

The HDFS DataNode Heap Memory is insufficient.

Handling Procedure

Delete unnecessary files.

Step 1 Log in to the HDFS client as user **root**. Run **cd** to switch to the client installation directory, and run **source bigdata_env**.

If the cluster uses the security mode, perform security authentication.

Run the **kinit hdfs** command and enter the password as prompted. Obtain the password from the administrator.

Step 2 Run the **hdfs dfs -rm -r** *file or directory* command to delete unnecessary files.

Step 3 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 4**.

Check the DataNode JVM memory usage and configuration.

Step 4 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **HDFS**.

Step 5 In the **Basic Information** area, click **NameNode(Active)** to go to the HDFS WebUI.

NOTE

By default, the **admin** user does not have the permissions to manage other components. If the page cannot be opened or the displayed content is incomplete when you access the native UI of a component due to insufficient permissions, you can manually create a user with the permissions to manage that component.

Step 6 On the HDFS WebUI, click the **DataNodes** tab, and check the number of blocks of all DataNodes related to the alarm.

Step 7 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **HDFS** > **Configurations** > **All Configurations**. In **Search**, enter **GC_OPTS** to check the GC_OPTS memory parameter of **HDFS->DataNode**.

Adjust the configuration in the system.

Step 8 Check whether the memory is configured properly based on the number of block in **Step 6** and the DataNode Heap Memory parameters in **Step 7**.

- If yes, go to **Step 9**.
- If no, go to **Step 11**.

NOTE

The mapping between the average number of blocks of a DataNode instance and the DataNode memory is as follows:

- If the average number of blocks of a DataNode instance reaches 2,000,000, the reference values of the JVM parameters of the DataNode are as follows: -Xms6G -Xmx6G -XX:NewSize=512M -XX:MaxNewSize=512M
- If the average number of blocks of a DataNode instance reaches 5,000,000, the reference values of the JVM parameters of the DataNode are as follows: -Xms12G -Xmx12G -XX:NewSize=1G -XX:MaxNewSize=1G

Step 9 Modify the heap memory parameters of the DataNode based on the mapping between the number of blocks and the memory. Click **Save** and choose **Dashboard** > **More** > **Restart Service**.

Step 10 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 11**.

Collect fault information.

Step 11 On the FusionInsight Manager portal, choose **O&M** > **Log > Download**.

Step 12 Select **HDFS** in the required cluster from the **Service**.

Step 13 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 14 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.114 ALM-14009 Number of Dead DataNodes Exceeds the Threshold

Alarm Description

The system periodically detects the number of dead DataNodes in the HDFS cluster every 30 seconds, and compares the number with the threshold. The number of DataNodes in the Dead state has a default threshold. This alarm is generated when the number exceeds the threshold.

You can change the threshold in **O&M** > **Alarm > Thresholds** > *Name of the desired cluster* **> HDFS**.

When the **Trigger Count** is 1, this alarm is cleared when the number of Dead DataNodes is less than or equal to the threshold. When the **Trigger Count** is greater than 1, this alarm is cleared when the number of Dead DataNodes is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
14009	Major	Quality of service	Tenant plane	HDFS	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.

Type	Parameter	Description
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm is generated.
	HostName	Specifies the host for which the alarm is generated.
	NameServiceName	Specifies the NameService for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

DataNodes that are in the Dead state cannot provide HDFS services. As a result, users cannot read or write files.

Possible Causes

- DataNodes are faulty or overloaded.

- The network between the NameNode and the DataNode is disconnected or busy.
- NameNodes are overloaded.
- The NameNodes are not restarted after the DataNode is deleted.

Handling Procedure

Check whether DataNodes are faulty.

Step 1 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **HDFS**. The **HDFS Status** page is displayed.

Step 2 In the **Basic Information** area, click **NameNode(Active)** to go to the HDFS WebUI.

NOTE

By default, the **admin** user does not have the permissions to manage other components. If the page cannot be opened or the displayed content is incomplete when you access the native UI of a component due to insufficient permissions, you can manually create a user with the permissions to manage that component.

Step 3 On the HDFS WebUI, click the **Datanodes** tab. In the **In operation** area, click **Filter** to check whether **down** is in the drop-down list.

- If yes, select **down**, record the information about the filtered DataNodes, and go to **Step 4**.
- If no, go to **Step 8**.

Step 4 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* > **Services** > **HDFS** > **Instance** to check whether recorded DataNodes exist in the instance list.

- If all recorded DataNodes exist, go to **Step 5**.
- If none of the recorded DataNodes exists, go to **Step 6**.
- If some of the recorded DataNodes exist, go to **Step 7**.

Step 5 Locate the DataNode instance, click **More** > **Restart Instance** to restart it and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Step 6 Select all NameNode instances, choose **More** > **Instance Rolling Restart** to restart them and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 16**.

Step 7 Select all NameNode instances, choose **More** > **Instance Rolling Restart** to restart them. Locate the DataNode instance, click **More** > **Restart Instance** to restart it and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Check the status of the network between the NameNode and the DataNode.

Step 8 Log in to the faulty DataNode on the management page as user **root**, and run the **ping** *IP address of the NameNode* command to check whether the network between the DataNode and the NameNode is abnormal.

On the FusionInsight Manager page, choose **Cluster >** *Name of the desired cluster* **> Services** > **HDFS** > **Instance**. In the instance list, view the service plane IP address of the faulty DataNode.

- If yes, go to **Step 9**.
- If no, go to **Step 10**.

Step 9 Rectify the network fault, and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 10**.

Check whether the DataNode is overloaded.

Step 10 On the FusionInsight Manager portal, choose **O&M > Alarm > Alarms** and check whether the alarm **ALM-14008 HDFS DataNode Memory Usage Exceeds the Threshold** exists.

- If yes, go to **Step 11**.
- If no, go to **Step 13**.

Step 11 See **ALM-14008 HDFS DataNode Memory Usage Exceeds the Threshold** to handle the alarm and check whether the alarm is cleared.

- If yes, go to **Step 12**.
- If no, go to **Step 13**.

Step 12 Check whether the alarm is cleared from the alarm list.

- If yes, no further action is required.
- If no, go to **Step 13**.

Check whether the NameNode is overloaded.

Step 13 On the FusionInsight Manager portal, choose **O&M > Alarm > Alarms** and check whether the alarm **ALM-14007 HDFS NameNode Memory Usage Exceeds the Threshold** exists.

- If yes, go to **Step 14**.
- If no, go to **Step 16**.

Step 14 See **ALM-14007 HDFS NameNode Memory Usage Exceeds the Threshold** to handle the alarm and check whether the alarm is cleared.

- If yes, go to **Step 15**.
- If no, go to **Step 16**.

Step 15 Check whether the alarm is cleared from the alarm list.

- If yes, no further action is required.
- If no, go to **Step 16**.

Collect fault information.

Step 16 On the FusionInsight Manager portal, choose **O&M** > **Log > Download**.

Step 17 Select **HDFS** in the required cluster from the **Service**.

Step 18 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 19 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.115 ALM-14010 NameService Service Is Abnormal

Alarm Description

The system checks the NameService service status every 180 seconds. This alarm is generated when the NameService service is unavailable.

This alarm is cleared when the NameService service recovers.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
14010	Major	Quality of service	Tenant plane	HDFS	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.

Type	Parameter	Description
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	NameService Name	Specifies the NameService for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

HDFS fails to provide services for upper-layer components based on the NameService service, such as HBase and MapReduce. As a result, users cannot read or write files.

Possible Causes

- The KrbServer service is abnormal.
- The JournalNode is faulty.
- The DataNode is faulty.
- The disk capacity is insufficient.
- The NameNode enters safe mode.

Handling Procedure

Check the KrbServer service status.

Step 1 On FusionInsight Manager, choose **Cluster** > **Services**.

Step 2 Check whether the KrbServer service exists.

- If yes, go to **Step 3**.

- If no, go to **Step 6**.

Step 3 Click **KrbServer**.

Step 4 Click **Instances**. On the KrbServer management page, select the faulty instance, and choose **More** > **Restart Instance**. Check whether the instance successfully restarts.

- If yes, go to **Step 5**.
- If no, go to **Step 24**.

Step 5 Choose **O&M** > **Alarm** > **Alarms** and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Check the JournalNode instance status.

Step 6 On FusionInsight Manager, choose **Cluster** > **Services**.

Step 7 Choose **HDFS** > **Instances**.

Step 8 Check whether the **Running Status** of the JournalNode is **Normal**.

- If yes, go to **Step 11**.
- If no, go to **Step 9**.

Step 9 Select the faulty JournalNode, and choose **More** > **Restart Instance**. Check whether the JournalNode successfully restarts.

- If yes, go to **Step 10**.
- If no, go to **Step 24**.

Step 10 Choose **O&M** > **Alarm** > **Alarms** and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 11**.

Check the DataNode instance status.

Step 11 On FusionInsight Manager, choose **Cluster** > **Services** > **HDFS**.

Step 12 Click **Instances** and check whether **Running Status** of all DataNodes is **Normal**.

- If yes, go to **Step 15**.
- If no, go to **Step 13**.

Step 13 Click **Instances**. On the DataNode management page, select the faulty instance, and choose **More** > **Restart Instance**. Check whether the DataNode successfully restarts.

- If yes, go to **Step 14**.
- If no, go to **Step 15**.

Step 14 Choose **O&M** > **Alarm** > **Alarms** and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 15**.

Check disk status.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 15 On FusionInsight Manager, choose **Hosts**.

Step 16 In the **Disk** column, check whether the disk space is insufficient.

- If yes, go to **Step 17**.
- If no, go to **Step 19**.

Step 17 Expand the disk capacity. For details, see MapReduce Service (MRS) 3.3.1-LTS Physical Machine Cluster Capacity Expansion Guide (for Huawei Cloud Stack 8.3.1).

Step 18 Choose **O&M** > **Alarm** > **Alarms** and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 19**.

Check whether NameNode is in the safe mode.

Step 19 On FusionInsight Manager, choose **Cluster** > **Services** > **HDFS**.

Step 20 In the **Basic Information** area on the **Dashboard** page of HDFS (or in the **NameService Summary** area on the **Dashboard** page of HDFS), check whether the value of **Safe Mode** is **ON**.

ON indicates that the safe mode is enabled.

- If yes, go to **Step 21**.
- If no, go to **Step 24**.

Step 21 Log in to the client as user **root**. Run the **cd** command to go to the client installation directory and run the **source bigdata_env** command. If the cluster uses the security mode, perform security authentication. Run the **kinit hdfs** command and enter the password as prompted. The password can be obtained from the MRS cluster administrator. If the cluster uses the non-security mode, log in as user **omm** and run the command. Ensure that user **omm** has the client execution permission.

Step 22 Run **hdfs dfsadmin -safemode leave**.

Step 23 Choose **O&M** > **Alarm** > **Alarms** and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 24**.

Collect fault information.

Step 24 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 25 In the **Service** area, select the following nodes of the desired cluster.

- ZooKeeper
- HDFS

Step 26 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 27 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.116 ALM-14011 DataNode Data Directory Is Not Configured Properly

Alarm Description

The DataNode parameter **dfs.datanode.data.dir** specifies DataNode data directories. This alarm is generated when a configured data directory cannot be created, a data directory uses the same disk as other critical directories in the system, or multiple directories use the same disk immediately.

This alarm is cleared when the DataNode data directory is configured properly and this DataNode for which the alarm is generated is restarted.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
14011	Major	Operation	Tenant plane	HDFS	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm is generated.
	HostName	Specifies the host for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

If the DataNode data directory is mounted to the root directory or a critical directory, the disk space of the root directory or critical directory will be used up after long time running and the system will be faulty.

If the DataNode data directory is not configured properly, HDFS performance will deteriorate.

Possible Causes

- The DataNode data directory fails to be created.
- The DataNode data directory uses the same disk with critical directories, such as **/** or **/boot**.
- Multiple directories in the DataNode data directory use the same disk.

Handling Procedure

Check the alarm cause and information about the DataNode for which the alarm is generated.

Step 1 On the FusionInsight Manager portal, choose **O&M > Alarm > Alarms**. In the alarm list, click the alarm.

Step 2 In **HostName** of **Location**, obtain the host name of the DataNode for which the alarm is generated.

Delete directories that do not comply with the disk plan from the DataNode data directory.

Step 3 Choose **Cluster** > *Name of the desired cluster* > **Services** > **HDFS** > **Instance**. In the instance list, click the DataNode instance on the node for which the alarm is generated.

Step 4 Click **Instance Configurations** and view the value of the DataNode parameter **dfs.datanode.data.dir**.

Step 5 Check whether all DataNode data directories are consistent with the disk plan.

- If yes, go to **Step 6**.
- If no, go to **Step 9**.

Step 6 Modify the DataNode parameter **dfs.datanode.data.dir** and delete the incorrect directories.

Step 7 Choose **Cluster** > *Name of the desired cluster* > **Services** > **HDFS** > **Instance** and restart the DataNode instance.

Step 8 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Step 9 Log in to the DataNode for which the alarm is generated as user **root**.

- If the alarm cause is "The DataNode data directory fails to be created", go to **Step 10**.
- If the alarm cause is "The DataNode data directory uses the same disk with critical directories, such **/** or **/boot**", go to **Step 17**.
- If the alarm cause is "Multiple directories in the DataNode data directory uses the same disk", go to **Step 21**.

Check whether the DataNode data directory fails to be created.

Step 10 Run the **su - omm** command to switch to user **omm**.

Step 11 Run the **ls** command to check whether the directories exist in the DataNode data directory.

- If yes, go to **Step 26**.
- If no, go to **Step 12**.

Step 12 Run the **mkdir** *data directory* command to create the directory and check whether the directory can be successfully created.

- If yes, go to **Step 24**.
- If no, go to **Step 13**.

Step 13 On the FusionInsight Manager portal, choose **O&M** > **Alarm** > **Alarms** to check whether alarm **ALM-12017 Insufficient Disk Capacity** exists.

- If yes, go to **Step 14**.
- If no, go to **Step 15**.

Step 14 Adjust the disk capacity and check whether alarm **ALM-12017 Insufficient Disk Capacity** is cleared. For details, see **ALM-12017 Insufficient Disk Capacity**.

- If yes, go to **Step 12**.
- If no, go to **Step 15**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 15 Check whether user **omm** has the **rwx** or **x** permission of all the upper-layer directories of the directory. (For example, for **/tmp/abc/**, user **omm** has the **x** permission for directory **tmp** and the **rwx** permission for directory **abc**.)

- If yes, go to **Step 24**.
- If no, go to **Step 16**.

Step 16 Run the **chmod u+rwx** *path* or **chmod u+x** *path* command as user **root** to assign the **rwx** or **x** permission of these directories to user **omm**. Then go to **Step 12**.

Check whether the DataNode data directory use the same disk as other critical directories in the system.

Step 17 Run the **df** command to obtain the disk mounting information of each directory in the DataNode data directory.

Step 18 Check whether the directories mounted to the disk are critical directories, such as **/** or **/boot**.

- If yes, go to **Step 19**.
- If no, go to **Step 24**.

Step 19 Change the value of the DataNode parameter **dfs.datanode.data.dir** and delete the directories that use the same disk as critical directories.

Step 20 Go to **Step 24**.

Check whether multiple directories in the DataNode data directory use the same disk.

Step 21 Run the **df** command to obtain the disk mounting information of each directory in the DataNode data directory. Record the mounted directory in the command output.

Step 22 Modify the DataNode node parameters **dfs.datanode.data.dir** to reserve only one directory among the directories that mounted to the same disk directory.

Step 23 Go to **Step 24**.

Restart the DataNode and check whether the alarm is cleared.

Step 24 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services** > **HDFS** > **Instance** and restart the DataNode instance

Step 25 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 26**.

Collect fault information.

Step 26 On the FusionInsight Manager portal, choose **O&M** > **Log** > **Download**.

Step 27 Select **HDFS** in the required cluster from the **Service**.

Step 28 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 29 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.117 ALM-14012 JournalNode Is Out of Synchronization

Alarm Description

On the active NameNode, the system checks the data consistency of all JournalNodes in the cluster every 5 minutes. This alarm is generated when the data on a JournalNode is inconsistent with the data on the other JournalNodes.

This alarm is cleared in 5 minutes after the data on JournalNodes is consistent.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
14012	Major	Quality of service	Tenant plane	HDFS	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm is generated.
	HostName	Specifies the host for which the alarm is generated.
	NameService Name	Specifies the NameService for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

When a JournalNode is working incorrectly, the data on the node becomes inconsistent with that on the other JournalNodes. If data on more than half of JournalNodes is inconsistent, the NameNode cannot work correctly, making the HDFS service unavailable.

Possible Causes

- The JournalNode instance does not exist (deleted or migrated).
- The JournalNode instance has not been started or has been stopped.
- The JournalNode instance is working incorrectly.
- The network of the JournalNode is unreachable.

Handling Procedure

Check whether the JournalNode instance has been started up.

Step 1 On the FusionInsight Manager portal, choose **O&M > Alarm > Alarms**. In the alarm list, click the alarm.

Step 2 Check **Location** and obtain the IP address of the JournalNode for which the alarm is generated.

Step 3 Choose **Cluster >** *Name of the desired cluster* **> Services** > **HDFS** > **Instance**. In the instance list, check whether the JournalNode instance exists on the node for which the alarm is generated.

- If yes, go to **Step 5**.
- If no, go to **Step 4**.

Step 4 Choose **O&M** > **Alarm** > **Alarms**. In the alarm list, click **Clear** in the **Operation** column of the alarm. In the dialog box that is displayed, click **OK**. No further action is needed.

Step 5 Click the JournalNode instance and check whether its **Configuration Status** is **Synchronized**.

- If yes, go to **Step 8**.
- If no, go to **Step 6**.

Step 6 Select the JournalNode instance and choose **Start Instance** to start the instance.

Step 7 After 5 minutes, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 15**.

Check whether the JournalNode instance is working correctly.

Step 8 Check whether **Running Status** of the JournalNode instance is **Normal**.

- If yes, go to **Step 11**.
- If no, go to **Step 9**.

Step 9 Select the JournalNode instance and choose **More** > **Restart Instance** to start the instance.

Step 10 After 5 minutes, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 15**.

Check whether the network of the JournalNode is reachable.

Step 11 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **HDFS** > **Instance** to check the service IP address of the active NameNode.

Step 12 Log in to the active NameNode as user **root**.

Step 13 Run the **ping** command to check whether a timeout occurs or the network is unreachable between the active NameNode and the JournalNode.

ping *service IP address of the JournalNode*

- If yes, go to **Step 14**.
- If no, go to **Step 15**.

Step 14 Contact the network administrator to rectify the network fault and check whether the alarm is cleared 5 minutes later.

- If yes, no further action is required.
- If no, go to **Step 15**.

Collect fault information.

Step 15 On the FusionInsight Manager portal, choose **O&M** > **Log > Download**.

Step 16 Select **HDFS** in the required cluster from the **Service**.

Step 17 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 18 Contact the technical support and send the collected logs.

----End

Alarm Clearing

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.118 ALM-14013 Failed to Update the NameNode FsImage File

Alarm Description

HDFS metadata is stored in the FsImage file of the NameNode data directory, which is specified by the **dfs.namenode.name.dir** configuration item. The standby NameNode periodically combines existing FsImage files and Editlog files stored in the JournalNode to generate a new FsImage file, and then pushes the new FsImage file to the data directory of the active NameNode. This period is specified by the **dfs.namenode.checkpoint.period** configuration item of HDFS. The default value is 3600s, namely, one hour. If the FsImage file in the data directory of the active NameNode is not updated, the HDFS metadata combination function is abnormal and requires rectification.

On the active NameNode, the system checks the FsImage file information every five minutes. This alarm is generated when no FsImage file is generated within three combination periods.

This alarm is cleared when a new FsImage file is generated and pushed to the active NameNode, which indicates that the HDFS metadata combination function can be properly used.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
14013	Major	Quality of service	Tenant plane	HDFS	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm is generated.
	HostName	Specifies the host for which the alarm is generated.
	NameServiceName	Specifies the NameService for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

If the FsImage file in the data directory of the active NameNode is not updated, the HDFS metadata combination function is abnormal and requires rectification. If it is not rectified, the Editlog files increase continuously after HDFS runs for a period. In this case, HDFS restart is time-consuming because a large number of Editlog files need to be loaded. In addition, this alarm also indicates that the standby NameNode is abnormal and the NameNode high availability (HA)

mechanism becomes invalid. When the active NameNode is faulty, the HDFS service becomes unavailable.

Possible Causes

- The standby NameNode is stopped.
- The standby NameNode instance is working incorrectly.
- The standby NameNode fails to generate a new FsImage file.
- Space of the data directory on the standby NameNode is insufficient.
- The standby NameNode fails to push the FsImage file to the active NameNode.
- Space of the data directory on the active NameNode is insufficient.

Handling Procedure

Check whether the standby NameNode is stopped.

Step 1 On the FusionInsight Manager portal, choose **O&M > Alarm > Alarms**. In the alarm list, click the alarm.

Step 2 View **Location** and obtain the host name of the active NameNode for which the alarm is generated and name of the NameService where the active NameNode resides.

Step 3 Choose **Cluster >** *Name of the desired cluster* **> Services** > **HDFS** > **Instance**, find the standby NameNode instance of the NameService in the instance list, and check whether its **Configuration Status** is **Synchronized**.

- If yes, go to **Step 6**.
- If no, go to **Step 4**.

Step 4 Select the standby NameNode instance, choose **Start Instance**, and wait until the startup is complete.

Step 5 Wait for a NameNode metadata combination period and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Check whether the NameNode instance is working correctly.

Step 6 Check whether **Running Status** of the standby NameNode instance is **Normal**.

- If yes, go to **Step 9**.
- If no, go to **Step 7**.

Step 7 Select the standby NameNode instance, choose **More** > **Restart Instance**, and wait until the startup is complete.

Step 8 Wait for a NameNode metadata combination period and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 30**.

Check whether the standby NameNode fails to generate a new FsImage file.

Step 9 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **HDFS** > **Configurations** > **All Configurations**, and search and obtain the value of **dfs.namenode.checkpoint.period**. This value is the period of NameNode metadata combination.

Step 10 Choose **Cluster >** *Name of the desired cluster* **> Services** > **HDFS** > **Instance** and obtain the service IP addresses of the active and standby NameNodes of the NameService for which the alarm is generated.

Step 11 Click the **NameNode(***xx***,Standy)** and **Instance Configurations** to obtain the value of **dfs.namenode.name.dir**. This value is the FsImage storage directory of the standby NameNode.

Step 12 Log in to the standby NameNode as user **root** or **omm**.

Step 13 Go to the FsImage storage directory and check the generation time of the newest FsImage file.

cd *Storage directory of the standby NameNode***/current**

stat -c %y $(ls -t | grep "fsimage_[0-9]*$" | head -1)

Step 14 Run the **date** command to obtain the current system time.

Step 15 Calculate the time difference between the generation time of the newest FsImage file and the current system time and check whether the time difference is greater than three times of the metadata combination period.

- If yes, go to **Step 16**.
- If no, go to **Step 20**.

Step 16 The metadata combination function of the standby NameNode is faulty. Run the following command to check whether the fault is caused by insufficient storage space.

Go to the FsImage storage directory and check the size of the newest FsImage file (in MB).

cd *Storage directory of the standby NameNode***/current**

du -m $(ls -t | grep "fsimage_[0-9]*$" | head -1) | awk '{print $1}'

Step 17 Run the following command to check the available disk space of the standby NameNode (in MB).

df -m ./ | awk 'END{print $4}'

Step 18 Compare the FsImage file size and the available disk space and determine whether another FsImage file can be stored on the disk.

- If yes, go to **Step 7**.
- If no, go to **Step 19**.

Step 19 Clear the redundant files on the disk where the directory resides to reserve sufficient space for metadata. After the clearance, wait for a NameNode metadata combination period and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 20**.

Check whether the standby NameNode fails to push the FsImage file to the active NameNode.

Step 20 Log in to the standby NameNode as user **root**.

Step 21 Run the **su - omm** command to switch to user **omm**.

Step 22 Run the following command to check whether the standby NameNode can push the file to the active NameNode.

tmpFile=/tmp/tmp_test_$(date +%s)

echo "test" > $tmpFile

scp $tmpFile *Service IP address of the active NameNode***:/tmp**

- If yes, go to **Step 24**.
- If no, go to **Step 23**.

Step 23 When the standby NameNode fails to push data to the active NameNode as user **omm**, contact the system administrator to handle the fault. Wait for a NameNode metadata combination period and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 24**.

Check whether space on the data directory of the active NameNode is insufficient.

Step 24 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **HDFS** > **Instance**, click the active NameNode of the NameService for which the alarm is generated, and then click **Instance Configurations** to obtain the value of **dfs.namenode.name.dir**. This value is the FsImage storage directory of the active NameNode.

Step 25 Log in to the active NameNode as user **root** or **omm**.

Step 26 Go to the FsImage storage directory and check the size of the newest FsImage file (in MB).

cd *Storage directory of the active NameNode***/current**

du -m $(ls -t | grep "fsimage_[0-9]*$" | head -1) | awk '{print $1}'

Step 27 Run the following command to check the available disk space of the active NameNode (in MB).

df -m ./ | awk 'END{print $4}'

Step 28 Compare the FsImage file size and the available disk space and determine whether another FsImage file can be stored on the disk.

- If yes, go to **Step 30**.
- If no, go to **Step 29**.

Step 29 Clear the redundant files on the disk where the directory resides to reserve sufficient space for metadata. After the clearance, wait for a NameNode metadata combination period and check whether the alarm is cleared.

- If yes, no further action is required.

- If no, go to **Step 30**.

Collect fault information.

Step 30 On the FusionInsight Manager portal, choose **O&M** > **Log** > **Download**.

Step 31 Select **NameNode** in the required cluster from the **Service**.

Step 32 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 33 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.119 ALM-14014 NameNode GC Time Exceeds the Threshold

Alarm Description

The system checks the garbage collection (GC) duration of the NameNode process every 60 seconds. This alarm is generated when the GC duration exceeds the threshold.

This alarm is cleared when the GC duration is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
14014	Critical (default threshold: 15000ms) Major (default threshold: 10000ms)	Quality of service	Tenant plane	HDFS	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm is generated.
	HostName	Specifies the host for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

A long GC duration of the NameNode process may interrupt the services and users cannot read or write files.

Possible Causes

The heap memory of the NameNode instance is overused or the heap memory is inappropriately allocated. As a result, GCs occur frequently.

Handling Procedure

Check the GC duration.

Step 1 On the FusionInsight Manager portal, choose **O&M** > **Alarm** > **Alarms**. On the displayed interface, click the drop-down button of **ALM-14014 NameNode GC Time Exceeds the Threshold.** Then check the role name in **Location** and confirm the IP adress of the instance.

Step 2 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **HDFS** > **Instance** > **NameNode (IP address for which the alarm is generated)**. Click the drop-down menu in the upper right corner of **Chart**, choose **Customize** > **Garbage Collection**, and select **NameNode Garbage Collection (GC)** to check the GC duration statistics of the NameNode process collected every minute.

Step 3 Check whether the GC duration of the NameNode process collected every minute exceeds the threshold.

- If yes, go to **Step 4**.
- If no, go to **Step 7**.

Step 4 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **HDFS** > **Configurations** > **All Configurations** > **NameNode** > **System** to increase the value of **GC_OPTS** parameter as required.

NOTE

The recommended mapping between the number of HDFS file objects (filesystem objects = files + blocks) and the JVM parameters configured for NameNode is as follows:

- If the number of file objects reaches 10,000,000, you are advised to set the JVM parameters as follows: -Xms6G -Xmx6G -XX:NewSize=512M -XX:MaxNewSize=512M
- If the number of file objects reaches 20,000,000, you are advised to set the JVM parameters as follows: -Xms12G -Xmx12G -XX:NewSize=1G -XX:MaxNewSize=1G
- If the number of file objects reaches 50,000,000, you are advised to set the JVM parameters as follows: -Xms32G -Xmx32G -XX:NewSize=3G -XX:MaxNewSize=3G
- If the number of file objects reaches 100,000,000, you are advised to set the JVM parameters as follows: -Xms64G -Xmx64G -XX:NewSize=6G -XX:MaxNewSize=6G
- If the number of file objects reaches 200,000,000, you are advised to set the JVM parameters as follows: -Xms96G -Xmx96G -XX:NewSize=9G -XX:MaxNewSize=9G
- If the number of file objects reaches 300,000,000, you are advised to set the JVM parameters as follows: -Xms164G -Xmx164G -XX:NewSize=12G -XX:MaxNewSize=12G

Step 5 Save the configuration and restart the NameNode instance.

Step 6 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect fault information.

Step 7 On the FusionInsight Manager portal, choose **O&M** > **Log** > **Download**.

Step 8 Select **NameNode** in the required cluster from the **Service**.

Step 9 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.120 ALM-14015 DataNode GC Time Exceeds the Threshold

Alarm Description

The system checks the garbage collection (GC) duration of the DataNode process every 60 seconds. This alarm is generated when the GC duration exceeds the threshold.

This alarm is cleared when the GC duration is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
14015	Critical (default threshold: 20000ms) Major (default threshold: 12000ms)	Quality of service	Tenant plane	HDFS	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.

Type	Parameter	Description
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm is generated.
	HostName	Specifies the host for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

A long GC duration of the DataNode process may interrupt the services and users cannot read or write files.

Possible Causes

The heap memory of the DataNode instance is overused or the heap memory is inappropriately allocated. As a result, GCs occur frequently.

Handling Procedure

Check the GC duration.

Step 1 On the FusionInsight Manager portal, choose **O&M** > **Alarm** > **Alarms**. On the displayed interface, click the drop-down button of **ALM-14015 DataNode GC Time Exceeds the Threshold**. Then check the role name in **Location** and confirm the IP adress of the instance.

Step 2 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **HDFS** > **Instance** > **DataNode (IP address for which the alarm is generated)**. Click the drop-down menu in the upper right corner of **Chart**, choose **Customize** > **Garbage Collection**, and select **DataNode Garbage Collection (GC)** to check the GC duration statistics of the DataNode process collected every minute.

Step 3 Check whether the GC duration of the DataNode process collected every minute exceeds the threshold.

- If yes, go to **Step 4**.
- If no, go to **Step 7**.

Step 4 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **HDFS** > **Configurations** > **All Configurations** > **DataNode** > **System** to increase the value of **GC_OPTS** parameter as required.

NOTE

The mapping between the average number of blocks of a DataNode instance and the DataNode memory is as follows:

- If the average number of blocks of a DataNode instance reaches 2,000,000, the reference values of the JVM parameters of the DataNode are as follows: -Xms6G -Xmx6G -XX:NewSize=512M -XX:MaxNewSize=512M
- If the average number of blocks of a DataNode instance reaches 5,000,000, the reference values of the JVM parameters of the DataNode are as follows: -Xms12G -Xmx12G -XX:NewSize=1G -XX:MaxNewSize=1G

Step 5 Save the configuration and restart the DataNode instance.

Step 6 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect fault information.

Step 7 On the FusionInsight Manager portal, choose **O&M** > **Log > Download**.

Step 8 Select **DataNode** in the required cluster from the **Service**.

Step 9 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.121 ALM-14016 DataNode Direct Memory Usage Exceeds the Threshold

Alarm Description

The system checks the direct memory usage of HDFS every 30 seconds. This alarm is generated when the direct memory usage of DataNode instances exceeds the threshold (90% of the maximum memory).

This alarm is automatically cleared when the direct memory usage is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
14016	Critical (default threshold: 95%) Major (default threshold: 90%)	Quality of service	Tenant plane	HDFS	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

If the available direct memory of DataNode instances is insufficient, a memory overflow may occur and the service breaks down.

Possible Causes

The direct memory of DataNode instances is overused or the direct memory is inappropriately allocated.

Handling Procedure

Check the direct memory usage.

Step 1 On the **Home** page of FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. On the page that is displayed, click the drop-down list in the row containing **ALM-14016 DataNode Direct Memory Usage Exceeds the Threshold**, and view the role name and IP address of the instance for which the alarm is generated in the **Location** area.

Step 2 On the **Home** page of FusionInsight Manager, choose **Cluster** > **Services** > **HDFS**. On the page that is displayed, click the **Instance** tab. In the instance list, select **DataNode** (IP address of the instance for which this alarm is generated). Click the drop-down list in the upper right corner of the chart, choose **Customize** > **Resource**, and select **DataNode Memory** to check the direct memory usage.

Step 3 Check whether the used direct memory of a DataNode instance reaches 90% (default threshold) of the maximum direct memory allocated to it.

- If yes, go to **Step 4**.
- If no, go to **Step 8**.

Step 4 On the **Home** page of FusionInsight Manager, choose **Cluster** > **Services** > **HDFS**. On the page that is displayed, click the **Configuration** tab then the **All Configurations** sub-tab, and select **DataNode** > **System**. Check whether **-XX:MaxDirectMemorySize** exists in the **GC_OPTS** parameter.

- If yes, go to **Step 5**.
- If no, go to **Step 6**.

Step 5 Adjust the value of **-XX:MaxDirectMemorySize**.

1. In **GC_OPTS**, check the value of **-Xmx** and check whether the node memory is sufficient.

   NOTE

   You can determine whether the node memory is sufficient based on the actual environment. For example, you can use the following method:

   Use the IP address to log in to the instance for which the alarm is generated as user **root** and run the **free -g** command to check the value of **Mem** in the **free** column. The value indicates the available memory of the node. In the following example, the available memory of the node is 4 GB.

   ```
   total used free shared buff/cache available
   Mem: 112 48 4 10 58 46
   ......
   ```

   If the value of **Mem** is at least that of **-Xmx**, the node memory is sufficient. If the value of **Mem** is less than that of **-Xmx**, the node memory is insufficient.

   – If yes, change the value of **-XX:MaxDirectMemorySize** to that of **-Xmx**.
   – If no, increase **-XX:MaxDirectMemorySize** to a value no larger than that of **Mem**.

2. Save the configuration and restart the DataNode instances.

Step 6 Check whether **ALM-14008 DataNode Heap Memory Usage Exceeds the Threshold** exists.

- If yes, rectify the fault by referring to **ALM-14008 DataNode Heap Memory Usage Exceeds the Threshold**.
- If no, go to **Step 7**.

Step 7 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Collect the fault information.

Step 8 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 9 Expand the **Service** drop-down list, and select **DataNode** for the target cluster.

Step 10 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 11 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.122 ALM-14017 NameNode Direct Memory Usage Exceeds the Threshold

Alarm Description

The system checks the direct memory usage of the HDFS service every 30 seconds. This alarm is generated when the direct memory usage of a NameNode instance exceeds the threshold (90% of the maximum memory).

The alarm is cleared when the direct memory usage is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
14017	Critical (default threshold: 95%) Major (default threshold: 90%)	Quality of service	Tenant plane	HDFS	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.

Type	Parameter	Description
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm is generated.
	HostName	Specifies the host for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

If the available direct memory of the HDFS service is insufficient, a memory overflow occurs and the service breaks down.

Possible Causes

The direct memory of the NameNode instance is overused or the direct memory is inappropriately allocated.

Handling Procedure

Check the direct memory usage.

Step 1 On the FusionInsight Manager portal, choose **O&M > Alarm > Alarms.** On the displayed interface, click the drop-down button of **ALM-14017 NameNode Direct Memory Usage Exceeds the Threshold**. Then check the role name in **Location** and confirm the IP adress of the instance.

Step 2 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **HDFS** > **Instance** > **NameNode (IP address for which the alarm is generated)**. Click the drop-down menu in the upper right corner of **Chart**, choose **Customize** > **Resource**, and select **NameNode Memory** to check the direct memory usage.

Step 3 Check whether the used direct memory of NameNode reaches 90% of the maximum direct memory specified for NameNode by default.

- If yes, go to **Step 4**.
- If no, go to **Step 8**.

Step 4 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **HDFS** > **Configurations** > **All Configurations** > **NameNode** > **System** to check whether "-XX:MaxDirectMemorySize" exists in the **GC_OPTS** parameter.

- If yes, go to **Step 5**.
- If no, go to **Step 6**.

Step 5 In the **GC_OPTS** parameter, delete "-XX:MaxDirectMemorySize". Save the configuration and restart the NameNode instance.

Step 6 Check whether the **ALM-14007 NameNode Heap Memory Usage Exceeds the Threshold** exists.

- If yes, handle the alarm by referring to **ALM-14007 NameNode Heap Memory Usage Exceeds the Threshold**.
- If no, go to **Step 7**.

Step 7 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Collect fault information.

Step 8 On the FusionInsight Manager portal, choose **O&M** > **Log > Download**.

Step 9 Select **NameNode** in the required cluster from the **Service**.

Step 10 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 11 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.None.

1.3.123 ALM-14018 NameNode Non-heap Memory Usage Exceeds the Threshold

Alarm Description

The system checks the non-heap memory usage of the HDFS NameNode every 30 seconds and compares the actual usage with the threshold. The non-heap memory usage of the HDFS NameNode has a default threshold. This alarm is generated when the non-heap memory usage of the HDFS NameNode exceeds the threshold.

Users can choose **O&M > Alarm > Thresholds >** *Name of the desired cluster* > **HDFS** to change the threshold.

This alarm is cleared when the no-heap memory usage of the HDFS NameNode is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
14018	Critical (default threshold: 95%) Major (default threshold: 90%)	Quality of service	Tenant plane	HDFS	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.

Type	Parameter	Description
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm is generated.
	HostName	Specifies the host for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

If the memory usage of the HDFS NameNode is too high, data read/write performance of HDFS will be affected.

Possible Causes

Non-heap memory of the HDFS NameNode is insufficient.

Handling Procedure

Delete unnecessary files.

Step 1 Log in to the HDFS client as user **root**. Run the **cd** command to go to the client installation directory, and run the **source bigdata_env** command.

If the cluster adopts the security mode, perform security authentication.

Run the **kinit hdfs** command and enter the password as prompted. Obtain the password from the administrator.

Step 2 Run the **hdfs dfs -rm -r** *file or directory path* command to delete unnecessary files.

Step 3 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 4**.

Check the NameNode JVM non-heap memory usage and configuration.

Step 4 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services** > **HDFS**. The HDFS status page is displayed.

Step 5 In the **Basic Information** area, click **NameNode(Active)**. The HDFS WebUI is displayed.

NOTE

By default, the **admin** user does not have the permissions to manage other components. If the page cannot be opened or the displayed content is incomplete when you access the native UI of a component due to insufficient permissions, you can manually create a user with the permissions to manage that component.

Step 6 On the HDFS WebUI, click the **Overview** tab. In **Summary**, check the numbers of files, directories, and blocks in HDFS.

Step 7 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services** > **HDFS** > **Configurations** > **All Configurations**. In **Search**, enter **GC_OPTS** to check the **GC_OPTS** non-heap memory parameter of **HDFS->NameNode**.

Adjust system configurations.

Step 8 Check whether the non-heap memory is properly configured based on the number of file objects in **Step 6** and the non-heap parameters configured for NameNode in **Step 7**.

- If yes, go to **Step 9**.
- If no, go to **Step 12**.

NOTE

The recommended mapping between the number of HDFS file objects (filesystem objects = files + blocks) and the JVM parameters configured for NameNode is as follows:

- If the number of file objects reaches 10,000,000, you are advised to set the JVM parameters as follows: -Xms6G -Xmx6G -XX:NewSize=512M -XX:MaxNewSize=512M
- If the number of file objects reaches 20,000,000, you are advised to set the JVM parameters as follows: -Xms12G -Xmx12G -XX:NewSize=1G -XX:MaxNewSize=1G
- If the number of file objects reaches 50,000,000, you are advised to set the JVM parameters as follows: -Xms32G -Xmx32G -XX:NewSize=3G -XX:MaxNewSize=3G
- If the number of file objects reaches 100,000,000, you are advised to set the JVM parameters as follows: -Xms64G -Xmx64G -XX:NewSize=6G -XX:MaxNewSize=6G
- If the number of file objects reaches 200,000,000, you are advised to set the JVM parameters as follows: -Xms96G -Xmx96G -XX:NewSize=9G -XX:MaxNewSize=9G
- If the number of file objects reaches 300,000,000, you are advised to set the JVM parameters as follows: -Xms164G -Xmx164G -XX:NewSize=12G -XX:MaxNewSize=12G

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 9 Modify the **GC_OPTS** parameter of the NameNode based on the mapping between the number of file objects and non-heap memory.

Step 10 Save the configuration and click **Dashboard** > **More** > **Restart Service**.

Step 11 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 12**.

Collect fault information.

Step 12 On the FusionInsight Manager portal, choose **O&M** > **Log > Download**.

Step 13 Select the following services in the required cluster from the **Service**.

- ZooKeeper
- HDFS

Step 14 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 15 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.124 ALM-14019 DataNode Non-heap Memory Usage Exceeds the Threshold

Alarm Description

The system checks the non-heap memory usage of the HDFS DataNode every 30 seconds and compares the actual usage with the threshold. The non-heap memory usage of the HDFS DataNode has a default threshold. This alarm is generated when the non-heap memory usage of the HDFS DataNode exceeds the threshold.

Users can choose **O&M > Alarm > Thresholds>** *Name of the desired cluster* **> HDFS** to change the threshold.

This alarm is cleared when the no-heap memory usage of the HDFS DataNode is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
14019	Critical (default threshold: 95%) Major (default threshold: 90%)	Quality of service	Tenant plane	HDFS	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm is generated.
	HostName	Specifies the host for which the alarm is generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

If the memory usage of the HDFS DataNode is too high, data read/write performance of HDFS will be affected.

Possible Causes

Non-heap memory of the HDFS DataNode is insufficient.

Handling Procedure

Delete unnecessary files.

Step 1 Log in to the HDFS client as user **root**. Run the **cd** command to go to the client installation directory, and run the **source bigdata_env** command.

If the cluster adopts the security mode, perform security authentication.

Run the **kinit hdfs** command and enter the password as prompted. Obtain the password from the administrator.

Step 2 Run the **hdfs dfs -rm -r** *file or directory path* command to delete unnecessary files.

Step 3 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 4**.

Check the DataNode JVM non-heap memory usage and configuration.

Step 4 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services** > **HDFS**.

Step 5 In the **Basic Information** area, click **NameNode(Active)**. The HDFS WebUI is displayed.

NOTE

By default, the **admin** user does not have the permissions to manage other components. If the page cannot be opened or the displayed content is incomplete when you access the native UI of a component due to insufficient permissions, you can manually create a user with the permissions to manage that component.

Step 6 On the HDFS WebUI, click the **Datanodes** tab to view the number of blocks of all DataNodes that report alarms.

Step 7 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **HDFS** > **Configurations** > **All Configurations**. In **Search**, enter **GC_OPTS** to check the **GC_OPTS** non-heap memory parameter of **HDFS->DataNode**.

Adjust system configurations.

Step 8 Check whether the memory is properly configured based on the number of blocks in **Step 6** and the memory parameters configured for DataNode in **Step 7**.

- If yes, go to **Step 9**.
- If no, go to **Step 12**.

NOTE

The mapping between the average number of blocks of a DataNode instance and the DataNode memory is as follows:

- If the average number of blocks of a DataNode instance reaches 2,000,000, the reference values of the JVM parameters of the DataNode are as follows: -Xms6G -Xmx6G -XX:NewSize=512M -XX:MaxNewSize=512M
- If the average number of blocks of a DataNode instance reaches 5,000,000, the reference values of the JVM parameters of the DataNode are as follows: -Xms12G -Xmx12G -XX:NewSize=1G -XX:MaxNewSize=1G

Step 9 Modify the **GC_OPTS** parameter of the DataNode based on the mapping between the number of blocks and memory.

Step 10 Save the configuration and click **Dashboard** > **More** > **Restart Service**.

Step 11 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 12**.

Collect fault information.

Step 12 On the FusionInsight Manager portal, choose **O&M** > **Log > Download**.

Step 13 Select the following services in the required cluster from the **Service**.

- ZooKeeper
- HDFS

Step 14 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 15 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.125 ALM-14020 Number of Entries in the HDFS Directory Exceeds the Threshold

Alarm Description

The system obtains the number of subfiles and subdirectories in a specified directory every hour and checks whether it reaches the percentage of the threshold (the maximum number of subfiles and subdirectories in an HDFS directory, the threshold for triggering an alarm is **90%** by default). If it exceeds the percentage of the threshold, an alarm is triggered.

When the number of subfiles and subdirectories in the directory the alarm is lower than the percentage of the threshold, the alarm is automatically cleared. When the monitoring switch is disabled, alarms corresponding to all directories are cleared. If a directory is removed from the monitoring list, alarms corresponding to the directory are cleared.

NOTE

- The **dfs.namenode.fs-limits.max-directory-items** parameter specifies the maximum number of subfiles and subdirectories in the HDFS directory. Its default value is **1048576**. If the number of subfiles and subdirectories in a directory exceeds the parameter value, subfiles and subdirectories cannot be created in the directory.
- The **dfs.namenode.directory-items.monitor** parameter specifies the list of directories to be monitored. Its default value is **/tmp,/mr-history**.
- The **dfs.namenode.directory-items.monitor.enabled** parameter is used to enable or disable the monitoring switch. Its default value is **true**, which means the monitoring switch is enabled by default.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
14020	Critical (default threshold: 95%) Major (default threshold: 90%)	Quality of service	Tenant plane	HDFS	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm is generated.
	NameServiceName	Specifies the NameService service for which the alarm is generated.
	Directory	Specifies the directory for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

If the number of entries in the monitored directory exceeds 90% of the threshold, an alarm is triggered, but entries can be added to the directory. Once the maximum threshold is exceeded, entries will fail to be added to the directory.

Possible Causes

The number of entries in the monitored directory exceeds 90% of the threshold.

Handling Procedure

Check whether unnecessary files exist in the system.

Step 1 Log in to the HDFS client as user **root**. Run the **cd** command to go to the client installation directory, and run the **source bigdata_env** command to set the environment variables.

If the cluster is in security mode, security authentication is required.

Run the **kinit hdfs** command and enter the password as prompted. Obtain the password from the administrator.

Step 2 Run the following command to check whether files and directories in the directory with the alarm can be deleted:

hdfs dfs -ls *Directory with the alarm*

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 Run the following command to delete unnecessary files.

hdfs dfs -rm -r -f *File or directory path*

NOTE

Deleting a file or folder is a high-risk operation. Ensure that the file or folder is no longer required before performing this operation.

Step 4 Wait 1 hour and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check whether the threshold is correctly configured.

Step 5 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **HDFS** > **Configurations** > **All Configurations**. Search for the **dfs.namenode.fs-limits.max-directory-items** parameter and check whether the parameter value is appropriate.

- If yes, go to **Step 9**.
- If no, go to **Step 6**.

Step 6 Increase the parameter value.

Step 7 Save the configuration and click **Dashboard** > **More** > **Restart Service**.

Step 8 Wait 1 hour and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Collect fault information.

Step 9 On the FusionInsight Manager portal, choose **O&M** > **Log > Download**.

Step 10 Select **HDFS** in the required cluster from the **Service**.

Step 11 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.126 ALM-14021 NameNode Average RPC Processing Time Exceeds the Threshold

Alarm Description

The system checks the average RPC processing time of NameNode every 30 seconds, and compares the actual average RPC processing time with the threshold. This alarm is generated when the system detects that the average RPC processing time exceeds the threshold for several consecutive times (10 times by default).

You can choose **O&M > Alarm > Thresholds >** *Name of the desired cluster* > **HDFS** to change the threshold.

When the **Trigger Count** is 1, this alarm is cleared when the average RPC processing time of NameNode is less than or equal to the threshold. When the **Trigger Count** is greater than 1, this alarm is cleared when the average RPC processing time of NameNode is less than or equal to 90% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
14021	Critical (default threshold: 200ms) Major (default threshold: 100ms)	Quality of service	Tenant plane	HDFS	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm is generated.
	HostName	Specifies the host for which the alarm is generated.
	NameServiceName	Specifies the NameService service for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

NameNode cannot process the RPC requests from HDFS clients, upper-layer services that depend on HDFS, and DataNode in a timely manner. Specifically, the services that access HDFS run slowly or the HDFS service is unavailable.

Possible Causes

- The CPU performance of NameNode nodes is insufficient and therefore NameNode nodes cannot process messages in a timely manner.
- The configured NameNode memory is too small and frame freezing occurs on the JVM due to frequent full garbage collection.
- NameNode parameters are not configured properly, so NameNode cannot make full use of system performance.

Handling Procedure

Obtain alarm information.

Step 1 On the FusionInsight Manager portal, choose **O&M > Alarm > Alarms**. In the alarm list, click the alarm.

Step 2 Check the alarm. Obtain the host name of the NameNode node involved in this alarm from the **HostName** information of **Location**. Then obtain the name of the NameService node involved in this alarm from the **NameServiceName** information of **Location**.

Check whether the threshold is too small.

Step 3 Check the status of the services that depend on HDFS. Check whether the services run slowly or task execution times out.

- If yes, go to **Step 8**.
- If no, go to **Step 4**.

Step 4 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **HDFS**. Click the drop-down menu in the upper right corner of **Chart**, choose **Customize** > **RPC**, and select **Average Time of Active NameNode RPC Processing** and click **OK**.

Step 5 On the **Average Time of Active NameNode RPC Processing** monitoring page, obtain the value of the NameService node involved in this alarm.

Step 6 On the FusionInsight Manager portal, choose **O&M > Alarm > Thresholds >** *Name of the desired cluster* **> HDFS**. Locate **Average Time of Active NameNode RPC Processing** and click the **Modify** in the **Operation** column of the default rule. The **Modify Rule** page is displayed. Change **Threshold** to 150% of the peak value within one day before and after the alarm is generated. Click **OK** to save the new threshold.

Step 7 Wait for 5 minutes and then check whether the alarm is automatically cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Check whether the CPU performance of the NameNode node is sufficient.

Step 8 On the FusionInsight Manager portal, click **O&M > Alarm >Alarms** and check whether **ALM-12016 CPU Usage Exceeds the Threshold** is generated for the NameNode node.

- If yes, go to **Step 9**.
- If no, go to **Step 11**.

Step 9 Handle **ALM-12016 CPU Usage Exceeds the Threshold** by taking recommended actions.

Step 10 Wait for 10 minutes and check whether alarm 14021 is automatically cleared.

- If yes, no further action is required.
- If no, go to **Step 11**.

Check whether the memory of the NameNode node is too small.

Step 11 On the FusionInsight Manager portal, click **O&M > Alarm >Alarms** and check whether **ALM-14007 HDFS NameNode Heap Memory Usage Exceeds the Threshold** is generated for the NameNode node.

- If yes, go to **Step 12**.
- If no, go to **Step 14**.

Step 12 Handle **ALM-14007 HDFS NameNode Heap Memory Usage Exceeds the Threshold** by taking recommended actions.

Step 13 Wait for 10 minutes and check whether alarm 14021 is automatically cleared.

- If yes, no further action is required.
- If no, go to **Step 14**.

Check whether NameNode parameters are configured properly.

Step 14 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **HDFS** > **Configurations** > **All Configurations**. Search for parameter **dfs.namenode.handler.count** and view its value. If the value is less than or equal to 128, change it to **128**. If the value is greater than 128 but less than 192, change it to **192**.

Step 15 Search for parameter **ipc.server.read.threadpool.size** and view its value. If the value is less than 5, change it to **5**.

Step 16 Click **Save** and click **OK**.

Step 17 On the **Instance** page of HDFS, select the standby NameNode of NameService involved in this alarm and choose **More** > **Restart Instance**. Enter the password and click **OK**. Wait until the standby NameNode is started up.

Step 18 On the **Instance** page of HDFS, select the active NameNode of NameService involved in this alarm and choose **More** > **Restart Instance**. Enter the password and click **OK**. Wait until the active NameNode is started up.

Step 19 Wait for 1 hour and then check whether the alarm is automatically cleared.

- If yes, no further action is required.
- If no, go to **Step 20**.

Collect fault information.

Step 20 On the FusionInsight Manager portal, choose **O&M** > **Log > Download**.

Step 21 Select the following node in the required cluster from the **Service**.

- HDFS

Step 22 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 23 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.127 ALM-14022 NameNode Average RPC Queuing Time Exceeds the Threshold

Alarm Description

The system checks the average RPC queuing time of NameNode every 30 seconds, and compares the actual average RPC queuing time with the threshold. This alarm is generated when the system detects that the average RPC queuing time exceeds the threshold for several consecutive times (10 times by default).

You can choose **O&M > Alarm > Thresholds >** *Name of the desired cluster* > **HDFS** to change the threshold.

When the **Trigger Count** is 1, this alarm is cleared when the average RPC queuing time of NameNode is less than or equal to the threshold. When the **Trigger Count** is greater than 1, this alarm is cleared when the average RPC queuing time of NameNode is less than or equal to 90% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
14022	Critical (default threshold: 300ms) Major (default threshold: 200ms)	Quality of service	Tenant plane	HDFS	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm is generated.
	HostName	Specifies the host for which the alarm is generated.
	NameServiceName	Specifies the NameService service for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

NameNode cannot process the RPC requests from HDFS clients, upper-layer services that depend on HDFS, and DataNode in a timely manner. Specifically, the services that access HDFS run slowly or the HDFS service is unavailable.

Possible Causes

- The CPU performance of NameNode nodes is insufficient and therefore NameNode nodes cannot process messages in a timely manner.
- The configured NameNode memory is too small and frame freezing occurs on the JVM due to frequent full garbage collection.
- NameNode parameters are not configured properly, so NameNode cannot make full use of system performance.
- The volume of services that access HDFS is too large and therefore NameNode is overloaded.

Handling Procedure

Obtain alarm information.

Step 1 On the FusionInsight Manager portal, choose **O&M > Alarm > Alarms**. In the alarm list, click the alarm.

Step 2 Check the alarm. Obtain the alarm generation time from **Generated**. Obtain the host name of the NameNode node involved in this alarm from the **HostName** information of **Location**. Then obtain the name of the NameService node involved in this alarm from the **NameServiceName** information of **Location**.

Check whether the threshold is too small.

Step 3 Check the status of the services that depend on HDFS. Check whether the services run slowly or task execution times out.

- If yes, go to **Step 8**.
- If no, go to **Step 4**.

Step 4 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **HDFS**. Click the drop-down menu in the upper right corner of **Chart**, choose **Customize** > **RPC**, and select **Average Time of Active NameNode RPC Queuing** and click **OK**.

Step 5 On the **Average Time of Active NameNode RPC Queuing** monitoring page, obtain the value of the NameService node involved in this alarm.

Step 6 On the FusionInsight Manager portal, choose **O&M > Alarm > Thresholds >** *Name of the desired cluster* **> HDFS**. Locate **Average Time of Active NameNode RPC Queuing** and click the **Modify** in the **Operation** column of the default rule. The **Modify Rule** page is displayed. Change **Threshold** to 150% of the monitored value. Click **OK** to save the new threshold.

Step 7 Wait for 1 minute and then check whether the alarm is automatically cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Check whether the CPU performance of the NameNode node is sufficient.

Step 8 On the FusionInsight Manager portal, click **O&M > Alarm > Alarms** and check whether **ALM-12016 HDFS NameNode Memory Usage Exceeds the Threshold** is generated.

- If yes, go to **Step 9**.

- If no, go to **Step 11**.

Step 9 Handle **ALM-12016 CPU Usage Exceeds the Threshold** by taking recommended actions.

Step 10 Wait for 10 minutes and check whether alarm 14022 is automatically cleared.

- If yes, no further action is required.
- If no, go to **Step 11**.

Check whether the memory of the NameNode node is too small.

Step 11 On the FusionInsight Manager portal, click **O&M > Alarm > Alarms** and check whether **ALM-14007 HDFS NameNode Memory Usage Exceeds the Threshold** is generated.

- If yes, go to **Step 12**.
- If no, go to **Step 14**.

Step 12 Handle **ALM-14007 CPU Usage Exceeds the Threshold** by taking recommended actions.

Step 13 Wait for 10 minutes and check whether alarm 14022 is automatically cleared.

- If yes, no further action is required.
- If no, go to **Step 14**.

Check whether NameNode parameters are configured properly.

Step 14 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **HDFS** > **Configurations** > **All Configurations**. Search for parameter **dfs.namenode.handler.count** and view its value. If the value is less than or equal to 128, change it to **128**. If the value is greater than 128 but less than 192, change it to **192**.

Step 15 Search for parameter **ipc.server.read.threadpool.size** and view its value. If the value is less than 5, change it to **5**.

Step 16 Click **Save**, and click **OK**.

Step 17 On the **Instance** page of HDFS, select the standby NameNode of NameService involved in this alarm and choose **More** > **Restart Instance**. Enter the password and click **OK**. Wait until the standby NameNode is started up.

Step 18 On the **Instance** page of HDFS, select the active NameNode of NameService involved in this alarm and choose **More** > **Restart Instance**. Enter the password and click **OK**. Wait until the active NameNode is started up.

Step 19 Wait for 1 hour and then check whether the alarm is automatically cleared.

- If yes, no further action is required.
- If no, go to **Step 20**.

Check whether the HDFS workload changes and reduce the workload properly.

Step 20 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **HDFS**. Click the drop-down menu in the upper right corner of **Chart**, click **Customize**, select **Average Time of Active NameNode RPC Queuing** and click **OK**.

Step 21 Click . The **Details** page is displayed.

Step 22 Set the monitoring data display period, from 5 days before the alarm generation time to the alarm generation time. Click **OK**.

Step 23 On the **Average RPC Queuing Time** monitoring page, check whether the point in time when the queuing time increases abruptly exists.

- If yes, go to **Step 24**.
- If no, go to **Step 27**.

Step 24 Confirm and check the point in time. Check whether a new task frequently accesses HDFS and whether the access frequency can be reduced.

Step 25 If a Balancer task starts at the point in time, stop the task or specify a node for the task to reduce the HDFS workload.

Step 26 Wait for 1 hour and then check whether the alarm is automatically cleared.

- If yes, no further action is required.
- If no, go to **Step 27**.

Collect fault information.

Step 27 On the FusionInsight Manager portal, choose **O&M** > **Log** > **Download**.

Step 28 Select **HDFS** in the required cluster from the **Service**.

Step 29 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 30 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.128 ALM-14023 Percentage of Total Reserved Disk Space for Replicas Exceeds the Threshold

Alarm Description

The system checks the percentage of total reserved disk space for replicas (Total reserved disk space for replicas/(Total reserved disk space for replicas + Total remaining disk space)) every 30 seconds and compares the actual percentage with the threshold (**90%** by default). This alarm is generated when the percentage of total reserved disk space for replicas exceeds the threshold for multiple consecutive times (**Trigger Count**).

The alarm is cleared in the following two scenarios: The value of **Trigger Count** is **1** and the percentage of total reserved disk space for replicas is less than or equal to the threshold; the value of **Trigger Count** is greater than **1** and the percentage of total reserved disk space for replicas is less than or equal to 90% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
14023	Major (default threshold: 95%) Minor (default threshold: 90%)	Quality of service	Tenant plane	HDFS	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	RoleName	Specifies the role for which the alarm is generated.
	HostName	Specifies the host for which the alarm is generated.
	NameService Name	Specifies the NameService service for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

The performance of writing data to HDFS is affected. If all remaining DataNode space is reserved for replicas, writing HDFS data fails.

Possible Causes

- The alarm threshold is improperly configured.
- The disk space configured for the HDFS cluster is insufficient.
- The volume of services that access HDFS is too large and therefore DataNode is overloaded.

Handling Procedure

Check whether the alarm threshold is appropriate.

Step 1 On the FusionInsight Manager portal, choose **O&M > Alarm > Thresholds >** *Name of the desired cluster* > **HDFS** > **Disk** > **Percentage of Reserved Space for Replicas of Unused Space** to check whether the alarm threshold is appropriate. (The default threshold is **90%**. Users can change it as required.)

- If yes, go to **Step 4**.
- If no, go to **Step 2**.

Step 2 Choose **O&M > Alarm > Thresholds >** *Name of the desired cluster* > **HDFS** > **Disk** > **Percentage of Reserved Space for Replicas of Unused Space** and Click **Modify,** change the threshold based on the actual usage.

Step 3 Wait 5 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 4**.

Check whether an alarm indicating insufficient disk space is generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 4 On the FusionInsight Manager portal, check whether **ALM-14001 HDFS Disk Usage Exceeds the Threshold** or **ALM-14002 DataNode Disk Usage Exceeds the Threshold** exists on the **O&M > Alarm > Alarms** page.

- If yes, go to **Step 5**.
- If no, go to **Step 7**.

Step 5 Handle the alarm by referring to instructions in **ALM-14001 HDFS Disk Usage Exceeds the Threshold** or **ALM-14002 DataNode Disk Usage Exceeds the Threshold** and check whether the alarm is cleared.

- If yes, go to **Step 6**.
- If no, go to **Step 7**.

Step 6 Wait 5 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Expand the DataNode capacity.

Step 7 Expand the DataNode capacity. For details, see the *MapReduce Service (MRS) 3.3.1-LTS Physical Machine Cluster Component Migration Guide (for Huawei Cloud Stack 8.3.1)*.

Step 8 Wait 5 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Collect fault information.

Step 9 On the FusionInsight Manager portal, choose **O&M** > **Log > Download**.

Step 10 Select **HDFS** in the required cluster from the **Service**.

Step 11 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 20 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.129 ALM-14024 Tenant Space Usage Exceeds the Threshold

Alarm Description

The system checks the space usage (used space of each directory/space allocated to each directory) of each directory associated with a tenant every hour and compares the space usage of each directory with the threshold set for the directory. This alarm is generated when the space usage exceeds the threshold.

This alarm is cleared when the space usage is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
14024	Major (default threshold: 95%) Minor (default threshold: 90%)	Quality of service	Tenant plane	HDFS	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm is generated.
	HostName	Specifies the host for which the alarm is generated.
	TenantName	Specifies the tenant for which the alarm is generated.
	DirectoryNam e	Specifies the directory for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

This alarm is generated if the space usage of the tenant directory exceeds the custom threshold. File writing to the directory is not affected. If the used space exceeds the maximum storage space allocated to the directory, the HDFS fails to write data to the directory.

Possible Causes

- The alarm threshold is improperly configured.
- The space allocated to the tenant is improper.

Handling Procedure

Check whether the alarm threshold is appropriate.

Step 1 View the alarm location information to obtain the tenant name and tenant directory for which the alarm is generated.

Step 2 On the FusionInsight Manager portal, choose the **Tenant Resources** page, select the tenant for which the alarm is generated, and click **Resources**. Check whether the storage space threshold configured for the tenant directory for which the

alarm is generated is proper. (The default value 90% is a proper value. You can set it based on the site requirements.)

- If yes, go to **Step 5**.
- If no, go to **Step 3**.

Step 3 On the **Resources** page, click **Modify** to modify or delete the storage space threshold.

Step 4 About one minute later, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check whether the space allocated to the tenant is appropriate.

Step 5 On the FusionInsight Manager portal, choose the **Tenant Resources** page, select the tenant for which the alarm is generated, and click **Resources**. Check whether the storage space quota of the tenant directory for which the alarm is generated is proper based on the actual service status of the tenant directory.

- If yes, go to **Step 8**.
- If no, go to **Step 6**.

Step 6 On the **Resources** page, click **Modify** to modify the storage space quota.

Step 7 About one minute later, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Collect fault information.

Step 8 On the FusionInsight Manager portal, choose **O&M** > **Log** > **Download**.

Step 9 Select **HDFS** in the required cluster and **NodeAgent** under **Manager** from the **Service**.

Step 10 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 20 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 11 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.130 ALM-14025 Tenant File Object Usage Exceeds the Threshold

Alarm Description

The system checks the file object usage (used file objects of each directory/number of file objects allocated to each directory) of each directory associated with a tenant every hour and compares the file object usage of each directory with the threshold set for the directory. This alarm is generated when the file object usage exceeds the threshold.

This alarm is cleared when the file object usage is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
14025	Major (default threshold: 95%) Minor (default threshold: 90%)	Quality of service	Tenant plane	HDFS	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm is generated.
	HostName	Specifies the host for which the alarm is generated.
	TenantName	Specifies the tenant for which the alarm is generated.
	DirectoryNam e	Specifies the directory for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

This alarm is generated if the usage of file objects in a tenant directory exceeds the custom threshold. File writing to the directory is not affected. If the number of used file objects exceeds the maximum number of file objects allocated to the directory, the HDFS fails to write data to the directory.

Possible Causes

- The alarm threshold is improperly configured.
- The maximum number of file objects allocated to the tenant directory is inappropriate.

Handling Procedure

Check whether the alarm threshold is appropriate.

Step 1 View the alarm location information to obtain the tenant name and tenant directory for which the alarm is generated.

Step 2 On the FusionInsight Manager portal, choose the **Tenant Resources** page, select the tenant for which the alarm is generated, and click **Resources**. Check whether the file object threshold configured for the tenant directory for which the alarm is

generated is proper. (The default value 90% is a proper value. You can set it based on the site requirements.)

- If yes, go to **Step 5**.
- If no, go to **Step 3**.

Step 3 On the **Resources** page, click **Modify** to modify or delete the file object threshold of the tenant directory for which the alarm is generated.

Step 4 About one minute later, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check whether the maximum number of file objects allocated to the tenant is appropriate.

Step 5 On the FusionInsight Manager portal, choose the **Tenant Resources** page, select the tenant for which the alarm is generated, and click **Resources**. Check whether the maximum number of file objects configured for the tenant directory for which the alarm is generated is proper based on the actual service status of the tenant directory.

- If yes, go to **Step 8**.
- If no, go to **Step 6**.

Step 6 On the **Resources** page, click **Modify** to modify or delete the maximum number of file objects configured for the tenant directory.

Step 7 About one minute later, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Collect fault information.

Step 8 On the FusionInsight Manager portal, choose **O&M** > **Log** > **Download**.

Step 9 Select **HDFS** in the required cluster and **NodeAgent** under **Manager** from the **Service**.

Step 10 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 20 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 11 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.131 ALM-14026 Blocks on DataNode Exceed the Threshold

Alarm Description

The system checks the number of blocks on each DataNode every 30 seconds. This alarm is generated when the number of blocks on the DataNode exceeds the threshold.

If **Trigger Count** is **1** and the number of blocks on the DataNode is less than or equal to the threshold, this alarm is cleared. If **Trigger Count** is greater than **1** and the number of blocks on the DataNode is less than or equal to 90% of the threshold, this alarm is cleared.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
14026	Major	Quality of service	Tenant plane	HDFS	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
Modify	3.3.1	Alarm Severity: changed from minor to major.	Alarm Severity: Accuracy optimized

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

If this alarm is reported, there are too many blocks on the DataNode. In this case, data writing into the HDFS may fail due to insufficient disk space.

Possible Causes

- The alarm threshold is improperly configured.
- Data skew occurs among DataNodes.
- The disk space configured for the HDFS cluster is insufficient.

Handling Procedure

Change the threshold.

Step 1 On FusionInsight Manager, choose **Cluster**, click the name of the desired cluster, and choose **HDFS**. Then choose **Configurations** > **All Configurations**. On the displayed page, find the **GC_OPTS** parameter under **HDFS->DataNode**.

Step 2 Set the threshold of the DataNode blocks. Specifically, change the value of **Xmx** of the **GC_OPTS** parameter. **Xmx** specifies the memory, and each GB memory supports a maximum of 500,000 DataNode blocks. Set the memory as required. Confirm that **GC_PROFILE** is set to **custom** and save the configuration.

Step 3 Choose **Cluster**, click the name of the desired cluster, and choose **HDFS** > **Instance**. Select the DataNode instance whose status is **Expired**, click **More**, and select **Restart Instance** to make the **GC_OPTS** configuration take effect.

Step 4 Wait 5 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check whether associated alarms are reported.

Step 5 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**, and check whether the **ALM-14002 DataNode Disk Usage Exceeds the Threshold** alarm exists.

- If yes, go to **Step 6**.
- If no, go to **Step 8**.

Step 6 Handle the alarm by following the instructions in **ALM-14002 DataNode Disk Usage Exceeds the Threshold** and check whether the alarm is cleared.

- If yes, go to **Step 7**.
- If no, go to **Step 8**.

Step 7 Wait 5 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Expand the DataNode capacity.

Step 8 Expand the DataNode capacity by referring to MapReduce Service (MRS) 3.3.1-LTS Physical Machine Cluster Capacity Expansion Guide (for Huawei Cloud Stack 8.3.1).

Step 9 On FusionInsight Manager, wait for 5 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 10**.

Collect fault information.

Step 10 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 11 Expand the drop-down list next to the **Service** field. In the **Services** dialog box that is displayed, select **HDFS** for the target cluster.

Step 12 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 20 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 13 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

Configuration rules of the DataNode JVM parameter.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Default value of the DataNode JVM parameter **GC_OPTS**:

-Xms2G -Xmx4G -XX:NewSize=128M -XX:MaxNewSize=256M -XX:MetaspaceSize=128M -XX:MaxMetaspaceSize=128M -XX:+UseConcMarkSweepGC -XX:+CMSParallelRemarkEnabled -XX:CMSInitiatingOccupancyFraction=65 -XX:+PrintGCDetails -Dsun.rmi.dgc.client.gcInterval=0x7FFFFFFFFFFFFE -Dsun.rmi.dgc.server.gcInterval=0x7FFFFFFFFFFFFE -XX:-OmitStackTraceInFastThrow -XX:+PrintGCDateStamps -XX:+UseGCLogFileRotation -XX:NumberOfGCLogFiles=10 -XX:GCLogFileSize=1M -Djdk.tls.ephemeralDHKeySize=2048

The average number of blocks stored in each DataNode instance in the cluster is: Number of HDFS blocks x 3/Number of DataNodes. If the average number of blocks changes, you need to change **-Xms2G -Xmx4G -XX:NewSize=128M -XX:MaxNewSize=256M** in the default value. The following table lists the reference values.

Table 1-3 DataNode JVM configuration

Average Number of Blocks in a DataNode Instance	Reference Value
2,000,000	-Xms6G -Xmx6G -XX:NewSize=512M -XX:MaxNewSize=512M
5,000,000	-Xms12G -Xmx12G -XX:NewSize=1G -XX:MaxNewSize=1G

Xmx specifies memory which corresponds to the threshold of the number of DataNode blocks, and each GB memory supports a maximum of 500,000 DataNode blocks. Set the memory as required.

1.3.132 ALM-14027 DataNode Disk Fault

Alarm Description

The system checks the disk status on DataNodes every 60 seconds. This alarm is generated when a disk is faulty.

After all faulty disks on the DataNode are recovered, you need to manually clear the alarm and restart the DataNode.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
14027	Major	Environment	Tenant plane	HDFS	No

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Faulty Disk	Specifies the list of faulty disks.

Impact on the System

If this alarm is reported, there are abnormal disk partitions on the DataNode. This may cause the loss of written files.

Possible Causes

- The hard disk is faulty.

- The disk permissions are configured improperly.

Handling Procedure

Check whether a disk alarm is generated.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** and check whether **ALM-12014 Partition Lost** or **ALM-12033 Slow Disk Fault** exists.

- If yes, go to **Step 2**.
- If no, go to **Step 4**.

Step 2 Rectify the fault by referring to the handling procedure of **ALM-12014 Partition Lost** or **ALM-12033 Slow Disk Fault**. Then, check whether the alarm is cleared.

- If yes, go to **Step 3**.
- If no, go to **Step 4**.

Step 3 Wait 5 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 4**.

Modify disk permissions.

Step 4 Choose **O&M** > **Alarm** > **Alarms** and view **Location** and **Additional Information** of the alarm to obtain the location of the faulty disk.

Step 5 Log in to the node for which the alarm is generated as user **root**. Go to the directory where the faulty disk is located, and run the **ll** command to check whether the permission of the faulty disk is **711** and whether the user is **omm**.

- If yes, go to **Step 8**.
- If no, go to **Step 6**.

Step 6 Modify the permission of the faulty disk. For example, if the faulty disk is **data1**, run the following commands:

chown omm:wheel data1

chmod 711 data1

Step 7 In the alarm list on Manager, click **Clear** in the **Operation** column of the alarm to manually clear the alarm. Choose **Cluster** > **Services** > **HDFS** > **Instance**, select the DataNode, choose **More** > **Restart Instance**, wait for 5 minutes, and check whether a new alarm is reported.

- If no, no further action is required.
- If yes, go to **Step 8**.

Collect the fault information.

Step 8 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 9 Expand the **Service** drop-down list, and select **HDFS** and **OMS** for the target cluster.

Step 10 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 20 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 11 Contact technical support and provide the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system does not automatically clear this alarm and you need to manually clear the alarm.

Related Information

None.

1.3.133 ALM-14028 Number of Blocks to Be Supplemented Exceeds the Threshold

Alarm Description

The system checks the number of blocks to be supplemented every 30 seconds and compares the number with the threshold. The number of blocks to be supplemented has a default threshold. This alarm is generated when the number of blocks to be supplemented exceeds the threshold.

You can change the threshold specified by **Blocks Under Replicated (NameNode)** by choosing **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **HDFS** > **File and Block**.

If **Trigger Count** is set to **1** and the number of blocks to be supplemented is less than or equal to the threshold, this alarm is cleared. If **Trigger Count** is greater than **1** and the number of blocks to be supplemented is less than or equal to the threshold, this alarm is cleared.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
14028	Major (default threshold: 10000) Major (default threshold: 1000)	Quality of service	Tenant plane	HDFS	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	NameServiceName	Specifies the NameService for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

Data stored in HDFS is lost. HDFS may enter the security mode and cannot provide write services. Lost block data cannot be restored.

Possible Causes

- The DataNode instance is abnormal.
- Data is deleted.
- The number of replicas written into the file is greater than the number of DataNodes.

Handling Procedure

Step 1 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**. On the page that is displayed, check whether alarm **ALM-14003 Number of Lost HDFS Blocks Exceeds the Threshold** is generated.

- If yes, go to **Step 2**.
- If no, go to **Step 3**.

Step 2 Rectify the fault according to the handling procedure of **ALM-14003 Number of Lost HDFS Blocks Exceeds the Threshold**. Five minutes later, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 3**.

Step 3 Log in to the HDFS client as user **root**. The user password is defined by the user before the installation. Contact the MRS cluster administrator to obtain the password. Run the following commands:

- Security mode:

  cd *Client installation directory*

  source bigdata_env

  kinit hdfs

- Normal mode:

  su - omm

  cd *Client installation directory*

  source bigdata_env

Step 4 Run the **hdfs fsck / >> fsck.log** command to obtain the status of the current cluster.

Step 5 Run the following command to count the number (*M*) of blocks to be replicated:

cat fsck.log | grep "Under-replicated"

Step 6 Run the following command to count the number (*N*) of blocks to be replicated in the **/tmp/hadoop-yarn/staging/** directory:

cat fsck.log | grep "Under replicated" | grep "/tmp/hadoop-yarn/staging/" | wc -l

NOTE

/tmp/hadoop-yarn/staging/ is the default directory. If the directory is modified, obtain it from the configuration item **yarn.app.mapreduce.am.staging-dir** in the **mapred-site.xml** file.

Step 7 Check whether the percentage of *N* is greater than 50% (N/M > 50%).

- If yes, go to **Step 8**.
- If no, go to **Step 9**.

Step 8 Run the following command to reconfigure the number of file replicas in the directory (set the number of file replicas to the number of DataNodes or the default number of file replicas):

hdfs dfs -setrep -w *Number of file replicas*/tmp/hadoop-yarn/staging/

NOTE

To obtain the default number of file replicas:

Log in to FusionInsight Manager, choose **Cluster** > **Services** > **HDFS** > **Configurations** > **All Configurations**, and search for the **dfs.replication** parameter. The value of this parameter is the default number of file replicas.

Check whether the alarm is cleared 5 minutes later.

- If yes, no further action is required.
- If no, go to **Step 9**.

Collect the fault information.

Step 9 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 10 Expand the drop-down list next to the **Service** field. In the **Services** dialog box that is displayed, select **HDFS** for the target cluster.

Step 11 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.134 ALM-14029 Number of Blocks in a Replica Exceeds the Threshold

Alarm Description

The system checks the number of blocks in a single replica every four hours and compares the number with the threshold. There is a threshold for the number of blocks in a single replica. This alarm is generated when the actual number of blocks in a single replica exceeds the threshold.

This alarm is cleared when the number of blocks to be supplemented is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
14029	Major (default threshold: 10000) Major (default threshold: 100)	Quality of service	Tenant plane	HDFS	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	HostName	Specifies the host for which the alarm was generated.
	NameService Name	Specifies the NameService for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

Replica data is prone to be lost when a node is faulty. Too many files of a single replica affect the security of the HDFS file system.

Possible Causes

- The DataNode is faulty.
- The disk is faulty.
- Files are written to a single replica.

Handling Procedure

Step 1 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**. On the page that is displayed, check whether alarm **ALM-14003 Number of Lost HDFS Blocks Exceeds the Threshold** is generated.

- If yes, go to **Step 2**.
- If no, go to **Step 3**.

Step 2 Rectify the fault according to the handling procedure of **ALM-14003 Number of Lost HDFS Blocks Exceeds the Threshold**. In the next detection period, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 3**.

Step 3 Check whether files of a single replica have been written into the service.

- If yes, go to **Step 4**.
- If no, go to **Step 7**.

Step 4 Log in to the HDFS client as user **root**. The user password is defined by the user before the installation. Contact the MRS cluster administrator to obtain the password. Run the following commands:

- Security mode:

  cd *Client installation directory*

source bigdata_env

kinit hdfs

- Normal mode:

  su - omm

  cd *Client installation directory*

  source bigdata_env

Step 5 Run the following command on the client node to increase the number of replicas for a single replica file:

hdfs dfs -setrep -w *file replica number file name or file path*

Step 6 In the next detection period, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect the fault information.

Step 7 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 8 Expand the drop-down list next to the **Service** field. In the **Services** dialog box that is displayed, select **HDFS** for the target cluster.

Step 9 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.135 ALM-14030 HDFS Allows Write of Single-Replica Data

Alarm Description

This alarm is generated when **dfs.single.replication.enable** is set to **true**, indicating that HDFS is configured to allow write of single-replica data.

This alarm is cleared when this function is disabled on HDFS.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
14030	Major	Quality of service	Tenant plane	HDFS	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

Data of a single replica may be lost. Therefore, the system does not allow write of single-replica data by default. If this configuration is enabled on HDFS and the number of HDFS replicas configured on the client is 1, single-replica data can be written to HDFS.

Possible Causes

The HDFS configuration item **dfs.single.replication.enable** is set to **true**.

Handling Procedure

Step 1 Log in to FusionInsight Manager and choose **Cluster** > **Services** > **HDFS**. On the page that is displayed, click the **Configurations** tab then the **All Configurations** sub-tab.

Step 2 Search for **dfs.single.replication.enable** in the search box, change the value of the configuration item to **false**, and click **Save**.

Step 3 On the **Dashboard** page of the HDFS service, click **More** and select **Service Rolling Restart** in the upper right corner.

Step 4 After the HDFS service is started, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Collect fault information.

Step 5 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 6 Expand the drop-down list next to the **Service** field. In the **Services** dialog box that is displayed, select **HDFS** for the target cluster.

Step 7 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 8 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.136 ALM-14031 DataNode Process Is Abnormal

Alarm Description

The DataNode process checks the process status every 20 seconds. This alarm is generated when the process status is abnormal and does not recover for a long time.

This alarm is cleared when the process status recovers.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
14031	Major	Quality of service	Tenant plane	HDFS	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

If the process status is abnormal, the process cannot provide services properly. As a result, the entire service may become abnormal.

Possible Causes

The host responds slowly to I/O (disk I/O and network I/O) requests and some processes are in the D state and Z state. The process may also be suspended and enter the T state.

Handling Procedure

Check whether the process is in the D, Z, or T state.

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Alarms**. Wait for about 10 minutes and check whether the alarm is automatically cleared.

- If the alarm is not in the list, no further action is required.
- If the alarm is in the list, view the alarm details and record the IP address of the host where the alarm is generated. Run the command in **Step 2**.

Step 2 Log in to the host where the alarm is generated as the **root** user and run the **su -omm** command to switch to the **omm** user.

Step 3 Run the following command to check the process state:

```
ps ww -eo stat,cmd| grep -w
org.apache.hadoop.hdfs.server.datanode.DataNode | grep -v grep | awk '{print
$1}'
```

Step 4 Check whether the command output contains any abnormal state (D, Z, or T).

- If the output contains any abnormal state, go to **Step 5**.
- If the output does not contain abnormal states, go to **Step 7**.

Step 5 Switch to user **root** and run the **reboot** command to restart the host for which the alarm is generated. (Restarting a host is risky. Ensure that the service process is normal after the restart.)

Step 6 Wait 5 minutes and check whether the alarm is cleared.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If the alarm is cleared, no further action is required.
- If the alarm fails to be cleared, go to **Step 7**.

Collect fault information.

Step 7 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 8 Expand the drop-down list next to the **Service** field. In the **Services** dialog box that is displayed, select **HDFS** for the target cluster.

Step 9 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.137 ALM-14032 JournalNode Process Is Abnormal

Alarm Description

The JournalNode process checks the process status every 20 seconds. This alarm is generated when the process status is abnormal and does not recover for a long time.

This alarm is cleared when the process status recovers.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
14032	Major	Quality of service	Tenant plane	HDFS	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.

Type	Parameter	Description
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

If the process status is abnormal, the process cannot provide services properly. As a result, the entire service may become abnormal.

Possible Causes

The host responds slowly to I/O (disk I/O and network I/O) requests and some processes are in the D state and Z state. The process may also be suspended and enter the T state.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Handling Procedure

Check whether the process is in the D, Z, or T state.

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Alarms**. Wait for about 10 minutes and check whether the alarm is automatically cleared.

- If the alarm is not in the list, no further action is required.
- If the alarm is in the list, view the alarm details and record the IP address of the host where the alarm is generated. Run the command in **Step 2**.

Step 2 Log in to the host where the alarm is generated as the **root** user and run the **su - omm** command to switch to the **omm** user.

Step 3 Run the following command to check the process state:

```
ps ww -eo stat,cmd| grep -w
org.apache.hadoop.hdfs.qjournal.server.JournalNode | grep -v grep | awk
'{print$1}'
```

Step 4 Check whether the command output contains any abnormal state (D, Z, or T).

- If the output contains any abnormal state, go to **Step 5**.
- If the output does not contain abnormal states, go to **Step 7**.

Step 5 Switch to user **root** and run the **reboot** command to restart the host for which the alarm is generated. (Restarting a host is risky. Ensure that the service process is normal after the restart.)

Step 6 Wait 5 minutes and check whether the alarm is cleared.

- If the alarm is cleared, no further action is required.
- If the alarm fails to be cleared, go to **Step 7**.

Collect fault information.

Step 7 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 8 Expand the drop-down list next to the **Service** field. In the **Services** dialog box that is displayed, select **HDFS** for the target cluster.

Step 9 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

1.3.138 ALM-14033 ZKFC Process Is Abnormal

Alarm Description

The ZKFC process checks the process status every 20 seconds. This alarm is generated when the process status is abnormal and does not recover for a long time.

This alarm is cleared when the process status recovers.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
14033	Major	Quality of service	Tenant plane	HDFS	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

If the process status is abnormal, the process cannot provide services properly. As a result, the entire service may become abnormal.

Possible Causes

The host responds slowly to I/O (disk I/O and network I/O) requests and some processes are in the D state and Z state. The process may also be suspended and enter the T state.

Handling Procedure

Check whether the process is in the D, Z, or T state.

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Alarms**. Wait for about 10 minutes and check whether the alarm is automatically cleared.

- If the alarm is not in the list, no further action is required.
- If the alarm is in the list, view the alarm details and record the IP address of the host where the alarm is generated. Run the command in **Step 2**.

Step 2 Log in to the host where the alarm is generated as the **root** user and run the **su -omm** command to switch to the **omm** user.

Step 3 Run the following command to check whether the process state is abnormal:

```
ps ww -eo stat,cmd| grep -w
org.apache.hadoop.hdfs.tools.DFSZKFailoverController | grep -v grep | awk
'{print$1}'
```

Step 4 Check whether the command output contains any abnormal state (D, Z, or T).

- If the output contains any abnormal state, go to **Step 5**.
- If the output does not contain abnormal states, go to **Step 7**.

Step 5 Switch to user **root** and run the **reboot** command to restart the host for which the alarm is generated. (Restarting a host is risky. Ensure that the service process is normal after the restart.)

Step 6 Wait 5 minutes and check whether the alarm is cleared.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If the alarm is cleared, no further action is required.
- If the alarm fails to be cleared, go to **Step 7**.

Collect fault information.

Step 7 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 8 Expand the drop-down list next to the **Service** field. In the **Services** dialog box that is displayed, select **HDFS** for the target cluster.

Step 9 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.139 ALM-14034 Router Process Is Abnormal

Alarm Description

The Router process checks the process status every 20 seconds. This alarm is generated when the process status is abnormal and does not recover for a long time.

This alarm is cleared when the process status recovers.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
14034	Major	Quality of service	Tenant plane	HDFS	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

If the process status is abnormal, the process cannot provide services properly. As a result, the entire service may become abnormal.

Possible Causes

The host responds slowly to I/O (disk I/O and network I/O) requests and some processes are in the D state and Z state. The process may also be suspended and enter the T state.

Handling Procedure

Check whether the process is in the D, Z, or T state.

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Alarms**. Wait for about 10 minutes and check whether the alarm is automatically cleared.

- If the alarm is not in the list, no further action is required.
- If the alarm is in the list, view the alarm details and record the IP address of the host where the alarm is generated. Run the command in **Step 2**.

Step 2 Log in to the host where the alarm is generated as the **root** user and run the **su - omm** command to switch to the **omm** user.

Step 3 Run the following command to check whether the process state is abnormal:

```
ps ww -eo stat,cmd| grep -w
org.apache.hadoop.hdfs.server.federation.router.DFSRouter | grep -v grep |
awk '{print$1}'
```

Step 4 Check whether the command output contains any abnormal state (D, Z, or T).

- If the output contains any abnormal state, go to **Step 5**.
- If the output does not contain abnormal states, go to **Step 7**.

Step 5 Switch to user **root** and run the **reboot** command to restart the host for which the alarm is generated. (Restarting a host is risky. Ensure that the service process is normal after the restart.)

Step 6 Wait 5 minutes and check whether the alarm is cleared.

- If the alarm is cleared, no further action is required.
- If the alarm fails to be cleared, go to **Step 7**.

Collect fault information.

Step 7 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 8 Expand the drop-down list next to the **Service** field. In the **Services** dialog box that is displayed, select **HDFS** for the target cluster.

Step 9 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.140 ALM-14035 HttpFS Process Is Abnormal

Alarm Description

The HttpFS process checks the process status every 20 seconds. This alarm is generated when the process status is abnormal and does not recover for a long time.

This alarm is cleared when the process status recovers.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
14035	Major	Quality of service	Tenant plane	HDFS	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

If the process status is abnormal, the process cannot provide services properly. As a result, the entire service may become abnormal.

Possible Causes

The host responds slowly to I/O (disk I/O and network I/O) requests and some processes are in the D state and Z state. The process may also be suspended and enter the T state.

Handling Procedure

Check whether the process is in the D, Z, or T state.

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Alarms**. Wait for about 10 minutes and check whether the alarm is automatically cleared.

- If the alarm is not in the list, no further action is required.
- If the alarm is in the list, view the alarm details and record the IP address of the host where the alarm is generated. Run the command in **Step 2**.

Step 2 Log in to the host where the alarm is generated as the **root** user and run the **su -omm** command to switch to the **omm** user.

Step 3 Run the following command to check whether the process state is abnormal:

```
ps ww -eo stat,cmd| grep -w
org.apache.hadoop.fs.http.server.HttpFSServerWebServer | grep -v grep | awk
'{print$1}'
```

Step 4 Check whether the command output contains any abnormal state (D, Z, or T).

- If the output contains any abnormal state, go to **Step 5**.
- If the output does not contain abnormal states, go to **Step 7**.

Step 5 Switch to user **root** and run the **reboot** command to restart the host for which the alarm is generated. (Restarting a host is risky. Ensure that the service process is normal after the restart.)

Step 6 Wait 5 minutes and check whether the alarm is cleared.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If the alarm is cleared, no further action is required.
- If the alarm fails to be cleared, go to **Step 7**.

Collect fault information.

Step 7 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 8 Expand the drop-down list next to the **Service** field. In the **Services** dialog box that is displayed, select **HDFS** for the target cluster.

Step 9 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.141 ALM-14036 NameNode Is In Safe Mode

Alarm Description

The system checks the NameNode process status every 30 seconds. This alarm is generated when the NameNode is in the safe mode.

This alarm is cleared when the process status recovers.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
14036	Major	Quality of service	Tenant plane	HDFS	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
New	3.3.1	New alarm	New alarm

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	Alarm Severity	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

After a NameNode enters the safe mode, data cannot be written to the NameNode.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Possible Causes

Block loss occurs when a user manually enters the safe mode or restarts the NameNode.

Handling Procedure

Check whether NameNode is in the security mode.

Step 1 Log in to FusionInsight Manager, click **O&M**, and choose **Alarm** > **Alarms** to view the alarm details. In the **Location** column, check the name of the host for which the alarm is generated.

Step 2 Choose **Cluster** > **Services** > **HDFS**, and click **NameNode(***host name recorded in Step 1,x***)** next to **NameNode Web UI**.

NOTE

By default, the **admin** user does not have the permissions to manage other components. If the page cannot be opened or the displayed content is incomplete when you access the native UI of a component due to insufficient permissions, you can manually create a user with the permissions to manage that component.

Step 3 In the **Basic Information** area on the **Dashboard** page of HDFS (or in the **NameService Summary** area on the **Dashboard** page of HDFS), check whether the value of **Safe Mode** is **ON**.

ON indicates that the safe mode is enabled.

- If yes, go to **Step 4**.
- If no, go to **Step 7**.

Step 4 Log in to the HDFS client.

1. Log in to the node where the HDFS client is installed.
   - If Kerberos authentication is enabled for the cluster (the cluster is in security mode), log in as the **root** user.
   - If Kerberos authentication is disabled for the cluster (the cluster is in normal mode), log in as user **omm** and ensure that user **omm** has the execute permission on the client.

   (Note that you need to decide with cluster security/normal mode, not the HDFS safe/common mode.)
2. Run the following commands to go to the client installation directory and configure environment variables:

   cd *HDFS client installation directory*

   source bigdata_env
3. If Kerberos authentication is enabled for the cluster (the cluster is in security mode), run the following command to authenticate the user. If Kerberos authentication is disabled for the cluster (the cluster is in normal mode), skip this step.

   kinit hdfs

   Enter the password as prompted. You can obtain the password from the MRS cluster administrator. Change the password upon the first authentication.

4. Run the following command to exit from the safe mode:

   hdfs dfsadmin -safemode leave

Step 5 Wait 5 minutes and check whether the alarm is cleared.

- If yes, go to **Step 6**.
- If no, go to **Step 7**.

Step 6 In the **Basic Information** area on the **Dashboard** page of HDFS (or in the **NameService Summary** area on the **Dashboard** page of HDFS), check whether the value of **Missing Blocks** is **0**.

- If yes, no further action is required.
- If no, check whether "ALM-14003 Number of Lost HDFS Blocks Exceeds the Threshold" is reported and rectify the fault according to the alarm help.

Collect fault information.

Step 7 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 8 Expand the drop-down list next to the **Service** field. In the **Services** dialog box that is displayed, select **HDFS** for the target cluster.

Step 9 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.142 ALM-14037 DataNodes Outside the Cluster

Alarm Description

The NameNode checks whether there are DataNodes that are not managed in the cluster every 8 hours. This alarm is generated when there is a DataNode outside the cluster. This alarm is cleared when no DataNode is outside the cluster.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
14037	Major	Quality of service	Tenant plane	HDFS	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
New	3.3.1	New alarm	New alarm

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	NameService Name	Specifies the NameService for which the alarm was generated.
	Alarm Severity	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	Trigger Condition	Specifies the alarm triggering condition, that is, the IP address and port of a DataNode outside the cluster is detected.

Impact on the System

Data may be lost.

Possible Causes

After a host is forcibly deleted, the host is powered on again, and the process is restarted.

Handling Procedure

Step 1 Log in to FusionInsight Manager, click **O&M**, and choose **Alarm** > **Alarms** to view the alarm details. In the additional information area, check the IP address of the host for which the alarm is generated.

Step 2 Stop the DataNode process on the host for which the alarm is reported.

NOTICE

If there are multiple IP addresses of the host, you can **stop only one DataNode process at a time** and stop the next DataNode process only after **Number of Blocks to Be Replicated** changes to **0**.

1. Log in to the host for which the alarm is generated as the **root** user and change the permission on the **hadoop** directory in the installation directory **$ {BIGDATA_HOME}/FusionInsight_HD_*/install**.

   chmod 000 ${BIGDATA_HOME}/FusionInsight_HD_8.3.1/install/FusionInsight-Hadoop-3.3.1

2. Run the following commands to obtain the PID of the DataNode process and stop it on the host:

   ps -ef | grep Dproc_datanode

   kill -15 *PID*

3. Choose **Cluster** > **Services** > **HDFS**. Check the **Basic Information** area in the **Dashboard** tab (or the **NameService Summary** area in the **Dashboard** tab of HDFS), and wait until the value of **Blocks to be Replicated** changes to **0**.

Step 3 Wait for 8 hours and check whether the alarm is cleared and whether the number of blocks to be replicated is 0.

- If yes, no further action is required.
- If no, go to **Step 4**.

Collect fault information.

Step 4 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 5 Expand the drop-down list next to the **Service** field. In the **Services** dialog box that is displayed, select **HDFS** for the target cluster.

Step 6 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 7 Contact technical support and provide the collected logs.

----End

1.3.143 ALM-16000 Percentage of Sessions Connected to the HiveServer to Maximum Number Allowed Exceeds the Threshold

Alarm Description

The system detects the percentage of sessions connected to the HiveServer to the maximum number of allowed sessions every 30 seconds. This indicator can be viewed on the **Cluster** > *Name of the desired cluster* > **Services** > **Hive > Instance** > *HiveServer instance***.** This alarm is generated when the percentage exceeds the default value.

To change the threshold, choose **O&M > Alarm > Thresholds >** *Name of the desired cluster* > **Hive > Percentage of Sessions Connected to the HiveServer to Maximum Number of Sessions Allowed by the HiveServer**.

When the **Trigger Count** is 1, this alarm is cleared when the percentage is less than or equal to the threshold. When the **Trigger Count** is greater than 1, this alarm is cleared when the percentage is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
16000	Critical (default threshold: 90%) Major (default threshold: 80%)	Quality of service	Tenant plane	Hive	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger condition	Specifies the threshold for triggering the alarm.

Impact on the System

If a connection number alarm is generated, the number of sessions connected to HiveServer is too large. As a result, new connections cannot be established, new tasks fail, or even services restart unexpectedly.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Possible Causes

Too many clients are connected to HiveServer.

Handling Procedure

Increase the maximum number of connections to Hive.

Step 1 On the FusionInsight Manager portal, Choose **Cluster** > *Name of the desired cluster* > **Services** > **Hive** > **Configurations >All Configurations**.

Step 2 Search for **hive.server.session.control.maxconnections** and increase the value of this parameter. If the value of this parameter is **A**, the threshold is **B**, and the number of sessions connected to the HiveServer is **C**, adjust the value of this parameter according to **A x B > C**. To view the number of sessions connected to the HiveServer, check the value of **Statistics for Sessions of the HiveServer** on the Hive monitoring page.

Step 3 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 4**.

Collect fault information.

Step 4 On the FusionInsight Manager portal, choose **O&M** > **Log > Download**.

Step 5 Select **Hive** in the required cluster from the **Service**.

Step 6 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 7 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.144 ALM-16001 Hive Warehouse Space Usage Exceeds the Threshold

Alarm Description

The system checks the Hive warehouse space usage every 30 seconds. You can view **Percentage of HDFS Space Used by Hive to the Available Space** on the Hive service monitoring page. This alarm is generated when the Hive warehouse space usage exceeds the specified threshold.

To change the threshold, choose **O&M**. In the navigation pane on the left, click **Alarm** > **Thresholds** > Name of the desired cluster > **Hive** > **Percentage of HDFS Space Used by Hive to the Available Space**.

When the number of trigger times is 1, this alarm is cleared if the Hive warehouse space usage is less than or equal to the threshold. When the number of trigger times is greater than 1, this alarm is cleared if the Hive warehouse space usage is less than or equal to 90% of the threshold.

NOTE

The MRS cluster administrator can reduce the repository space usage by increasing the repository capacity or releasing some used space.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
16001	Critical (default threshold: 95%) Major (default threshold: 85%)	Quality of service	Tenant plane	Hive	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

The system cannot write data properly. Some data may be lost.

Possible Causes

- The upper limit of the HDFS capacity available for Hive is too small.
- The HDFS space is insufficient.
- Some data nodes break down.

Handling Procedure

Extend system capacity.

Step 1 Analyze the cluster HDFS space usage and increase the HDFS capacity for Hive.

Log in to FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Hive** > **Configuration**, select **All Configurations**, search for **hive.metastore.warehouse.size.percent**, and increase the value. Assume that the value of the configuration item is A, total HDFS storage space is B, the threshold is C, and HDFS space used by Hive is D. Adjust the value by complying with A x B x C > D. You can view the total HDFS storage space on the HDFS NameNode page, and the HDFS space used by Hive on the Hive monitoring page.

Step 2 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 3**.

Perform capacity expansion for the system.

Step 3 Expand the system.

For details, see MapReduce Service (MRS) 3.3.1-LTS Physical Machine Cluster Capacity Expansion Guide (for Huawei Cloud Stack 8.3.1).

Step 4 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check whether the data node is normal.

Step 5 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Alarms**.

Step 6 Check whether **ALM-12006 NodeAgent Process Is Abnormal**, **ALM-12007 Process Fault**, and **ALM-14002 DataNode Disk Usage Exceeds the Threshold** are reported.

- If yes, go to **Step 7**.
- If no, go to **Step 9**.

Step 7 Clear the alarm by following the steps provided in **ALM-12006 NodeAgent Process Is Abnormal**, **ALM-12007 Process Fault**, or **ALM-14002 DataNode Disk Usage Exceeds the Threshold**.

Step 8 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Collect fault information.

Step 9 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 10 Expand the **Service** drop-down list, and select **Hive** for the target cluster.

Step 11 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

1.3.145 ALM-16002 Hive SQL Execution Success Rate Is Lower Than the Threshold

Alarm Description

The system checks the percentage of the HQL statements that are executed successfully in every 30 seconds. The formula is: Percentage of HQL statements that are executed successfully = Number of HQL statements that are executed successfully by Hive in a specified period/Total number of HQL statements that are executed by Hive. This indicator can be viewed on the **Cluster > Services** > **Hive > Instance** > *HiveServer instance* **.** By default, a threshold is provided for the percentage of successful HQL executions. This alarm is generated when the percentage of successful HQL executions is less than the threshold. Users can view the name of the host where an alarm is generated in the location information about the alarm. The IP address of the host is the IP address of the HiveServer node.

Users can modify the threshold by choosing **O&M > Alarm > Thresholds >** *Name of the desired cluster* > **Hive** > **Percentage of HQL Statements That Are Executed Successfully by Hive**.

This alarm is cleared when the execution success rate is higher than 110% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
16002	Critical (default threshold: 90%) Major (default threshold: 80%)	Quality of service	Tenant plane	Hive	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger condition	Specifies the threshold for triggering the alarm.

Impact on the System

The service execution capability of the system is too low and cannot properly respond to customer requests. The Hive service is not affected. You need to check HiveServer logs to locate the SQL failure cause.

Possible Causes

- A syntax error occurs in HQL statements.
- The HBase service is abnormal when a Hive on HBase task is performed.
- The Spark service is abnormal when a Hive on Spark task is performed.
- The dependent basic services, such as HDFS, Yarn, and ZooKeeper, are abnormal.

Handling Procedure

Check whether the HQL statements comply with syntax.

Step 1 On the FusionInsight Manager page, choose **O&M** > **Alarm** to view the alarm details and obtain the node where the alarm is generated.

Step 2 Use the Hive client to log in to the HiveServer node where an alarm is reported. Query the HQL syntax provided by Apache, and check whether the HQL commands are correct.

- If yes, go to **Step 4**.
- If no, go to **Step 3**.

NOTE

To view the user who runs an incorrect statement, you can download the hiveserver audit log file of the HiveServer node where this alarm is generated. **Start Data** and **End Data** are 10 minutes before and after the alarm generation time respectively. Open the log file and search for the **Result=FAIL** keyword to filter the log information about the incorrect statement, and then view the user who runs the incorrect statement according to **UserName** in the log information.

Step 3 Enter the correct HQL statements, and check whether the command can be properly executed.

- If yes, go to **Step 12**.
- If no, go to **Step 4**.

Check whether the HBase service is abnormal.

Step 4 Check whether an Hive on HBase task is performed with the user who runs the HQL command.

- If yes, go to **Step 5**.
- If no, go to **Step 8**.

Step 5 On the FusionInsight Manager page, click **Cluster** > *Name of the desired cluster* > **Services**, check whether the HBase service is normal in the service list.

- If yes, go to **Step 8**.
- If no, go to **Step 6**.

Step 6 Choose **O&M** > **Alarm**, check the related alarms displayed on the alarm page and clear them according to related alarm help.

Step 7 Enter the correct HQL statements, and check whether the command can be properly executed.

- If yes, go to **Step 12**.
- If no, go to **Step 8**.

Check whether the HDFS, Yarn, and ZooKeeper are normal.

Step 8 On the FusionInsight Manager portal, click **Cluster** > *Name of the desired cluster* > **Services**.

Step 9 In the service list, check whether the services, such as HDFS, Yarn, and ZooKeeper are normal.

- If yes, go to **Step 12**.
- If no, go to **Step 10**.

Step 10 Check the related alarms displayed on the alarm page and clear them according to related alarm help.

Step 11 Enter the correct HQL statements, and check whether the command can be properly executed.

- If yes, go to **Step 12**.
- If no, go to **Step 13**.

Step 12 After 1 minute, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 13**.

Collect fault information.

Step 13 On the FusionInsight Manager home page, choose **O&M** > **Log** > **Download**.

Step 14 Select the following nodes in the required cluster from the **Service**:

- MapReduce
- Hive

Step 15 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 16 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.146 ALM-16003 Background Thread Usage Exceeds the Threshold

Alarm Description

The system checks the background thread usage in every 30 seconds. This alarm is generated when the usage of the background thread pool of Hive exceeds the threshold.

NOTE

MRS 3.X supports the multi-instance function. If the multi-instance function is enabled in the cluster and multiple Hive services are installed, determine the Hive service for which the alarm is generated based on the value of **ServiceName** in **Location** of the alarm. For example, if Hive1 service is unavailable, **ServiceName** is set to **Hive1** in **Location**, and the operation object in the handling procedure is changed from Hive to Hive1.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
16003	Critical (default threshold: 90%) Major (default threshold: 80%)	Quality of service	Tenant plane	Hive	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger condition	Specifies the threshold for triggering the alarm.

Impact on the System

There are too many background threads, so the newly submitted task cannot run in time.

Possible Causes

The usage of the background thread pool of Hive is excessively high when:

- There are many tasks executed in the background thread pool of HiveServer.
- The capacity of the background thread pool of HiveServer is too small.

Handling Procedure

Check the number of tasks executed in the background thread pool of HiveServer.

Step 1 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services** > **Hive**. On the displayed page, click **HiveServer Instance** and check values of **Background Thread Count** and **Background Thread Usage**.

Step 2 Check whether the number of background threads in the latest half an hour is excessively high. (By default, the queue number is 100, and the thread number is considered as high if it is 90 or larger.)

- If it is, go to **Step 3**.
- If it is not, go to **Step 5**.

Step 3 Adjust the number of tasks submitted to the background thread pool. (For example, cancel some time-consuming tasks with low performance.)

Step 4 Check whether the values of Background Thread Count and Background Thread Usage decrease.

- If it is, go to **Step 7**.
- If it is not, go to **Step 5**.

Check the capacity of the HiveServer background thread pool.

Step 5 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services** > **Hive**. On the displayed page, click **HiveServer Instance** and check values of Background Thread Count and Background Thread Usage.

Step 6 Increase the value of **hive.server2.async.exec.threads** in the **${BIGDATA_HOME}/FusionInsight_HD_8.3.1/1_23_HiveServer/etc/hive-site.xml** file. For example, increase the value by 20%.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 7 Save the modification.

Step 8 Check whether the alarm is cleared.

- If it is, no further action is required.
- If it is not, go to **Step 9**.

Collect fault information.

Step 9 On the FusionInsight Manager portal, choose **O&M** > **Log** > **Download**.

Step 10 Select **Hive** in the required cluster from the **Service**.

Step 11 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.147 ALM-16004 Hive Service Unavailable

Alarm Description

This alarm is generated when the HiveServer service is unavailable. The system checks the HiveServer service status every 60 seconds.

This alarm is cleared when the HiveServer service is normal.

NOTE

MRS 3.X supports the multi-instance function. If the multi-instance function is enabled in the cluster and multiple Hive service instances are installed, you need to determine the Hive service instance where the alarm is generated based on the value of **ServiceName** in **Location**. For example, if the Hive1 service is unavailable, **ServiceName=Hive1** is displayed in **Location**, and the operation object in the procedure needs to be changed from Hive to Hive1.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
16004	Critical	Quality of service	Tenant plane	Hive	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

The system cannot provide data loading, query, and extraction services.

Possible Causes

- Hive service unavailability may be related to the faults of the Hive process as well as basic services, such as ZooKeeper, Hadoop distributed file system (HDFS), Yarn, and DBService.
  - The ZooKeeper service is abnormal.

  - The HDFS service is abnormal.
  - The Yarn service is abnormal.
  - The DBService service is abnormal.
  - The Hive service process is abnormal. If the alarm is caused by Hive process fault, the alarm report has a delay of about 5 minutes.
- The network communication between the Hive and basic services is interrupted.
- The permission on the HDFS temporary directory of Hive is abnormal.
- The local disk space of the Hive node is insufficient.

Handling Procedure

Check the HiveServer/MetaStore process status.

Step 1 On the FusionInsight Manager portal, click **Cluster >** *Name of the desired cluster* **> Services** > **Hive** > **Instance**. In the Hive instance list, check whether the HiveServer or MetaStore instances are in the Unknown state.

- If yes, go to **Step 2**.
- If no, go to **Step 4**.

Step 2 In the Hive instance list, choose **More** > **Restart Instance** to restart the HiveServer/MetaStore process.

Step 3 In the alarm list, check whether **Hive Service Unavailable** is cleared.

- If yes, no further action is required.
- If no, go to **Step 4**.

Check the ZooKeeper service status.

Step 4 On the FusionInsight Manager, check whether the alarm list contains **Process Fault**.

- If yes, go to **Step 5**.
- If no, go to **Step 8**.

Step 5 In the **Process Fault**, check whether **ServiceName** is **ZooKeeper**.

- If yes, go to **Step 6**.
- If no, go to **Step 8**.

Step 6 Rectify the fault by following the steps provided in "ALM-12007 Process Fault".

Step 7 In the alarm list, check whether **Hive Service Unavailable** is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Check the HDFS service status.

Step 8 On the FusionInsight Manager, check whether the alarm list contains **HDFS Service Unavailable**.

- If yes, go to **Step 9**.
- If no, go to **Step 11**.

Step 9 Rectify the fault by following the steps provided in "ALM-14000 HDFS Service Unavailable".

Step 10 In the alarm list, check whether **Hive Service Unavailable** is cleared.

- If yes, no further action is required.
- If no, go to **Step 11**.

Check the Yarn service status.

Step 11 In FusionInsight Manager alarm list, check whether **Yarn Service Unavailable** is generated.

- If yes, go to **Step 12**.
- If no, go to **Step 14**.

Step 12 Rectify the fault. For details, see "ALM-18000 Yarn Service Unavailable".

Step 13 In the alarm list, check whether **Hive Service Unavailable** is cleared.

- If yes, no further action is required.
- If no, go to **Step 14**.

Check the DBService service status.

Step 14 In FusionInsight Manager alarm list, check whether **DBService Service Unavailable** is generated.

- If yes, go to **Step 15**.
- If no, go to **Step 17**.

Step 15 Rectify the fault. For details, see "ALM-27001 DBService Service Unavailable".

Step 16 In the alarm list, check whether **Hive Service Unavailable** is cleared.

- If yes, no further action is required.
- If no, go to **Step 17**.

Check the network connection between the Hive and ZooKeeper, HDFS, Yarn, and DBService.

Step 17 On the FusionInsight Manager, choose **Cluster >** *Name of the desired cluster* **> Services** > **Hive**.

Step 18 Click **Instance**.

The HiveServer instance list is displayed.

Step 19 Click **Host Name** in the row of **HiveServer**.

The active HiveServer host status page is displayed.

Step 20 Record the IP address under **Basic Information**.

Step 21 Use the IP address obtained in **Step 20** to log in to the host where the active HiveServer runs as user **omm**.

Step 22 Run the **ping** command to check whether communication between the host that runs the active HiveServer and the hosts that run the ZooKeeper, HDFS, Yarn, and DBService services is normal. (Obtain the IP addresses of the hosts that run the ZooKeeper, HDFS, Yarn, and DBService services in the same way as that for obtaining the IP address of the active HiveServer.)

- If yes, go to **Step 31**.
- If no, go to **Step 23**.

Step 23 Contact the administrator to restore the network.

Step 24 In the alarm list, check whether **Hive Service Unavailable** is cleared.

- If yes, no further action is required.
- If no, go to **Step 25**.

Check the permission on the HDFS temporary directory.

Step 25 Log in to the node where the HDFS client is located and run the following command to go to the HDFS client installation directory:

cd *Client installation directory*

source bigdata_env

kinit *user with the supergroup permission* (Skip this step for common clusters.)

Step 26 Run the following command to check whether the permission on the data warehouse directory is 770:

hdfs dfs -ls /tmp | grep hive-scratch

- If yes, go to **Step 29**.
- If no, go to **Step 27**.

Step 27 Run the following command to restore the default data warehouse permission:

hdfs dfs -chmod 770 /tmp/hive-scratch

Step 28 Wait for several minutes and check whether the Hive Service Unavailable alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 29**.

Check whether the local disk space is normal.

Step 29 Run the **df -h** command to check the disk usage. Check whether the disk usage of the **/**, **/srv**, **/var**, and cluster installation directory (**/opt** by default) exceeds 95%.

- If yes, go to **Step 30**.
- If no, go to **Step 31**.

Step 30 Clear unnecessary information in the corresponding directory to ensure that the available disk space is greater than 80%. Wait for several minutes and check whether the Hive Service Unavailable alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 31**.

Collect fault information.

Step 31 On the FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 32 Select the following nodes in the required cluster from the **Service**:

- ZooKeeper

- HDFS
- Yarn
- DBService
- Hive

Step 33 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 34 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.148 ALM-16005 The Heap Memory Usage of the Hive Process Exceeds the Threshold

Alarm Description

The system checks the Hive service status every 30 seconds. The alarm is generated when the heap memory usage of an Hive service exceeds the threshold.

Users can choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Hive** to change the threshold.

The alarm is cleared when the heap memory usage is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
16005	Critical (default threshold: 95%) Major (default threshold: 85%)	Quality of service	Tenant plane	Hive	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger condition	Specifies the threshold for triggering the alarm.

Impact on the System

When the heap memory usage of Hive is overhigh, the performance of Hive task operation is affected. In addition, a memory overflow may occur so that the Hive service is unavailable.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Possible Causes

The heap memory of the Hive instance on the node is overused or the heap memory is inappropriately allocated. As a result, the usage exceeds the threshold.

Handling Procedure

Check heap memory usage.

Step 1 On the FusionInsight Manager portal, click **O&M > Alarm > Alarms** and select the alarm whose **Alarm ID** is **16005**. Then check the role name in **Location** and confirm the IP adress of the instance.

- If the role for which the alarm is generated is HiveServer, go to **Step 2**.
- If the role for which the alarm is generated is MetaStore, go to **Step 3**.

Step 2 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* **> Services** > **Hive** > **Instance** and click the HiveServer for which the alarm is generated to go to the **Dashboard** page. Click the drop-down menu in the **Chart** area and choose **Customize** > **CPU and Memory**, and select **HiveServer Memory Usage Statistics** and click **OK**, check whether the used heap memory of the HiveServer service reaches the threshold(default value: 95%) of the maximum heap memory specified for HiveServer.

- If yes, go to **Step 4**.
- If no, go to **Step 7**.

Step 3 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services** > **Hive** > **Instance** and click the MetaStore for which the alarm is generated to go to the **Dashboard** page. Click the drop-down menu in the **Chart** area and choose **Customize** > **CPU and Memory**, and select **MetaStore Memory Usage Statistics** and click **OK**, check whether the used heap memory of the MetaStore service reaches the threshold(default value: 95%) of the maximum heap memory specified for MetaStore.

- If yes, go to **Step 4**.
- If no, go to **Step 7**.

Step 4 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services** > **Hive** > **Configurations > All Configurations**. Choose **HiveServer/MetaStore** > **JVM**. Adjust the value of **-Xmx** in **HIVE_GC_OPTS/METASTORE_GC_OPTS** as the following rules. Click **Save**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

NOTE

Suggestions for GC parameter settings for the HiveServer:

- When the heap memory used by the HiveServer process reaches the threshold (default value: 95%) of the maximum heap memory set by the HiveServer process, change the value of **-Xmx** to twice the default value. For example, if **-Xmx** is set to 2GB by default, change the value of **-Xmx** to 4GB. You are advised to change the value of **-Xms** to set the ratio of **-Xms** and **-Xmx** to 1:2 to avoid performance problems when JVM dynamically. On the FusionInsight Manager home page, choose **O&M**> **Alarm**> **Thresholds** > *Name of the desired cluster* **> Hive** > **CPU and Memory** > **HiveServer Heap Memory Usage Statistics (HiveServer)** to view **Threshold**.

Suggestions for GC parameter settings for the MetaServer:

- When the heap memory used by the MetaStore process reaches the threshold (default value: 95%) of the maximum heap memory set by the MetaStore process, change the value of **-Xmx** to twice the default value. For example, if **-Xmx** is set to 2GB by default, change the value of **-Xmx** to 4GB. On the FusionInsight Manager home page, choose **O&M**> **Alarm**> **Thresholds** > *Name of the desired cluster* **> Hive** > **CPU and Memory** > **MetaStore Heap Memory Usage Statistics (MetaStore)** to view **Threshold**.
- You are advised to change the value of **-Xms** to set the ratio of **-Xms** and **-Xmx** to 1:2 to avoid performance problems when JVM dynamically.

Step 5 Click **More > Restart Service** to restart the service.

Step 6 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect fault information.

Step 7 On the FusionInsight Manager portal, choose **O&M** > **Log > Download**.

Step 8 Select **Hive** in the required cluster from the **Service**.

Step 9 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.149 ALM-16006 The Direct Memory Usage of the Hive Process Exceeds the Threshold

Alarm Description

The system checks the Hive service status every 30 seconds. The alarm is generated when the direct memory usage of an Hive service exceeds the threshold.

Users can choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Hive** to change the threshold.

The alarm is cleared when the direct memory usage is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
16006	Critical (default threshold: 95%) Major (default threshold: 85%)	Quality of service	Tenant plane	Hive	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger condition	Specifies the threshold for triggering the alarm.

Impact on the System

When the direct memory usage of Hive is overhigh, the performance of Hive task operation is affected. In addition, a memory overflow may occur so that the Hive service is unavailable.

Possible Causes

The direct memory of the Hive instance on the node is overused or the direct memory is inappropriately allocated. As a result, the usage exceeds the threshold.

Handling Procedure

Check direct memory usage.

Step 1 On the FusionInsight Manager portal, click **O&M > Alarm > Alarms** and select the alarm whose **Alarm ID** is **16006**. Then check the role name in **Location** and confirm the IP adress of the instance.

- If the role for which the alarm is generated is HiveServer, go to **Step 2**.
- If the role for which the alarm is generated is MetaStore, go to **Step 3**.

Step 2 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services > Hive > Instance** and click the HiveServer for which the alarm is generated to go to the **Dashboard** page. Click the drop-down menu in the **Chart** area and choose **Customize** > **CPU and Memory**, and select **HiveServer Memory Usage Statistics** and click **OK**, check whether the used direct memory of

the HiveServer service reaches the threshold(default value: 95%) of the maximum direct memory specified for HiveServer.

- If yes, go to **Step 4**.
- If no, go to **Step 7**.

Step 3 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services** > **Hive** > **Instance** and click the MetaStore for which the alarm is generated to go to the **Dashboard** page. Click the drop-down menu in the **Chart** area and choose **Customize** > **CPU and Memory**, and select **MetaStore Memory Usage Statistics** and click **OK**, check whether the used direct memory of the MetaStore service reaches the threshold(default value: 95%) of the maximum direct memory specified for MetaStore.

- If yes, go to **Step 4**.
- If no, go to **Step 7**.

Step 4 On the FusionInsight Manager portal, choose **Cluster** >*Name of the desired cluster* > **Services** > **Hive** > **Configurations > All Configurations**. Choose **HiveServer/MetaStore** > **JVM**. Adjust the value of **-XX:MaxDirectMemorySize** in **HIVE_GC_OPTS/METASTORE_GC_OPTS** as the following rules. Click **Save**.

NOTE

Suggestions for GC parameter settings for the HiveServer:

- It is recommended that you set the value of **-XX:MaxDirectMemorySize** to 1/8 of the value of **-Xmx**. For example, if **-Xmx** is set to 8 GB, **-XX:MaxDirectMemorySize** is set to 1024 MB. If **-Xmx** is set to 4 GB, **-XX:MaxDirectMemorySize** is set to 512 MB. It is recommended that the value of **-XX:MaxDirectMemorySize** be greater than or equal to 512 MB.

Suggestions for GC parameter settings for the MetaServer:

- It is recommended that you set the value of **-XX:MaxDirectMemorySize** to 1/8 of the value of **-Xmx**. For example, if **-Xmx** is set to 8 GB, **-XX:MaxDirectMemorySize** is set to 1024 MB. If **-Xmx** is set to 4 GB, **-XX:MaxDirectMemorySize** is set to 512 MB. It is recommended that the value of **-XX:MaxDirectMemorySize** be greater than or equal to 512 MB.

Step 5 Click **More > Restart Service** to restart the service.

Step 6 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect fault information.

Step 7 On the FusionInsight Manager portal, choose **O&M** > **Log > Download**.

Step 8 Select **Hive** in the required cluster from the **Service**.

Step 9 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact the technical support and send the collected fault logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.150 ALM-16007 Hive GC Time Exceeds the Threshold

Alarm Description

The system checks the garbage collection (GC) time of the Hive service every 60 seconds. This alarm is generated when the detected GC time exceeds the threshold (exceeds 12 seconds for three consecutive checks.) To change the threshold, choose **O&M > Alarm > Thresholds >** *Name of the desired cluster* > **Hive**. This alarm is cleared when the Hive GC time is shorter than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
16007	Major	Quality of service	Tenant plane	Hive	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger condition	Specifies the threshold for triggering the alarm.

Impact on the System

If the GC time exceeds the threshold, Hive data read and write are affected, task execution may slow down, or services may restart unexpectedly.

Possible Causes

The memory of Hive instances is overused, the heap memory is inappropriately allocated. As a result, GCs occur frequently.

Handling Procedure

Check the GC time.

Step 1 On the FusionInsight Manager portal, click **O&M > Alarm > Alarms** and select the alarm whose **Alarm ID** is **16007**. Then check the role name in **Location** and confirm the IP adress of the instance.

- If the role for which the alarm is generated is HiveServer, go to **Step 2**.
- If the role for which the alarm is generated is MetaStore, go to **Step 3**.

Step 2 On the FusionInsight Manager portal, choose **Cluster** >*Name of the desired cluster* > **Services** > **Hive** > **Instance** and click the HiveServer for which the alarm is generated to go to the **Dashboard** page. Click the drop-down menu in the **Chart** area and choose **Customize** > **GC**, and select **Garbage Collection (GC) Time of HiveServer** and click **OK** to check whether the GC time is longer than 12 seconds.

- If yes, go to **Step 4**.
- If no, go to **Step 7**.

Step 3 On the FusionInsight Manager portal, choose **Cluster** >*Name of the desired cluster* > **Services** > **Hive** > **Instance** and click the MetaStore for which the alarm

is generated to go to the **Dashboard** page. Click the drop-down menu in the **Chart** area and choose **Customize** > **GC**, and select **Garbage Collection (GC) Time of MetaStore** and click **OK** to check whether the GC time is longer than 12 seconds.

- If yes, go to **Step 4**.
- If no, go to **Step 7**.

Check the current JVM configuration.

Step 4 On the FusionInsight Manager portal, choose **Cluster** >*Name of the desired cluster* > **Services > Hive > Configurations > All Configurations**. Choose **HiveServer/MetaStore** > **JVM**. Adjust the value of **-Xmx** in **HIVE_GC_OPTS/METASTORE_GC_OPTS** as the following rules. Click **Save**.

NOTE

Suggestions for GC parameter settings for the HiveServer:

- When the Hive GC time exceeds the threshold, change the value of **-Xmx** to twice the default value. For example, if **-Xmx** is set to 2 GB by default, change the value of **-Xmx** to 4 GB.
- You are advised to change the value of **-Xms** to set the ratio of **-Xms** and **-Xmx** to 1:2 to avoid performance problems when JVM dynamically.

Suggestions for GC parameter settings for the MetaServer:

- When the Meta GC time exceeds the threshold, change the value of **-Xmx** to twice the default value. For example, if **-Xmx** is set to 2 GB by default, change the value of **-Xmx** to 4 GB.
- You are advised to change the value of **-Xms** to set the ratio of **-Xms** and **-Xmx** to 1:2 to avoid performance problems when JVM dynamically.

Step 5 Click **More > Restart Service** to restart the service.

Step 6 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect fault information.

Step 7 On the FusionInsight Manager portal of active and standby clusters, choose **O&M** > **Log > Download**.

Step 8 In the **Service**, select **Hive** in the required cluster.

Step 9 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.151 ALM-16008 Non-Heap Memory Usage of the Hive Process Exceeds the Threshold

Alarm Description

The system checks the Hive service status every 30 seconds. The alarm is generated when the non-heap memory usage of an Hive service exceeds the threshold.

Users can choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Hive** to change the threshold.

The alarm is cleared when the non-heap memory usage is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
16008	Critical (default threshold: 95%) Major (default threshold: 85%)	Quality of service	Tenant plane	Hive	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger condition	Specifies the threshold for triggering the alarm.

Impact on the System

When the non-heap memory usage of Hive is overhigh, the performance of Hive task operation is affected. In addition, a memory overflow may occur so that the Hive service is unavailable.

Possible Causes

The non-heap memory of the Hive instance on the node is overused or the non-heap memory is inappropriately allocated. As a result, the usage exceeds the threshold.

Handling Procedure

Check non-heap memory usage.

Step 1 On the FusionInsight Manager portal, click **O&M** > **Alarm** > **Alarms** and select the alarm whose **Alarm ID** is **16008**. Then check the role name in **Location** and confirm the IP adress of the instance.

- If the role for which the alarm is generated is HiveServer, go to **Step 2**.
- If the role for which the alarm is generated is MetaStore, go to **Step 3**.

Step 2 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services** > **Hive** > **Instance** and click the HiveServer for which the alarm is generated to go to the **Dashboard** page. Click the drop-down menu in the **Chart** area and choose **Customize** > **CPU and Memory**, and select **HiveServer Memory Usage Statistics** and click **OK**, check whether the used non-heap memory of the HiveServer service reaches the threshold(default value: 95%) of the maximum non-heap memory specified for HiveServer.

- If yes, go to **Step 4**.
- If no, go to **Step 7**.

Step 3 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services** > **Hive** > **Instance** and click the MetaStore for which the alarm is generated to go to the **Dashboard** page. Click the drop-down menu in the **Chart** area and choose **Customize** > **CPU and Memory**, and select **MetaStore Memory Usage Statistics** and click **OK**, check whether the used non-heap memory of the MetaStore service reaches the threshold(default value: 95%) of the maximum non-heap memory specified for MetaStore.

- If yes, go to **Step 4**.
- If no, go to **Step 7**.

Step 4 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* > **Services** > **Hive** > **Configurations > All Configurations**. Choose **HiveServer/MetaStore** > **JVM**. Adjust the value of **-XX:MaxMetaspaceSize** in **HIVE_GC_OPTS/METASTORE_GC_OPTS** as the following rules. Click **Save**.

NOTE

Suggestions for GC parameter settings for the HiveServer:

- It is recommended that you set the value of **-XX:MaxMetaspaceSize** to 1/8 of the value of **-Xmx**. For example, if **-Xmx** is set to 2 GB, **-XX:**

  MaxMetaspaceSize is set to 256 MB. If **-Xmx** is set to 4 GB, **-XX:MaxMetaspaceSize** is set to 512 MB.

Suggestions for GC parameter settings for the MetaServer:

- It is recommended that you set the value of **-XX:MaxMetaspaceSize** to 1/8 of the value of **-Xmx**. For example, if **-Xmx** is set to 2 GB, **-XX:**

  MaxMetaspaceSize is set to 256 MB. If **-Xmx** is set to 4 GB, **-XX:MaxMetaspaceSize** is set to 512 MB

Step 5 Click **More > Restart Service** to restart the service.

Step 6 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect fault information.

Step 7 On the FusionInsight Manager portal, choose **O&M** > **Log > Download**.

Step 8 Select **Hive** in the required cluster from the **Service**.

Step 9 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.152 ALM-16009 Map Number Exceeds the Threshold

Alarm Description

The system checks the number of HQL maps in every 30 seconds. This alarm is generated if the number exceeds the threshold. By default, **Trigger Count** is set to **3**, and the threshold is 5000.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
16009	Major	Quality of service	Tenant plane	Hive	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger condition	Specifies the threshold for triggering the alarm.

Impact on the System

If the number of HQL maps executed by Hive is too large, a large number of Yarn queue resources are occupied, which may take a long time and affect other tasks running using this queue.

Possible Causes

The HQL statements are not the optimal.

Handling Procedure

Check the number of HQL maps.

Step 1 On FusionInsight Manager portal, choose **Cluster** >*Name of the desired cluster*> **Services** > **Hive** > **Resource**. Check the HQL statements with the excessively large number (5000 or more) of maps in **HQL Map Count**.

Step 2 Locate the corresponding HQL statements, optimize them by following the instructions in *MapReduce Service (MRS) 3.3.1-LTS Performance Tuning Guide (for Huawei Cloud Stack 8.3.1)*, and execute them again.

Step 3 Check whether the alarm is cleared.

- If it is, no further action is required.
- If it is not, go to **Step 4**.

Collect fault information.

Step 4 On the FusionInsight Manager, choose **O&M** > **Log > Download**.

Step 5 Select **Hive** in the required cluster from the **Service**.

Step 6 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 7 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.153 ALM-16045 Hive Data Warehouse Is Deleted

Alarm Description

The system checks the Hive data warehouse in every 60 seconds.This alarm is generated when the Hive data warehouse is deleted.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
16045	Critical	Operation	Tenant plane	Hive	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

The default Hive data warehouse is deleted. As a result, creating databases or tables in the default data warehouse fails, and services are affected.

Possible Causes

Hive periodically checks the status of the default data warehouse and finds that the default data warehouse is deleted.

Handling Procedure

Check the default Hive data warehouse.

Step 1 Log in to the node where the client is located as user **root**.

Step 2 Run the following command to check whether the **warehouse** directory exists in **hdfs://hacluster/user/***<username>***/.Trash/Current/**.

hdfs dfs -ls hdfs://hacluster/user/*<username>***/.Trash/Current/**

For example, if **user/hive/warehouse** exists:

```
host01:/opt/hadoopclient # hdfs dfs -ls hdfs://hacluster/user/test/.Trash/Current/
Found 1 items
drwx------   - test hadoop          0 2019-06-17 19:53 hdfs://hacluster/user/test/.Trash/Current/user
```

- If yes, go to **Step 3**.

- If no, go to **Step 5**.

Step 3 By default, there is an automatic recovery mechanism for the data warehouse. You can wait for 5 ~10s to check whether the default data warehouse is restored. If the data warehouse is not recovered, manually run the following command to restore the data warehouse.

hdfs dfs -mv hdfs://hacluster/user/*<username>***/.Trash/Current/user/hive/warehouse /user/hive/warehouse**

Step 4 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Collect fault information.

Step 5 Collect related information in the **.Trash/Current/** directory on the client background.

Step 6 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.154 ALM-16046 Hive Data Warehouse Permission Is Modified

Alarm Description

The system checks the Hive data warehouse permission in every 60 seconds. This alarm is generated if the permission is modified.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
16046	Critical	Operation	Tenant plane	Hive	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

If the permission on the Hive default data warehouse is modified, the permission for users or user groups to create databases or tables in the default data warehouse is changed.

Possible Causes

Hive periodically checks the status of the default data warehouse and finds that default data warehouse permission is changed.

Handling Procedure

Check the Hive default data warehouse permission.

Step 1 Log in to the node where the client is located as user **root**.

Step 2 Run the following command to go to the HDFS client installation directory:

cd *Client installation directory*

source bigdata_env

kinit *User who has the supergroup permission* (Skip this step for a common cluster.)

Step 3 Run the following command to restore the default data warehouse permission:

- Kerberos authentication is enabled for the cluster (the cluster is in security mode):

  hdfs dfs -chmod 770 hdfs://hacluster/user/hive/warehouse

  hdfs dfs -chown hive:hive hdfs://hacluster/user/hive/warehouse

- Kerberos authentication is disabled for the cluster (the cluster is in normal mode):

  hdfs dfs -chmod 777 hdfs://hacluster/user/hive/warehouse

  hdfs dfs -chown hive:hive hdfs://hacluster/user/hive/warehouse

NOTE

If multiple Hive services are installed in the cluster, change the default data warehouse directory and owner group. For example, if the default data warehouse directory of the Hive-1 service is **/user/hive-1/warehouse** and the owner group is **hive-1**, run the following command:

hdfs dfs -chown hive:hive-1 /user/hive-1/warehouse

Step 4 Check whether the alarm is cleared.

- If it is, no further action is required.
- If it is not, go to **Step 5**.

Collect fault information.

Step 5 Collect related information in the **hdfs://hacluster/user/hive/warehouse** directory on the client background.

Step 6 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.155 ALM-16047 HiveServer Has Been Deregistered from ZooKeeper

Alarm Description

The system checks the Hive service every 60 seconds. This alarm is generated when Hive registration information on ZooKeeper is lost or Hive cannot connect to ZooKeeper.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
16047	Major	Quality of service	Tenant plane	Hive	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

When a Hive client sets up a new connection, it cannot select the HiveServer node that has been deregistered from ZooKeeper. If all HiveServer nodes have been deregistered from ZooKeeper, the HiveServer service will be unavailable.

Possible Causes

- The ZooKeeper instance is abnormal.
- Some Hive configurations are incorrect.

Handling Procedure

Check the ZooKeeper service status.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** and check whether **ALM-12007 Process Fault** exists in the alarm list.

- If yes, go to **Step 2**.
- If no, go to **Step 5**.

Step 2 In **Location** of **ALM-12007 Process Fault**, check whether the service name is **ZooKeeper**.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 Rectify the fault by following steps provided in **ALM-12007 Process Fault**.

Step 4 In the alarm list, check whether this alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check whether the Hive configurations are correctly modified.

Step 5 On FusionInsight Manager, choose **Audit**. On the **Audit** page, click **Advanced Search**, click ··· on the right of **Operation Type**, select **Save configuration**, click **OK**, and click **Search**.

Step 6 In the search result, check the historical configurations of Hive- and ZooKeeper-related services in the **Service** column. **Table 1-4** lists some configurations that may affect the connection between Hive and ZooKeeper.

Table 1-4 Configurations related to connection between Hive and ZooKeeper

Service	Parameter	Description
Hive	HIVE_GC_OPTS	HiveServer memory configuration. If the configuration is abnormal, HiveServer may restart repeatedly. In this case, you need to check the health status of the instance processes.
	hive.zookeeper.quorum	IP address of the node accommodating ZooKeeper that is connected to Hive.
	hive.zookeeper.client.port	Port of the ZooKeeper client connected to Hive.
	hive.zookeeper.session.timeout	Timeout interval of the session set up between Hive and ZooKeeper.
	hive.zookeeper.connection.timeout	Timeout interval for Hive to connect to ZooKeeper.
	hive.zookeeper.connection.max.retries	Maximum number of retries for Hive to connect to ZooKeeper.
ZooKeeper	clientPort	Port number of the ZooKeeper client.
	ssl.enabled	Whether to enable SSL connections of ZooKeeper.

Restart related instances.

Step 7 Log in to FusionInsight Manager. Choose **O&M** > **Alarm** > **Alarms**, click the drop-down list in the row that contains the alarm, and view role and the IP address of the node for which the alarm is generated in **Location**.

Step 8 Choose **Cluster**, click the name of the desired cluster, and choose **Services** > **Hive** > **Instance**. On the page that is displayed, select the instance at the IP address for which the alarm is generated, click **More**, and select **Restart Instance**.

Step 9 Wait 5 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 10**.

Collect fault information.

Step 10 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 11 Expand the **Service** drop-down list, and select **Hive** for the target cluster.

Step 12 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 13 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.156 ALM-16048 Tez or Spark Library Path Does Not Exist

Alarm Description

The system checks the Tez and Spark library paths every 180 seconds. This alarm is generated when the Tez or Spark library path does not exist.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
16048	Major	Quality of service	Tenant plane	Hive	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

The Hive on Tez and Hive on Spark functions are affected.

Possible Causes

The Tez or Spark library path is deleted from the HDFS.

Handling Procedure

Check the default Hive data warehouse.

Step 1 Log in to the node where the client is located as user **root**.

Step 2 Run the following command to check whether the **tezlib** or **sparklib** directory exists in the **hdfs://hacluster/user/{User name}/.Trash/Current/** director:

hdfs dfs -ls hdfs://hacluster/user/*<username>***/.Trash/Current/**

For example, the following information shows that **/user/hive/tezlib/8.3.1/** and **/user/hive/sparklib/8.3.1/** exist.

```
host01:/opt/hadoopclient # hdfs dfs -ls hdfs://hacluster/user/test/.Trash/Current/
Found 1 items
drwx------   - test hadoop          0 2019-06-17 19:53 hdfs://hacluster/user/test/.Trash/Current/user
```

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 Run the following command to restore **tezlib** and **sparklib**.

hdfs dfs -mv hdfs://hacluster/user/*<username>***/.Trash/Current/user/hive/tezlib/8.3.1/tez.tar.gz /user/hive/tezlib/8.3.1/tez.tar.gz**

Step 4 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Collect fault information.

Step 5 Collect related information in the **.Trash/Current/** directory on the client background.

Step 6 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.157 ALM-16049 Connection Between Hive MetaStore and Redis Is Abnormal

Alarm Description

The system checks the connection between Hive MetaStore and Redis every 180 seconds. This alarm is generated when the connection is detected to have failed for three consecutive times.

This alarm is cleared when the connection between Hive MetaStore and Redis becomes normal.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
16049	Major	Quality of service	Tenant plane	Hive	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

MetaStore operations are directly delivered to the metabase, which does not affect SQL operations but increases the data processing pressure on the metabase. MetaStore queries become slow.

Possible Causes

- Redis-based cache is incorrectly configured for Hive MetaStore.
- The Redis cluster is abnormal.

Handling Procedure

Check the Redis cache configuration of MetaStore.

Step 1 Log in to FusionInsight Manager and choose **Cluster** > **Services** > **Hive**. On the page that is displayed, click the **Configurations** tab then the **All Configurations** sub-tab.

Step 2 Search for **redis.cluster.host.and.port** in the search box and check whether the IP addresses and port numbers configured for the Redis cluster nodes are correct. The format is **IP1:PORT1;IP2:PORT2;...**.

- If yes, go to **Step 4**.
- If no, go to **Step 3**.

Step 3 Modify the **redis.cluster.host.and.port** configuration and save the modification. Choose **Dashboard** > **More** > **Restart Service**. After the restart is complete, wait for a while and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 4**.

Step 4 Log in to the node where the Redis client is installed as user **root** and run the following commands to authenticate the user:

cd *Client installation directory*

source bigdata_env

kinit *Component service user* (Skip this step for clusters with Kerberos authentication disabled.)

Step 5 Run the following commands to check whether the Redis connection and data read are normal:

redis-cli -c -h *IP* **-p** *Port*

setnx test_key "my_test"

get test_key

quit

NOTE

In the commands, **IP** and **Port** indicate any IP address and port number obtained in **Step 2**.

- If yes, the preceding commands have been successfully executed. Go to **Step 6**.
- If no, contact technical support personnel to rectify the fault.

Check the status of the Redis cluster connected to MetaStore.

Step 6 Check whether the Redis node configured for MetaStore in **Step 2** belongs to the current cluster.

- If yes, go to **Step 7**.
- If no, go to **Step 8**.

Step 7 Log in to FusionInsight Manager and choose **Cluster** > **Services** > **Redis**. On the page that is displayed, click **Redis Manager**, and check whether the cluster status is normal.

- If yes, go to **Step 9**.
- If no, the Redis cluster is abnormal. Contact technical support personnel to rectify the fault.

Step 8 Log in to the cluster management page and check whether the Redis cluster status is normal.

- If yes, go to **Step 9**.
- If no, the Redis cluster is abnormal. Contact technical support personnel to rectify the fault.

Collect fault information.

Step 9 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 10 Choose **Services** > **Hive** > **MetaStore**.

Step 11 In the **Hosts** area, select the host where the role is located.

Step 12 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 13 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.158 ALM-16050 Redis Cache of Hive MetaStore Is Unavailable

Alarm Description

The system checks whether the Redis cache of Hive MetaStore is available every 180 seconds. This alarm is generated when the Redis cache is unavailable. This alarm is cleared after the Redis cache is cleared and new data is cached from the metastore.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
16050	Major	Quality of service	Tenant plane	Hive	Yes

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

- MetaStore operations are directly delivered to the metabase, which does not affect SQL operations but increases the data processing pressure on the metabase. MetaStore queries become slow.
- After this alarm is generated, if the Redis cache synchronization period is configured, this alarm is automatically cleared when the next synchronization is normal.
- This alarm can also be manually cleared. During this period, the existing Redis cache is cleared and new metadata is loaded, increasing the pressure on the metadata. Therefore, perform this operation during off-peak hours.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Possible Causes

- Redis-based cache is incorrectly configured for Hive MetaStore.
- The Redis cluster is abnormal.

Handling Procedure

Check the Redis configuration of MetaStore.

Step 1 Log in to FusionInsight Manager and choose **Cluster** > **Services** > **Hive**. On the page that is displayed, click the **Configurations** tab then the **All Configurations** sub-tab.

Step 2 Search for **redis.cluster.host.and.port** in the search box and check whether the IP addresses and port numbers configured for the Redis cluster nodes are correct. The format is **IP1:PORT1;IP2:PORT2;...**.

- If yes, go to **Step 4**.
- If no, go to **Step 3**.

Step 3 Modify the **redis.cluster.host.and.port** configuration and save the modification. Choose **Dashboard** > **More** > **Restart Service**. After the restart is complete, wait for a while and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 4**.

Step 4 Log in to the node where the Redis client is installed as user **root** and run the following commands to authenticate the user:

cd *Client installation directory*

source bigdata_env

kinit *Component service user* (Skip this step for clusters with Kerberos authentication disabled.)

Step 5 Run the following commands to check whether the Redis connection and data read are normal:

redis-cli -c -h *IP* **-p** *Port*

setnx test_key "my_test"

get test_key

quit

NOTE

In the commands, **IP** and **Port** indicate any IP address and port number obtained in **Step 2**.

- If yes, the preceding commands have been successfully executed. Go to **Step 6**.
- If no, contact technical support personnel to rectify the fault.

Check the status of the Redis cluster connected to MetaStore.

Step 6 Check whether the Redis node configured for MetaStore in **Step 2** belongs to the current cluster.

- If yes, go to **Step 7**.
- If no, go to **Step 8**.

Step 7 Log in to FusionInsight Manager and choose **Cluster** > **Services** > **Redis**. On the page that is displayed, click **Redis Manager**, and check whether the cluster status is normal.

- If yes, go to **Step 9**.
- If no, the Redis cluster is abnormal. Contact technical support personnel to rectify the fault.

Step 8 Log in to the cluster management page and check whether the Redis cluster status is normal.

- If yes, go to **Step 9**.
- If no, the Redis cluster is abnormal. Contact technical support personnel to rectify the fault.

Step 9 Log in to FusionInsight Manager and choose **Cluster** > **Services** > **Hive**. On the page that is displayed, click the **Configurations** tab then the **All Configurations** sub-tab. On the displayed tab page, search for **redis.cache.prewarm.cron** in the search box, and check whether the configuration item exists.

- If yes, this alarm will be automatically cleared when the Redis cache becomes available in the next period. To manually clear this alarm, perform **Step 10** during off-peak hours.
- If no, manually clear this alarm by performing **Step 10** during off-peak hours.

Step 10 Log in to the node where the Redis client is installed as user **root** and authenticate the user. For details, see **Step 4**.

Step 11 Run the following commands to delete the keys related to the Redis cache to trigger a task synchronization:

redis-cli -c -h *IP* **-p** *Port*

set hive-hive-isRedisAvailable "false"

del hive-hive-isCanPrewarm

quit

NOTE

In the commands, **IP** and **Port** indicate any IP address and port number obtained in **Step 2**.

Step 12 Wait for a while and check whether the alarm is cleared. If a large amount of metadata is cached, task synchronization takes a long time.

- If yes, no further action is required.
- If no, go to **Step 13**.

Collect fault information.

Step 13 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 14 Expand the **Service** drop-down list, and select **Hive** for the target cluster.

Step 15 In the **Hosts** area, select the host where the role is located.

Step 16 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 17 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.159 ALM-16051 Percentage of Sessions Connected to MetaStore Exceeds the Threshold

Alarm Description

The system checks the percentage of sessions connected to MetaStore to the maximum number of sessions allowed by MetaStore every 30 seconds. This alarm is generated when the percentage exceeds the threshold.

This alarm is cleared when the percentage of MetaStore sessions is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
16051	Critical (default threshold: 90%) Major (default threshold: 80%)	Quality of service	Tenant plane	Hive	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.

Type	Parameter	Description
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

If this alarm is generated, sessions connected to MetaStore are too many. As a result, new connections cannot be set up.

Possible Causes

Too many clients are connected to MetaStore.

Handling Procedure

Change the maximum number of MetaStore connections.

Step 1 On FusionInsight Manager, choose **Cluster** > **Services** > **Hive**, click **Configuration** and then **All Configurations**.

Step 2 In the **All Configurations** tab, search for **hive.metastore.server.max.threads** and check whether the value is the maximum **10000**.

- If yes, go to **Step 6**.
- If no, go to **Step 3**.

Step 3 Change the value of **hive.metastore.server.max.threads** to **10000** and click **Save**.

Step 4 Click **Instances**, select all MetaStore instances, and choose **More** > **Restart Instance**.

Step 5 Check whether this alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **Hive** for the target cluster.

Step 8 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 On FusionInsight Manager, choose **Cluster** > **Services** > **Hive**. On the displayed **Dashboard** page, click **More** > **Collect Stack Information**. On the displayed page, set the following parameters:

- Select **MetaStore** for the role where you want to collect data.
- Select **jstack** and **Enable continuous collection of jstack and jmap -histo information**.
- Set the collection interval to 10 seconds and the duration to 2 minutes.

Step 10 Click **OK**. After the collection is complete, click **Download**.

Step 11 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.160 ALM-17003 Oozie Service Unavailable

Alarm Description

The system checks the Oozie service status in every 5 seconds. This alarm is generated when Oozie or a component on which Oozie depends cannot provide services properly.

This alarm is automatically cleared when the Oozie service recovers.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
17003	Critical	Error handling	Tenant plane	Oozie	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Details	Supplement to the alarm information.

Impact on the System

Oozie cannot be used to schedule jobs.

Possible Causes

- The DBService service is abnormal or the data of Oozie stored in DBService is damaged.
- The HDFS service is abnormal or the data of Oozie stored in HDFS is damaged.
- The Yarn service is abnormal.
- The Nodeagent process is abnormal.

Handling Procedure

Query the Oozie service health status code.

Step 1 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* >**Services** > **Oozie**. Click **oozie** (any one is OK) on the **oozie WebUI**. to go to the Oozie WebUI.

NOTE

By default, the **admin** user does not have the permissions to manage other components. If the page cannot be opened or the displayed content is incomplete when you access the native UI of a component due to insufficient permissions, you can manually create a user with the permissions to manage that component.

Step 2 Add **/servicehealth** to the URL in the address box of the browser and access again. The value of **statusCode** is the current Oozie service health status code.

For example, visit **https://10.10.0.117:20026/Oozie/oozie/130/oozie/servicehealth**. The result is as follows:

```
{"beans":[{"name":"serviceStatus","statusCode":0}]}
```

If the health status code cannot be displayed or the browser does not respond, the service may be unavailable due to Oozie process fault. See **Step 13** to rectify the fault.

Step 3 Perform the operations based on the error code. For details, see **Table 1-5**.

Table 1-5 Oozie service health status code

Status Code	Description	Error Cause	Solution
0	The service is running properly.	None	None
18002	The DBService service is abnormal.	Oozie fails to connect to DBService or the data stored in DBService is damaged.	See **Step 4**.
18003	The HDFS service is abnormal.	Oozie fails to connect to HDFS or the data stored in HDFS is damaged.	See **Step 7**.
18005	The MapReduce service is abnormal.	The Yarn service is abnormal.	See **Step 11**.

Check the DBService service.

Step 4 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services**, and check whether the DBService service is running properly.

- If yes, go to **Step 6**.
- If no, go to **Step 5**.

Step 5 Resolve the problem of DBService based on the alarm help and check whether the Oozie alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 18**.

Step 6 Log in to the Oozie database to check whether the data is complete.

1. Log in to the active DBService node as user **root**.

   On the FusionInsight Manager page, choose **Cluster** > *Name of the desired cluster* > **Services** > **DBService > Instance** to view the IP address of the active DBservice node.

2. Run the following command to log in to the Oozie database:

   su - omm

   source ${BIGDATA_HOME}/FusionInsight_BASE_8.3.1/install/FusionInsight-dbservice-2.7.0/.dbservice_profile

   gsql -U compdbuser -W *compdbuser user password* **-p 20051 -d oozie**

3. After the login is successful, enter **\d** to check whether there are 15 data tables.

   The Oozie service has 15 data tables by default. If these data tables are deleted or the table structure is modified, the Oozie service may be

unavailable. Contact the technical support to back up the data and perform restoration.

Check the HDFS service.

Step 7 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services**, and check whether the HDFS service is running properly.

- If yes, go to **Step 9**.
- If no, go to **Step 8**.

Step 8 Resolve the problem of HDFS based on the alarm help and check whether the Oozie alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 18**.

Step 9 Log in to HDFS to check whether the Oozie file directory structure is complete.

1. Download and install an HDFS client. For details, see "Installing a Client" in the *MapReduce Service (MRS) 3.3.1-LTS User Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Usage Guide (for Huawei Cloud Stack 8.3.1)*.
2. Log in to the client node as user **root** and run the following commands to check whether **/user/oozie/share** exists.

   If the cluster uses the security mode, perform security authentication.

   kinit admin

   hdfs dfs -ls /user/oozie/share

- If yes, go to **Step 18**.
- If no, go to **Step 10**.

Step 10 In the Oozie client installation directory, manually upload the share directory to **/user/oozie** in HDFS, and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 18**.

Check the Yarn and MapReduce service.

Step 11 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* > **Services**, and check whether the Yarn and MapReduce services are running properly.

- If yes, go to **Step 18**.
- If no, go to **Step 12**.

Step 12 Resolve the problem of Yarn and MapReduce based on the alarm help and check whether the Oozie alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 18**.

Check the Oozie process.

Step 13 Log in to each node of Oozie as user **root**.

Step 14 Run the **ps -ef | grep oozie** command to check whether the Oozie process exists.

- If yes, go to **Step 15**.
- If no, go to **Step 18**.

Step 15 Collect fault information in **prestartDetail.log**, **oozie.log**, and **catalina.out** in the Oozie log directory **/var/log/Bigdata/oozie**. If the alarm is not caused by manual misoperation, go to **Step 16**.

Check the Nodeagent process.

Step 16 Log in to each node of Oozie as user **root**. Run the **ps -ef | grep nodeagent** command to check whether the Nodeagent process exists.

- If yes, go to **Step 17**.
- If no, go to **Step 18**.

Step 17 Run the **kill -9** *The process ID of nodeagent* command, wait 10 minutes, and check whether alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 18**.

Step 18 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.161 ALM-17004 Oozie Heap Memory Usage Exceeds the Threshold

Alarm Description

The system checks the heap memory usage of the Oozie service every 60 seconds. The alarm is generated when the heap memory usage of a Metadata instance exceeds the threshold (95% of the maximum memory). The alarm is cleared when the heap memory usage is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
17004	Major	Quality of service	Tenant plane	Oozie	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger condition	Specifies the threshold for triggering the alarm.

Impact on the System

The heap memory overflow may cause a service breakdown. After the service breaks down, the Oozie service cannot be used to schedule tasks.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Possible Causes

The heap memory of the Oozie instance is overused or the heap memory is inappropriately allocated.

Handling Procedure

Check heap memory usage.

Step 1 On the FusionInsight Manager portal, choose **O&M > Alarm > Alarms** > **Oozie Heap Memory Usage Exceeds the Threshold** > **Location**. Check the IP address of the instance involved in this alarm.

Step 2 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* > **Services** > **Oozie** > **Instance**. Click the instance for which the alarm is generated to go to the page for the instance. Click the drop-down menu in the chart area and choose **Customize** > **Memory** > **Oozie Heap Memory Resource Percentage**. Click **OK**.

Step 3 Check whether the used heap memory of Oozie reaches the threshold (the default value is 95% of the maximum heap memory) specified for Oozie.

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* > **Services** > **Oozie** > **Configurations > All Configurations**. Set Search **GC_OPTS** in the search box. Increase the value of **-Xmx** as required, and click **Save** > **OK**.

NOTE

Suggestions on GC parameter settings for Oozie:

You are advised to set **-Xms** and **-Xmx** to the same value to prevent adverse impact on performance when JVM dynamically adjusts the heap memory size.

Step 5 Restart the affected services or instances and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On the FusionInsight Manager portal, choose **O&M** > **Log** > **Download**.

Step 7 Select **Oozie** in the required cluster from the **Service**.

Step 8 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.162 ALM-17005 Oozie Non Heap Memory Usage Exceeds the Threshold

Alarm Description

The system checks the non heap memory usage of Oozie every 30 seconds. This alarm is reported if the non heap memory usage of Oozie exceeds the threshold (80%). This alarm is cleared if the non heap memory usage is lower than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
17005	Major	Quality of service	Tenant plane	Oozie	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

The service may break down and the Oozie service cannot be used to schedule tasks.

Possible Causes

The non-heap memory of the Oozie instance is overused or the non-heap memory is inappropriately allocated.

Handling Procedure

Check non-heap memory usage.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** > **Oozie Non Heap Memory Usage Exceeds the Threshold**. On the displayed page, check the location information of the alarm. Check the name of the instance host for which the alarm is generated.

Step 2 On FusionInsight Manager, choose **Cluster** > *Name of the target cluster* > **Services** > **Oozie** and click the **Instance** tab. On the displayed page, select the role corresponding to the host name for which the alarm is generated and select **Customize** from the drop-down list in the upper right corner of the chart area. Choose **Memory** and select **Oozie Non Heap Memory Resource Percentage**. Click **OK**.

Step 3 Check whether the non-heap memory used by Oozie reaches the threshold (80% of the maximum non-heap memory by default).

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On FusionInsight Manager, choose **Cluster** > *Name of the target cluster* > **Services** > **Oozie** and click the **Configurations** and then **All Configurations**. On the displayed page, search for the **GC_OPTS** parameter in the search box and

check whether it contains **-XX: MaxMetaspaceSize**. If yes, increase the value of **-XX: MaxMetaspaceSize** based on the site requirements. If no, manually add **-XX: MaxMetaspaceSize** and set its value to 1/8 of the value of **-Xmx**. Click **Save**, and then click **OK**

NOTE

JDK1.8 does not support the **MaxPermSize** parameter.

Suggestions on GC parameter settings for Oozie:

Set the value of **-XX:MaxMetaspaceSize** to 1/8 of the value of **-Xmx**. For example, if **-Xmx** is set to 2 GB, **-XX:MaxMetaspaceSize** is set to 256 MB. If **-Xmx** is set to 4 GB, **-XX:MaxMetaspaceSize** is set to 512 MB.

Step 5 Restart the affected services or instances and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect the fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **Oozie** for the target cluster.

Step 8 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.163 ALM-17006 Oozie Direct Memory Usage Exceeds the Threshold

Alarm Description

The system checks the direct memory usage of the Oozie service every 30 seconds. The alarm is generated when the direct memory usage of an Oozie instance exceeds the threshold (80% of the maximum memory). The alarm is cleared when the direct memory usage of Oozie is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
17006	Major	Quality of service	Tenant plane	Oozie	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger condition	Specifies the threshold for triggering the alarm.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

The direct memory overflow may cause a service breakdown. After the service breaks down, the Oozie service cannot be used to schedule tasks.

Possible Causes

The direct memory of the Oozie instance is overused or the direct memory is inappropriately allocated.

Handling Procedure

Check direct memory usage.

Step 1 On the FusionInsight Manager portal, choose **O&M** > **Alarm** > **Alarms** > **Oozie Direct Memory Usage Exceeds the Threshold** > **Location**. Check the IP address of the instance involved in this alarm.

Step 2 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* > **Services** > **Oozie** > **Instance**. Click the instance for which the alarm is generated to go to the page for the instance. Click the drop-down menu in the chart area and choose **Customize** > **Memory** > **Oozie Direct Buffer Resource Percentage**. Click **OK**.

Step 3 Check whether the used direct memory of Oozie reaches the threshold (the default value is 80% of the maximum direct memory) specified for Oozie.

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* > **Services** > **Oozie** > **Configurations**. Click **All Configurations**. Search **GC_OPTS** in the search box. Increase the value of **-XX:MaxDirectMemorySize** as required, and click **Save**. Click **OK**.

NOTE

Suggestions on GC parameter settings for Oozie:

You are advised to set the value of **-XX:MaxDirectMemorySize** to 1/4 of the value of **-Xmx**. For example, if **-Xmx** is set to 4 GB, **-XX:MaxDirectMemorySize** is set to 1024 MB. If **-Xmx** is set to 2 GB, **-XX:MaxDirectMemorySize** is set to 512 MB. It is recommended that the value of **-XX:MaxDirectMemorySize** be greater than or equal to 512 MB.

Step 5 Restart the affected services or instances and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On the FusionInsight Manager portal, choose **O&M** > **Log** > **Download**.

Step 7 Select **Oozie** in the required cluster from the **Service** drop-down list.

Step 8 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.164 ALM-17007 Garbage Collection (GC) Time of the Oozie Process Exceeds the Threshold

Alarm Description

The system checks GC time of the Oozie process every 60 seconds. The alarm is generated when GC time of the Oozie process exceeds the threshold (default value: **12 seconds**). The alarm is cleared when GC time is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
17007	Critical (default threshold: 20000ms) Major (default threshold: 12000ms)	Quality of service	Tenant plane	Oozie	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.

Type	Parameter	Description
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger condition	Specifies the threshold for triggering the alarm.

Impact on the System

Oozie scheduling task responds slowly until the service is unavailable.

Possible Causes

The heap memory of the Oozie instance is overused or the heap memory is inappropriately allocated.

Handling Procedure

Check GC time.

Step 1 On the FusionInsight Manager portal, choose **O&M** > **Alarm** > **Alarms** > **Garbage Collection (GC) Time of the Oozie Process Exceeds the Threshold** > **Location**. Check the IP address of the instance involved in this alarm.

Step 2 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* > **Services** > **Oozie** > **Instance**. Click the instance for which the alarm is generated to go to the page for the instance. Click the drop-down menu in the

chart area and choose **Customize** > **GC** > **Garbage Collection (GC) Time of Oozie**. Click **OK**.

Step 3 Check whether GC time of the Oozie process every second exceeds the threshold (default value: **12 seconds**).

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* > **Services** > **Oozie** > **Configurations**. Click **All Configurations**. Search **GC_OPTS** in the search box. Increase the value of **-Xmx** as required, and click **Save**. Click **OK**.

NOTE

Suggestions on GC parameter settings for Oozie:

You are advised to set **-Xms** and **-Xmx** to the same value to prevent adverse impact on performance when JVM dynamically adjusts the heap memory size.

Step 5 Restart the affected services or instances and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On the FusionInsight Manager portal, choose **O&M** > **Log** > **Download**.

Step 7 Select **Oozie** in the required cluster from the **Service** drop-down list.

Step 8 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.165 ALM-17008 Abnormal Connection Between Oozie and ZooKeeper

Alarm Description

In HA mode, Oozie depends on ZooKeeper. This alarm is generated when the connection between Oozie and ZooKeeper is abnormal for three consecutive times.

This alarm is cleared when the connection between Oozie and ZooKeeper becomes normal.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
17008	Minor	Error handling	Tenant plane	Oozie	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

Running scheduling tasks are blocked and new scheduling tasks cannot be submitted. In HA mode, the Oozie service will restart if this alarm is reported.

Possible Causes

- The ZooKeeper service is abnormal.
- Oozie fails to connect to ZooKeeper.

Handling Procedure

Check the ZooKeeper service status.

Step 1 In the service list on FusionInsight Manager, check whether **Running Status** of ZooKeeper is **Normal**.

- If yes, go to **Step 5**.
- If no, go to **Step 2**.

Step 2 In the alarm list, check whether **ALM-13000 ZooKeeper Service Unavailable** is reported.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 Rectify the fault by performing the operations provided for **ALM-13000 ZooKeeper Service Unavailable**.

Step 4 Wait for several minutes and check whether the alarm **Abnormal Connection Between Oozie and ZooKeeper** is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check the connectivity between Oozie and ZooKeeper.

Step 5 Log in to FusionInsight Manager, choose **O&M** > **Log** > **Online Search**, select the Oozie service, and search for the keyword **[Oozie Alarm Enhancement] [ZooKeeper]** in the log. View the cause in the log, and rectify the fault. In the alarm list, check whether the alarm **Abnormal Connection Between Oozie and ZooKeeper** is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Select **Oozie** for **Service** and click **OK**.

Step 8 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.166 ALM-17009 Abnormal Connection Between Oozie and DBService

Alarm Description

Oozie depends on DBService. After a task is submitted, the system checks DBService connectivity. This alarm is generated when the service fails the check for 10 consecutive times.

This alarm is cleared when the connection between Oozie and DBService becomes normal.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
17009	Minor	Error handling	Tenant plane	Oozie	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

Running scheduling tasks are blocked and new scheduling tasks cannot be submitted.

Possible Causes

- The DBService service is abnormal.
- Oozie fails to connect to DBService.

Handling Procedure

Check the DBService status.

Step 1 In the service list on FusionInsight Manager, check whether **Running Status** of DBService is **Normal**.

- If yes, go to **Step 5**.
- If no, go to **Step 2**.

Step 2 In the alarm list, check whether **ALM-27001 DBService Service Unavailable** is reported.

- If yes, go to **Step 3**.

- If no, go to **Step 5**.

Step 3 Rectify the fault by performing the operations provided for **ALM-27001 DBService Service Unavailable**.

Step 4 Wait for several minutes and check whether the alarm **Abnormal Connection Between Oozie and DBService** is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check the connectivity between Oozie and DBService.

Step 5 Log in to FusionInsight Manager, choose **O&M** > **Log** > **Online Search**, select the Oozie service, and search for the keyword **[Oozie Alarm Enhancement][DB Service]** in the log. View the cause in the log, and rectify the fault. In the alarm list, check whether the alarm **Abnormal Connection Between Oozie and DBService** is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Select **Oozie** for **Service** and click **OK**.

Step 8 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.167 ALM-17010 Abnormal Connection Between Oozie and HDFS

Alarm Description

Oozie depends on HDFS. After a task is submitted, the system checks HDFS connectivity. This alarm is generated when the service fails the check for 3 consecutive times.

This alarm is cleared when the connection between Oozie and HDFS becomes normal.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
17010	Minor	Error handling	Tenant plane	Oozie	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

Running scheduling tasks are blocked and new scheduling tasks cannot be submitted.

Possible Causes

The HDFS service restarts, there is a fault, or the network connectivity is abnormal.

Handling Procedure

Check the HDFS service status.

Step 1 In the service list on FusionInsight Manager, check whether **Running Status** of HDFS is **Normal**.

- If yes, go to **Step 5**.
- If no, go to **Step 2**.

Step 2 In the alarm list, check whether the "ALM-14000 HDFS Service Unavailable" alarm is generated.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 Rectify the fault by performing the operations provided for **ALM-14000 HDFS Service Unavailable**.

Step 4 Wait for several minutes and check whether the alarm **Abnormal Connection Between Oozie and HDFS** is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check the connectivity between Oozie and HDFS.

Step 5 Log in to FusionInsight Manager, choose **O&M** > **Log** > **Online Search**, select the Oozie service, and search for the keyword **[Oozie Alarm Enhancement][HDFS]** in the log. View the cause in the log, and rectify the fault. In the alarm list, check whether the alarm **Abnormal Connection Between Oozie and HDFS** is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Select **Oozie** for **Service** and click **OK**.

Step 8 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.168 ALM-17011 Abnormal Connection Between Oozie and Yarn

Alarm Description

Oozie depends on Yarn. After a task is submitted, the system checks Yarn connectivity. This alarm is generated when the service fails the check for 5 consecutive times.

This alarm is cleared when the connection between Oozie and Yarn becomes normal.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
17011	Minor	Error handling	Tenant plane	Oozie	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

Running scheduling tasks are blocked and new scheduling tasks cannot be submitted.

Possible Causes

- The Yarn service is abnormal.
- The connection between Oozie and Yarn is abnormal.

Handling Procedure

Check the YARN service status.

Step 1 In the service list on FusionInsight Manager, check whether **Running Status** of Yarn is **Normal**.

- If yes, go to **Step 5**.
- If no, go to **Step 2**.

Step 2 In the alarm list, check whether **ALM-18000 YARN Service Unavailable** is generated.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 Rectify the fault by performing the operations provided for **ALM-18000 Yarn Service Unavailable**.

Step 4 Wait for several minutes and check whether the alarm **Abnormal Connection Between Oozie and Yarn** is cleared.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check the connectivity between Oozie and Yarn.

Step 5 Log in to FusionInsight Manager, choose **O&M** > **Log** > **Online Search**, select the Oozie service, and search for the keyword **[Oozie Alarm Enhancement][Yarn]** in the log. View the cause in the log, and rectify the fault. In the alarm list, check whether the alarm **Abnormal Connection Between Oozie and Yarn** is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Select **Oozie** for **Service** and click **OK**.

Step 8 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.169 ALM-18000 Yarn Service Unavailable

Alarm Description

This alarm is generated when the Yarn service is unavailable. The alarm module checks the Yarn service status every 60 seconds.

The alarm is cleared when the Yarn service recovers.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
18000	Critical	Error handling	Tenant plane	Yarn	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm is generated.
	HostName	Specifies the host for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

The cluster cannot provide Yarn services. Users cannot run new applications. Submitted applications cannot be run.

Possible Causes

- The ZooKeeper service is abnormal.
- The HDFS service is abnormal.
- There is no active ResourceManager instance in the Yarn cluster.

- All the NodeManagers in the Yarn cluster are abnormal.

Handling Procedure

Check ZooKeeper service status.

Step 1 On the FusionInsight Manager, check whether the alarm list contains **ALM-13000 ZooKeeper Service Unavailable**.

- If yes, go to **Step 2**.
- If no, go to **Step 3**.

Step 2 Rectify the fault by following the steps provided in **ALM-13000 ZooKeeper Service Unavailable**, and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 3**.

Check the HDFS service status.

Step 3 On the FusionInsight Manager, check whether the alarm list contains the HDFS alarms.

- If yes, go to **Step 4**.
- If no, go to **Step 5**.

Step 4 Choose **O&M > Alarm > Alarms**, handle HDFS alarms based on the alarm help, and check whether the Yarn alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check the ResourceManager status in the Yarn cluster.

Step 5 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **Yarn**.

Step 6 In **Dashboard**, check whether there is an active ResourceManager instance in the Yarn cluster.

- If yes, go to **Step 7**.
- If no, go to **Step 10**.

Check the NodeManager node status in the Yarn cluster.

Step 7 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **Yarn** > **Instance**.

Step 8 Query NodeManager **Running Status**, and check whether there are unhealthy nodes.

- If yes, go to **Step 9**.
- If no, go to **Step 10**.

Step 9 Rectify the fault by following the steps provided in **ALM-18002 NodeManager Heartbeat Lost** or **ALM-18003 NodeManager Unhealthy**. After the fault is rectified, check whether the Yarn alarm is cleared.

- If yes, no further action is required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If no, go to **Step 10**.

Collect fault information.

Step 10 On the FusionInsight Manager portal of the active cluster, choose **O&M** > **Log** > **Download**.

Step 11 Select **Yarn** in the required cluster from the **Service**.

Step 12 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 13 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.170 ALM-18002 NodeManager Heartbeat Lost

Alarm Description

The system checks the number of lost NodeManager nodes every 30 seconds, and compares the number with the threshold. The Number of Lost Nodes indicator has a default threshold. The alarm is generated when the value of Number of Lost Nodes exceeds the threshold.

To change the threshold, on FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Yarn**. On the displayed page, choose **Configurations** > **All Configurations**, and change the value of **yarn.nodemanager.lost.alarm.threshold**. You do not need to restart Yarn to make the change take effect.

The default threshold is 0. The alarm is generated when the number of lost nodes exceeds the threshold, and is cleared when the number of lost nodes is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
18002	Major	Error handling	Tenant plane	Yarn	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm is generated.
	HostName	Specifies the host for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Lost Host	Specifies the list of hosts with lost nodes.

Impact on the System

- The lost NodeManager node cannot provide the Yarn service.
- The number of containers decreases, so the cluster performance deteriorates.

Possible Causes

- NodeManager is forcibly deleted without decommission.

- All the NodeManager instances are stopped or the NodeManager process is faulty.
- The host where the NodeManager node resides is faulty.
- The network between the NodeManager and ResourceManager is disconnected or busy.

Handling Procedure

Check the NodeManager status.

Step 1 On the FusionInsight Manager, and choose **O&M** > **Alarm** > **Alarms**. Click ⌄ before the alarm and obtain lost nodes in **Additional Information**.

Step 2 Check whether the lost nodes are hosts that have been manually deleted without decommission.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 After the setting, Choose **Cluster** > *Name of the desired cluster* > **Services** > **Yarn**. On the displayed page, choose **Configurations** > **All Configurations**. Search for **yarn.nodemanager.lost.alarm.threshold** and change its value to the number of hosts that are not out of service and proactively deleted. After the setting, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 4**.

Step 4 Manually clear the alarm. Note that decommission must be performed before deleting hosts.

Step 5 On the FusionInsight Manager portal, choose **Hosts**, and check whether the nodes obtained in **Step 1** are healthy.

- If yes, go to **Step 7**.
- If no, go to **Step 6**.

Step 6 Rectify the node fault based on **ALM-12006 NodeAgent Process Is Abnormal** and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Check the process status.

Step 7 On the FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Yarn** > **Instance**, and check whether there are NodeManager instances whose status is not **Good**.

- If yes, go to **Step 10**.
- If no, go to **Step 8**.

Step 8 Check whether the NodeManager instance is deleted.

- If yes, go to **Step 9**.
- If no, go to **Step 11**.

Step 9 Restart the active and standby ResourceManager instances, and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 13**.

Check the instance status.

Step 10 Select NodeManager instances which running state is not **Normal** and restart them. Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 11**.

Check the network status.

Step 11 Log in to the management node, **ping** the IP address of the lost NodeManager node to check whether the network is disconnected or busy.

- If yes, go to **Step 12**.
- If no, go to **Step 13**.

Step 12 Rectify the network, and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 13**.

Collect fault information.

Step 13 On the FusionInsight Manager in the active cluster, choose **O&M** > **Log** > **Download**.

Step 14 Select **Yarn** in the required cluster from the **Service**.

Step 15 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 16 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.171 ALM-18003 NodeManager Unhealthy

Alarm Description

The system checks the number of unhealthy NodeManager nodes every 30 seconds, and compares the number with the threshold. The Unhealthy Nodes indicator has a default threshold. This alarm is generated when the value of the Unhealthy Nodes indicator exceeds the threshold.

To change the threshold, on FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Yarn**. On the displayed page, choose **Configurations** > **All Configurations**, and change the value of **yarn.nodemanager.unhealthy.alarm.threshold**. You do not need to restart Yarn to make the change take effect.

The default threshold is 0. The alarm is generated when the number of unhealthy nodes exceeds the threshold, and is cleared when the number of unhealthy nodes is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
18003	Major	Error handling	Tenant plane	Yarn	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm is generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	HostName	Specifies the host for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Unhealthy Host	Specifies the list of hosts with unhealthy nodes.

Impact on the System

- The faulty NodeManager node cannot provide the Yarn service.
- The number of containers decreases, so the cluster performance deteriorates.

Possible Causes

- The hard disk space of the host where the NodeManager node resides is insufficient.
- User **omm** does not have the permission to access a local directory on the NodeManager node.

Handling Procedure

Check the hard disk space of the host.

Step 1 On the FusionInsight Manager, and choose **O&M** > **Alarm** > **Alarms**. Click ⌄ before the alarm and obtain unhealthy nodes in **Additional Information**.

Step 2 Choose **Cluster** > *Name of the desired cluster* > **Services** > **Yarn** > **Instance**, select the NodeManager instance corresponding to the host, choose **Instance Configurations** > **All Configurations** and view disks corresponding to **yarn.nodemanager.local-dirs** and **yarn.nodemanager.log-dirs**.

Step 3 Choose **O&M** > **Alarm** > **Alarms**. In the alarm list, check whether the related disk has the alarm **ALM-12017 Insufficient Disk Capacity**.

- If yes, go to **Step 4**.
- If no, go to **Step 5**.

Step 4 Rectify the disk fault based on **ALM-12017 Insufficient Disk Capacit** and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Step 5 Choose **Hosts** > *Name of the desired host* . On the **Dashboard** page, check the disk usage of the corresponding partition. Check whether the percentage of the used space of the mounted disk exceeds the value of **yarn.nodemanager.disk-health-checker.max-disk-utilization-per-disk-percentage**

- If yes, go to **Step 6**.
- If no, go to **Step 7**.

Step 6 Reduce the disk usage to less than the value of **yarn.nodemanager.disk-health-checker.max-disk-utilization-per-disk-percentage**, wait for 10 to 20 minutes, and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Check the access permission of the local directory on each NodeManager node.

Step 7 Obtain the NodeManager directory viewed in **Step 2**, log in to each NodeManager node as user **root**, and go to the obtained directory.

Step 8 Run the **ll** command to check whether the permission of the **localdir** and **containerlogs** folders is **755** and whether **User:Group** is **omm:ficommon**.

- If yes, no further action is required.
- If no, go to **Step 9**.

Step 9 Run the following command to set the permission to **755** and **User:Group** to **omm:ficommon**:

chmod 755 *<folder_name>*

chown omm:ficommon *<folder_name>*

Step 10 Wait for 10 to 20 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 11**.

Collect fault information.

Step 11 On the FusionInsight Manager in the active cluster, choose **O&M** > **Log** > **Download**.

Step 12 Select **Yarn** in the required cluster from the **Service**.

Step 13 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 14 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.172 ALM-18008 Heap Memory Usage of ResourceManager Exceeds the Threshold

Alarm Description

The system checks the heap memory usage of Yarn ResourceManager every 30 seconds and compares the actual usage with the threshold. The alarm is generated when the heap memory usage of Yarn ResourceManager exceeds the threshold.

Users can choose **O&M > Alarm > Thresholds** > *Name of the desired cluster* > **Yarn** to change the threshold.

When the **Trigger Count** is 1, this alarm is cleared when the heap memory usage of Yarn ResourceManager is less than or equal to the threshold. When the **Trigger Count** is greater than 1, this alarm is cleared when the heap memory usage of Yarn ResourceManager is less than or equal to 95% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
18008	Critical (default threshold is 95% of the maximum memory size.) Major (default threshold is 90% of maximum memory)	Quality of service	Tenant plane	Yarn	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm is generated.
	HostName	Specifies the host for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

When the heap memory usage of Yarn ResourceManager is overhigh, the performance of Yarn task submission and operation is affected. In addition, a memory overflow may occur so that the Yarn service is unavailable.

Possible Causes

The heap memory of the Yarn ResourceManager instance on the node is overused or the heap memory is inappropriately allocated. As a result, the usage exceeds the threshold.

Handling Procedure

Check the heap memory usage.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 1 On the FusionInsight Manager portal, choose **O&M > Alarm > Alarms** > **Heap Memory Usage of Yarn ResourceManager Exceeds the Threshold** > **Location**. Check the HostName of the instance for which the alarm is generated.

Step 2 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* **> Services** > **Yarn** > **Instance** > **ResourceManager** (Indicates the host name of the instance for which the alarm is generated)**.** Click the drop-down menu in the upper right corner of **Chart**, choose **Customize** > **ResourceManager > Percentage of Used Memory of the ResourceManager**. Check the heap memory usage.

Step 3 Check whether the used heap memory of ResourceManager reaches 95% of the maximum heap memory specified for ResourceManager.

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* **> Services** > **Yarn** > **Configurations** > **All Configurations** > **ResourceManager** > **System**. Increase the value of **GC_OPTS** parameter as required, click **Save**. Restart the role instance.

NOTE

The mapping between the number of NodeManager instances in a cluster and the memory size of ResourceManager is as follows:

- If the number of NodeManager instances in the cluster reaches 100, the recommended JVM parameters of the ResourceManager instance are as follows: -Xms4G -Xmx4G -XX:NewSize=512M -XX:MaxNewSize=1G
- If the number of NodeManager instances in the cluster reaches 200, the recommended JVM parameters of the ResourceManager instance are as follows: -Xms6G -Xmx6G -XX:NewSize=512M -XX:MaxNewSize=1G
- If the number of NodeManager instances in the cluster reaches 500, the recommended JVM parameters of the ResourceManager instance are as follows: -Xms10G -Xmx10G -XX:NewSize=1G -XX:MaxNewSize=2G
- If the number of NodeManager instances in the cluster reaches 1000, the recommended JVM parameters of the ResourceManager instance are as follows: -Xms20G -Xmx20G -XX:NewSize=1G -XX:MaxNewSize=2G
- If the number of NodeManager instances in the cluster reaches 2000, the recommended JVM parameters of the ResourceManager instance are as follows: -Xms40G -Xmx40G -XX:NewSize=2G -XX:MaxNewSize=4G
- If the number of NodeManager instances in the cluster reaches 3000, the recommended JVM parameters of the ResourceManager instance are as follows: -Xms60G -Xmx60G -XX:NewSize=2G -XX:MaxNewSize=4G
- If the number of NodeManager instances in the cluster reaches 4000, the recommended JVM parameters of the ResourceManager instance are as follows: -Xms80G -Xmx80G -XX:NewSize=2G -XX:MaxNewSize=4G
- If the number of NodeManager instances in the cluster reaches 5000, the recommended JVM parameters of the ResourceManager instance are as follows: -Xms100G -Xmx100G -XX:NewSize=3G -XX:MaxNewSize=6G

Step 5 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On the FusionInsight Manager portal, choose **O&M** > **Log > Download**.

Step 7 Select the following node in the required cluster from the **Service**.

- NodeAgent
- Yarn

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.173 ALM-18009 Heap Memory Usage of JobHistoryServer Exceeds the Threshold

Alarm Description

The system checks the heap memory usage of Mapreduce JobHistoryServer every 30 seconds and compares the actual usage with the threshold. The alarm is generated when the heap memory usage of Mapreduce JobHistoryServer exceeds the threshold.

Users can choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **MapReduce** to change the threshold.

When the **Trigger Count** is 1, this alarm is cleared when the heap memory usage of MapReduce JobHistoryServer is less than or equal to the threshold. When the **Trigger Count** is greater than 1, this alarm is cleared when the heap memory usage of MapReduce JobHistoryServer is less than or equal to the threshold.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
18009	Critical (default threshold is 95% of the maximum memory size.) Major (default threshold is 90% of maximum memory)	Quality of service	Tenant plane	MapReduce	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	RoleName	Specifies the role for which the alarm is generated.
	HostName	Specifies the host for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

When the heap memory usage of Mapreduce JobHistoryServer is overhigh, the performance of Mapreduce log archiving is affected. In addition, a memory overflow may occur so that the Yarn service is unavailable.

Possible Causes

The heap memory of the Mapreduce JobHistoryServer instance on the node is overused or the heap memory is inappropriately allocated. As a result, the usage exceeds the threshold.

Handling Procedure

Check the memory usage.

Step 1 On the FusionInsight Manager portal, choose **O&M > Alarm > Alarms** > **ALM-18009 Heap Memory Usage of MapReduce JobHistoryServer Exceeds the Threshold** > **Location**. Check the HostName of the instance for which the alarm is generated.

Step 2 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* **> Services** > **Mapreduce** > **Instance** > **JobHistoryServer.** Click the drop-down menu in the upper right corner of **Chart**, choose **Customize** > **JobHistoryServer heap memory usage statistics**. JobHistoryServer indicates the corresponding HostName of the instance for which the alarm is generated. Check the heap memory usage.

Step 3 Check whether the used heap memory of JobHistoryServer reaches 95% of the maximum heap memory specified for JobHistoryServer.

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* **> Services** > **Mapreduce** > **Configurations** > **All Configurations** >

JobHistoryServer > **System**. Increase the value of **GC_OPTS** parameter as required, click **Save**. Click **OK** and restart the role instance.

NOTE

The mapping between the number of historical tasks (10000) and the memory of JobHistoryServer is as follows:

-Xms30G -Xmx30G -XX:NewSize=1G -XX:MaxNewSize=2G

Step 5 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On the FusionInsight Manager portal, choose **O&M** > **Log** > **Download**.

Step 7 Select the following node in the required cluster from the **Service**.

- NodeAgent
- Mapreduce

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.174 ALM-18010 ResourceManager GC Time Exceeds the Threshold

Alarm Description

The system checks the garbage collection (GC) duration of the ResourceManager process every 60 seconds. This alarm is generated when the GC duration exceeds the threshold.

This alarm is cleared when the GC duration is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
18010	Critical (default threshold: 15000ms) Major (default threshold: 10000ms)	Quality of service	Tenant plane	Yarn	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm is generated.
	HostName	Specifies the host for which the alarm is generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

A long GC duration of the ResourceManager process may interrupt the services.

Possible Causes

The heap memory of the ResourceManager instance is overused or the heap memory is inappropriately allocated. As a result, GCs occur frequently.

Handling Procedure

Check the GC duration.

Step 1 On the FusionInsight Manager portal, choose **O&M > Alarm > Alarms** > **ALM-18010 ResourceManager GC Time Exceeds the Threshold** > **Location** to check the IP address of the instance for which the alarm is generated.

Step 2 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* **> Services** > **Yarn** > **Instance** > **ResourceManager (IP address for which the alarm is generated)**. Click the drop-down menu in the upper right corner of **Chart**, choose **Customize** > **Garbage Collection (GC) Time of ResourceManager** to check the GC duration statistics of the Broker process collected every minute.

Step 3 Check whether the GC duration of the ResourceManager process collected every minute exceeds the threshold.

- If yes, go to **Step 4**.
- If no, go to **Step 7**.

Step 4 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services** > **Yarn** > **Configurations** > **All Configurations** > **ResourceManager** > **System** to increase the value of **GC_OPTS** parameter as required.

NOTE

The mapping between the number of NodeManager instances in a cluster and the memory size of ResourceManager is as follows:

- If the number of NodeManager instances in the cluster reaches 100, the recommended JVM parameters of the ResourceManager instance are as follows: -Xms4G -Xmx4G -XX:NewSize=512M -XX:MaxNewSize=1G
- If the number of NodeManager instances in the cluster reaches 200, the recommended JVM parameters of the ResourceManager instance are as follows: -Xms6G -Xmx6G -XX:NewSize=512M -XX:MaxNewSize=1G
- If the number of NodeManager instances in the cluster reaches 500, the recommended JVM parameters of the ResourceManager instance are as follows: -Xms10G -Xmx10G -XX:NewSize=1G -XX:MaxNewSize=2G
- If the number of NodeManager instances in the cluster reaches 1000, the recommended JVM parameters of the ResourceManager instance are as follows: -Xms20G -Xmx20G -XX:NewSize=1G -XX:MaxNewSize=2G
- If the number of NodeManager instances in the cluster reaches 2000, the recommended JVM parameters of the ResourceManager instance are as follows: -Xms40G -Xmx40G -XX:NewSize=2G -XX:MaxNewSize=4G
- If the number of NodeManager instances in the cluster reaches 3000, the recommended JVM parameters of the ResourceManager instance are as follows: -Xms60G -Xmx60G -XX:NewSize=2G -XX:MaxNewSize=4G
- If the number of NodeManager instances in the cluster reaches 4000, the recommended JVM parameters of the ResourceManager instance are as follows: -Xms80G -Xmx80G -XX:NewSize=2G -XX:MaxNewSize=4G
- If the number of NodeManager instances in the cluster reaches 5000, the recommended JVM parameters of the ResourceManager instance are as follows: -Xms100G -Xmx100G -XX:NewSize=3G -XX:MaxNewSize=6G

Step 5 Save the configuration and restart the ResourceManager instance.

Step 6 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect fault information.

Step 7 On the FusionInsight Manager portal, choose **O&M** > **Log** > **Download**.

Step 8 Select **ResourceManager** in the required cluster from the **Service**.

Step 9 Click edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.175 ALM-18011 NodeManager GC Time Exceeds the Threshold

Alarm Description

The system checks the garbage collection (GC) duration of the NodeManager process every 60 seconds. This alarm is generated when the GC duration exceeds the threshold.

This alarm is cleared when the GC duration is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
18011	Critical (default threshold: 20000ms) Major (default threshold: 12000ms)	Quality of service	Tenant plane	Yarn	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm is generated.
	HostName	Specifies the host for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

A long GC duration of the NodeManager process may interrupt the services.

Possible Causes

The heap memory of the NodeManager instance is overused or the heap memory is inappropriately allocated. As a result, GCs occur frequently.

Handling Procedure

Check the GC duration.

Step 1 On the FusionInsight Manager portal, choose **O&M > Alarm > Alarms** > **ALM-18011 NodeManager GC Time Exceeds the Threshold** > **Location** to check the IP address of the instance for which the alarm is generated.

Step 2 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **Yarn** > **Instance** > **NodeManager (IP address for which the alarm is generated)**. Click the drop-down menu in the upper right corner of **Chart**, choose **Customize** > **Garbage Collection (GC) Time of NodeManager** to check the GC duration statistics of the Broker process collected every minute.

Step 3 Check whether the GC duration of the NodeManager process collected every minute exceeds the threshold.

- If yes, go to **Step 4**.
- If no, go to **Step 7**.

Step 4 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **Yarn** > **Configurations** > **All Configurations** > **NodeManager** > **System** to increase the value of **GC_OPTS** parameter as required.

NOTE

The mapping between the number of NodeManager instances in a cluster and the memory size of NodeManager is as follows:

- If the number of NodeManager instances in the cluster reaches 100, the recommended JVM parameters for NodeManager instances are as follows: -Xms2G -Xmx4G -XX:NewSize=512M -XX:MaxNewSize=1G
- If the number of NodeManager instances in the cluster reaches 200, the recommended JVM parameters for NodeManager instances are as follows: -Xms4G -Xmx4G -XX:NewSize=512M -XX:MaxNewSize=1G
- If the number of NodeManager instances in the cluster reaches 500, the recommended JVM parameters for NodeManager instances are as follows: -Xms8G -Xmx8G -XX:NewSize=1G -XX:MaxNewSize=2G

Step 5 Save the configuration and restart the NodeManager instance.

Step 6 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect fault information.

Step 7 On the FusionInsight Manager portal, choose **O&M** > **Log** > **Download**.

Step 8 Select **NodeManager** in the required cluster from the **Service**.

Step 9 Click edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.176 ALM-18012 JobHistoryServer GC Time Exceeds the Threshold

Alarm Description

The system checks the garbage collection (GC) duration of the JobHistoryServer process every 60 seconds. This alarm is generated when the GC duration exceeds the threshold.

This alarm is cleared when the GC duration is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
18012	Critical (default threshold: 20000ms) Major (default threshold: 12000ms)	Quality of service	Tenant plane	MapReduce	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm is generated.
	HostName	Specifies the host for which the alarm is generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

A long GC duration of the JobHistoryServer process may interrupt the services.

Possible Causes

The heap memory of the JobHistoryServer instance is overused or the heap memory is inappropriately allocated. As a result, GCs occur frequently.

Handling Procedure

Check the GC duration.

Step 1 On the FusionInsight Manager portal, choose **O&M > Alarm > Alarms** > **ALM-18012 JobHistoryServer GC Time Exceeds the Threshold** > **Location** to check the IP address of the instance for which the alarm is generated.

Step 2 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **MapReduce** > **Instance** > **JobHistoryServer (IP address for which the alarm is generated)**. Click the drop-down menu in the upper right corner of **Chart**, choose **Customize** > **Garbage Collection (GC) Time of the JobHistoryServer** to check the GC duration statistics of the Broker process collected every minute.

Step 3 Check whether the GC duration of the JobHistoryServer process collected every minute exceeds the threshold.

- If yes, go to **Step 4**.
- If no, go to **Step 7**.

Step 4 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **MapReduce** > **Configurations** > **All Configurations** > **JobHistoryServer** > **System** to increase the value of **GC_OPTS** parameter as required.

NOTE

The mapping between the number of historical tasks (10000) and the memory of the JobHistoryServer is as follows:

-Xms30G -Xmx30G -XX:NewSize=1G -XX:MaxNewSize=2G

Step 5 Save the configuration and restart the JobHistoryServer instance.

Step 6 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect fault information.

Step 7 On the FusionInsight Manager portal, choose **O&M** > **Log** > **Download**.

Step 8 Select **JobHistoryServer** in the required cluster from the **Service**.

Step 9 Click edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.177 ALM-18013 ResourceManager Direct Memory Usage Exceeds the Threshold

Alarm Description

The system checks the direct memory usage of the Yarn service every 30 seconds. This alarm is generated when the direct memory usage of a ResourceManager instance exceeds the threshold.

The alarm is cleared when the direct memory usage is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
18013	Critical (default threshold is 95% of the maximum memory size.) Major (default threshold is 90% of maximum memory)	Quality of service	Tenant plane	Yarn	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	RoleName	Specifies the role for which the alarm is generated.
	HostName	Specifies the host for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

If the available direct memory of the Yarn service is insufficient, a memory overflow occurs and the service breaks down.

Possible Causes

The direct memory of the ResourceManager instance is overused or the direct memory is inappropriately allocated.

Handling Procedure

Check the direct memory usage.

Step 1 On the FusionInsight Manager portal, choose **O&M > Alarm > Alarms** > **ALM-18013 ResourceManager Direct Memory Usage Exceeds the Threshold** > **Location** to check the IP address of the instance for which the alarm is generated.

Step 2 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **Yarn** > **Instance** > **ResourceManager (IP address for which the alarm is generated)**. Click the drop-down menu in the upper right corner of **Chart**, choose **Customize** > **Memory Usage Status of ResourceManager** to check the direct memory usage.

Step 3 Check whether the used direct memory of ResourceManager reaches 90% of the maximum direct memory specified for ResourceManager by default.

- If yes, go to **Step 4**.
- If no, go to **Step 9**.

Step 4 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **Yarn** > **Configurations** > **All Configurations** > **ResourceManager** > **System** to increase the value of check whether **-XX:MaxDirectMemorySize** exists in the **GC_OPTS** parameter.

- If yes, go to **Step 5**.
- If no, go to **Step 7**.

Step 5 In the **GC_OPTS** parameter, delete **-XX:MaxDirectMemorySize**.

Step 6 Save the configuration and restart the ResourceManager instance.

Step 7 Check whether the **ALM-18008 Heap Memory Usage of ResourceManager Exceeds the Threshold** exists.

- If yes, handle the alarm by referring to **ALM-18008 Heap Memory Usage of ResourceManager Exceeds the Threshold**.
- If no, go to **Step 8**.

Step 8 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Collect fault information.

Step 9 On the FusionInsight Manager portal, choose **O&M** > **Log** > **Download**.

Step 10 Select **ResourceManager** in the required cluster from the **Service**.

Step 11 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.178 ALM-18014 NodeManager Direct Memory Usage Exceeds the Threshold

Alarm Description

The system checks the direct memory usage of the Yarn service every 30 seconds. This alarm is generated when the direct memory usage of a NodeManager instance exceeds the threshold.

The alarm is cleared when the direct memory usage is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
18014	Critical (default threshold is 95% of the maximum memory size.) Major (default threshold is 90% of maximum memory)	Quality of service	Tenant plane	Yarn	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	RoleName	Specifies the role for which the alarm is generated.
	HostName	Specifies the host for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

If the available direct memory of the Yarn service is insufficient, a memory overflow occurs and the service breaks down.

Possible Causes

The direct memory of the NodeManager instance is overused or the direct memory is inappropriately allocated.

Handling Procedure

Check the direct memory usage.

Step 1 On the FusionInsight Manager portal, choose **O&M** > **Alarm > Alarms** > **ALM-18014 NodeManager Direct Memory Usage Exceeds the Threshold** > **Location** to check the IP address of the instance for which the alarm is generated.

Step 2 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **Yarn** > **Instance** > **NodeManager (IP address for which the alarm is generated)**. Click the drop-down menu in the upper right corner of **Chart**, choose **Customize** > **Resource** > **Percentage of Used Memory of the NodeManager** to check the direct memory usage.

Step 3 Check whether the used direct memory of NodeManager reaches 90% of the maximum direct memory specified for NodeManager by default.

- If yes, go to **Step 4**.
- If no, go to **Step 9**.

Step 4 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **Yarn** > **Configurations** > **All Configurations**> **NodeManager** > **System** to check whether "-XX:MaxDirectMemorySize" exists in the **GC_OPTS** parameter.

- If yes, go to **Step 5**.
- If no, go to **Step 7**.

Step 5 In the **GC_OPTS** parameter, delete "-XX:MaxDirectMemorySize".

Step 6 Save the configuration and restart the NodeManager instance.

Step 7 Check whether the **ALM-18018 NodeManager Heap Memory Usage Exceeds the Threshold** exists.

- If yes, handle the alarm by referring to **ALM-18018 NodeManager Heap Memory Usage Exceeds the Threshold**.
- If no, go to **Step 8**.

Step 8 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Collect fault information.

Step 9 On the FusionInsight Manager portal, choose **O&M** > **Log > Download**.

Step 10 Select **NodeManager** in the required cluster from the **Service**.

Step 11 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.179 ALM-18015 JobHistoryServer Direct Memory Usage Exceeds the Threshold

Alarm Description

The system checks the direct memory usage of the MapReduce service every 30 seconds. This alarm is generated when the direct memory usage of a JobHistoryServer instance exceeds the threshold.

The alarm is cleared when the direct memory usage is less than the threshold.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
18015	Critical (default threshold is 95% of the maximum memory size.) Major (default threshold is 90% of maximum memory)	Quality of service	Tenant plane	MapReduce	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	RoleName	Specifies the role for which the alarm is generated.
	HostName	Specifies the host for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

If the available direct memory of the MapReduce service is insufficient, a memory overflow occurs and the service breaks down.

Possible Causes

The direct memory of the JobHistoryServer instance is overused or the direct memory is inappropriately allocated.

Handling Procedure

Check the direct memory usage.

Step 1 On the FusionInsight Manager portal, choose **O&M > Alarm > Alarms** > **ALM-18015 JobHistoryServer Direct Memory Usage Exceeds the Threshold** > **Location** to check the IP address of the instance for which the alarm is generated.

Step 2 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **MapReduce** > **Instance** > **JobHistoryServer (IP address for which the alarm is generated).** Click the drop-down menu in the upper right corner of **Chart**, choose **Customize** > **Memory Usage Status of JobHistoryServer** to check the direct memory usage.

Step 3 Check whether the used direct memory of JobHistoryServer reaches 90% of the maximum direct memory specified for JobHistoryServer by default.

- If yes, go to **Step 4**.
- If no, go to **Step 9**.

Step 4 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **MapReduce** > **Configurations** > **All Configurations** > **JobHistoryServer** > **System** to check whether "-XX:MaxDirectMemorySize" exists in the **GC_OPTS** parameter.

- If yes, go to **Step 5**.
- If no, go to **Step 7**.

Step 5 In the **GC_OPTS** parameter, delete "-XX:MaxDirectMemorySize".

Step 6 Save the configuration and restart the JobHistoryServer instance.

Step 7 Check whether the **ALM-18009 Heap Memory Usage of JobHistoryServer Exceeds the Threshold** exists.

- If yes, handle the alarm by referring to **ALM-18009 Heap Memory Usage of JobHistoryServer Exceeds the Threshold**.
- If no, go to **Step 8**.

Step 8 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Collect fault information.

Step 9 On the FusionInsight Manager portal, choose **O&M** > **Log** > **Download**.

Step 10 Select **JobHistoryServer** in the required cluster from the **Service**.

Step 11 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.180 ALM-18016 Non Heap Memory Usage of ResourceManager Exceeds the Threshold

Alarm Description

The system checks the Non Heap memory usage of Yarn ResourceManager every 30 seconds and compares the actual usage with the threshold. The alarm is generated when the Non Heap memory usage of Yarn ResourceManager exceeds the threshold.

Users can choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Yarn** to change the threshold.

The alarm is cleared when the Non Heap memory usage is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
18016	Critical (default threshold is 95% of the maximum memory size.) Major (default threshold is 90% of maximum memory)	Quality of service	Tenant plane	Yarn	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	RoleName	Specifies the role for which the alarm is generated.
	HostName	Specifies the host for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

When the Non Heap memory usage of Yarn ResourceManager is overhigh, the performance of Yarn task submission and operation is affected. In addition, a memory overflow may occur so that the Yarn service is unavailable.

Possible Causes

The Non Heap memory of the Yarn ResourceManager instance on the node is overused or the Non Heap memory is inappropriately allocated. As a result, the usage exceeds the threshold.

Handling Procedure

Check the Non Heap memory usage.

Step 1 On the FusionInsight Manager portal, choose **O&M > Alarm > Alarms** > **ALM-18016 Non Heap Memory Usage of Yarn ResourceManager Exceeds the Threshold** > **Location**. Check the HostName of the instance for which the alarm is generated.

Step 2 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **Yarn** > **Instance** > **ResourceManager**. Click the drop-down menu in the upper right corner of **Chart**, choose **Customize** > **Percentage of Used Memory of the ResourceManager**. ResourceManager indicates the corresponding HostName of the instance for which the alarm is generated. Check the Non Heap memory usage.

Step 3 Check whether the used Non Heap memory of ResourceManager reaches 90% of the maximum Non Heap memory specified for ResourceManager by default.

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **Yarn** > **Configurations** > **All Configurations** > **ResourceManager** > **System**. Adjust the **GC_OPTS** memory parameter of

ResourceManager. Save the configuration and restart the ResourceManager instance.

NOTE

The mapping between the number of NodeManager instances in a cluster and the memory size of ResourceManager is as follows:

- If the number of NodeManager instances in the cluster reaches 100, the recommended JVM parameters of the ResourceManager instance are as follows: -Xms4G -Xmx4G -XX:NewSize=512M -XX:MaxNewSize=1G
- If the number of NodeManager instances in the cluster reaches 200, the recommended JVM parameters of the ResourceManager instance are as follows: -Xms6G -Xmx6G -XX:NewSize=512M -XX:MaxNewSize=1G
- If the number of NodeManager instances in the cluster reaches 500, the recommended JVM parameters of the ResourceManager instance are as follows: -Xms10G -Xmx10G -XX:NewSize=1G -XX:MaxNewSize=2G
- If the number of NodeManager instances in the cluster reaches 1000, the recommended JVM parameters of the ResourceManager instance are as follows: -Xms20G -Xmx20G -XX:NewSize=1G -XX:MaxNewSize=2G
- If the number of NodeManager instances in the cluster reaches 2000, the recommended JVM parameters of the ResourceManager instance are as follows: -Xms40G -Xmx40G -XX:NewSize=2G -XX:MaxNewSize=4G
- If the number of NodeManager instances in the cluster reaches 3000, the recommended JVM parameters of the ResourceManager instance are as follows: -Xms60G -Xmx60G -XX:NewSize=2G -XX:MaxNewSize=4G
- If the number of NodeManager instances in the cluster reaches 4000, the recommended JVM parameters of the ResourceManager instance are as follows: -Xms80G -Xmx80G -XX:NewSize=2G -XX:MaxNewSize=4G
- If the number of NodeManager instances in the cluster reaches 5000, the recommended JVM parameters of the ResourceManager instance are as follows: -Xms100G -Xmx100G -XX:NewSize=3G -XX:MaxNewSize=6G

Step 5 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On the FusionInsight Manager portal, choose **O&M** > **Log** > **Download**.

Step 7 Select the following node in the required cluster from the **Service**.

- NodeAgent
- Yarn

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.181 ALM-18017 Non Heap Memory Usage of NodeManager Exceeds the Threshold

Alarm Description

The system checks the Non Heap memory usage of Yarn NodeManager every 30 seconds and compares the actual usage with the threshold. The alarm is generated when the Non Heap memory usage of Yarn NodeManager exceeds the threshold.

Users can choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Yarn** to change the threshold.

The alarm is cleared when the Non Heap memory usage is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
18017	Critical (default threshold is 95% of the maximum memory size.) Major (default threshold is 90% of maximum memory)	Quality of service	Tenant plane	Yarn	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm is generated.
	HostName	Specifies the host for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

When the Non Heap memory usage of Yarn NodeManager is overhigh, the performance of Yarn task submission and operation is affected. In addition, a memory overflow may occur so that the Yarn service is unavailable.

Possible Causes

The Non Heap memory of the Yarn NodeManager instance on the node is overused or the Non Heap memory is inappropriately allocated. As a result, the usage exceeds the threshold.

Handling Procedure

Check the Non Heap memory usage.

Step 1 On the FusionInsight Manager portal, choose **O&M > Alarm > Alarms** > **ALM-18017 Non Heap Memory Usage of Yarn NodeManager Exceeds the Threshold** > **Location**. Check the HostName of the instance for which the alarm is generated.

Step 2 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **Yarn** > **Instance** > **NodeManager**. Click the drop-down menu in the upper right corner of **Chart**, choose **Customize** > **Resource** > **Percentage of Used Memory of the NodeManager**. NodeManager indicates the corresponding HostName of the instance for which the alarm is generated. Check the Non Heap memory usage.

Step 3 Check whether the used Non Heap memory of NodeManager reaches 90% of the maximum Non Heap memory specified for NodeManager by default.

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **Yarn** > **Configurations** > **All Configurations** > **NodeManager** > **System**. Adjust the **GC_OPTS** memory parameter of NodeManager, click **Save**, and click **OK,** and restart the role instance.

NOTE

The mapping between the number of NodeManager instances in a cluster and the memory size of NodeManager is as follows:

- If the number of NodeManager instances in the cluster reaches 100, the recommended JVM parameters for NodeManager instances are as follows: -Xms2G -Xmx4G -XX:NewSize=512M -XX:MaxNewSize=1G
- If the number of NodeManager instances in the cluster reaches 200, the recommended JVM parameters for NodeManager instances are as follows: -Xms4G -Xmx4G -XX:NewSize=512M -XX:MaxNewSize=1G
- If the number of NodeManager instances in the cluster reaches 500, the recommended JVM parameters for NodeManager instances are as follows: -Xms8G -Xmx8G -XX:NewSize=1G -XX:MaxNewSize=2G

Step 5 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On the FusionInsight Manager portal, choose **O&M** > **Log > Download**.

Step 7 Select the following node in the required cluster from the **Service**.

- NodeAgent
- Yarn

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.182 ALM-18018 NodeManager Heap Memory Usage Exceeds the Threshold

Alarm Description

The system checks the heap memory usage of Yarn NodeManager every 30 seconds and compares the actual usage with the threshold. The alarm is generated when the heap memory usage of Yarn NodeManager exceeds the threshold.

The alarm is cleared when the heap memory usage is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
18018	Critical (default threshold is 95% of the maximum memory size.) Major (default threshold is 90% of maximum memory)	Quality of service	Tenant plane	Yarn	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm is generated.
	HostName	Specifies the host for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

When the heap memory usage of Yarn NodeManager is overhigh, the performance of Yarn task submission and operation is affected. In addition, a memory overflow may occur so that the Yarn service is unavailable.

Possible Causes

The heap memory of the Yarn NodeManager instance on the node is overused or the heap memory is inappropriately allocated. As a result, the usage exceeds the threshold.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Handling Procedure

Check the heap memory usage.

Step 1 On the FusionInsight Manager portal, choose **O&M > Alarm > Alarms** > **ALM-18018 NodeManager Heap Memory Usage Exceeds the Threshold** > **Location**. Check the HostName of the instance for which the alarm is generated.

Step 2 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **Yarn** > **Instance** > **NodeManager**. Click the drop-down menu in the upper right corner of **Chart**, choose **Customize** > **Resource** > **Percentage of Used Memory of the NodeManager** to check the heap memory usage.

Step 3 Check whether the used heap memory of NodeManager reaches 95% of the maximum heap memory specified for NodeManager.

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **Yarn** > **Configurations** > **All Configurations** > **NodeManager** > **System**. Increase the value of **GC_OPTS** parameter as required, click **Save**, and click **OK**, and restart the role instance.

NOTE

The mapping between the number of NodeManager instances in a cluster and the memory size of NodeManager is as follows:

- If the number of NodeManager instances in the cluster reaches 100, the recommended JVM parameters for NodeManager instances are as follows: -Xms2G -Xmx4G -XX:NewSize=512M -XX:MaxNewSize=1G
- If the number of NodeManager instances in the cluster reaches 200, the recommended JVM parameters for NodeManager instances are as follows: -Xms4G -Xmx4G -XX:NewSize=512M -XX:MaxNewSize=1G
- If the number of NodeManager instances in the cluster reaches 500, the recommended JVM parameters for NodeManager instances are as follows: -Xms8G -Xmx8G -XX:NewSize=1G -XX:MaxNewSize=2G

Step 5 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On the FusionInsight Manager portal, choose **O&M** > **Log > Download**.

Step 7 Select the following node in the required cluster from the **Service**.

- NodeAgent
- Yarn

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.183 ALM-18019 Non Heap Memory Usage of JobHistoryServer Exceeds the Threshold

Alarm Description

The system checks the Non Heap memory usage of MapReduce JobHistoryServer every 30 seconds and compares the actual usage with the threshold. The alarm is generated when the Non Heap memory usage of MapReduce JobHistoryServer exceeds the threshold.

Users can choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **MapReduce** to change the threshold.

The alarm is cleared when the Non Heap memory usage is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
18019	Critical (default threshold is 95% of the maximum memory size.) Major (default threshold is 90% of maximum memory)	Quality of service	Tenant plane	MapReduce	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm is generated.
	HostName	Specifies the host for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

When the Non Heap memory usage of MapReduce JobHistoryServer is overhigh, the performance of MapReduce task submission and operation is affected. In addition, a memory overflow may occur so that the MapReduce service is unavailable.

Possible Causes

The Non Heap memory of the MapReduce JobHistoryServer instance on the node is overused or the Non Heap memory is inappropriately allocated. As a result, the usage exceeds the threshold.

Handling Procedure

Check the Non Heap memory usage.

Step 1 On the FusionInsight Manager portal, choose **O&M > Alarm > Alarms** > **ALM-18019 Non Heap Memory Usage of MapReduce JobHistoryServer Exceeds the Threshold** > **Location**. Check the HostName of the instance for which the alarm is generated.

Step 2 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **MapReduce** > **Instance** > **JobHistoryServer.** Click the drop-down menu in the upper right corner of **Chart**, choose **Customize** > **JobHistoryServer Non Heap memory usage statistics**. JobHistoryServer indicates the corresponding HostName of the instance for which the alarm is generated. Check the Non Heap memory usage.

Step 3 Check whether the used Non Heap memory of JobHistoryServer reaches 90% of the maximum Non Heap memory specified for JobHistoryServer.

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* **> Services** > **MapReduce** > **Configurations** > **All Configurations** > **JobHistoryServer** > **System**. Adjust the **GC_OPTS** memory parameter of the NodeManager, click **Save**, and click **OK,** and restart the role instance.

NOTE

The mapping between the number of historical tasks (10000) and the memory of the JobHistoryServer is as follows:

-Xms30G -Xmx30G -XX:NewSize=1G -XX:MaxNewSize=2G

Step 5 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On the FusionInsight Manager portal, choose **O&M** > **Log > Download**.

Step 7 Select the following node in the required cluster from the **Service**.

- NodeAgent
- MapReduce

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.184 ALM-18020 Yarn Task Execution Timeout

Alarm Description

The system checks MapReduce and Spark tasks (except for permanent JDBC tasks) submitted to Yarn every 15 minutes. This alarm is generated when the task execution time exceeds the timeout duration specified by the user. However, the task can be properly executed. The client timeout parameter of MapReduce is mapreduce.application.timeout.alarm and that of Spark is spark.application.timeout.alarm. The unit is ms.

This alarm is cleared when the task is finished or terminated.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
18020	Minor	Quality of service	Tenant plane	Yarn	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm is generated.
	ApplicationName	Specifies the object (application ID) for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

The alarm persists after task execution times out. However, the task can still be properly executed, so this alarm does not exert any impact on the system.

Possible Causes

- The specified timeout duration is shorter than the required execution time.
- The queue resources for task running are insufficient.
- Task data skew occurs. As a result, some tasks process a large amount of data and take a long time to execute.

Handling Procedure

Check whether the timeout interval is correctly set.

Step 1 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**. The **Alarms** page is displayed.

Step 2 Select the alarm whose ID is **18020**. In the alarm details, view **Location** to obtain the timeout task name and timeout duration.

Step 3 Based on the task name and timeout interval, choose **Cluster** > *Name of the desired cluster* > **Services** > **Yarn** > **ResourceManager (Active)** to log in to the native Yarn page. Then find the task on the native page, check its **StartTime** and calculate the task execution time based on the current system time. Check whether the task execution time exceeds the timeout duration.

- If yes, go to **Step 4**.
- If no, go to **Step 10**.

Step 4 Evaluate the expected task execution time based on the service and compare it with the task timeout interval. If the timeout interval is too short, set the timeout interval (**mapreduce.application.timeout.alarm** or **spark.application.timeout.alarm**) of the client to the task expected execution time. Run the task again and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check whether the queue resources are sufficient.

Step 5 Find the task on the native page and view the queue name of the task. Click **Scheduler** on the left of the native page. On the **Applications Queues** page, find the corresponding queue name and expand the queue details, as shown in the following figure.

Step 6 Check whether the value of **Used Resources** in the queue details is approximately equal to the value of **Max Resources**, which indicates that the resources in the queue submitted by the task have been used up. If the queue resources are insufficient, choose **Tenant Resources** > **Dynamic Resource Plan** > **Resource Distribution Policy** on FusionInsight Manager and increase the value of **Max Resources** for the queue. Run the task again and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Check whether data skew occurs.

Step 7 On the native Yarn page, click *task ID* (for example, **application_1565337919723_0002**) > **Tracking URL:ApplicationMaster** > **job_1565337919723_0002**. The following page is displayed.

Step 8 Choose **Job** > **Map tasks** or **Job** > **Reduce tasks** on the left and check whether the execution time of each Map or Reduce task differs greatly. If yes, task data skew occurs. In this case, you need to balance the task data.

Step 9 Rectify the fault based on the preceding causes and perform the tasks again. Then, check whether the alarm persists.

- If yes, go to **Step 10**.
- If no, no further action is required.

Collect the fault information.

Step 10 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 11 Expand the **Service** drop-down list, and select **Yarn** for the target cluster.

Step 12 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 13 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.185 ALM-18021 Mapreduce Service Unavailable

Alarm Description

The alarm module checks the MapReduce service status every 60 seconds. This alarm is generated when the system detects that the MapReduce service is unavailable.

The alarm is cleared when the MapReduce service recovers.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
18021	Critical	Error handling	Tenant plane	MapReduce	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.

Type	Parameter	Description
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm is generated.
	HostName	Specifies the host for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

The cluster cannot provide the MapReduce service. For example, MapReduce cannot be used to view task logs or the log archive function is unavailable.

Possible Causes

- The JobHistoryServer instance is abnormal.
- The KrbServer service is abnormal.
- The ZooKeeper service abnormal.
- The HDFS service abnormal.
- The Yarn service is abnormal.

Handling Procedure

Check MapReduce service JobHistoryServer instance status.

Step 1 On the FusionInsight Manager home page, choose **Cluster** > *Name of the desired cluster* > **Services** > **MapReduce** > **Instance**.

Step 2 Check whether the running status of JobHistoryServer is **Normal**.

- If yes, go to **Step 11**.
- If no, go to **Step 3**.

Check the KrbServer service status.

Step 3 In the alarm list on FusionInsight Manager, check whether **ALM-25500 KrbServer Service Unavailable** exists.

- If yes, go to **Step 4**.
- If no, go to **Step 5**.

Step 4 Rectify the fault by following the steps provided in **ALM-25500 KrbServer Service Unavailable**, and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check the ZooKeeper service.

Step 5 In the alarm list on FusionInsight Manager, check whether **ALM-13000 ZooKeeper Service Unavailable** exists.

- If yes, go to **Step 6**.
- If no, go to **Step 7**.

Step 6 Rectify the fault by following the steps provided in **ALM-13000 ZooKeeper Service Unavailable**, and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Check the HDFS service status.

Step 7 In the alarm list on FusionInsight Manager, check whether **ALM-14000 HDFS Service Unavailable** exists.

- If yes, go to **Step 8**.
- If no, go to **Step 9**.

Step 8 Rectify the fault by following the steps provided in **ALM-14000 HDFS Service Unavailable**, and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Check the Yarn service status.

Step 9 In the alarm list on FusionInsight Manager, check whether **ALM-18000 Yarn Service Unavailable** exists.

- If yes, go to **Step 10**

- If no, go to **Step 11**.

Step 10 Rectify the fault by following the steps provided in **ALM-18000 Yarn Service Unavailable**, and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 11**.

Collect fault information.

Step 11 On the FusionInsight Manager home page of the active cluster, choose **O&M** > **Log** > **Download.**

Step 12 Select **MapReduce** in the required cluster from the **Service.**

Step 13 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 14 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.186 ALM-18022 Insufficient YARN Queue Resources

Alarm Description

The alarm module checks YARN queue resources periodically (controlled by the **alarm.resource.lack.check.times.threshold** parameter, in minutes). When the available queue resources or ApplicationMaster (AM) queue resources are insufficient:

- If **alarm.resource.lack.enable** is set to **true** and **alarm.resource.lack.enable.queues** is left blank, all queues are allowed to trigger this alarm.
- If **alarm.resource.lack.enable** is set to **true** and **alarm.resource.lack.enable.queues** is set to a queue name, only the specified queue is allowed to report this alarm.
- If **alarm.resource.lack.enable** is set to **false**, all queues are not allowed to report this alarm.

To set the preceding parameters, choose **Cluster** > **Services** > **Yarn**. On the displayed page, click **Configurations** > **All Configurations** on FusionInsight Manager.

This alarm is cleared when available resources are sufficient.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
18022	Minor	Quality of service	Tenant plane	Yarn	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	QueueName	Identifies the queue for which the alarm is generated.
	QueueMetric	Identifies the queue indicator for which the alarm is generated.
	Alarm Severity	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

- It takes long time to end an application.
- A new application cannot run after submission.

Possible Causes

- Alarm reporting needs to be adjusted .
- NodeManager node resources are insufficient.
- The maximum resource capacity of the queue is too small.
- The configured maximum ApplicationMaster resource percent is too small.

Handling Procedure

Adjusting the alarm reporting mechanism

Step 1 Check whether all queues need to report this alarm.

- If no queue needs to report alarms, log in to FusionInsight Manager, choose **Cluster** > **Services** > **Yarn**. On the displayed page, click **Configurations** > **All Configurations**, search for **alarm.resource.lack.enable**, change the value to **false**, and save the configuration.
- If only some queues need to report alarms: Log in to FusionInsight Manager, choose **Cluster** > **Services** > **Yarn**. On the displayed page, click **Configurations** > **All Configurations**, search for **alarm.resource.lack.enable.queues** and change the value to the name of the queue for which this alarm needs to be reported, and save the configuration.
- If alarms need to be reported for all queues, go to **Step 3**.

Step 2 Check whether the alarm is cleared 5 minutes later.

- If yes, no further action is required.
- If no, go to **Step 3**.

Check NodeManager resources.

Step 3 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. The **Alarms** page is displayed.

Step 4 View the **Location** in the details page of **Insufficient YARN Queue Resources**. Check whether **QueueName** is **root** and **QueueMetric** is **Memory**, or **QueueName** is **root** and **QueueMetric** is **vCores**

- If yes, go to **Step 5**.
- If no, go to **Step 7**.

Step 5 The memory or CPU of the YARN cluster is insufficient. In this case, log in to the NodeManager node and run the **free –g** and **cat /proc/cpuinfo** commands to query the available memory and available CPU of the node, respectively. On the FusionInsight Manager, increase the values of **yarn.nodemanager.resource.memory-mb** and **yarn.nodemanager.resource.cpu-vcores** for the YARN NodeManager based on the query results. Then, restart the NodeManager instance.

Step 6 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Checking the maximum resource capacity of a queue

Step 7 Check the **Location** of this alarm in the details page. Check whether **QueueName** is the queue name and **QueueMetric** is **Memory**, or **QueueName** is the queue name and **QueueMetric** is **vCores**. Then, check whether **Additional Information** in the alarm details contains **Available Memory less than** or **Available vCores less than**.

- If yes, go to **Step 8**.
- If no, go to **Step 11**.

Step 8 The memory or CPU of the tenant queue is insufficient. In this case, choose **Tenant Resources** > **Dynamic Resource Plan** > **Resource Distribution Policy** and increase the value of **Max Resources**. Then check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Step 9 Choose **Cluster** > **Services** > **Yarn**. On the displayed page, click **Configurations** > **All Configurations**, enter the keyword **threshold**, click **ResourceManager**, and adjust the thresholds of the following parameters as you need:

- If **Additional Information** contains **Available Memory less than**, set **yarn.queue.memory.alarm.threshold** less than **Max Resources**.
- If **Additional Information** contains **Available vCores less than**, set **yarn.queue.vcore.alarm.threshold** less than **Max Resources**.

To obtain the value of **Max Resources**, log in to FusionInsight Manager, choose **Cluster** > **Services** > **Yarn**, click **ResourceManager (*xxx*, Active)** to go to the native YARN page. Choose **Scheduler** > **Application Queues**, and view the value of **Max Resources** in the queue the alarm is reported for.

Step 10 Check whether the alarm is cleared 5 minutes later.

- If yes, no further action is required.
- If no, go to **Step 11**.

Checking the maximum AM resource percentage

Step 11 If **Available AmMemory less than** or **Available AmvCores less than** is included in **Additional Information**, ApplicationMaster memory or CPU of the queue is insufficient. In this case, choose **Tenant Resources** > **Dynamic Resource Plan** > **Queue Configurations**, and increase the value of **Max Master Shares**. Then, check whether this alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 12**.

Step 12 Choose **Cluster** > **Services** > **Yarn**. On the displayed page, click **Configurations** > **All Configurations**, enter the keyword **threshold**, click **ResourceManager**, and adjust the thresholds of the following parameters:

- If **Additional Information** contains **Available AmMemory less than**, set **yarn.am.memory.alarm.threshold** less than **Max Application Master Resources**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If **Additional Information** contains **Available AmvCores less than**, set **yarn.am.vcore.alarm.threshold** less than **Max Application Master Resources**.

To obtain the value of **Max Application Master Resources**, log in to FusionInsight Manager, choose **Cluster** > **Services** > **Yarn**, click **ResourceManager (*xxx*, Active)** to go to the native YARN page. Choose **Scheduler** > **Application Queues**, and view the value of **Max Application Master Resources** in the queue the alarm is reported for.

Step 13 Check whether the alarm is cleared 5 minutes later.

- If yes, no further action is required.
- If no, go to **Step 14**.

Collect fault information.

Step 14 On FusionInsight Manager of the active cluster, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 15 Expand the **Service** drop-down list, and select **Yarn** for the target cluster.

Step 16 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 17 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.187 ALM-18023 Number of Pending Yarn Tasks Exceeds the Threshold

Alarm Description

The alarm module checks the number of pending applications in the Yarn root queue every 60 seconds. The alarm is generated when the number exceeds 60.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
18023	Major	Quality of service	Tenant plane	Yarn	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm is generated.
	HostName	Specifies the host for which the alarm is generated.
	QueueName	Identifies the queue for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

- It takes long time to end an application.
- A new application cannot run after submission.

Possible Causes

- NodeManager node resources are insufficient.

- The maximum resource capacity of the queue and the maximum AM resource percentage are too small.
- The monitoring threshold is too small.

Handling Procedure

Check NodeManager resources.

Step 1 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Yarn** > **ResourceManager (Active)** to access the ResourceManager web UI.

Step 2 Click **Scheduler** and check whether the root queue resources are used up in **Application Queues**.

- If yes, go to **Step 3**.
- If no, go to **Step 4**.

Step 3 Expand the capacity of the NodeManager instance of the Yarn service. After the capacity expansion, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Check the maximum queue resource capacity and the maximum AM resource percentage.

Step 4 Check whether the resources of the queue corresponding to the pending task are used up.

- If yes, go to **Step 5**.
- If no, go to **Step 6**.

Step 5 On FusionInsight Manager, choose **Tenant Resources** > **Dynamic Resource Plan** and add resources as required. Check whether the alarms are cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Adjust the monitoring thresholds.

Step 6 On FusionInsight Manager, choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Yarn** > **Applications** > **Pending Applications**, and increase the thresholds as required.

Step 7 Check whether the alarm is cleared 5 minutes later.

- If yes, no further action is required.
- If no, go to **Step 8**.

Collect fault information.

Step 8 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 9 Expand the **Service** drop-down list, and select **Yarn** for the target cluster.

Step 10 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 11 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.188 ALM-18024 Pending Yarn Memory Usage Exceeds the Threshold

Alarm Description

The alarm module checks the pending memory of Yarn every 60 seconds. The alarm is generated when the pending memory exceeds the threshold. Pending memory indicates the total memory that is not allocated to submitted Yarn applications.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
18024	Major	Quality of service	Tenant plane	Yarn	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.

Type	Parameter	Description
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm is generated.
	HostName	Specifies the host for which the alarm is generated.
	QueueName	Identifies the queue for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

- It takes long time to end an application.
- A new application cannot run after submission.

Possible Causes

- NodeManager node resources are insufficient.
- The maximum resource capacity of the queue and the maximum AM resource percentage are too small.
- The monitoring threshold is too small.

Handling Procedure

Check NodeManager resources.

Step 1 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Yarn** > **ResourceManager (Active)** to access the ResourceManager web UI.

Step 2 Click **Scheduler** and check whether the root queue resources are used up in **Application Queues**.

- If yes, go to **Step 3**.
- If no, go to **Step 4**.

Step 3 Expand the capacity of the NodeManager instance of the Yarn service. After the capacity expansion, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Check the maximum queue resource capacity and the maximum AM resource percentage.

Step 4 Check whether the resources of the queue corresponding to the pending task are used up.

- If yes, go to **Step 5**.
- If no, go to **Step 6**.

Step 5 On FusionInsight Manager, choose **Tenant Resources** > **Dynamic Resource Plan** and add resources as required. Check whether the alarms are cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Adjust the monitoring thresholds.

Step 6 On FusionInsight Manager, choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Yarn** > **CPU and Memory** > **Pending Memory**, and increase the threshold as required.

Step 7 Check whether the alarm is cleared 5 minutes later.

- If yes, no further action is required.
- If no, go to **Step 8**.

Collect fault information.

Step 8 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 9 Expand the **Service** drop-down list, and select **Yarn** for the target cluster.

Step 10 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 11 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.189 ALM-18025 Number of Terminated Yarn Tasks Exceeds the Threshold

Alarm Description

The alarm module checks the number of terminated applications in the Yarn root queue every 60 seconds. The alarm is generated when the number exceeds 50 for three consecutive times.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
18025	Major	Quality of service	Tenant plane	Yarn	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm is generated.
	HostName	Specifies the host for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

A large number of application tasks are forcibly terminated.

Possible Causes

- The user forcibly terminates a large number of tasks.
- The system terminates tasks due to some error.

Handling Procedure

Check the alarm details.

Step 1 On the FusionInsight Manager portal, choose **O&M > Alarm > Alarms** to go to the alarm page.

Step 2 View **Additional Information** in the alarm details to check whether the alarm threshold is too small.

- If yes, go to **Step 3**.
- If no, go to **Step 4**.

Step 3 Choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Yarn** > **Other** > **Terminated Applications of root queue** to modify the threshold. Go to **Step 6**.

Step 4 Choose **Cluster** > *Name of the desired cluster* > **Services** > **Yarn** > **ResourceManager(Active)** to access the ResourceManager web UI.

Step 5 Click **KILLED** in **Applications** and click the task on the top. View the description of **Diagnostics** and rectify the fault based on the task termination details (for example, the task is terminated by a user).

Step 6 Wait for 3 minutes and check whether the alarm is cleared.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect the fault information.

Step 7 On the FusionInsight Manager, choose **O&M > Log > Download**.

Step 8 Expand the **Service** drop-down list, and select **Yarn** for the target cluster.

Step 9 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.190 ALM-18026 Number of Failed Yarn Tasks Exceeds the Threshold

Alarm Description

The alarm module checks the number of failed applications in the Yarn root queue every 60 seconds. The alarm is generated when the number exceeds 50 for three consecutive times.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
18026	Major	Quality of service	Tenant plane	Yarn	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm is generated.
	HostName	Specifies the host for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

- A large number of application tasks fail to be executed.
- Failed tasks need to be submitted again.

Possible Causes

The task fails to be executed due to some error.

Handling Procedure

Check the alarm details.

Step 1 On the FusionInsight Manager portal, choose **O&M > Alarm > Alarms** to go to the alarm page.

Step 2 View **Additional Information** in the alarm details to check whether the alarm threshold is too small.

- If yes, go to **Step 3**.
- If no, go to **Step 4**.

Step 3 Choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Yarn** > **Other** > **Failed Applications of root queue** to modify the threshold. Go to **Step 6**.

Step 4 Choose **Cluster** > *Name of the desired cluster* > **Services** > **Yarn** > **ResourceManager(Active)** to access the ResourceManager web UI.

Step 5 Click **FAILED** in **Applications** and click the task on the top. View the description of **Diagnostics** and rectify the fault based on the task failure causes.

Step 6 Wait for 3 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect the fault information.

Step 7 On the FusionInsight Manager, choose O&M > Log > Download.

Step 8 Expand the **Service** drop-down list, and select **Yarn** for the target cluster.

Step 9 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.191 ALM-18027 JobHistoryServer Process Is Abnormal

Alarm Description

The JobHistoryServer process checks the process status every 20 seconds. This alarm is generated when the process status is abnormal and does not recover for a long time.

This alarm is cleared when the process status recovers.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
18027	Major	Quality of service	Tenant plane	Mapreduce	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
New	3.3.1	New alarm	New alarm

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

If the process status is abnormal, the process cannot provide services properly. As a result, the entire service may become abnormal.

Possible Causes

The host responds slowly to I/O (disk I/O and network I/O) requests and some processes are in the D state and Z state. The process may also be suspended and enter the T state.

Handling Procedure

Check whether the process is in the D, Z, or T state.

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Alarms**. Wait for about 10 minutes and check whether the alarm is automatically cleared.

- If the alarm is not in the list, no further action is required.
- If the alarm is in the list, view the alarm details and record the IP address of the host where the alarm is generated. Run the command in **Step 2**.

Step 2 Log in to the host where the alarm is generated as the **root** user and run the **su - omm** command to switch to the **omm** user.

Step 3 Run the following command to check the process state:

```
ps ww -eo stat,cmd| grep -w
org.apache.hadoop.mapreduce.v2.hs.JobHistoryServer | grep -v grep | awk
'{print$1}'
```

Step 4 Check whether the command output contains any abnormal state (D, Z, or T).

- If the output contains any abnormal state, go to **Step 5**.
- If the output does not contain abnormal states, go to **Step 7**.

Step 5 Switch to user **root** and run the **reboot** command to restart the host for which the alarm is generated. (Restarting a host is risky. Ensure that the service process is normal after the restart.)

Step 6 Wait 5 minutes and check whether the alarm is cleared.

- If the alarm is cleared, no further action is required.
- If the alarm fails to be cleared, go to **Step 7**.

Collect fault information.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 7 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 8 Expand the drop-down list next to the **Service** field. In the **Services** dialog box that is displayed, select **Mapreduce** for the target cluster.

Step 9 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.192 ALM-18028 TimeLineServer Process Is Abnormal

Alarm Description

The TimeLineServer process checks the process status every 20 seconds. This alarm is generated when the process status is abnormal and does not recover for a long time.

This alarm is cleared when the process status recovers.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
18028	Major	Quality of service	Tenant plane	Yarn	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
New	3.3.1	New alarm	New alarm

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

If the process status is abnormal, the process cannot provide services properly. As a result, the entire service may become abnormal.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Possible Causes

The host responds slowly to I/O (disk I/O and network I/O) requests and some processes are in the D state and Z state. The process may also be suspended and enter the T state.

Handling Procedure

Check whether the process is in the D, Z, or T state.

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Alarms**. Wait for about 10 minutes and check whether the alarm is automatically cleared.

- If the alarm is not in the list, no further action is required.
- If the alarm is in the list, view the alarm details and record the IP address of the host where the alarm is generated. Run the command in **Step 2**.

Step 2 Log in to the host where the alarm is generated as the **root** user and run the **su -omm** command to switch to the **omm** user.

Step 3 Run the following command to check the process state:

ps ww -eo stat,cmd| grep -w org.apache.hadoop.yarn.server.applicationhistoryservice.ApplicationHistoryServer | grep -v grep | awk '{print$1}'

Step 4 Check whether the command output contains any abnormal state (D, Z, or T).

- If the output contains any abnormal state, go to **Step 5**.
- If the output does not contain abnormal states, go to **Step 7**.

Step 5 Switch to user **root** and run the **reboot** command to restart the host for which the alarm is generated. (Restarting a host is risky. Ensure that the service process is normal after the restart.)

Step 6 Wait 5 minutes and check whether the alarm is cleared.

- If the alarm is cleared, no further action is required.
- If the alarm fails to be cleared, go to **Step 7**.

Collect fault information.

Step 7 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 8 Expand the drop-down list next to the **Service** field. In the **Services** dialog box that is displayed, select **Yarn** for the target cluster.

Step 9 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.193 ALM-19000 HBase Service Unavailable

Alarm Description

This alarm is generated when the HBase service is unavailable. The alarm module checks the HBase service status every 120 seconds.

This alarm is cleared when the HBase service recovers.

NOTE

If the multi-instance function is enabled in the cluster and multiple HBase service instances are installed, you need to determine the HBase service instance where the alarm is generated based on the value of **ServiceName** in **Location**. For example, if the HBase1 service is unavailable, ServiceName=HBase1 is displayed in **Location**, and the operation object in the procedure needs to be changed from HBase to HBase1.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
19000	Critical	Error handling	Tenant plane	HBase	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

Operations, such as reading or writing data and creating tables, cannot be performed.

Possible Causes

- The ZooKeeper service is abnormal.
- The HDFS service is abnormal.
- The HBase service is abnormal.
- The network is abnormal.
- The service configuration value is incorrect.

Handling Procedure

Check the ZooKeeper service status.

Step 1 On the FusionInsight Manager, check whether the running status of ZooKeeper is **Normal** on service list.

- If yes, go to **Step 5**.
- If no, go to **Step 2**.

Step 2 In the alarm list, check whether **ALM-13000 ZooKeeper Service Unavailable** exists.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 Rectify the fault by following the steps provided in **ALM-13000 ZooKeeper Service Unavailable**.

Step 4 Wait several minutes, and check whether alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check the HDFS service status.

Step 5 In the alarm list, check whether **ALM-14000 HDFS Service Unavailable** exists.

- If yes, go to **Step 6**.
- If no, go to **Step 8**.

Step 6 Rectify the fault by following the steps provided in **ALM-14000 HDFS Service Unavailable**.

Step 7 Wait several minutes, and check whether alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Step 8 On the FusionInsight Manager portal, choose **Cluster** > **Services** > **HDFS**. Check whether **Safe Mode** is **ON**.

- If yes, go to **Step 9**.
- If no, go to **Step 12**.

Step 9 Log in to the node where the HDFS client is installed as the **root** user. Run the following commands to configure environment variables and authenticate the user:

cd *Client installation directory*

source bigdata_env

kinit hdfs (Skip this step if Kerberos authentication is disabled for the cluster (the cluster is in normal mode).)

For details about the password of user **hdfs**, see **Huawei Cloud Stack 8.3.1 Account List** or obtain it from the cluster administrator.

Step 10 Run the following command to manually exit the safe mode:

hdfs dfsadmin -safemode leave

Step 11 Wait several minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 12**.

Check the HBase service status.

Step 12 On the FusionInsight Manager portal, click **Cluster** > **Services** > **HBase**.

Step 13 Check whether there is one active HMaster and one standby HMaster.

- If yes, go to **Step 15**.
- If no, go to **Step 14**.

Step 14 Click **Instances**, select the HMaster whose status is not **Active**, click **More**, and select **Restart Instance** to restart the HMaster. After the restart is successful, check whether there is one active HMaster and one standby HMaster again.

NOTE

During the HMaster restart, table-related operations cannot be performed and the HBase WebUI cannot be accessed. However, data read and write operations are not affected.

- If yes, go to **Step 15**.
- If no, go to **Step 21**.

Step 15 Choose **Cluster** > **Services** > **HBase**. Click the HMaster (Active) hyperlink on the right of **HMaser Web UI** and check whether the HMaster WebUI page can be displayed.

- If yes, go to **Step 16**.
- If no, go to **Step 23**.

Step 16 Check whether at least one RegionServer exists under **Region Servers**.

- If yes, go to **Step 17**.
- If no, go to **Step 21**.

Step 17 Check **Tables** > **System Tables**, as shown in **Figure 1-6**. Check whether **hbase:meta**, **hbase:namespace**, and **hbase:acl** exist in the **Table Name** column.

- If yes, go to **Step 18**.
- If no, go to **Step 19**.

Figure 1-6 HBase system table

Step 18 As shown in **Figure 1-6**, click the **hbase:meta**, **hbase:namespace**, and **hbase:acl** hyperlinks and check whether the pages are properly displayed. If the pages are properly displayed, the tables are normal.

If they are, go to **Step 19**.

If they are not, go to **Step 23**.

NOTE

In normal mode, **ACL** is enabled for HBase by default. The **hbase:acl** table is generated only when **ACL** is manually enabled. In this case, check this table. In other scenarios, this table does not need to be checked.

Step 19 View the HMaster startup status.

In **Figure 1-7**, if the **RUNNING** state exists in **Tasks**, HMaster is being started. In the **State** column, you can view the time when HMaster is in the **RUNNING** state. In **Figure 1-8**, if the state is **COMPLETE**, HMaster is started.

Check whether HMaster is in the **RUNNING** state for a long time.

Figure 1-7 HMaster is being started

Figure 1-8 HMaster is started

- If yes, go to **Step 20**.
- If no, go to **Step 21**.

Step 20 On the HMaster WebUI, check whether any hbase:meta is in the **Region in Transition** state for a long time.

Figure 1-9 Region in Transition

- If yes, go to **Step 21**.
- If no, go to **Step 22**.

Step 21 In the precondition that services are not affected, log in to the FusionInsight Manager portal and choose **Cluster** > **Services** > **HBase** > **More** > **Restart Service**. Enter the administrator password and click **OK**.

NOTE

During the restart of the HBase service, the HBase service is unavailable, including data read and write, table-related operations, and access to the HBase WebUI.

- If yes, go to **Step 22**.
- If no, go to **Step 23**.

Step 22 Wait several minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 23**.

Check whether the HBase configurations are correctly modified.

Step 23 On FusionInsight Manager, choose **Audit**. On the **Audit** page, click **Advanced Search**, click ··· on the right of **Operation Type**, select **Save configuration**, click **OK**, and click **Search**.

Step 24 In the search result, check whether the historical configurations of HBase-related services in the **Service** column, such as ZooKeeper, HDFS, and HBase, may affect the HBase service status. **Table 1-6** lists some configurations that may affect the HBase service status.

Table 1-6 Configurations affecting the HBase service status

Parameter	Possible Impact
GC_OPTS	The memory configuration may be improper. You need to check the health status of instance processes.
hbase.rpc.protection	If the HBase service is not restarted offline after the value of this parameter is changed, the connection authentication fails and the HBase service becomes abnormal.
hbase.regionserver.metahandler.count	If there are too many regions in the cluster but this parameter is set to a small value, RIT may occur and regions cannot be brought online for a long time.
hbase.regionserver.thread.compaction.large	If this parameter is set to a large value, the node CPU usage may be too high.
hbase.regionserver.thread.compaction.small	If this parameter is set to a large value, the node CPU usage may be too high.
hbase.coprocessor.master.classes	If a custom coprocessor is used in the configuration, a logic error may cause the service to be unavailable.
hbase.coprocessor.region.classes	If a custom coprocessor is used in the configuration, a logic error may cause the service to be unavailable.
hbase.coprocessor.regionserver.classes	If a custom coprocessor is used in the configuration, a logic error may cause the service to be unavailable.
zookeeper.session.timeout	If this parameter is set to a small value, the connection between HBase and ZooKeeper times out too quickly. As a result, the HMaster instance and RegionServer may restart repeatedly.

Check the network connection between HMaster and dependent components.

Step 25 On the FusionInsight Manager, choose **Cluster** > **Services** > **HBase**.

Step 26 Click **Instance** and the HMaster instance list is displayed. Record the **management IP Address** in the row of **HMaster(Active)**.

Step 27 Use the IP address obtained in **Step 26** to log in to the host where the active HMaster runs as user **omm** .

Step 28 Run the **ping** command to check whether communication between the host that runs the active HMaster and the hosts that run the dependent components. (The dependent components include ZooKeeper, HDFS and Yarn. Obtain the IP addresses of the hosts that run these services in the same way as that for obtaining the IP address of the active HMaster.)

- If yes, go to **Step 31**.
- If no, go to **Step 29**.

Step 29 Contact the administrator to restore the network.

Step 30 In the alarm list, check whether **HBase Service Unavailable** is cleared.

- If yes, no further action is required.
- If no, go to **Step 31**.

Collect fault information.

Step 31 On the FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 32 Select the following nodes in the required cluster from the **Service** drop-down list:

- ZooKeeper
- HDFS
- HBase

Step 33 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 34 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.194 ALM-19006 HBase Replication Sync Failed

Alarm Description

The alarm module checks the HBase DR data synchronization status every 30 seconds. When disaster recovery (DR) data fails to be synchronized to a standby cluster, the alarm is triggered.

When DR data synchronization succeeds, the alarm is cleared.

NOTE

If the multi-instance function is enabled in the cluster and multiple HBase service instances are installed, you need to determine the HBase service instance where the alarm is generated based on the value of **ServiceName** in **Location**. For example, if the HBase1 service is unavailable, **ServiceName=HBase1** is displayed in **Location**, and the operation object in the procedure needs to be changed from HBase to HBase1.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
19006	Critical	Error handling	Tenant plane	HBase	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger condition	Specifies the threshold for triggering the alarm.

Impact on the System

HBase data in the cluster cannot be synchronized to the standby cluster. Synchronization data is stacked, causing a large amount of active/standby data inconsistency. As a result, the latest data cannot be read from the standby cluster after an active/standby DR switchover or dual-read. If the alarm persists, the storage space of the primary cluster and ZooKeeper nodes will be stacked, leading to service faults in the primary cluster.

Possible Causes

- The HBase service on the standby cluster is abnormal.
- A network exception occurs.

Handling Procedure

Observe whether the system automatically clears the alarm.

Step 1 On the FusionInsight Manager portal of the active cluster, click **O&M** > **Alarm** > **Alarms.**

Step 2 In the alarm list, click the alarm to obtain alarm generation time from **Generated** of the alarm. Check whether the alarm has existed for five minutes.

- If yes, go to **Step 4**.
- If no, go to **Step 3**.

Step 3 Wait five minutes and check whether the system automatically clears the alarm.

- If yes, no further action is required.
- If no, go to **Step 4**.

Check the HBase service status of the standby cluster.

Step 4 Log in to the FusionInsight Manager portal of the active cluster, and click **O&M** > **Alarm** > **Alarms.**

Step 5 In the alarm list, click the alarm to obtain **HostName** from **Location**.

Step 6 Access the node where the HBase client of the active cluster resides as user **omm**.

If the cluster uses a security mode, perform security authentication first and then access the **hbase shell** interface as user **hbase**.

cd /opt/hadoopclient

source ./bigdata_env

kinit *hbaseuser*

Step 7 Run the **status 'replication', 'source'** command to check the DR synchronization status of the faulty node.

The DR synchronization status of a node is as follows.

```
10-10-10-153:
SOURCE: PeerID=abc, SizeOfLogQueue=0, ShippedBatches=2, ShippedOps=2, ShippedBytes=320,
LogReadInBytes=1636, LogEditsRead=5, LogEditsFiltered=3, SizeOfLogToReplicate=0,
TimeForLogToReplicate=0, ShippedHFiles=0, SizeOfHFileRefsQueue=0, AgeOfLastShippedOp=0,
TimeStampsOfLastShippedOp=Mon Jul 18 09:53:28 CST 2016, Replication Lag=0,
FailedReplicationAttempts=0
SOURCE: PeerID=abc1, SizeOfLogQueue=0, ShippedBatches=1, ShippedOps=1, ShippedBytes=160,
LogReadInBytes=1636, LogEditsRead=5, LogEditsFiltered=3, SizeOfLogToReplicate=0,
TimeForLogToReplicate=0, ShippedHFiles=0, SizeOfHFileRefsQueue=0, AgeOfLastShippedOp=16788,
TimeStampsOfLastShippedOp=Sat Jul 16 13:19:00 CST 2016, Replication Lag=16788,
FailedReplicationAttempts=5
```

Step 8 Obtain **PeerID** corresponding to a record whose **FailedReplicationAttempts** value is greater than 0.

In the preceding step, data on the faulty node 10-10-10-153 fails to be synchronized to a standby cluster whose **PeerID** is **abc1**.

Step 9 Run the **list_peers** command to find the cluster and the HBase instance corresponding to the **PeerID** value.

```
PEER_ID CLUSTER_KEY STATE TABLE_CFS
abc1 10.10.10.110,10.10.10.119,10.10.10.133:24002:/hbase2 ENABLED
abc 10.10.10.110,10.10.10.119,10.10.10.133:24002:/hbase ENABLED
```

In the preceding information, **/hbase2** indicates that data is synchronized to the HBase2 instance of the standby cluster.

Step 10 In the service list of FusionInsight Manager of the standby cluster, check whether the running status of the HBase instance obtained by using **Step 9** is **Normal**.

- If yes, go to **Step 14**.
- If no, go to **Step 11**.

Step 11 In the alarm list, check whether the **ALM-19000 HBase Service Unavailable** alarm is generated.

- If yes, go to **Step 12**.
- If no, go to **Step 14**.

Step 12 Follow troubleshooting procedures in **ALM-19000 HBase Service Unavailable** to rectify the fault.

Step 13 Wait for a few minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 14**.

Check network connections between RegionServers on active and standby clusters.

Step 14 Log in to the FusionInsight Manager portal of the active cluster, and click **O&M** > **Alarm** > **Alarms.**

Step 15 In the alarm list, click the alarm to obtain **HostName** from **Location**.

Step 16 Use the IP address obtained in **Step 15** to log in to a faulty RegionServer node as user **omm**.

Step 17 Run the **ping** command to check whether network connections between the faulty RegionServer node and the host where RegionServer of the standby cluster resides are in the normal state.

- If yes, go to **Step 20**.
- If no, go to **Step 18**.

Step 18 Contact the network administrator to restore the network.

Step 19 After the network is running properly, check whether the alarm is cleared in the alarm list.

- If yes, no further action is required.
- If no, go to **Step 20**.

Collect fault information.

Step 20 On the FusionInsight Manager interface of active and standby clusters, choose **O&M** > **Log** > **Download**.

Step 21 In the **Service** drop-down list box, select **HBase** in the required cluster.

Step 22 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 23 Contact the technical support and send the collected fault logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.195 ALM-19007 HBase GC Time Exceeds the Threshold

Alarm Description

The system checks the old generation garbage collection (GC) time of the HBase service every 60 seconds. This alarm is generated when the detected old generation GC time exceeds the threshold (exceeds 5 seconds for three consecutive checks by default). To change the threshold, on the FusionInsight Manager portal, choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **HBase > GC > GC time for old generation**. This alarm is cleared when the old generation GC time of the HBase service is shorter than or equal to the threshold.

NOTE

If the multi-instance function is enabled in the cluster and multiple HBase service instances are installed, you need to determine the HBase service instance where the alarm is generated based on the value of **ServiceName** in **Location**. For example, if the HBase1 service is unavailable, **ServiceName=HBase1** is displayed in **Location**, and the operation object in the procedure needs to be changed from HBase to HBase1.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
19007	Major	Quality of service	Tenant plane	HBase	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

If the GC time of the old generation exceeds the threshold, the read and write of HBase data will slow down. In severe cases, the request times out.

Possible Causes

The memory of HBase instances is overused, the heap memory is inappropriately allocated, or a large number of I/O operations exist in HBase. As a result, GCs occur frequently.

Handling Procedure

Check the GC time.

Step 1 On the FusionInsight Manager portal, click **O&M** > **Alarm** > **Alarms** and select the alarm whose **ID** is **19007**. Then check the role name in **Location** and confirm the IP adress of the instance.

- If the role for which the alarm is generated is HMaster, go to **Step 2**.
- If the role for which the alarm is generated is RegionServer, go to **Step 3**.

Step 2 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services** > **HBase** > **Instance** and click the HMaster for which the alarm is generated to go to the **Dashboard** page. Click the drop-down menu in the **Chart** area and choose **Customize** > **GC** > **Garbage Collection (GC) Time of HMaster** and click **OK** to check whether the value of **GC time for old generation** is greater than the threshold (exceeds 5 seconds for three consecutive checks periods by default).

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 3 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services** > **HBase** > **Instance** and click the RegionServer for which the alarm is generated to go to the **Dashboard** page. Click the drop-down menu in the **Chart** area and choose **Customize** > **GC** > **Garbage Collection (GC) Time of RegionServer** and click **OK** to check whether the value of **GC time for old generation** is greater than the threshold (exceeds 5 seconds for three consecutive checks periods by default).

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Check the current JVM configuration.

Step 4 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services** > **HBase** > **Configurations**, and click **All Configurations**. In

Search, enter **GC_OPTS** to check the **GC_OPTS** memory parameter of role HMaster(HBase->HMaster), RegionServer(HBase->RegionServer). Adjust the values of **-Xmx** and **-XX:CMSInitiatingOccupancyFraction** of the GC_OPTS parameter by referring to the Note.

NOTE

1. Suggestions on GC parameter configurations for HMaster
   - Set **-Xms** and **-Xmx** to the same value to prevent JVM from dynamically adjusting the heap memory size and affecting performance.
   - Set **-XX:NewSize** to the value of **-XX:MaxNewSize**, which is one eighth of **-Xmx**.
   - For large-scale HBase clusters with a large number of regions, increase values of **GC_OPTS** parameters for HMaster. Specifically, set **-Xmx** to 4 GB if the number of regions is less than 100,000. If the number of regions is more than 100,000, set -Xmx to be greater than or equal to 6 GB. For each increased 35,000 regions, increase the value of **-Xmx** by 2 GB. The maximum value of **-Xmx** is 32 GB.
2. Suggestions on GC parameter configurations for RegionServer
   - Set **-Xms** and **-Xmx** to the same value to prevent JVM from dynamically adjusting the heap memory size and affecting performance.
   - Set **-XX:NewSize** to one eighth of **-Xmx**.
   - Set the memory for RegionServer to be greater than that for HMaster. If sufficient memory is available, increase the heap memory.
   - Set **-Xmx** based on the machine memory size. Specifically, set **-Xmx** to 32 GB if the machine memory is greater than 200 GB, to 16 GB if the machine memory is greater than 128 GB and less than 200 GB, and to 8 GB if the machine memory is less than 128 GB. When **-Xmx** is set to 32 GB, a RegionServer node supports 2000 regions and 200 hotspot regions.
   - **XX:CMSInitiatingOccupancyFraction** to be less than and equal to **85**, and it is calculated as follows: 100 x (hfile.block.cache.size + hbase.regionserver.global.memstore.size)

Step 5 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On the FusionInsight Manager interface of active and standby clusters, choose **O&M** > **Log** > **Download**.

Step 7 In the **Service** drop-down list box, select **HBase** in the required cluster.

Step 8 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact the technical support and send the collected fault logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.196 ALM-19008 Heap Memory Usage of the HBase Process Exceeds the Threshold

Alarm Description

The system checks the HBase service status every 30 seconds. The alarm is generated when the heap memory usage of an HBase service exceeds the threshold (90% of the maximum memory).

NOTE

If the multi-instance function is enabled in the cluster and multiple HBase service instances are installed, you need to determine the HBase service instance where the alarm is generated based on the value of **ServiceName** in **Location**. For example, if the HBase1 service is unavailable, **ServiceName=HBase1** is displayed in **Location**, and the operation object in the procedure needs to be changed from HBase to HBase1.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
19008	Major	Quality of service	Tenant plane	HBase	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

The available HBase memory is insufficient, which may cause node restart. During the node restart, the read/write request delay on the node increases or fails.

Possible Causes

The heap memory of the HBase service is overused or the heap memory is inappropriately allocated.

Handling Procedure

Check heap memory usage.

Step 1 On the FusionInsight Manager portal, click **O&M** > **Alarm** > **Alarms** and select the alarm whose **ID** is **19008**. Then check the role name in **Location** and confirm the IP adress of the instance.

- If the role for which the alarm is generated is HMaster, go to **Step 2**.
- If the role for which the alarm is generated is RegionServer, go to **Step 3**.

Step 2 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services** > **HBase** > **Instance** and click the HMaster for which the alarm is generated to go to the **Dashboard** page. Click the drop-down menu in the **Chart** area and choose **Customize** > **CPU and Memory** > **HMaster Heap Memory Usage and Direct Memory Usage Statistics** and click **OK**, check whether the used heap memory of the HBase service reaches 90% of the maximum heap memory specified for HBase.

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 3 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services** > **HBase** > **Instance** and click the RegionServer for which the alarm is generated to go to the **Dashboard** page. Click the drop-down menu in the **Chart** area and choose **Customize** > **CPU and Memory** > **RegionServer Heap Memory Usage and Direct Memory Usage Statistics** and click **OK**, check whether the used heap memory of the HBase service reaches 90% of the maximum heap memory specified for HBase.

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services** > **HBase** > **Configurations**, and click **All Configurations**. Choose **HMaster/RegionServer** > **System**. Increase the value of **-Xmx** in **GC_OPTS** by referring to the Note.

NOTE

1. Suggestions on GC parameter configurations for HMaster
   - Set **-Xms** and **-Xmx** to the same value to prevent JVM from dynamically adjusting the heap memory size and affecting performance.
   - Set **-XX:NewSize** to the value of **-XX:MaxNewSize**, which is one eighth of **-Xmx**.
   - For large-scale HBase clusters with a large number of regions, increase values of **GC_OPTS** parameters for HMaster. Specifically, set **-Xmx** to 4 GB if the number of regions is less than 100,000. If the number of regions is more than 100,000, set -Xmx to be greater than or equal to 6 GB. For each increased 35,000 regions, increase the value of **-Xmx** by 2 GB. The maximum value of **-Xmx** is 32 GB.
2. Suggestions on GC parameter configurations for RegionServer
   - Set **-Xms** and **-Xmx** to the same value to prevent JVM from dynamically adjusting the heap memory size and affecting performance.
   - Set **-XX:NewSize** to the value of **-XX:MaxNewSize**, which is one eighth of **-Xmx**.
   - Set the memory for RegionServer to be greater than that for HMaster. If sufficient memory is available, increase the heap memory.
   - Set **-Xmx** based on the machine memory size. Specifically, set **-Xmx** to 32 GB if the machine memory is greater than 200 GB, to 16 GB if the machine memory is greater than 128 GB and less than 200 GB, and to 8 GB if the machine memory is less than 128 GB. When **-Xmx** is set to 32 GB, a RegionServer node supports 2000 regions and 200 hotspot regions.

Step 5 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On the FusionInsight Manager portal, choose **O&M** > **Log** > **Download**.

Step 7 Select **HBase** in the required cluster from the **Service** drop-down list.

Step 8 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact the technical support and send the collected fault logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.197 ALM-19009 Direct Memory Usage of the HBase Process Exceeds the Threshold

Alarm Description

The system checks the HBase service status every 30 seconds. The alarm is generated when the direct memory usage of an HBase service exceeds the threshold (90% of the maximum memory).

The alarm is cleared when the direct memory usage is less than the threshold.

NOTE

If the multi-instance function is enabled in the cluster and multiple HBase service instances are installed, you need to determine the HBase service instance where the alarm is generated based on the value of **ServiceName** in **Location**. For example, if the HBase1 service is unavailable, **ServiceName=HBase1** is displayed in **Location**, and the operation object in the procedure needs to be changed from HBase to HBase1.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
19009	Major	Quality of service	Tenant plane	HBase	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

The available HBase direct memory is insufficient, which may cause node restart. During the node restart, the read/write request delay on the node increases or fails.

Possible Causes

The direct memory of the HBase service is overused or the direct memory is inappropriately allocated.

Handling Procedure

Check direct memory usage.

Step 1 On the FusionInsight Manager portal, click **O&M** > **Alarm** > **Alarms** and select the alarm whose **ID** is **19009**. Check the **RoleName** in **Location** and confirm the IP address of **HostName**.

- If the role for which the alarm is generated is HMaster, go to **Step 2**.
- If the role for which the alarm is generated is RegionServer, go to **Step 3**.

Step 2 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services** > **HBase** > **Instance** and click the HMaster for which the alarm is generated to go to the **Dashboard** page. Click the drop-down menu in the **Chart** area and choose **Customize** > **CPU and Memory** > **HMaster Heap Memory Usage and Direct Memory Usage Statistics** and click **OK** to check whether the

used direct memory of the HBase service reaches 90% of the maximum direct memory specified for HBase.

- If yes, go to **Step 4**.
- If no, go to **Step 8**.

Step 3 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services** > **HBase** > **Instance** and click the RegionServer for which the alarm is generated to go to the **Dashboard** page. Click the drop-down menu in the **Chart** area and choose **Customize** > **CPU and Memory** > **RegionServer Heap Memory Usage and Direct Memory Usage Statistics** and click **OK** to check whether the used direct memory of the HBase service reaches 90% of the maximum direct memory specified for HBase.

- If yes, go to **Step 4**.
- If no, go to **Step 8**.

Step 4 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services** > **HBase** > **Configurations**, and click **All Configurations**. Choose **HMaster/RegionServer** > **System** and check whether **XX:MaxDirectMemorySize** exists in **GC_OPTS**.

- If yes, go to **Step 5**.
- If no, go to **Step 6**.

Step 5 On the FusionInsight Manager portal, choose **Cluster** > *Nameof the desired cluster* > **Services** > **HBase** > **Configurations**, and click **All Configurations**. Choose **HMaster/RegionServer** > **System** and delete **XX:MaxDirectMemorySize** from **GC_OPTS**.

Step 6 Check whether the **ALM-19008 Heap Memory Usage of the HBase Process Exceeds the Threshold** alarm is generated.

If yes, handle the alarm by referring to **ALM-19008 Heap Memory Usage of the HBase Process Exceeds the Threshold**.

If no, go to **Step 8**.

Step 7 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Collect fault information.

Step 8 On the FusionInsight Manager interface of active and standby clusters, choose **O&M** > **Log** > **Download**.

Step 9 In the **Service** in the required cluster drop-down list box, select **HBase**.

Step 10 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 11 Contact the technical support and send the collected fault logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.198 ALM-19011 RegionServer Region Number Exceeds the Threshold

Alarm Description

The system checks the number of regions on each RegionServer in each HBase service instance every 30 seconds. The region number is displayed on the HBase service monitoring page and RegionServer role monitoring page. This alarm is generated when the number of regions on a RegionServer exceeds the threshold for 20 consecutive times. The threshold can be changed by choosing **O&M** > **Alarms** > **Thresholds** > *Name of the desired cluster* > **HBase**. This alarm is cleared when the number of regions is less than or equal to the threshold.

NOTE

If the multi-instance function is enabled in the cluster and multiple HBase service instances are installed, you need to determine the HBase service instance where the alarm is generated based on the value of **ServiceName** in **Location**. For example, if the HBase1 service is unavailable, **ServiceName=HBase1** is displayed in **Location**, and the operation object in the procedure needs to be changed from HBase to HBase1.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
19011	Critical (default threshold: 5000) Major (default threshold: 2000)	Quality of service	Tenant plane	HBase	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.

Type	Parameter	Description
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

If the number of RegionServer regions exceeds the threshold, too many Regions increase the load of RegionServer, causing resource bottlenecks such as memory, disk I/O, and CPU. As a result, request response becomes slow or even times out.

Possible Causes

- The RegionServer region distribution is unbalanced.
- The HBase cluster scale is too small.

Handling Procedure

View alarm location information.

Step 1 On the FusionInsight Manager home page, choose **O&M** > **Alarm** > **Alarms**, select this alarm, and view the service instance and host name in **Location**.

Step 2 On the FusionInsight Manager home page, choose **Cluster** > *Name of the desired cluster* > **Services**, click the HBase service instance for which the alarm is generated, and click **HMaster(Active)**. On the displayed WebUI of the HBase instance, check whether the region distribution on the RegionServer is balanced.

NOTE

By default, the **admin** user does not have the permissions to manage other components. If the page cannot be opened or the displayed content is incomplete when you access the native UI of a component due to insufficient permissions, you can manually create a user with the permissions to manage that component.

- If yes, go to **Step 9**.
- If no, go to **Step 3**.

Figure 1-10 WebUI of HBase instance

Enable load balancing.

Step 3 Log in to the node where the HBase client is located as user **root**. Go to the client installation directory, and set environment variables.

cd *client installation directory*

source bigdata_env

If the cluster adopts the security mode, perform security authentication. Specifically, run the **kinit hbase** command and enter the password as prompted (obtain the password from the administrator).

Step 4 Run the following commands to go to the HBase shell command window and check whether the load balancing function is enabled.

hbase shell

balancer_enabled

- If yes, go to **Step 6**.
- If no, go to **Step 5**.

Step 5 On the HBase shell command window, run the following commands to enable the load balancing function and check whether the function is enabled.

balance_switch true

balancer_enabled

Step 6 On the HBase shell command window, run the **balancer** command to manually trigger the load balancing function.

NOTE

You are advised to enable and manually trigger the load balancing function during off-peak hours.

Step 7 On the FusionInsight Manager home page, choose **Cluster** > *Name of the desired cluster* > **Services** > **HBase**, and click **HMaster(Active)**. On the displayed WebUI of the HBase instance, refresh the page and check whether the region distribution is balanced.

- If yes, go to **Step 8**.
- If no, go to **Step 21**.

Step 8 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Delete unwanted HBase tables.

NOTE

Exercise caution when deleting data to ensure data is deleted correctly.

Step 9 On the FusionInsight Manager home page, choose **Cluster** > *Name of the desired cluster* > **Services** > **HBase**, and click **HMaster(Active)**. On the displayed WebUI of the HBase instance, view tables stored in the HBase service instance and record unwanted tables that can be deleted.

Step 10 On the HBase shell command window, run the **disable** command and **drop** command to delete the table to decrease the number of regions.

disable '*name of the table to be deleted'*

drop '*name of the table to be deleted'*

Step 11 On the HBase shell command window, run the following command to check whether the load balancing function is enabled.

balancer_enabled

- If yes, go to **Step 13**.
- If no, go to **Step 12**.

Step 12 On the HBase shell command window, run the following commands to enable the load balancing function and confirm that the function is enabled.

balance_switch true

balancer_enabled

Step 13 On the HBase shell command window, run the **balancer** command to manually trigger the load balancing function.

Step 14 On the FusionInsight Manager home page, choose **Cluster** > *Name of the desired cluster* > **Services** > **HBase**, and click **HMaster(Active)**. On the displayed WebUI of the HBase instance, refresh the page and check whether the region distribution is balanced.

- If yes, go to **Step 15**.

- If no, go to **Step 21**.

Step 15 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 16**.

Adjust the threshold.

Step 16 On the FusionInsight Manager home page, choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **HBase** > **Regions(RegionServer)**, select the applied rule, and click **Modify** to check whether the threshold is proper.

- If it is excessively small, increase the threshold as required and go to **Step 17**.
- If it is proper, go to **Step 18**.

Step 17 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 18**.

Perform system capacity expansion.

Step 18 Add nodes to the HBase cluster and add RegionServer instances to the nodes. Then enable and manually trigger the load balancing function.

Step 19 On the FusionInsight Manager home page, choose **Cluster** > *Name of the desired cluster* > **Services**, click the HBase service instance for which the alarm is generated, and click **HMaster(Active)**. On the displayed WebUI of the HBase instance, refresh the page and check whether the region distribution is balanced.

- If yes, go to **Step 20**.
- If no, go to **Step 21**.

Step 20 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 21**.

Collect fault information.

Step 21 On the FusionInsight Manager home page of the active and standby clusters, choose **O&M**> **Log** > **Download**.

Step 22 Select **HBase** in the required cluster from the **Service**.

Step 23 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 24 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.199 ALM-19012 HBase System Table Directory or File Lost

Alarm Description

The system checks whether HBase directories and files exist on the HDFS every 120 seconds. This alarm is generated when the system detects that the files or directories do not exist. This alarm is cleared when the files or directories are restored.

The HBase directories and files are as follows:

- Directory of the namespace **hbase** on the HDFS
- **hbase.version** file
- Directory of the table **hbase:meta** on the HDFS, .tableinfo file, and .regioninfo file
- Directory of the table **hbase:namespace** on the HDFS, .tableinfo file, and .regioninfo file
- Directory of the table **hbase:hindex** on the HDFS, .tableinfo file, and .regioninfo file
- Directory of the **hbase:acl** table on the HDFS, .tableinfo, and .regioninfo file (This table does not exist in the common mode cluster by default.)

NOTE

If the multi-instance function is enabled in the cluster and multiple HBase service instances are installed, you need to determine the HBase service instance where the alarm is generated based on the value of **ServiceName** in **Location**. For example, if the HBase1 service is unavailable, **ServiceName=HBase1** is displayed in **Location**, and the operation object in the procedure needs to be changed from HBase to HBase1.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
19012	Critical	Error handling	Tenant plane	HBase	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.

Type	Parameter	Description
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

The HBase service fails to be restarted or started. As a result, all HBase service requests fail.

Possible Causes

Files or directories on the HDFS are missing.

Handling Procedure

Locate the alarm cause.

Step 1 On the FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. Click this alarm and check whether **Alarm Cause** indicates unknown errors.

- If yes, go to **Step 4**.
- If no, go to **Step 2**

Step 2 On the FusionInsight Manager home page, choose **O&M** > **Backup and Restoration** > **Backup Management**. Check whether there are success records of the backup task named **default** or other HBase metadata backup tasks that have been successfully executed.

- If yes, go to **Step 3**.
- If no, go to **Step 4**.

Step 3 Use the latest backup metadata to restore the metadata of the HBase service. For details, see section "Recovering HBase Metadata" in *MapReduce Service (MRS) 3.3.1-LTS User Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Usage Guide (for Huawei Cloud Stack 8.3.1)*.

Collect fault information.

Step 4 On the FusionInsight Manager page of the active and standby clusters, choose **O&M** > **Log** > **Download**.

Step 5 In the **Service** area, select faulty HBase services in the required cluster.

Step 6 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 7 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.200 ALM-19013 Duration of Regions in transaction State Exceeds the Threshold

Alarm Description

The system checks the number of regions in transaction state on HBase every 300 seconds. This alarm is generated when the system detects that the duration of regions in transaction state exceeds the threshold for two consecutive times. This alarm is cleared when all timeout regions are restored.

NOTE

If the multi-instance function is enabled in the cluster and multiple HBase service instances are installed, you need to determine the HBase service instance where the alarm is generated based on the value of **ServiceName** in **Location**. For example, if the HBase1 service is unavailable, **ServiceName=HBase1** is displayed in **Location**, and the operation object in the procedure needs to be changed from HBase to HBase1.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
19013	Major	Quality of service	Tenant plane	HBase	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

Some data in the service table gets lost or becomes unavailable.

Possible Causes

- Compaction is permanently blocked.
- The HDFS files are abnormal.

Handling Procedure

Locate the alarm cause.

Step 1 On the FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**, select this alarm, and view the **HostName** and **RoleName** in **Location**.

Step 2 Choose **Cluster** > *Name of the desired cluster* > **Services > HBase**, Click the drop-down menu in the chartarea and choose **Customize > Service** >

Region in transaction count to view **Region in transaction count over threshold**. Check whether the monitoring item detects a value in three consecutive detection periods. (The default threshold is 60 seconds.)

- If yes, go to **Step 3**.
- If no, go to **Step 7**.

Step 3 Choose **Cluster** > *Name of the desired cluster* > **Services** > **HBase** > **HMaster (Active)** > **Tables** to check whether the regions of only one table transaction status time out.

- If yes, go to **Step 4**.
- If no, go to **Step 7**.

Step 4 Run the **hbase hbck** command on the client and check whether the error message "No table descriptor file under hdfs://hacluster/hbase/data/default/table" is displayed.

- If yes, go to **Step 5**.
- If no, go to **Step 7**.

Step 5 Log in to the client as user **root**. Run the following command:

cd *client installation directory*

source bigdata_env

If the cluster is in security mode, run the **kinit hbase** command

Log in to the HMaster WebUI, choose **Procedure & Locks** in the navigation tree, and check whether any process ID is in the **Waiting** state in **Procedures**. If yes, run the following command to release the procedure lock:

hbase hbck -j *client installation directory*/**HBase/hbase/tools/hbase-hbck2-*.jar bypass -o** *pid*

Check whether the state is in the **Bypass** state. If the procedure on the UI is always in **RUNNABLE(Bypass)** state, perform an active/standby switchover. Run the **assigns** command to bring the region online again.

hbase hbck -j *client installation directory*/**HBase/hbase/tools/hbase-hbck2-*.jar assigns -o** *regionName*

Step 6 Repeat **Step 4**. Run the **hbase hbck** command on the client and check whether the error message "No table descriptor file under hdfs://hacluster/hbase/data/default/table" is displayed.

- If yes, go to **Step 7**.
- If no, no further action is required.

Collect fault information.

Step 7 On the FusionInsight Manager page of the active and standby clusters, choose **O&M** > **Log** > **Download**.

Step 8 In the **Service** area, select faulty HBase services in the required cluster.

Step 9 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.201 ALM-19014 Capacity Quota Usage on ZooKeeper Exceeds the Threshold Severely

Alarm Description

The system checks the ZNode usage of the HBase service every 120 seconds. This alarm is generated when the ZNode capacity usage of the HBase service exceeds the critical alarm threshold (90% by default).

This alarm is cleared when the ZNode capacity usage is less than the critical alarm threshold.

NOTE

If the multi-instance function has been enabled in the cluster and multiple HBase services have been installed, determine the HBase service for which the alarm is generated based on the value of **ServiceName** in **Location**. For example, if the value of **ServiceName** is **HBase-1**, change the operation object in the procedure from **HBase** to **HBase-1**.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
19014	Critical	Quality of service	Tenant plane	HBase	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Threshold	Specifies the threshold for generating the alarm.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

This alarm indicates that the capacity usage of the ZNode of HBase has exceeded the threshold severely. As a result, the write request of the HBase service fails.

Possible Causes

- DR is configured for HBase, and data synchronization fails or is slow in DR.
- A large number of WAL files are being split in the HBase cluster.

Handling Procedure

Check the capacity configuration and usage of ZNodes.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**, select the alarm whose ID is **19014**, and view the threshold in **Additional Information**.

Step 2 Log in to the HBase client as user **root**. Run the following command to go to the client installation directory:

cd *Client installation directory*

Run the following command to set environment variables:

source bigdata_env

If the cluster uses the security mode, run the following command to perform security authentication:

kinit hbase

Enter the password as prompted (obtain the password from the MRS cluster administrator).

Step 3 Run the **hbase zkcli** command to log in to the ZooKeeper client and run the **listquota /hbase** command to check the ZNode capacity quota of the HBase service. The ZNode root directory in the command is specified by the **zookeeper.znode.parent** parameter of the HBase service. The marked area in the following figure shows the capacity configuration of the root ZNode of the HBase service.

```
[zk:                    :24002,                    :24002,                    :24002(CONNECTED) 145] listquota /hbase
absolute path is /zookeeper/quota/hbase
Output quota for /hbase count=1500000,bytes=10240
Output stat for /hbase count=42,bytes=1601
```

Step 4 Run the **getusage /hbase/splitWAL** command to check the capacity usage of the ZNode. Check whether the ratio of **Data size** to the ZNode capacity quota is close to the alarm threshold.

- If yes, go to **Step 5**.
- If no, go to **Step 6**.

Step 5 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. Check whether the alarm whose ID is **12007**, **19000**, or **19013** and the **ServiceName** in **Location** is the current HBase service exists.

- If yes, click **View Help** next to the alarm and rectify the fault by referring to the help document. Then, go to **Step 8**.

- If no, go to **Step 9**.

Step 6 Run the **getusage /hbase/replication** command to check the capacity usage of the ZNode. Check whether the ratio of **Data size** to the ZNode capacity quota is close to the alarm threshold.

- If yes, go to **Step 7**.
- If no, go to **Step 9**.

Step 7 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. Check whether the alarm whose ID is **19006** and **ServiceName** in **Location** is the current HBase service exists.

- If yes, click **View Help** next to the alarm and rectify the fault by referring to the help document. Then, go to **Step 8**.
- If no, go to **Step 9**.

Step 8 Check whether the alarm is cleared five minutes later.

- If yes, no further action is required.
- If no, go to **Step 9**.

Collect fault information.

Step 9 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 10 Expand the **Service** drop-down list, and select **HBase** for the target cluster.

Step 11 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.202 ALM-19015 Quantity Quota Usage on ZooKeeper Exceeds the Threshold

Alarm Description

The system checks the ZNode usage of the HBase service every 120 seconds. This alarm is generated when the system detects that the ZNode quantity usage of the HBase service exceeds the alarm threshold (75% by default).

This alarm is cleared when the ZNode quantity usage is less than the alarm threshold.

NOTE

If the multi-instance function has been enabled in the cluster and multiple HBase services have been installed, determine the HBase service for which the alarm is generated based on the value of **ServiceName** in **Location**. For example, if the value of **ServiceName** is **HBase-1**, change the operation object in the procedure from **HBase** to **HBase-1**.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
19015	Major	Quality of service	Tenant plane	HBase	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Threshold	Specifies the threshold for generating the alarm.

Impact on the System

This alarm indicates that the ZNode quantity usage in the HBase service has exceeded the threshold. If this alarm is not handled in a timely manner, the problem severity may be escalated to **Critical** and data fails to be written.

Possible Causes

- DR is configured for HBase, and data synchronization fails or is slow in DR.
- A large number of WAL files are being split in the HBase cluster.

Handling Procedure

Check the quantity quota and usage of ZNodes.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**, select the alarm whose ID is **19015**, and view the threshold in **Additional Information**.

Step 2 Log in to the HBase client as user **root**. Run the following command to go to the client installation directory:

cd *Client installation directory*

Run the following command to set environment variables:

source bigdata_env

If the cluster uses the security mode, run the following command to perform security authentication:

kinit hbase

Enter the password as prompted (obtain the password from the MRS cluster administrator).

Step 3 Run the **hbase zkcli** command to log in to the ZooKeeper client and run the **listquota /hbase** command to check the ZNode quantity quota of the HBase service. The ZNode root directory in the command is specified by the **zookeeper.znode.parent** parameter of the HBase service. The marked area in the following figure shows the quantity quota configuration of the root ZNode of the HBase service.

```
[zk: [redacted]:24002,[redacted]:24002,[redacted]:24002(CONNECTED) 7] listquota /hbase
absolute path is /zookeeper/quota/hbase
Output quota for /hbase count=1500000,bytes=10240
Output stat for /hbase count=59,bytes=1902
```

Step 4 Run the **getusage /hbase/splitWAL** command to check the ZNode quantity usage and check whether the ratio of **Node count** in the command output to the ZNode quantity quota is close to the alarm threshold.

- If yes, go to **Step 5**.
- If no, go to **Step 6**.

Step 5 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. Check whether the alarm whose ID is **12007**, **19000**, or **19013** and the **ServiceName** in **Location** is the current HBase service exists.

- If yes, click **View Help** next to the alarm and rectify the fault by referring to the help document. Then, go to **Step 8**.
- If no, go to **Step 9**.

Step 6 Run the **getusage /hbase/replication** command to check the ZNode quantity usage and check whether the ratio of **Node count** in the command output to the ZNode quantity quota is close to the alarm threshold.

- If yes, go to **Step 7**.
- If no, go to **Step 9**.

Step 7 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. Check whether the alarm whose ID is **19006** and **ServiceName** in **Location** is the current HBase service exists.

- If yes, click **View Help** next to the alarm and rectify the fault by referring to the help document. Then, go to **Step 8**.
- If no, go to **Step 9**.

Step 8 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Collect fault information.

Step 9 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 10 Expand the **Service** drop-down list, and select **HBase** for the target cluster.

Step 11 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.203 ALM-19016 Quantity Quota Usage on ZooKeeper Exceeds the Threshold Severely

Alarm Description

The system checks the ZNode usage of the HBase service every 120 seconds. This alarm is generated when the ZNode usage of the HBase service exceeds the critical alarm threshold (90% by default).

This alarm is cleared when the quantity usage of the ZNode is less than the critical alarm threshold.

NOTE

If the multi-instance function has been enabled in the cluster and multiple HBase services have been installed, determine the HBase service for which the alarm is generated based on the value of **ServiceName** in **Location**. For example, if the value of **ServiceName** is **HBase-1**, change the operation object in the procedure from **HBase** to **HBase-1**.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
19016	Critical	Quality of service	Tenant plane	HBase	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Threshold	Specifies the threshold for generating the alarm.

Impact on the System

This alarm indicates that the quantity usage of the ZNode of HBase has exceeded the threshold severely. As a result, the write request of the HBase service fails.

Possible Causes

- DR is configured for HBase, and data synchronization fails or is slow in DR.
- A large number of WAL files are being split in the HBase cluster.

Handling Procedure

Check the quantity quota and usage of ZNodes.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**, select the alarm whose ID is **19016**, and view the threshold in **Additional Information**.

Step 2 Log in to the HBase client as user **root**. Run the following command to go to the client installation directory:

cd *Client installation directory*

Run the following command to set environment variables:

source bigdata_env

If the cluster uses the security mode, run the following command to perform security authentication:

kinit hbase

Enter the password as prompted (obtain the password from the MRS cluster administrator).

Step 3 Run the **hbase zkcli** command to log in to the ZooKeeper client and run the **listquota /hbase** command to check the ZNode quantity quota of the HBase service. The ZNode root directory in the command is specified by the **zookeeper.znode.parent** parameter of the HBase service. The marked area in the following figure shows the quantity configuration of the root ZNode of the HBase service.

```
[zk:                :24002,              :24002,              :24002(CONNECTED) 7] listquota /hbase
absolute path is /zookeeper/quota/hbase
Output quota for /hbase count=1500000,bytes=10240
Output stat for /hbase count=59,bytes=1902
```

Step 4 Run the **getusage /hbase/splitWAL** command to check the ZNode usage and check whether the ratio of **Node count** in the command output to the ZNode quantity quota is close to the alarm threshold.

- If yes, go to **Step 5**.
- If no, go to **Step 6**.

Step 5 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. Check whether the alarm whose ID is **12007**, **19000**, or **19013** and the **ServiceName** in **Location** is the current HBase service exists.

- If yes, click **View Help** next to the alarm and rectify the fault by referring to the help document. Then, go to **Step 8**.
- If no, go to **Step 9**.

Step 6 Run the **getusage /hbase/replication** command to check the ZNode usage and check whether the ratio of **Node count** in the command output to the ZNode quantity quota is close to the alarm threshold.

- If yes, go to **Step 7**.
- If no, go to **Step 9**.

Step 7 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. Check whether the alarm whose ID is **19006** and **ServiceName** in **Location** is the current HBase service exists.

- If yes, click **View Help** next to the alarm and rectify the fault by referring to the help document. Then, go to **Step 8**.
- If no, go to **Step 9**.

Step 8 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Collect fault information.

Step 9 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 10 Expand the **Service** drop-down list, and select **HBase** for the target cluster.

Step 11 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.204 ALM-19017 Capacity Quota Usage on ZooKeeper Exceeds the Threshold

Alarm Description

The system checks the ZNode usage of the HBase service every 120 seconds. This alarm is generated when the system detects that the ZNodes capacity usage of the HBase service exceeds the alarm threshold (75% by default).

This alarm is cleared when the capacity usage of the ZNode capacity is less than the threshold.

NOTE

If the multi-instance function has been enabled in the cluster and multiple HBase services have been installed, determine the HBase service for which the alarm is generated based on the value of **ServiceName** in **Location**. For example, if the value of **ServiceName** is **HBase-1**, change the operation object in the procedure from **HBase** to **HBase-1**.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
19017	Major	Quality of service	Tenant plane	HBase	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.

Type	Parameter	Description
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Threshold	Specifies the threshold for generating the alarm.

Impact on the System

This alarm indicates that the ZNodes capacity usage in the HBase service has exceeded the threshold. If this alarm is not handled in a timely manner, the problem severity may be escalated to **Critical**, affecting data writing.

Possible Causes

- DR is configured for HBase, and data synchronization fails or is slow in DR.
- A large number of WAL files are being split in the HBase cluster.

Handling Procedure

Check the capacity configuration and usage of ZNodes.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**, select the alarm whose ID is **19017**, and view the threshold in **Additional Information**.

Step 2 Log in to the HBase client as user **root**. Run the following command to go to the client installation directory:

cd *Client installation directory*

Run the following command to set environment variables:

source bigdata_env

If the cluster uses the security mode, run the following command to perform security authentication:

kinit hbase

Enter the password as prompted (obtain the password from the MRS cluster administrator).

Step 3 Run the **hbase zkcli** command to log in to the ZooKeeper client and run the **listquota /hbase** command to check the ZNode quantity quota of the HBase service. The ZNode root directory in the command is specified by the **zookeeper.znode.parent** parameter of the HBase service. The marked area in the following figure shows the quantity configuration of the root ZNode of the HBase service.

```
[zk:                    :24002,                    :24002,                    .:24002(CONNECTED) 145] listquota /hbase
absolute path is /zookeeper/quota/hbase
Output quota for /hbase count=1500000,bytes=10240
Output stat for /hbase count=42,bytes=1601
```

Step 4 Run the **getusage /hbase/splitWAL** command to check the capacity usage of the ZNode. Check whether the ratio of **Data size** to the ZNode capacity quota is close to the alarm threshold.

- If yes, go to **Step 5**.
- If no, go to **Step 6**.

Step 5 On FusionInsight Manager, check whether the alarm whose ID is **12007**, **19000**, or **19013** and **ServiceName** in **Location** is the current HBase service exists.

- If yes, click **View Help** next to the alarm and rectify the fault by referring to the help document. Then, go to **Step 8**.
- If no, go to **Step 7**.

Step 6 Run the **getusage /hbase/replication** command to check the capacity usage of the ZNode. Check whether the ratio of **Data size** to the ZNode capacity quota is close to the alarm threshold.

- If yes, go to **Step 7**.
- If no, go to **Step 9**.

Step 7 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. Check whether the alarm whose ID is **19006** and **ServiceName** in **Location** is the current HBase service exists.

- If yes, click **View Help** next to the alarm and rectify the fault by referring to the help document. Then, go to **Step 8**.
- If no, go to **Step 9**.

Step 8 Check whether the alarm is cleared.

- If yes, no further action is required.

- If no, go to **Step 9**.

Collect fault information.

Step 9 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 10 Expand the **Service** drop-down list, and select **HBase** for the target cluster.

Step 11 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.205 ALM-19018 HBase Compaction Queue Size Exceeds the Threshold

Alarm Description

The system checks the HBase compaction queue size every 30 seconds. This alarm is generated when the compaction queue size exceeds the alarm threshold (**100** by default) for three consecutive times. This alarm is cleared when the compaction queue size is less than the threshold.

NOTE

If the multi-instance function has been enabled in the cluster and multiple HBase services have been installed, determine the HBase service for which the alarm is generated based on the value of **ServiceName** in **Location**. For example, if the value of **ServiceName** is **HBase-1**, change the operation object in the procedure from **HBase** to **HBase-1**.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
19018	Minor	Quality of service	Tenant plane	HBase	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

Write pressure on the HBase node continues going up, and the disk I/O and CPU may be overloaded. Read and write requests are responded slowly or even time out.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Possible Causes

- The number of HBase RegionServers is too small.
- There are excessive regions on a single RegionServer of HBase.
- The HBase RegionServer heap size is small.
- Resources are insufficient.
- Related parameters are not configured properly.

Handling Procedure

Check whether related parameters are properly configured.

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Alarms**. On the page that is displayed, check whether the alarm whose **Alarm ID** is **19008** or **19011** exists.

- If yes, click **View Help** next to the alarm and rectify the fault by referring to the help document. Then, go to **Step 3**.
- If no, go to **Step 2**.

Step 2 On FusionInsight Manager, choose **Cluster**, click the name of the desired cluster, and choose **Services** > **HBase**. On the page that is displayed, click the **Configuration** tab then the **All Configurations** sub-tab, search for **hbase.hstore.compaction.min**, **hbase.hstore.compaction.max**, **hbase.regionserver.thread.compaction.small**, and **hbase.regionserver.thread.compaction.throttle**, and set them to larger values.

Step 3 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 4**.

Collect fault information.

Step 4 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 5 Expand the **Service** drop-down list, and select **HBase** for the target cluster.

Step 6 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 7 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

1.3.206 ALM-19019 Number of HBase HFiles to Be Synchronized Exceeds the Threshold

Alarm Description

The system checks the number of HFiles to be synchronized by the RegionServer of each HBase service instance every 30 seconds. This indicator can be viewed on the RegionServer role monitoring page. This alarm is generated when the number of HFiles to be synchronized on a RegionServer exceeds the threshold (exceeding 128 for 20 consecutive times by default). To change the threshold, choose **O&M** > **Alarm** > **Threshold Configuration** > *Name of the desired cluster* > **HBase** . This alarm is cleared when the number of HFiles to be synchronized is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
19019	Major	Quality of service	Tenant plane	HBase	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

A large number of HFile files are stacked. Data is inconsistent between the active and standby nodes, and the latest data cannot be read from the standby cluster during an active/standby switchover or during HBase dual-read. If the fault persists, the storage space of the active cluster and ZooKeeper nodes will be used up. As a result, the active cluster service will be interrupted.

Possible Causes

- The network is abnormal.
- The RegionServer region distribution is unbalanced.
- The HBase service scale of the standby cluster is too small.

Handling Procedure

View alarm location information.

Step 1 Log in to FusionInsight Manager and choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**. On the page that is displayed, locate the row containing the alarm whose **Alarm ID** is **19019**, and view the service instance and host name in **Location**.

Check the network connection between RegionServers on active and standby clusters.

Step 2 Run the **ping** command to check whether the network connection between the faulty RegionServer node and the host where RegionServer of the standby cluster resides is normal.

- If yes, go to **Step 5**.
- If no, go to **Step 3**.

Step 3 Contact the network administrator to restore the network.

Step 4 After the network recovers, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check the RegionServer region distribution in the active cluster.

Step 5 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **HBase**. Click **HMaster(Active)** to go to the web UI of the HBase instance and check whether regions are evenly distributed on the Region Server.

ServerName	Start time	Last contact	Version	Requests Per Second	Num. Regions
kwephispra44947,21302,1620614446704	2021-05-10T02:40:46.704Z	1 s	2.2.3-hw-ei-311001-SNAPSHOT	13	10
kwephispra44948,21302,1620614361509	2021-05-10T02:39:21.509Z	0 s	2.2.3-hw-ei-311001-SNAPSHOT	0	12
kwephispra44949,21302,1620614361123	2021-05-10T02:39:21.123Z	2 s	2.2.3-hw-ei-311001-SNAPSHOT	0	13
kwephisprb10223,21302,1621424421459	2021-05-19T11:40:21.459Z	1 s	2.2.3-hw-ei-311001-SNAPSHOT	0	8
Total:4				13	43

Step 6 Log in to the faulty RegionServer node as user **omm**.

Step 7 Run the following commands to go to the client installation directory and set the environment variable:

cd *Client installation directory*

source bigdata_env

If the cluster uses the security mode, perform security authentication. Run the **kinit hbase** command and enter the password as prompted (obtain the password from the MRS cluster administrator).

Step 8 Run the following commands to check whether the load balancing function is enabled.

hbase shell

balancer_enabled

- If yes, go to **Step 10**.
- If no, go to **Step 9**.

Step 9 Run the following commands in HBase Shell to enable the load balancing function and check whether the function is enabled.

balance_switch true

balancer_enabled

Step 10 Run the **balancer** command to manually trigger the load balancing function.

NOTE

You are advised to enable and manually trigger the load balancing function during off-peak hours.

Step 11 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 12**.

Check the HBase service scale of the standby cluster.

Step 12 Expand the HBase cluster, add a node, and add a RegionServer instance on the node. Then, perform **Step 6** to **Step 10** to enable the load balancing function and manually trigger it.

Step 13 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **HBase**. Click **HMaster(Active)** to go to the web UI of the HBase instance, refresh the page, and check whether regions are evenly distributed.

- If yes, go to **Step 14**.
- If no, go to **Step 15**.

Step 14 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 15**.

Collect fault information.

Step 15 On FusionInsight Manager of the standby cluster, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 16 Expand the **Service** drop-down list, and select **HBase** for the target cluster.

Step 17 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 18 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.207 ALM-19020 Number of HBase WAL Files to Be Synchronized Exceeds the Threshold

Alarm Description

The system checks the number of WAL files to be synchronized by the RegionServer of each HBase service instance every 30 seconds. This indicator can be viewed on the RegionServer role monitoring page. This alarm is generated when the number of WAL files to be synchronized on a RegionServer exceeds the threshold (exceeding 128 for 20 consecutive times by default). To change the threshold, choose **O&M** > **Alarm** > **Threshold Configuration** > *Name of the desired cluster* > **HBase** . This alarm is cleared when the number of WAL files to be synchronized is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
19020	Major	Quality of service	Tenant plane	HBase	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

A large number of WAL files are stacked. Data is inconsistent between the active and standby nodes, and the latest data cannot be read from the standby cluster during an active/standby switchover or during HBase dual-read. If the fault persists, the storage space of the active cluster and ZooKeeper nodes will be used up. As a result, the active cluster service will be interrupted.

Possible Causes

- The network is abnormal.
- The RegionServer region distribution is unbalanced.
- The HBase service scale of the standby cluster is too small.

Handling Procedure

View alarm location information.

Step 1 Log in to FusionInsight Manager and choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**. On the page that is displayed, locate the row containing the alarm whose **Alarm ID** is **19020**, and view the service instance and host name in **Location**.

Check the network connection between RegionServers on active and standby clusters.

Step 2 Run the **ping** command to check whether the network connection between the faulty RegionServer node and the host where RegionServer of the standby cluster resides is normal.

- If yes, go to **Step 5**.
- If no, go to **Step 3**.

Step 3 Contact the network administrator to restore the network.

Step 4 After the network recovers, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check the RegionServer region distribution in the active cluster.

Step 5 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **HBase**. Click **HMaster(Active)** to go to the web UI of the HBase instance and check whether regions are evenly distributed on the Region Server.

ServerName	Start time	Last contact	Version	Requests Per Second	Num. Regions
kwephispra44947,21302,1620614446704	2021-05-10T02:40:46.704Z	1 s	2.2.3-hw-ei-311001-SNAPSHOT	13	10
kwephispra44948,21302,1620614361509	2021-05-10T02:39:21.509Z	0 s	2.2.3-hw-ei-311001-SNAPSHOT	0	12
kwephispra44949,21302,1620614361123	2021-05-10T02:39:21.123Z	2 s	2.2.3-hw-ei-311001-SNAPSHOT	0	13
kwephisprb10223,21302,1621424421459	2021-05-19T11:40:21.459Z	1 s	2.2.3-hw-ei-311001-SNAPSHOT	0	8
Total:4				13	43

Step 6 Log in to the faulty RegionServer node as user **omm**.

Step 7 Run the following commands to go to the client installation directory and set the environment variable:

cd *Client installation directory*

source bigdata_env

If the cluster uses the security mode, perform security authentication. Run the **kinit hbase** command and enter the password as prompted (obtain the password from the MRS cluster administrator).

Step 8 Run the following commands to check whether the load balancing function is enabled.

hbase shell

balancer_enabled

- If yes, go to **Step 10**.
- If no, go to **Step 9**.

Step 9 Run the following commands in HBase Shell to enable the load balancing function and check whether the function is enabled.

balance_switch true

balancer_enabled

Step 10 Run the **balancer** command to manually trigger the load balancing function.

NOTE

You are advised to enable and manually trigger the load balancing function during off-peak hours.

Step 11 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 12**.

Check the HBase service scale of the standby cluster.

Step 12 Expand the HBase cluster, add a node, and add a RegionServer instance on the node. Then, perform **Step 6** to **Step 10** to enable the load balancing function and manually trigger it.

Step 13 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **HBase**. Click **HMaster(Active)** to go to the web UI of the HBase instance, refresh the page, and check whether regions are evenly distributed.

- If yes, go to **Step 14**.
- If no, go to **Step 15**.

Step 14 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 15**.

Collect fault information.

Step 15 On FusionInsight Manager of the standby cluster, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 16 Expand the **Service** drop-down list, and select **HBase** for the target cluster.

Step 17 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 18 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.208 ALM-19021 Handler Usage of RegionServer Exceeds the Threshold

Alarm Description

The system checks the RegionServer handler usage of each HBase service instance every 30 seconds. This alarm is generated when the handler usage of a RegionServer exceeds the threshold for five consecutive times by default. This alarm is cleared if the handler usage is lower than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
19021	Critical (default threshold: 100%) Major (default threshold: 90%)	Quality of service	Tenant plane	HBase	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.

Type	Parameter	Description
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Threshold	Specifies the threshold for generating the alarm.

Impact on the System

RegionServer may not be able to provide services externally. As a result, the concurrent read/write processing become slow, or requests fail.

Possible Causes

- The value of a handler is too small.
- Hotspotting occurs.

Handling Procedure

View alarm location information.

Step 1 Log in to FusionInsight Manager and choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**, locate the row that contains the alarm whose **Alarm ID** is **19021**, and view the service instance and host name in **Location**.

Check the handler configuration.

Step 2 Choose **Cluster** > **Services** > **HBase** and click the **Configurations** tab. In the upper right corner of the page, search for **hbase.regionserver.handler.count** and check whether its value is too small. The default value is **200**.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 Change the value of this parameter to a greater value and save the configuration. Choose **Cluster** > **Services** > **HBase**, click the **Instance** tab, select the affected RegionServer instances, and choose **More** > **Instance Rolling Restart**. In the displayed dialog box, enter the username and password. In the **Instance Rolling Restart** dialog box, click **OK** and wait until the rolling restart is complete.

Step 4 After the configuration takes effect, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check whether cluster hotspotting occurs.

Step 5 On FusionInsight Manager, choose **Cluster** > **Services** > **HBase** and click **HMaster(Active)** following **HMaster WebUI** to go to the web UI of the HBase instance. In the **Region Servers** area of the **Home** page, click **Requests** and check whether the requests in the **Filtered Read Request Count** and **Write Request Count** columns are evenly distributed.

- If yes, go to **Step 13**.
- If no, go to **Step 6**.

Step 6 Check whether regions are evenly distributed.

On FusionInsight Manager, choose **Cluster** > **Services** > **HBase** and click **HMaster(Active)** following **HMaster WebUI** to go to the web UI of the HBase instance. In the **Region Servers** area of the **Home** page, click **Base Stats** and check whether the regions in the **Num.Regions** column are evenly distributed.

- If yes, go to **Step 13**.
- If no, go to **Step 7**.

Step 7 Log in to the faulty RegionServer node as user **omm**.

Step 8 Run the following commands to go to the client installation directory and set the environment variable:

cd *Client installation directory*

source bigdata_env

If the cluster uses the security mode, run the following command to perform security authentication:

kinit hbase

Enter the password as prompted (obtain the password from the MRS cluster administrator).

Step 9 Run the following commands to check whether the load balancing function is enabled. If the command output is **true**, the load balancing function is enabled.

hbase shell

balancer_enabled

```
hbase:004:0> balancer_enabled
true
Took 0.0165 seconds
=> true
```

- If yes, go to **Step 13**.
- If no, go to **Step 10**.

Step 10 Run the following commands in HBase Shell to enable the load balancing function and check whether the function is enabled.

balance_switch true

balancer_enabled

NOTE

You are advised to enable and manually trigger the load balancing function during off-peak hours.

Step 11 Run the following command to manually trigger' the load balancing function:

balancer

Step 12 After the load balancing is complete, log in to FusionInsight Manager and choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms** and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 13**.

Collect the fault information.

Step 13 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 14 Expand the **Service** drop-down list, and select **HBase** for the target cluster.

Step 15 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 16 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.209 ALM-19022 HBase Hotspot Detection Is Unavailable

Alarm Description

When the MetricController instance is installed for HBase, the alarm module checks the health status of the active HBase MetricController instance every 120 seconds. This alarm is generated when the active HBase MetricController instance does not exist or is unavailable and the hotspot detection function is unavailable.

This alarm is cleared when the active HBase MetricController instance recovers.

NOTE

If the multi-instance function has been enabled in the cluster and multiple HBase services have been installed, determine the HBase service for which the alarm is generated based on the value of **ServiceName** in **Location**. For example, if HBase-1 is unavailable, the **ServiceName** value displayed in **Location** is **HBase-1**, and the operation object in the procedure should be changed to **HBase-1**.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
19022	Major	Error handling	Tenant plane	HBase	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.

Type	Parameter	Description
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

The HBase hotspot detection function is unavailable. Services are not affected. However, if request/data skew occurs, the system cannot report alarms and automatically recovers from hotspotting. Service requests may cause node overload, slow response, and request timeout.

Possible Causes

- The ZooKeeper service is abnormal.
- The HBase service is abnormal.
- In the current HBase service, the MetricController instance on the same node as the active HMaster instance is not started.
- The network is abnormal.

Handling Procedure

Check the ZooKeeper service status.

Step 1 In the service list on FusionInsight Manager, check whether **Running Status** of ZooKeeper is **Normal**.

- If yes, go to **Step 5**.
- If no, go to **Step 2**.

Step 2 In the alarm list, check whether **ALM-13000 ZooKeeper Service Unavailable** exists.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 Rectify the fault by performing the operations provided for **ALM-13000 ZooKeeper Service Unavailable**.

Step 4 Wait for several minutes and check whether the alarm **HBase Hotspot Detection Is Unavailable** is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check the HBase service status.

Step 5 In the service list on FusionInsight Manager, check whether **Running Status** of HBase is **Normal**.

- If yes, go to **Step 9**.
- If no, go to **Step 6**.

Step 6 In the alarm list, check whether the alarm ALM-19000 HBase Service Unavailable exists.

- If yes, go to **Step 7**.
- If no, go to **Step 9**.

Step 7 Rectify the fault by following the steps provided for **ALM-19000 HBase Service Unavailable**.

Step 8 Wait for several minutes and check whether the alarm **HBase Hotspot Detection Is Unavailable** is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Check whether the MetricController instance deployed on the same node as the active HMaster instance is started.

Step 9 On FusionInsight Manager, choose **Cluster** > **Service** > **HBase**, and click **Instances** to check whether the **MetricController(Active)** instance exists.

- If yes, go to **Step 12**.
- If no, go to **Step 10**.

Step 10 Select the MetricController instance whose management IP address is the same as that of the active HMaster instance, and click **Start Instance**.

Step 11 After the MetricController instance is restarted, check whether the alarm **HBase Hotspot Detection Is Unavailable** is cleared.

- If yes, no further action is required.
- If no, go to **Step 12**.

Check the network connectivity between the started MetricController instances and the active HMaster node.

Step 12 Log in to the node where the active HMaser instance is deployed and run **ping** *IP address of the node where the standby MetricController instance is deployed* to check whether the network connection between the started MetricController instances and the host where the active HMaster instance is deployed is normal.

- If yes, go to **Step 15**.
- If no, go to **Step 13**.

Step 13 Contact the network administrator to restore the network.

Step 14 After the network recovers, check whether the alarm **HBase Hotspot Detection Is Unavailable** is cleared.

- If yes, no further action is required.
- If no, go to **Step 15**.

Collect fault information.

Step 15 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 16 Expand the **Service** drop-down list, and select **HBase** for the target cluster.

Step 17 In the **Host** area, select the host where the HMaster instance is deployed.

Step 18 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 19 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.210 ALM-19023 Region Traffic Restriction for HBase

Alarm Description

When the MetricController instance is installed for the HBase service, self-healing from hotspotting is automatically enabled. The alarm module checks whether there are regions whose request traffic is restricted due to hotspot issues in HBase

every 120 seconds. This alarm is generated when the region where hotspot traffic is restricted is detected in HBase.

This alarm is cleared when the region is no longer a hotspot.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
19023	Critical	Quality of service	Tenant plane	HBase	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Hot Regions	Name of the region where the request traffic is restricted due to hotspotting.

Impact on the System

If the traffic of a hotspot region is restricted, the number of handlers for processing the requests in the region is limited. As a result, services requesting the region may slow down or retry upon failure.

Possible Causes

Too many requests are directed to a single region when the HBase service is accessed.

Handling Procedure

Check whether there are too many requests in a single region of HBase.

Step 1 Log in to FusionInsight Manager, and Choose **O&M** > **Alarm** > **Alarms**.

Step 2 In **Additional Information** of **Region Traffic Restriction for HBase**, view the reported table name and region information.

Step 3 On FusionInsight Manager, choose **Cluster** > **Service** > **HBase** and click the hyperlink on the right of HMaster web UI.

Step 4 Click **Table Details** and adjust service configurations in the region where the table in **Step 2** is deployed.

Step 5 Wait a moment and then check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **HBase** for the target cluster.

Step 8 In the **Host** area, select the host where the HMaster instance is deployed.

Step 9 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm will be automatically cleared.

Related Information

None.

1.3.211 ALM-19024 RPC Requests P99 Latency on RegionServer Exceeds the Threshold

Alarm Description

The system checks P99 latency for RPC requests on each RegionServer instance of the HBase service every 30 seconds. This alarm is generated when P99 latency for RPC requests on a RegionServer exceeds the threshold for 10 consecutive times.

This alarm is cleared when P99 latency for RPC requests on a RegionServer instance is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
19024	• **Critical**: The default threshold is 10 seconds. • **Major**: The default threshold is 5 seconds.	Quality of service	Tenant plane	HBase	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.

Type	Parameter	Description
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Threshold	Specifies the threshold for generating the alarm.

Impact on the System

If RPC requests P99 latency exceeds the threshold, the RegionServer cannot deliver normal service performance externally. For latency-sensitive services, a large number of service read and write requests may time out.

Possible Causes

- RegionServer GC duration is too long.
- The HDFS RPC response is too slow.
- RegionServer request concurrency is too high.

Handling Procedure

Step 1 Log in to FusionInsight Manager and choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**. On the page that is displayed, locate the row

containing the alarm whose **Alarm ID** is **19024**, and view the service instance and host name in **Location**.

Check the GC duration of RegionServer.

Step 2 In the alarm list on FusionInsight Manager, check whether the "HBase GC Duration Exceeds the Threshold" alarm is generated for the service instance in **Step 1**.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 Rectify the fault by following the handling procedure of "ALM-19007 HBase GC Duration Exceeds the Threshold".

Step 4 Wait several minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check HDFS RPC response time.

Step 5 In the alarm list on FusionInsight Manager, check whether alarm "Average NameNode RPC Processing Time Exceeds the Threshold" is generated for the HDFS service on which the HBase service depends.

- If yes, go to **Step 6**.
- If no, go to **Step 8**.

Step 6 Rectify the fault by following the handling procedure of "ALM-14021 Average NameNode RPC Processing Time Exceeds the Threshold".

Step 7 Wait several minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Check the number of concurrent processes on a RegionServer.

Step 8 In the alarm list on FusionInsight Manager, check whether the "Handler Usage of RegionServer Exceeds the Threshold" alarm is generated for the service instance in **Step 1**.

- If yes, go to **Step 9**.
- If no, go to **Step 11**.

Step 9 Rectify the fault by following the handling procedure of "ALM-19021 Handler Usage of RegionServer Exceeds the Threshold".

Step 10 Wait several minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 11**.

Collect fault information.

Step 11 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 12 Expand the **Service** drop-down list, and select **HBase** for the target cluster.

Step 13 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 14 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.212 ALM-19025 Damaged StoreFile in HBase

Alarm Description

The system checks the **hdfs://hacluster/hbase/autocorrupt** and **hdfs://hacluster/hbase/MasterData/autocorrupt** directories on HDFS of each HBase service every 120 seconds. This alarm is generated when there are files in the directories.

This alarm is cleared when the **hdfs://hacluster/hbase/autocorrupt** and **hdfs://hacluster/hbase/MasterData/autocorrupt** directories do not exist or are empty.

NOTE

hdfs://hacluster indicates the name of the file system used by HBase, and **/hbase** indicates the root directory of HBase in the file system. You can log in to FusionInsight Manager, choose **Cluster** > **Services** > **HBase** and click **Configuration**. Search for **fs.defaultFS** and **hbase.data.rootdir**.

If multiple HBase services have been installed, determine the HBase service for which the alarm is generated based on the value of **ServiceName** in **Location**. For HBase-1, for example, the service name displayed in the **Location** column is **HBase-1**, and the root directory of the file system in the handling procedure **/hbase-1**.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
19025	Major	Error handling	Tenant plane	HBase	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

Data in the file may be lost, and data queried by the service may be inconsistent.

Possible Causes

The StoreFile files are damaged.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Handling Procedure

Step 1 Log in to FusionInsight Manager and choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**. On the page that is displayed, locate the row containing the alarm whose **Alarm ID** is **19025**, and view the service in **Location**.

Step 2 Log in to the node where the HDFS and HBase clients are installed as the client installation user and run the following commands:

cd *Client installation directory*

source bigdata_env

kinit *Component service user* (If Kerberos authentication is disabled for the cluster (the cluster is in normal mode), skip this step.)

Step 3 Check the damaged StoreFile file.

- Run the following command to check whether the **/hbase/autocorrupt** directory of HDFS is empty. If it is not, go to **Step 4**.

  hdfs dfs -ls -R hdfs://hacluster/hbase/autocorrupt

- Run the following command to check whether the **/hbase/MasterData/autocorrupt** directory of HDFS is empty. If it is not, go to **Step 9**.

  hdfs dfs -ls -R hdfs://hacluster/hbase/MasterData/autocorrupt

Step 4 Run the following command to restore the StoreFile files in the **hdfs://hacluster/hbase/autocorrupt** directory:

hdfs debug recoverLease -path hdfs://hacluster/hbase/autocorrupt/*Name space***/**Table**/**Region**/**Column family**/***StoreFile files*

Step 5 Check whether the damaged StoreFile files are restored. If the following information is displayed, the restoration is successful:

```
recoverLease SUCCEEDED on hdfs://hacluster/hbase/autocorrupt/
default/h1/865665fe32db62dadada68b644359809/cf1/95f210f931ad44c99e4028470be7d292
```

If yes, go to **Step 6**.

If no, go to **Step 9**.

Step 6 Run the following command to move the files back to the **hdfs://hacluster/hbase/data** directory:

hdfs dfs -mv hdfs://hacluster/hbase/autocorrupt/*Name space***/**Table**/**Region**/**Column family**/***StoreFile files***hdfs://hacluster/hbase/data/***Name space***/**Table**/**Region**/**Column family**/***StoreFile files*

Step 7 Run the following command on HBase Shell to bring the region online again:

hbase shell

unassign'*Region***'**

assign'*Region***'**

Step 8 Wait several minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Collect fault information.

Step 9 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 10 Expand the **Service** drop-down list, and select **HBase** for the target cluster.

Step 11 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.213 ALM-19026 Damaged WAL Files in HBase

Alarm Description

The system checks the **hdfs://hacluster/hbase/corrupt** directory on the HDFS of each HBase service every 120 seconds. This alarm is generated when there are WAL files in the **/hbase/corrupt** directory.

This alarm is cleared when the **/hbase/corrupt** directory does not exist or does not contain WAL files.

NOTE

hdfs://hacluster indicates the name of the file system used by HBase, and **/hbase** indicates the root directory of HBase in the file system. You can log in to FusionInsight Manager, choose **Cluster** > **Services** > **HBase** and click **Configuration**. Search for **fs.defaultFS** and **hbase.data.rootdir**.

If multiple HBase services have been installed, determine the HBase service for which the alarm is generated based on the value of **ServiceName** in **Location**. For HBase-1, for example, the service name displayed in the **Location** column is **HBase-1**, and the root directory of the file system in the handling procedure **/hbase-1**.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
19026	Major	Error handling	Tenant plane	HBase	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

If the data in the damaged file is not flushed to disks, the data will be lost. As a result, some data queried by the service is inconsistent.

Possible Causes

The WAL files are damaged.

Handling Procedure

Step 1 Log in to FusionInsight Manager and choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**. On the page that is displayed, locate the row containing the alarm whose **Alarm ID** is **19026**, and view the service in **Location**.

Step 2 Log in to the node where the HDFS clients are installed as the client installation user and run the following commands:

cd *Client installation directory*

source bigdata_env

kinit *Component service user* (If Kerberos authentication is disabled for the cluster (the cluster is in normal mode), skip this step.)

Step 3 Run the following command to check the damaged WAL files and go to **Step 4**:

hdfs dfs -ls hdfs://hacluster/hbase/corrupt/*%2C*

Collect fault information.

Step 4 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 5 Expand the **Service** drop-down list, and select **HBase** for the target cluster.

Step 6 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 7 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.214 ALM-19030 P99 Latency of RegionServer RPC Request Exceeds the Threshold

Alarm Description

The system checks the P99 latency for responding to RPC requests on each RegionServer instance of the HBase service every 30 seconds. This alarm is generated when P99 latency on a RegionServer instance exceeds the threshold for 10 consecutive times.

This alarm is cleared when the P99 latency on a RegionServer instance is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
19030	• **Critical**: The default threshold is 10 seconds. • **Major**: The default threshold is 5 seconds.	Quality of service	Tenant plane	HBase	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
New	3.3.1	New alarm	New alarm

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Threshold	Specifies the threshold for generating the alarm.

Impact on the System

The RegionServer's capability of providing services for external systems is affected. For latency-sensitive services, a large number of service read and write requests may time out.

Possible Causes

- RegionServer GC duration is too long.
- The HDFS RPC response is too slow.
- The client requests are at scale with high concurrency.

Handling Procedure

Step 1 Log in to FusionInsight Manager and choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**. On the page that is displayed, locate the row containing the alarm whose **Alarm ID** is **19030**, and view the service instance and host name in **Location**. Click the host name and record the service IP address of the host.

Check the GC duration of the RegionServer.

Step 2 In the alarm list on FusionInsight Manager, check whether the "HBase GC Duration Exceeds the Threshold" alarm is generated for the service instance in **Step 1**.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 Rectify the fault by following the handling procedure of "ALM-19007 HBase GC Duration Exceeds the Threshold".

Step 4 Wait several minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check HDFS RPC response time.

Step 5 In the alarm list on FusionInsight Manager, check whether an alarm is generated for the DataNode instance of the HDFS service on which HBase depends, or whether the alarm "Slow Disk Fault", "Disk Unavailable", or "Average NameNode RPC Processing Time Exceeds the Threshold" is generated on the node where the alarm is generated.

- If yes, go to **Step 6**.
- If no, go to **Step 8**.

Step 6 Rectify the fault by following the handling procedure of the DataNode alarms: "ALM-12033 Slow Disk Fault", "ALM-12063 Disk Unavailable", or "ALM-14021 Average NameNode RPC Processing Time Exceeds the Threshold".

Step 7 Wait several minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Step 8 Log in to the node for which the alarm is generated, run the **iostat -x 2** command to check the disk I/O. In the command output, check whether the value in the **util** column of each disk is greater than 90%.

- If yes, go to **Step 9**.
- If no, go to **Step 11**.

Step 9 Choose **Cluster** > **Services** > **HDFS** > **Instances**, select the DataNode instance of the node for which the alarm is generated, choose **More** > **Stop Instance**, enter the password of the current user, and click **OK** to stop the DataNode instance.

Step 10 Wait several minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 11**.

Check the number of concurrent processes on a RegionServer.

Step 11 In the alarm list on FusionInsight Manager, check whether the "Handler Usage of RegionServer Exceeds the Threshold" alarm is generated for the service instance in **Step 1**.

- If yes, go to **Step 12**.
- If no, go to **Step 14**.

Step 12 Rectify the fault by following the handling procedure of "ALM-19021 Handler Usage of RegionServer Exceeds the Threshold".

Step 13 Wait several minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 14**.

Collect fault information.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 14 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 15 Expand the **Service** drop-down list, and select **HBase** for the target cluster.

Step 16 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 17 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.215 ALM-19031 Number of RegionServer RPC Connections Exceeds the Threshold

Alarm Description

The system checks the number of RegionServer RPC connections in each HBase service every 30 seconds. This alarm is generated when the number of RPC connections of a RegionServer instance exceeds the threshold for 10 consecutive times.

This alarm is cleared when the number of RPC connections of a RegionServer instance is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
19031	• Critical (default threshold: 200) • Major (default threshold: 100)	Quality of service	Tenant plane	HBase	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
New	3.3.1	New alarm	New alarm

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Threshold	Specifies the threshold for generating the alarm.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

There are a large amount of concurrent access requests on the RegionServer node, which imposes great pressure and causes slow response. For latency-sensitive services, a large number of service read and write requests may time out.

Possible Causes

Too many concurrent requests are sent from applications to access HBase.

Handling Procedure

Step 1 Log in to FusionInsight Manager and choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**. On the page that is displayed, locate the row containing the alarm whose **Alarm ID** is **19031**, and view the service instance and host name in **Location**.

Check the number of concurrent requests accessing HBase.

Step 2 Log in to the node where the HBase client is installed and check whether **hbase.client.ipc.pool.size** in the *Client installation directory*/**HBase/hbase/conf/hbase-site.xml** file is set to a large value.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 Decrease the value of **hbase.client.ipc.pool.size** and save the change.

Step 4 Wait several minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Step 5 Check whether the number of concurrent requests accessing the HBase service is too large.

- If yes, go to **Step 6**.
- If no, go to **Step 8**.

Step 6 Decrease the number of concurrent requests based on the site requirements.

Step 7 Wait several minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Collect fault information.

Step 8 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 9 Expand the **Service** drop-down list, and select **HBase** for the target cluster.

Step 10 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 11 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.216 ALM-19032 Number of Tasks in the RegionServer RPC Write Queue Exceeds the Threshold

Alarm Description

The system checks the number of tasks waiting in the RPC write queue for the RegionServer instances of the HBase service every 30 seconds. This alarm is generated when the number of waiting tasks exceeds the threshold for 10 consecutive times.

This alarm is cleared when the number of waiting tasks is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
19032	• Critical (default threshold: 2000) • Major (default threshold: 1600)	Quality of service	Tenant plane	HBase	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
New	3.3.1	New alarm	New alarm

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Threshold	Specifies the threshold for generating the alarm.

Impact on the System

Request queues are stacked, and the RegionServer memory GC pressure increases. As a result, the response time of write requests increases. For latency-sensitive services, a large number of service write requests may time out.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Possible Causes

- The RegionServer heap memory is not properly configured.
- A slow disk fault occurred.
- The RegionServer configuration is improper.
- Regions of RegionServers are not evenly distributed and hotspotting occurred.
- The latency of WAL Sync operations is high.

Handling Procedure

Step 1 Log in to FusionInsight Manager and choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**. On the page that is displayed, locate the row containing the alarm whose **Alarm ID** is **19032**, and view the service instance and host name in **Location**.

Check RegionServer heap memory.

Step 2 In the alarm list on FusionInsight Manager, check whether the "Heap Memory Usage of the HBase Process Exceeds the Threshold" alarm is generated for the service instance in **Step 1**.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 Rectify the fault by following the handling procedure of "ALM-19008 Heap Memory Usage of the HBase Process Exceeds the Threshold".

Step 4 Wait several minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Step 5 On FusionInsight Manager, choose **Cluster** > **Services** > **HBase** > **Chart**, select **GC** from the chart category, and check whether the GC times and GC monitoring period are normal.

- If yes, go to **Step 6**.
- If no, go to **Step 9**.

Step 6 Click **Configurations**, search for **GC_OPTS**, and increase the value of **Xmx** of the RegionServer within the allowed memory range. Set the value to a number less than or equal to 31 GB. Click **Save**.

Step 7 Click **Dashboard** and click **More** > **Restart Service** to restart the HBase service.

Step 8 Wait several minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Check for slow disk fault.

Step 9 Check whether alarm "Slow Disk Fault" or "Disk Unavailable" are generated on the node.

- If yes, go to **Step 10**.
- If no, go to **Step 12**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 10 Rectify the fault by following the handling procedure of "ALM-12033 Slow Disk Fault" or "ALM-12063 Disk Unavailable".

Step 11 Wait several minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 12**.

Check the RegionServer configuration.

Step 12 On FusionInsight Manager, choose **Cluster** > **Service** > **HBase**, click **Configurations** > **All Configurations**, and check whether the values of **hbase.wal.hsync** and **hbase.hfile.hsync** are **true**.

- If yes, go to **Step 13**.
- If no, go to **Step 15**.

Step 13 Set both **hbase.wal.hsync** and **hbase.hfile.hsync** to **false** and click **Save**. Click **Dashboard** and click **More** > **Restart Service** to restart the HBase service.

Step 14 Wait several minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 15**.

Check whether RegionServer regions are evenly distributed.

Step 15 On FusionInsight Manager, choose **Cluster** > **Services** > **HBase**. Click **HMaster(Active)** on the right of **HMaster Web UI** to go to the web UI of the HBase instance. View the **Base Stats** tab in the **Region Servers** area. Check whether the number of regions in the **Num.Regions** column is even.

- If yes, go to **Step 20**.
- If no, go to **Step 16**.

Step 16 Log in to the node where the HBase client is deployed as the **omm** user.

Step 17 Run the following commands to go to the client installation directory and set the environment variable:

cd *Client installation directory*

source bigdata_env

kinit *the **supergroup** user group or a user with the Global Admin permission* (If Kerberos authentication is disabled for the cluster, skip this operation.)

Step 18 Run the following commands to enable HBase load balancing and check whether the function is successfully enabled:

hbase shell

balance_switch true

balancer_enabled

If the command output is **true**, load balancing is enabled.

Run the **balancer** command to manually trigger the load balancing function.

NOTE

You are advised to enable and trigger load balancing during off-peak hours.

Step 19 Wait several minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 20**.

Check the WAL sync latency.

Step 20 On FusionInsight Manager, choose **Cluster** > **Services** > **HBase** > **Chart**. In the **Chart Category** area, select **Operations**. Check whether the value of "**P99.9th Percentile of WAL Sync Operation Delay-All Instances**" exceeds 500 ms.

- If yes, go to **Step 21**.
- If no, go to **Step 22**.

Step 21 Click **Instances**, select the RegionServer instance for which the alarm is generated, and choose **More** > **Restart Instance**. You also need to perform **Step 22** and provide the logs to technical support for fault locating.

Collect fault information.

Step 22 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 23 Expand the **Service** drop-down list, and select **HBase** for the target cluster.

Step 24 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 25 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.217 ALM-19033 Number of Tasks in the RegionServer RPC Read Queue Exceeds the Threshold

Alarm Description

The system checks the number of tasks waiting in the RPC read queue for the RegionServer instances of the HBase service every 30 seconds. This alarm is generated when the number of waiting tasks exceeds the threshold for 10 consecutive times.

This alarm is cleared when the number of waiting tasks is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
19033	• Critical (default threshold: 2000) • Major (default threshold: 1600)	Quality of service	Tenant plane	HBase	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
New	3.3.1	New alarm	New alarm

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Threshold	Specifies the threshold for generating the alarm.

Impact on the System

Request queues are stacked, and the response time of read requests increases. For latency-sensitive services, a large number of service read requests may time out.

Possible Causes

- The RegionServer heap memory configuration is improper.
- The RegionServer configuration is improper.
- Regions of RegionServers are unevenly distributed, and read hotspotting occurred.
- A slow disk fault occurred.

Handling Procedure

Step 1 Log in to FusionInsight Manager and choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**. On the page that is displayed, locate the row containing the alarm whose **Alarm ID** is **19033**, and view the service instance and host name in **Location**.

Check the heap memory configuration.

Step 2 In the alarm list on FusionInsight Manager, check whether the "Heap Memory Usage of the HBase Process Exceeds the Threshold" alarm is generated for the service instance in **Step 1**.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 Rectify the fault by following the handling procedure of "ALM-19008 Heap Memory Usage of the HBase Process Exceeds the Threshold".

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 4 Wait several minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Step 5 On FusionInsight Manager, choose **Cluster** > **Services** > **HBase** > **Chart**, select **GC** from the chart category, and check whether the GC times and GC monitoring period are normal.

- If yes, go to **Step 6**.
- If no, go to **Step 9**.

Step 6 Click **Configurations**, search for **GC_OPTS**, and increase the value of **Xmx** of the RegionServer within the allowed memory range. Set the value to a number less than or equal to 31 GB. Click **Save**.

Step 7 Click **Dashboard** and click **More** > **Restart Service** to restart the HBase service.

Step 8 Wait several minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Check the RegionServer configuration.

Step 9 On FusionInsight Manager, choose **Cluster** > **Services** > **HBase**, click **Configurations** > **All Configurations**, and check whether **hbase.bucketcache.size** is properly set. A larger value indicates a larger read cache and higher read performance. Increase the value based on the remaining memory of the node and click **Save**. Click **Dashboard** and click **More** > **Restart Service** to restart the HBase service.

Step 10 Wait several minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 11**.

Step 11 On the HBase dashboard, click the hyperlink on the right of **HMaster Web UI**. In the **User Tables** tab in the **Tables** area, click the name of the table hit by a large number of user read requests. In the **Table Schema** area of the **Table** tab, check whether the value of **BLOCKCACHE** is false.

- If yes, go to **Step 12**.
- If no, go to **Step 14**.

Table Schema

Property \ Column Family Name	cf1	cf2
BLOOMFILTER	ROW	ROW
IN_MEMORY	false	false
VERSIONS	1	1
KEEP_DELETED_CELLS	FALSE	FALSE
DATA_BLOCK_ENCODING	NONE	NONE
COMPRESSION	NONE	NONE
TTL	2147483647	2147483647
MIN_VERSIONS	0	0
BLOCKCACHE	true	true
BLOCKSIZE	65536	65536
REPLICATION_SCOPE	0	0

Step 12 Log in to the node where the HBase client is installed as user **omm**. Run the following commands to change the value of **BLOCKCACHE** of the **Step 11** table column family to **true**:

cd *Client installation directory*

source bigdata_env

kinit *the **supergroup** user group or a user with the Global Admin permission* (If Kerberos authentication is disabled for the cluster, skip this operation.)

hbase shell

alter'*Table name***', {NAME =>'***Column family name***', BLOCKCACHE => true}**

Run the following command to check whether the value of **BLOCKCACHE** of the column family is changed to **true**:

describe'*Table name***'**

Step 13 Wait several minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 14**.

Check whether regions of RegionServers are evenly distributed.

Step 14 On FusionInsight Manager, choose **Cluster** > **Services** > **HBase** and click **HMaster(Active)**. On the HBase web UI, check whether regions are evenly distributed in the **Num.Regions** column in the **Base Stats** tab in the **Region Servers** area.

- If yes, go to **Step 20**.
- If no, go to **Step 15**.

Step 15 Log in to the faulty RegionServer node as user **omm**.

Step 16 Run the following commands to go to the client installation directory and set the environment variable:

cd *Client installation directory*

source bigdata_env

kinit *the **supergroup** user group or a user with the Global Admin permission* (If Kerberos authentication is disabled for the cluster, skip this operation.)

Step 17 Run the following commands to check whether the load balancing function is enabled:

hbase shell

balancer_enabled

If the command output is **true**, load balancing is enabled.

- If yes, go to **Step 20**.
- If no, go to **Step 18**.

Step 18 Run the following commands to enable load balancing and check whether the function is successfully enabled:

balance_switch true

balancer_enabled

Run the **balancer** command to manually trigger the load balancing function.

NOTE

You are advised to enable and trigger load balancing during off-peak hours.

Step 19 Wait several minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 20**.

Check for slow disk fault.

Step 20 Check whether alarm "Slow Disk Fault" or "Disk Unavailable" are generated on the node in **Step 1**.

- If yes, go to **Step 21**.
- If no, go to **Step 23**.

Step 21 Rectify the fault by following the handling procedure of "ALM-12033 Slow Disk Fault" or "ALM-12063 Disk Unavailable".

Step 22 Wait several minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 23**.

Collect fault information.

Step 23 On FusionInsight Manager, choose **Cluster** > **Services** > **HBase** > **Chart**, select **IO** from the **Chart Category** area, and view the values of **Maximum Pread Latency-All Instances** and **Maximum Read Latency-All Instances**. Normal values do not exceed 100 ms.

Step 24 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 25 Expand the **Service** drop-down list, and select **HBase** for the target cluster.

Step 26 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 27 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.218 ALM-19034 Number of RegionServer WAL Write Timesouts Exceeds the Threshold

Alarm Description

The system checks the number of RegionServer WAL write timeouts in each HBase service every 30 seconds. This alarm is generated when the number of WAL write timeouts on a RegionServer instance exceeds the threshold for 10 consecutive times.

This alarm is cleared when the number of WAL write timeouts on a RegionServer instance is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
19034	• Critical (default threshold: 500) • Major (default threshold: 300)	Quality of service	Tenant plane	HBase	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
New	3.3.1	New alarm	New alarm

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Threshold	Specifies the threshold for generating the alarm.

Impact on the System

The write operation latency increases. Too many WAL write timeouts may severely deteriorate the data write performance.

Possible Causes

- A slow disk fault occurred.
- RegionServer GC is abnormal.
- HBase is overloaded.
- The WAL configuration is improper.

Handling Procedure

Step 1 Log in to FusionInsight Manager and choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**. On the page that is displayed, locate the row

containing the alarm whose **Alarm ID** is **19034**, and view the service instance and host name in **Location**.

Check whether a slow disk fault occurred.

Step 2 In the alarm list on FusionInsight Manager, check whether the "Slow Disk Fault" or "Disk Unavailable" is displayed.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 Rectify the fault by following the handling procedure of "ALM-12033 Slow Disk Fault" or "ALM-12063 Disk Unavailable".

Step 4 Wait several minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check whether RegionServer GC is abnormal.

Step 5 In the alarm list on FusionInsight Manager, check whether "ALM-19007 HBase GC Duration Exceeds the Threshold" is displayed.

- If yes, go to **Step 6**.
- If no, go to **Step 8**.

Step 6 Rectify the fault by following the handling procedure of "ALM-19007 HBase GC Duration Exceeds the Threshold".

Step 7 Wait several minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Check the HBase load.

Step 8 In the alarm list on FusionInsight Manager, check whether "ALM-19018 HBase Compaction Queue Size Exceeds the Threshold" is displayed.

- If yes, go to **Step 9**.
- If no, go to **Step 11**.

Step 9 Rectify the fault by following the handling procedure of "ALM-19018 HBase Compaction Queue Size Exceeds the Threshold".

Step 10 Wait several minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 11**.

Check the WAL configuration.

Step 11 On FusionInsight Manager, choose **Cluster** > **Service** > **HBase**, click **Configurations** > **All Configurations**, and check whether the values of **hbase.wal.hsync** and **hbase.hfile.hsync** are **true**.

- If yes, go to **Step 12**.
- If no, go to **Step 14**.

Step 12 Set both **hbase.wal.hsync** and **hbase.hfile.hsync** to **false** and click **Save**. Click **Dashboard** and click **More** > **Restart Service** to restart the HBase service.

Step 13 Wait several minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 14**.

Collect fault information.

Step 14 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 15 Expand the **Service** drop-down list, and select **HBase** for the target cluster.

Step 16 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 17 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.219 ALM-19035 Size of the RegionServer Call Queue Exceeds the Threshold

Alarm Description

The system checks the size of the RegionServer call queue for each HBase service every 30 seconds. This alarm is generated when the call queue of a RegionServer instance is bigger than the threshold for 10 consecutive times.

This alarm is cleared when the call queue of a RegionServer instance is no bigger than the threshold.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
19035	• Critical (default threshold: 800 MB) • Major (default threshold: 600 MB)	Quality of service	Tenant plane	HBase	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
New	3.3.1	New alarm	New alarm

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Threshold	Specifies the threshold for generating the alarm.

Impact on the System

Request queues are stacked, and the RegionServer memory GC pressure increases. As a result, the response time of read requests increases. For latency-sensitive services, a large number of service read requests may time out.

Possible Causes

- The RegionServer heap memory configuration is improper.
- A slow disk fault occurred.
- The RegionServer configuration is improper.
- Regions of RegionServers are not evenly distributed and hotspotting occurred.
- The latency of WAL Sync operations is high.

Handling Procedure

Step 1 Log in to FusionInsight Manager and choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**. On the page that is displayed, locate the row containing the alarm whose **Alarm ID** is **19035**, and view the service instance and host name in **Location**.

Check the heap memory configuration.

Step 2 In the alarm list on FusionInsight Manager, check whether the "Heap Memory Usage of the HBase Process Exceeds the Threshold" alarm is generated for the service instance in **Step 1**.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 Rectify the fault by following the handling procedure of "ALM-19008 Heap Memory Usage of the HBase Process Exceeds the Threshold".

Step 4 Wait several minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Step 5 On FusionInsight Manager, choose **Cluster** > **Services** > **HBase** > **Chart**, select **GC** from the chart category, and check whether the GC times and GC monitoring period are normal.

- If yes, go to **Step 6**.
- If no, go to **Step 9**.

Step 6 Click **Configurations**, search for **GC_OPTS**, and increase the value of **Xmx** of the RegionServer within the allowed memory range. Set the value to a number less than or equal to 31 GB. Click **Save**.

Step 7 Click **Dashboard** and click **More** > **Restart Service** to restart the HBase service.

Step 8 Wait several minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Check for slow disk fault.

Step 9 Check whether alarm "Slow Disk Fault" or "Disk Unavailable" are generated for the same node in **Step 1**.

- If yes, go to **Step 10**.
- If no, go to **Step 12**.

Step 10 Rectify the fault by following the handling procedure of "ALM-12033 Slow Disk Fault" or "ALM-12063 Disk Unavailable".

Step 11 Wait several minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 12**.

Check the RegionServer configuration.

Step 12 On FusionInsight Manager, choose **Cluster** > **Service** > **HBase**, click **Configurations** > **All Configurations**, and check whether the values of **hbase.wal.hsync** and **hbase.hfile.hsync** are **true**.

- If yes, go to **Step 13**.
- If no, go to **Step 15**.

Step 13 Set both **hbase.wal.hsync** and **hbase.hfile.hsync** to **false** and click **Save**. Click **Dashboard** and click **More** > **Restart Service** to restart the HBase service.

Step 14 Wait several minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 15**.

Check whether RegionServer regions are evenly distributed.

Step 15 On FusionInsight Manager, choose **Cluster** > **Services** > **HBase**. Click **HMaster(Active)** on the right of **HMaster Web UI** to go to the web UI of the

HBase instance. View the **Base Stats** tab in the **Region Servers** area. Check whether the number of regions in the **Num.Regions** column is even.

- If yes, go to **Step 20**.
- If no, go to **Step 16**.

Step 16 Log in to the faulty RegionServer node as user **omm**.

Step 17 Run the following commands to go to the client installation directory and set the environment variable:

cd *Client installation directory*

source bigdata_env

kinit *the **supergroup** user group or a user with the Global Admin permission* (If Kerberos authentication is disabled for the cluster, skip this operation.)

Step 18 Run the following commands to enable load balancing and check whether the function is successfully enabled:

hbase shell

balance_switch true

balancer_enabled

If the command output is **true**, load balancing is enabled.

Run the **balancer** command to manually trigger the load balancing function.

NOTE

You are advised to enable and manually trigger the load balancing function during off-peak hours.

Step 19 Wait several minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 20**.

Check the WAL sync latency.

Step 20 On FusionInsight Manager, choose **Cluster** > **Services** > **HBase** > **Chart**. In the **Chart Category** area, select **Operations**. Check whether the value of "**P99.9th Percentile of WAL Sync Operation Delay-All Instances**" exceeds 500 ms.

- If yes, go to **Step 21**.
- If no, go to **Step 22**.

Step 21 Click **Instances**, select the RegionServer instance for which the alarm is generated, and choose **More** > **Restart Instance**. You also need to perform **Step 22** and provide the logs to technical support for fault locating.

Collect fault information.

Step 22 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 23 Expand the **Service** drop-down list, and select **HBase** for the target cluster.

Step 24 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 25 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.220 ALM-20002 Hue Service Unavailable

Alarm Description

The system checks the Hue service status every 60 seconds. This alarm is generated if the Hue service is unavailable.

This alarm is cleared when the Hue service is normal.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
20002	Critical	Error handling	Tenant plane	Hue	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.

Type	Parameter	Description
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

Users cannot perform interactive analysis and data processing with MRS on the Hue UI.

Possible Causes

- The KrbServer service on which Hue depends is abnormal.
- The DBService service on which Hue depends is abnormal.
- The network connection to DBService is abnormal.

Handling Procedure

Check whether the KrbServer service is normal.

Step 1 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services**. In the service list, check whether the status of KrbServer is **Normal**.

- If yes, go to **Step 4**.
- If no, go to **Step 2**.

Step 2 Manually restart the KrbServer service.

Step 3 Wait for several minutes. Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 4**.

Check whether DBService is normal.

Step 4 Log in to FusionInsight Manager, click **Cluster**, click the name of the desired cluster, and click **Services**.

Step 5 In the service list, check whether **Health Status** of **DBService** is **Good**.

- If yes, go to **Step 8**.
- If no, go to **Step 6**.

Step 6 Restart the DBService service.

NOTE

To restart the service, you need to enter the password of the FusionInsight Manager administrator.

Step 7 Wait for several minutes. Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Check whether the network connection to the DBService is normal.

Step 8 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services**, click **Hue**, and click the **Instances** tab. Record the IP address of the active Hue node.

Step 9 Log in to the IP address of the active Hue node.

Step 10 Run the **ping** command to check whether the network connection between the host where the active Hue is deployed and the host where DBService is deployed is normal. (The method of obtaining the DBService service IP address is the same as that of obtaining the active Hue IP address.)

- If yes, go to **Step 13**.
- If no, go to **Step 11**.

Step 11 Contact the network administrator to restore the network.

Step 12 Wait for several minutes. Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 13**.

Collect fault information.

Step 13 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 14 Select the following components for **Service**.

- Hue
- Controller

Step 15 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 16 On FusionInsight Manager, choose **Cluster**, click the name of the desired cluster, and choose **Services** > **Hue**.

Step 17 Choose **More** > **Restart Service** and click **OK**.

Step 18 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 19**.

Step 19 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.221 ALM-23001 Loader Service Unavailable

Alarm Description

The system checks the Loader service availability every 60 seconds. This alarm is generated if the Loader service is unavailable and is cleared after the Loader service recovers.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
23001	Critical	Error handling	Tenant plane	Loader	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.

Type	Parameter	Description
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

Data loading, import, and conversion are unavailable.

Possible Causes

- The services that Loader depends on are abnormal.
  - The ZooKeeper service is abnormal.
  - The HDFS service is abnormal.
  - The DBService service is abnormal.
  - The Yarn service is abnormal.
  - MapReduce is abnormal.
- The network is faulty. Loader cannot communicate with its dependent services.
- Loader is running improperly.

Handling Procedure

Check the ZooKeeper service status.

Step 1 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **ZooKeeper** to check whether ZooKeeper is running properly.

- If yes, go to **Step 3**.
- If no, go to **Step 2**.

Step 2 Choose **More** > **Restart Service** to restart ZooKeeper. After ZooKeeper starts, check whether the "Loader Service Unavailable" alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 3**.

Step 3 In the alarm list on the FusionInsight Manager, check whether the alarm "Process Fault" is generated.

- If yes, go to **Step 4**.
- If no, go to **Step 7**.

Step 4 In **Location** of **ALM-12007 Process Fault**, check whether the service name is **ZooKeeper**.

- If yes, go to **Step 5**.
- If no, go to **Step 7**.

Step 5 Rectify the fault by following steps provided in **ALM-12007 Process Fault**.

Step 6 In the alarm list, check whether this alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Check the HDFS service status.

Step 7 In the alarm list on FusionInsight Manager, check whether an alarm is generated indicating that the HDFS service is unavailable.

- If yes, go to **Step 8**.
- If no, go to **Step 10**.

Step 8 Rectify the fault by performing the operations provided for **ALM-14000 HDFS Service Unavailable**.

Step 9 In the alarm list, check whether this alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 10**.

Check the DBService status.

Step 10 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **DBService** to check whether DBService is running properly.

- If yes, go to **Step 12**.
- If no, go to **Step 11**.

Step 11 Choose **More** > **Restart Service** to restart DBService. After DBService starts, check whether the "Loader Service Unavailable" alarm is cleared.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If yes, no further action is required.
- If no, go to **Step 12**.

Check the MapReduce status.

Step 12 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Mapreduce** to check whether MapReduce is running properly.

- If yes, go to **Step 16**.
- If no, go to **Step 13**.

Step 13 Choose **More** > **Restart Service** to restart MapReduce. After MapReduce starts, check whether the "Loader Service Unavailable" alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 16**.

Check the Yarn service status.

Step 14 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Yarn** to check whether Yarn is running properly.

- If yes, go to **Step 16**.
- If no, go to **Step 15**.

Step 15 Choose **More** > **Restart Service** to restart Yarn. After Yarn starts, check whether the "Loader Service Unavailable" alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 16**.

Step 16 In the alarm list on FusionInsight Manager, check whether an alarm is generated indicating that the Yarn service is unavailable.

- If yes, go to **Step 17**.
- If no, go to **Step 19**.

Step 17 Rectify the fault by performing the operations provided for **ALM-18000 Yarn Service Unavailable**.

Step 18 In the alarm list, check whether this alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 19**.

Check the network connections between Loader and its dependent components.

Step 19 On FusionInsight Manager, choose **Cluster**, click the name of the desired cluster, and choose **Services** > **Loader**.

Step 20 Click **Instance**. The LoaderServer instance list is displayed.

Step 21 Record the management IP address in the **LoaderServer(Active)** row.

Step 22 Log in to the host where LoaderServer resides as user **omm** using the IP address obtained in **Step 21**.

Step 23 Run the **ping** command to check whether the network connection between the hosts where the LoaderServer instances reside and the dependent components is

normal. (The dependent components include ZooKeeper, DBService, HDFS, MapReduce, and Yarn. The method to obtain the IP addresses of the dependent components is the same as that used to obtain the IP addresses of the active LoaderServer instances.)

- If yes, go to **Step 26**.
- If no, go to **Step 24**.

Step 24 Contact the network administrator to restore the network.

Step 25 In the alarm list, check whether this alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 26**.

Collect fault information.

Step 26 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 27 Expand the **Service** drop-down list, and select the following services for the target cluster:

- Zookeeper
- HDFS
- DBService
- Yarn
- MapReduce
- Loader

Step 28 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 29 On FusionInsight Manager, choose **Cluster**, click the name of the desired cluster, and choose **Services** > **Loader**.

Step 30 Choose **More** > **Restart Service** and click **OK**.

Step 31 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 32**.

Step 32 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.222 ALM-23003 Loader Task Execution Failed

Alarm Description

This alarm is generated when the system detects that the Loader job fails. This alarm is cleared when the failed job is handled by a user. This alarm must be manually cleared.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
23003	Minor	Quality of service	Tenant plane	Loader	No

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	HostName	Specifies the host for which the alarm was generated.
	Alarm Severity	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Task ID	Identifies the failed Loader job.
	JobName	Specifies the name of the task that fails to be backed up.
	User Identification	Specifies the name of the user who submits the Loader job.
	Details	Specifies additional alarm information.

Impact on the System

This is a job-level alarm for Loader. The job execution fails, and you need to view specific logs to locate the failure cause. No execution result is returned. After the fault is rectified, you need to execute the task again. No impact on the Loader service.

Possible Causes

- Task parameters are incorrectly configured.
- Exceptions occur when Yarn is executing a task.

Handling Procedure

Check whether task parameters are incorrectly configured.

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Alarms**. In the alarm list, open the drop-down list and view the alarm cause.

Step 2 If the alarm cause is **Failed to submit the task**, view the error details in **Additional Information** and view the execution records of the task on the Loader page.

NOTE

By default, the **admin** user does not have the permissions to manage other components. If the page cannot be opened or the displayed content is incomplete when you access the native UI of a component due to insufficient permissions, you can manually create a user with the permissions to manage that component.

Step 3 Submit the task again.

Step 4 Check whether the task executed successfully.

- If yes, go to **Step 9**.

- If no, go to **Step 5**.

Check whether exceptions occur when Yarn is executing a task.

Step 5 Log in to FusionInsight Manager. In the alarm list, open the drop-down list to view the alarm cause.

Step 6 Check Yarn activities. If the alarm cause is "Yarn execution failed", the Yarn activity is abnormal.

- If yes, go to **Step 7**.
- If no, go to **Step 10**.

Step 7 Submit the task again.

Step 8 Check whether the task is executed successfully.

- If yes, go to **Step 9**.
- If no, go to **Step 10**.

Step 9 In the alarm list, click **Clear** in the **Operation** column of the alarm to manually clear the alarm. No further action is required.

Collect fault information.

Step 10 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 11 Expand the **Service** drop-down list, and select the following services for the target cluster:

- DBService
- HDFS
- Loader
- MapReduce
- Yarn
- ZooKeeper

Step 12 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 13 Contact technical support and provide the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system does not automatically clear this alarm and you need to manually clear the alarm.

Related Information

None.

1.3.223 ALM-23004 Loader Heap Memory Usage Exceeds the Threshold

Alarm Description

The system checks the heap memory usage of the Loader service every 60 seconds. This alarm is generated when the heap memory usage of the Loader instance exceeds the threshold for 10 consecutive times. The alarm is cleared when the heap memory usage is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
23004	Critical (default threshold: 95% of the maximum memory.) Major (default threshold: 90% of the maximum memory)	Environment	Tenant plane	Loader	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

Full GC occurs frequently in Loader. The performance deteriorates and page responses are slow. If the memory overflows, Loader may fail to provide services for external systems. The Loader page cannot be accessed, interfaces cannot be called, and active/standby switchover is frequently performed due to exceptions.

Possible Causes

The heap memory usage of the Loader instance is too high or the heap memory is inappropriately allocated.

Handling Procedure

Check heap memory usage.

Step 1 Log in to FusionInsight Manager and choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**. On the page that is displayed, locate the row containing **Loader Heap Memory Usage Exceeds the Threshold**, and view the **Location** information. Check the name of the instance host for which the alarm is generated.

Step 2 On FusionInsight Manager, choose **Cluster** > *Name of the target cluster* > **Services** > **Loader** and click the **Instance** tab. On the displayed page, select the role corresponding to the host name for which the alarm is generated and select **Customize** from the drop-down list in the upper right corner of the chart area.

Choose **Memory** and select **Loader Heap Memory Resource Percentage**. Click **OK**.

Step 3 Check whether the heap memory used by Loader reaches the threshold (95% of the maximum heap memory by default).

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Service** > **Loader** > **Configuration**, click **All Configurations**. Search for the **GC_OPTS** parameter, increase the value of **-Xmx** as you need, click **Save**, and click **OK**.

NOTE

- If this alarm is generated, the heap memory configured for the current Loader instance is not enough for data transmission. You are advised to open the instance monitoring page, display the Loader heap memory resource status monitoring chart, and observe the change trend of the heap memory used by Loader in the monitoring chart. Then change the value of **-Xmx** to twice the current heap memory usage or to another value to meet site requirements.
- When setting the heap memory, you can set **-Xms** and **-Xmx** to approximately the same value to prevent performance deterioration caused by heap size adjustment after each GC.
- The sum of **-Xmx** and **XX:MaxPermSize** cannot be greater than the actual physical memory of the node server.

Step 5 Restart the affected services or instances and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **Loader** for the target cluster.

Step 8 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.224 ALM-23005 Loader Non-Heap Memory Usage Exceeds the Threshold

Alarm Description

The system checks the non-heap memory usage of the Loader service every 30 seconds. This alarm is generated when the non-heap memory usage of the Loader instance exceeds the threshold for 5 consecutive times. This alarm is cleared if the non-heap memory usage is lower than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
23005	Critical (default threshold: 95% of the maximum memory.) Major (default threshold: 80% of the maximum memory)	Environment	Tenant plane	Loader	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

The Loader page may fail to be accessed and cannot provide services for external systems.

Possible Causes

The non-heap memory of the Loader instance is overused or the non-heap memory is inappropriately allocated.

Handling Procedure

Check non-heap memory usage.

Step 1 Log in to FusionInsight Manager and choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**. On the page that is displayed, locate the row containing **Loader Non-Heap Memory Usage Exceeds the Threshold**, and view the **Location** information. Check the name of the instance host for which the alarm is generated.

Step 2 On FusionInsight Manager, choose **Cluster** > *Name of the target cluster* > **Services** > **Loader** and click the **Instance** tab. On the displayed page, select the role corresponding to the host name for which the alarm is generated and select **Customize** from the drop-down list in the upper right corner of the chart area. Choose **Memory** and select **Loader Non-Heap Memory Resource Percentage**. Click **OK**.

Step 3 Check whether the non-heap memory used by Loader reaches the threshold (80% of the maximum non-heap memory by default).

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On FusionInsight Manager, choose **Cluster** > Name of the desired cluster > **Services** > **Loader**. Click **Configurations** and then the **All Configurations** tab. On the displayed page, search for **LOADER_GC_OPTS**. If the **-XX: MaxPermSize** parameter is not specified, you can set the initial value with **-XX: MaxPermSize=256M**. If the alarm persists, change the value again by referring to the note. Click **Save**, and then click **OK**

NOTE

Observe the change trend of the non-heap memory used by Loader in the "Loader non-heap memory resource status" monitoring chart. Then change the value of **-XX:MaxPermSize** to twice the current non-heap memory usage or to another value to meet site requirements.

Step 5 Restart the affected services or instances and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **Loader** for the target cluster.

Step 8 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.225 ALM-23006 Loader Direct Memory Usage Exceeds the Threshold

Alarm Description

The system checks the direct memory usage of the Loader service every 30 seconds. This alarm is generated when the direct memory usage of the Loader instance exceeds the threshold for five consecutive times. This alarm is cleared when the Loader direct memory usage is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
23006	Critical (default threshold: 95% of the maximum memory.) Major (default threshold: 80% of the maximum memory)	Environment	Tenant plane	Loader	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

Loader may fail to provide services for external systems. I/O or socket exceptions occur, and active/standby switchovers occur frequently.

Possible Causes

The direct memory of Loader instances is overused or the direct memory is inappropriately allocated.

Handling Procedure

Check the direct memory usage.

Step 1 Log in to FusionInsight Manager and choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**. On the page that is displayed, locate the row containing **Loader Direct Memory Usage Exceeds the Threshold**, and view the **Location** information. Check the name of the instance host for which the alarm is generated.

Step 2 On FusionInsight Manager, choose **Cluster** > *Name of the target cluster* > **Services** > **Loader** and click the **Instance** tab. On the displayed page, select the role corresponding to the host name for which the alarm is generated and select **Customize** from the drop-down list in the upper right corner of the chart area. Choose **Memory** and select **Loader Direct Memory Resource Usage Statistics**. Click **OK**.

Step 3 Check whether the direct memory used by Loader reaches the threshold (80% of the maximum direct memory by default).

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On FusionInsight Manager, choose **Cluster** > Name of the desired cluster > **Services** > **Loader**. Click **Configurations** and then the **All Configurations** tab. On the displayed page, search for **LOADER_GC_OPTS**. Increase the value of **-XX:MaxDirectMemorySize** as required, click **Save**, and click **OK**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

NOTE

Observe the change trend of the direct memory used by Loader in the "Loader direct memory resource status" monitoring chart. Then change the value of **-XX:MaxDirectMemorySize** to twice the current direct memory usage or to another value to meet site requirements.

Step 5 Restart the affected services or instances and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **Loader** for the target cluster.

Step 8 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.226 ALM-23007 GC Duration of the Loader Process Exceeds the Threshold

Alarm Description

The system checks the GC duration of the Loader process every 60 seconds. This alarm is generated when the GC duration of the Loader process exceeds the threshold for five consecutive times. This alarm is cleared when the GC duration is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
23007	Critical (default threshold: 20000 ms) Major (default threshold: 12000 ms)	Environment	Tenant plane	Loader	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

Full GC occurs frequently, and the Loader service responds slowly. The Loader service may even break down and cannot provide services properly.

Possible Causes

The heap memory of the Loader process is overused or inappropriately allocated, causing frequent occurrence of the GC process.

Handling Procedure

Check the GC duration.

Step 1 Log in to FusionInsight Manager and choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**. On the page that is displayed, locate the row containing **GC Duration of Loader Exceeds the Threshold**, and view the **Location** information. Check the name of the instance host for which the alarm is generated.

Step 2 On FusionInsight Manager, choose **Cluster** > *Name of the target cluster* > **Services** > **Loader** and click the **Instance** tab. On the displayed page, select the role corresponding to the host name for which the alarm is generated and select **Customize** from the drop-down list in the upper right corner of the chart area. Choose **GC** and select **GC Duration of Loader**. Click **OK**.

Step 3 Check whether the GC duration of the Loader process collected every minute exceeds the threshold (12 seconds by default).

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On FusionInsight Manager, choose **Cluster** > Name of the desired cluster > **Services** > **Loader**. Click **Configurations** and then the **All Configurations** tab. On the displayed page, search for **LOADER_GC_OPTS**. Increase the value of **-Xmx** as required, click **Save**, and click **OK**.

NOTE

If this alarm is generated, the heap memory configured for the current Loader instance cannot meet the heap memory requirements for data transmission. You are advised to handle this alarm by referring to **Step 4** (in **ALM-23004 Loader Heap Memory Usage Exceeds the Threshold**).

Step 5 Restart the affected services or instances and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **Loader** for the target cluster.

Step 8 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.227 ALM-24000 Flume Service Unavailable

Alarm Description

The alarm module checks the Flume service status every 180 seconds. This alarm is generated if the Flume service is abnormal.

This alarm is automatically cleared after the Flume service recovers.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
24000	Critical	Error handling	Tenant plane	Flume	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.

Type	Parameter	Description
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

Flume cannot work and data transmission is interrupted.

Possible Causes

All Flume instances are faulty.

Handling Procedure

Step 1 Log in to a Flume node as user **omm** and run the **ps -ef|grep "flume.role=server"** command to check whether the Flume process exists on the node.

- If yes, go to **Step 3**.

- If no, restart the faulty Flume node or Flume service and go to **Step 2**.

Step 2 In the alarm list, check whether alarm "Flume Service Unavailable" is cleared.

- If yes, no further action is required.
- If no, go to **Step 3**.

Collect the fault information.

Step 3 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 4 Expand the **Service** drop-down list, and select **Flume** for the target cluster.

Step 5 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 6 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.228 ALM-24001 Flume Agent Exception

Alarm Description

The Flume agent instance for which the alarm is generated cannot be started. This alarm is generated when the Flume agent process is faulty (The system checks in every 5 seconds.) or Flume agent fails to start (The system reporting alarms immediately).

This alarm is cleared when the Flume agent process recovers, Flume agent starts successfully and the alarm handling is completed.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
24001	Major	Error handling	Tenant plane	Flume	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	AgentId	Specifies the ID of the agent for which the alarm is generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

The Flume agent instance for which the alarm is generated cannot provide services properly, and the data transmission tasks of the instance are temporarily interrupted. Real-time data is lost during real-time data transmission.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Possible Causes

- The JAVA_HOME directory does not exist or the Java permission is incorrect.
- The Flume agent directory permission is incorrect.
- Flume agent fails to start.

Handling Procedure

Check whether the JAVA_HOME directory exists or whether the JAVA permission is correct.

Step 1 Log in to the host for which the alarm is generated as user **root**.

Step 2 Run the following command to obtain the installation directory of the Flume client for which the alarm is generated: (The value of **AgentId** can be obtained from **Location** of the alarm.)

ps -ef|grep *AgentId* **| grep -v grep | awk -F 'conf-file ' '{print $2}' | awk -F 'fusioninsight' '{print $1}'**

Step 3 Run the **su -** *Flume installation user* command to switch to the Flume installation user and run the **cd** *Flume client installation directory*/**fusioninsight-flume-1.11.0/conf/** command to go to the Flume configuration directory.

Step 4 Run the **cat ENV_VARS | grep JAVA_HOME** command.

Step 5 Check whether the **JAVA_HOME** directory exists. If the command output in **Step 4** is not empty and **ll $JAVA_HOME/** is not empty, the **JAVA_HOME** directory exists.

- If yes, go to **Step 7**.
- If no, go to **Step 6**.

Step 6 Specify a correct **JAVA_HOME** directory, for example, **export JAVA_HOME=${BIGDATA_HOME}/common/runtime0/jdk***Version number*.

Step 7 Run the **$JAVA_HOME/bin/java -version** command to check whether the Flume agent running user has the Java execution permission. If the Java version is displayed in the command output, the Java permission meets the requirement. Otherwise, the Java permission does not meet the requirement.

- If yes, go to **Step 9**.
- If no, go to **Step 8**.

NOTE

JAVA_HOME is the environment variable exported during Flume client installation. You can also go to *Flume client installation directory*/**fusioninsight-flume-1.11.0/conf** and run the **cat ENV_VARS | grep JAVA_HOME** command to view the variable value.

Step 8 Run the **chmod 750 $JAVA_HOME/bin/java** command to grant the Java execution permission to the Flume agent running user.

Check the directory permission of the Flume agent.

Step 9 Log in to the host for which the alarm is generated as user **root**.

Step 10 Run the following command to switch to the Flume agent installation directory:

cd *Flume client installation directory*/**fusioninsight-flume-1.11.0/conf/**

Step 11 Run the **ls -al * -R** command to check whether any file owner is the user who running the Flume agent.

- If yes, go to **Step 12**.
- If no, run the **chown** command to change the file owner to the user who runs the Flume agent.

Check the Flume agent configuration.

Step 12 Run the **cat properties.properties | grep spooldir** and **cat properties.properties | grep TAILDIR** commands to check whether the Flume source type is spoolDir or tailDir. If any command output is displayed, the Flume source type is spoolDir or tailDir.

- If yes, go to **Step 13**.
- If no, go to **Step 17**.

Step 13 Check whether the data monitoring directory exists.

- If yes, go to **Step 15**.
- If no, go to **Step 14**.

NOTE

- Run the **cat properties.properties | grep spoolDir** command to view the spoolDir monitoring directory.
- Run the **cat properties.properties | grep parentDir** command to view the tailDir monitoring directory.

Step 14 Specify a correct data monitoring directory.

Step 15 Check whether the Flume agent user has the read, write, and execute permissions on the monitoring directory specified in **Step 13**.

- If yes, go to **Step 17**.
- If no, go to **Step 16**.

NOTE

Go to the monitoring directory as the Flume running user. If files can be created, the Flume running user has the read, write, and execute permissions on the monitoring directory.

Step 16 Run the **chmod 777** *Flume monitoring directory* command to grant the Flume agent running user the read, write, and execute permissions on the monitoring directory specified in **Step 13**.

Step 17 Check whether the components connected to the Flume sink are in safe mode.

- If yes, go to **Step 18**.
- If no, go to **Step 23**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

NOTE

If the sinks in the **properties.properties** configuration file are the HDFS sink, Solr sink, and HBase sink, and the configuration file contains a keytab file, the components connected to the Flume sink are in safe mode.

If the sink in the **properties.properties** configuration file is the kafka sink and ***.security.protocol** is set to **SASL_PLAINTEXT** or **SASL_SSL**, Kafka connected to the Flume sink is in safe mode.

If the sink in the **properties.properties** configuration file is the ESSink and ***.securityEnable** is set to **true**, Elasticsearch connected to the Flume sink is in safe mode.

Step 18 Run the **ll** *ketab path* command to check whether the keytab authentication path specified by the ***.kerberosKeytab** parameter in the configuration file exists.

- If yes, go to **Step 20**.
- If no, go to **Step 19**.

NOTE

To view the ketab path, run the **cat properties.properties | grep keytab** command.

Step 19 Change the value of **kerberosKeytab** in **Step 18** to the custom keytab path and go to **Step 21**.

Step 20 Perform **Step 18** to check whether the Flume agent running user has the permission to access the keytab authentication file. If the keytab path is returned, the user has the permission. Otherwise, the user does not have the permission.

- If yes, go to **Step 22**.
- If no, go to **Step 21**.

Step 21 Run the **chmod 755** *ketab file* command to grant the read permission on the keytab file specified in **Step 19**, and restart the Flume process.

Step 22 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 23**.

Collect fault information.

Step 23 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 24 Expand the **Service** drop-down list, and select **Flume** for the target cluster.

Step 25 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 26 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.229 ALM-24003 Flume Client Connection Interrupted

Alarm Description

The alarm module monitors the port connection status on the Flume server. This alarm is generated if the Flume server fails to receive a connection message from the Flume client in three consecutive minutes.

This alarm is cleared after the Flume server receives a connection message from the Flume client.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
24003	Major	Communications	Tenant plane	Flume	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	Client IP Address	Specifies the IP address of the Flume client.
	Client Name	Specifies the agent name of the Flume client.
	Sink Name	Specifies the sink name of Flume Agent.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

The communication between the Flume client and the server fails. The Flume client cannot send data to the Flume server.

Possible Causes

- The network connection between the Flume client and the server is faulty.
- The Flume client's process is abnormal.
- The Flume client is incorrectly configured.

Handling Procedure

Check the network connection between the Flume client and the server.

Step 1 Log in to the host whose IP address is specified by **Flume ClientIP** in the alarm information as user **root**.

Step 2 Run the **ping** *Flume server IP address* command to check whether the network connection between the Flume client and the server is normal.

- If yes, go to **Step 3**.
- If no, go to **Step 11**.

Check whether the Flume client's process is normal.

Step 3 Log in to the host whose IP address is specified by **Flume ClientIP** in the alarm information as user **root**.

Step 4 Run the **ps -ef|grep flume |grep client** command to check whether the Flume client process exists.

- If yes, go to **Step 5**.
- If no, go to **Step 11**.

Check the Flume client configuration.

Step 5 Log in to the host whose IP address is specified by **Flume ClientIP** in the alarm information as user **root**.

Step 6 Run the **cd** *Flume client installation directory*/**fusioninsight-flume-1.11.0/conf/** command to go to Flume's configuration directory.

Step 7 Run the **cat properties.properties** command to query the current configuration file of the Flume client.

Step 8 Check whether the **properties.properties** file is correctly configured according to the configuration description of the Flume agent.

- If yes, go to **Step 9**.
- If no, go to **Step 11**.

Step 9 Modify the **properties.properties** configuration file.

Check whether the alarm is cleared.

Step 10 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 11**.

Collect the fault information.

Step 11 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 12 Expand the **Service** drop-down list, and select **Flume** for the target cluster.

Step 13 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 14 Collect logs in the **/var/log/Bigdata/flume-client** directory on the Flume client using a transmission tool.

Step 15 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.230 ALM-24004 Exception Occurs When Flume Reads Data

Alarm Description

The alarm module monitors the status of Flume Source. This alarm is generated immediately when the duration in which Source fails to read the data exceeds the threshold.

The default threshold is **0**, indicating that the threshold is disabled. You can change the threshold by modifying the **properties.properties** file in the **conf** directory. Specifically, modify the **NoDatatime** parameter of required the source.

The alarm is cleared when Source reads the data and the alarm handling is complete.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
24004	Major	Error handling	Tenant plane	Flume	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AgentId	Specifies the ID of the agent for which the alarm is generated.
	ComponentType	Specifies the component type for which the alarm is generated.
	ComponentName	Specifies the component for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

If data is found in the data source and Flume Source continuously fails to read data, the data collection is stopped.

Possible Causes

- Flume Source is faulty, so data cannot be sent.
- The network is faulty, so the data cannot be sent.

Handling Procedure

Check whether Flume Source is faulty.

Step 1 Open the **properties.properties** configuration file on the local PC, search for **keyword type = spooldir** in the file, and check whether the Flume source type is spoolDir.

- If yes, go to **Step 2**.
- If no, go to **Step 3**.

Step 2 View the spoolDir directory to check whether all files are already transferred.

- If yes, no further action is required.
- If no, go to **Step 5**.

NOTE

The monitoring directory of spoolDir is specified by the **.spoolDir** parameter in the **properties.properties** configuration file. If all files in the monitoring directory have been transferred, the file name extension of all files in the monitoring directory is **.COMPLETED**.

Step 3 Open the **properties.properties** configuration file on the local PC, search for **org.apache.flume.source.kafka.KafkaSource** in the file, and check whether the Flume source type is Kafka.

- If yes, go to **Step 4**.
- If no, go to **Step 7**.

Step 4 Check whether the topic data configured by Kafka Source has been used up. For details, see "Using a Client" in MapReduce Service (MRS) 3.3.1-LTS User Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Usage Guide (for Huawei Cloud Stack 8.3.1).

- If yes, no further action is required.
- If no, go to **Step 5**.

Step 5 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Flume** > **Instance**.

Step 6 Go to the Flume instance page of the faulty node to check whether the indicator **Source Speed Metrics** in the alarm is 0.

- If yes, go to **Step 11**.
- If no, go to **Step 7**.

Check the network connection between the faulty node and the node that corresponds to the Flume Source IP address.

Step 7 Open the **properties.properties** configuration file on the local PC, search for **type = avro** in the file, and check whether the Flume source type is Avro.

- If yes, go to **Step 8**.
- If no, go to **Step 11**.

Step 8 Log in to the faulty node as user **root**, and run the **ping** *IP address of the Flume source* command to check whether the peer host can be pinged successfully.

- If yes, go to **Step 11**.
- If no, go to **Step 9**.

Step 9 Contact the network administrator to restore the network.

Step 10 In the alarm list, check whether the alarm is cleared after a period.

- If yes, no further action is required.
- If no, go to **Step 11**.

Collect fault information.

Step 11 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 12 Expand the **Service** drop-down list, and select **Flume** for the target cluster.

Step 13 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 14 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.231 ALM-24005 Exception Occurs When Flume Transmits Data

Alarm Description

The alarm module monitors the capacity status of Flume Channel. The alarm is generated immediately when the duration that Channel is fully occupied exceeds

the threshold or the number of times that Source fails to send data to Channel exceeds the threshold.

You can change the threshold by modifying the **properties.properties** file in the **conf** directory. Specifically, modify the **channelfullcount** parameter of required the channel.

The alarm is cleared when the space of Flume Channel is released and the alarm handling is complete.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
24005	Major (default threshold: 10)	Error handling	Tenant plane	Flume	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	HostName	Specifies the host for which the alarm was generated.
	AgentId	Specifies the ID of the agent for which the alarm is generated.
	ComponentType	Specifies the type of the component for which the alarm is generated.
	ComponentName	Specifies the component for which the alarm is generated.
	Alarm Severity	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

If the disk usage of Flume Channel increases continuously, the time required for importing data to a specified destination prolongs. When the disk usage of Flume Channel reaches 100%, the Flume agent process pauses.

Possible Causes

- Flume Sink is faulty, so the data cannot be sent.
- The network is faulty, so the data cannot be sent.

Handling Procedure

Check whether Flume Sink is faulty.

Step 1 Open the **properties.properties** configuration file on the local PC, search for **type = hdfs** in the file, and check whether the Flume sink type is HDFS.

- If yes, go to **Step 2**.
- If no, go to **Step 3**.

Step 2 On FusionInsight Manager, check whether **HDFS Service Unavailable** alarm is generated in the alarm list and whether the HDFS service is stopped in the service list.

- If the alarm is reported, clear it according to the handling suggestions of ALM-14000 HDFS Service Unavailable; if the HDFS service is stopped, start it. Then, go to **Step 7**.
- If no, go to **Step 7**.

Step 3 Open the **properties.properties** configuration file on the local PC, search for **type = hbase** in the file, and check whether the Flume sink type is HBase.

- If yes, go to **Step 4**.
- If no, go to **Step 5**.

Step 4 On FusionInsight Manager, check whether **HBase Service Unavailable** alarm is generated in the alarm list and whether the HBase service is stopped in the service list.

- If the alarm is reported, clear it according to the handling suggestions of ALM-19000 HBase Service Unavailable; if the HBase service is stopped, start it. Then, go to **Step 7**.
- If no, go to **Step 7**.

Step 5 Open the **properties.properties** configuration file on the local PC, search for **org.apache.flume.sink.kafka.KafkaSink** in the file, and check whether the Flume sink type is Kafka.

- If yes, go to **Step 6**.
- If no, go to **Step 9**.

Step 6 On FusionInsight Manager, check whether **Kafka Service Unavailable** alarm is generated in the alarm list and whether the Kafka service is stopped in the service list.

- If the alarm is reported, clear it according to the handling suggestions of ALM-38000 Kafka Service Unavailable; if the Kafka service is stopped, start it. Then, go to **Step 7**.
- If no, go to **Step 7**.

Step 7 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Flume** > **Instance**.

Step 8 Go to the Flume instance page of the faulty node to check whether the indicator **Sink Speed Metrics** is 0.

- If yes, go to **Step 13**.
- If no, go to **Step 9**.

Check the network connection between the faulty node and the node that corresponds to the Flume Sink IP address.

Step 9 Open the **properties.properties** configuration file on the local PC, search for **type = avro** in the file, and check whether the Flume sink type is Avro.

- If yes, go to **Step 10**.
- If no, go to **Step 13**.

Step 10 Log in to the faulty node as user **root**, and run the **ping** *IP address of the Flume sink* command to check whether the peer host can be pinged successfully.

- If yes, go to **Step 13**.
- If no, go to **Step 11**.

Step 11 Contact the network administrator to restore the network.

Step 12 In the alarm list, check whether the alarm is cleared after a period.

- If yes, no further action is required.
- If no, go to **Step 13**.

Collect the fault information.

Step 13 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 14 Expand the **Service** drop-down list, and select **Flume** for the target cluster.

Step 15 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 16 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.232 ALM-24006 Heap Memory Usage of Flume Server Exceeds the Threshold

Alarm Description

The system checks the heap memory usage of the Flume service every 60 seconds. This alarm is generated when the heap memory usage of the Flume instance exceeds the threshold for 10 consecutive times. This alarm is cleared when the heap memory usage is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
24006	Critical (default threshold: 95%) Major (default threshold: 90%)	Quality of service	Tenant plane	Flume	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.

Type	Parameter	Description
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

If the heap memory overflows, the service may break down and the Flume instance may be unavailable.

Possible Causes

The heap memory of the Flume instance is overused or the heap memory is inappropriately allocated.

Handling Procedure

Check the heap memory usage.

Step 1 Log in to FusionInsight Manager and choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**. On the page that is displayed, locate the row containing **Flume Heap Memory Usage Exceeds the Threshold**, and view the **Location** information. Check the name of the host for which the alarm is generated.

Step 2 On FusionInsight Manager, choose **Cluster** > *Name of the target cluster* > **Services** > **Flume**. On the page that is displayed, click the **Instance** tab. On the displayed tab page, select the role corresponding to the host name for which the alarm is generated and select **Customize** from the drop-down list in the upper right corner of the chart area. Choose **Agent** and select **Flume Heap Memory Resource Percentage**. Then, click **OK**.

Step 3 Check whether the heap memory used by Flume reaches the threshold (95% of the maximum heap memory by default).

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Service** > **Flume** > **Configuration**. On the page that is displayed, click **All Configurations** and choose **Flume** > **System**. Set **-Xmx** in the **GC_OPTS** parameter to a larger value based on site requirements and save the configuration.

NOTE

If this alarm is generated, the heap memory configured for Flume is insufficient for data transmission. You are advised to change the heap memory to: Channel capacity x Maximum size of a single data record x Number of channels. Note that the value of **xmx** cannot exceed the remaining memory of the node.

Step 5 Restart the affected services or instances and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

NOTICE

- During the restart, the Flume service is interrupted.
- During the instance restart, if the failover mode of SinkGroup is configured and at least one instance is running properly, the Flume service is not interrupted. Otherwise, the Flume service is interrupted.

Collect the fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **Flume** for the target cluster.

Step 8 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.233 ALM-24007 Flume Server Direct Memory Usage Exceeds the Threshold

Alarm Description

The system checks the direct memory usage of the Flume service every 60 seconds. This alarm is generated when the direct memory usage of the Flume instance exceeds the threshold for five consecutive times. This alarm is cleared when the Flume direct memory usage is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
24007	Critical (default threshold: 90%) Major (default threshold: 80%)	Quality of service	Tenant plane	Flume	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.

Type	Parameter	Description
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

If the direct memory overflows, the service may break down and the Flume instance may be unavailable.

Possible Causes

The direct memory of the Flume process is overused or the direct memory is inappropriately allocated.

Handling Procedure

Check the direct memory usage.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 1 Log in to FusionInsight Manager and choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**. On the page that is displayed, locate the row containing **Flume Direct Memory Usage Exceeds the Threshold**, and view the **Location** information. Check the name of the host for which the alarm is generated.

Step 2 On FusionInsight Manager, choose **Cluster** > *Name of the target cluster* > **Services** > **Flume**. On the page that is displayed, click the **Instance** tab. On the displayed tab page, select the role corresponding to the host name for which the alarm is generated and select **Customize** from the drop-down list in the upper right corner of the chart area. Choose **Agent** and select **Flume Direct Memory Resource Percentage**. Then, click **OK**.

Step 3 Check whether the direct memory used by Flume reaches the threshold (80% of the maximum direct memory by default).

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Service** > **Flume** > **Configuration**. On the page that is displayed, click **All Configurations** and choose **Flume** > **System**. Set **-XX:MaxDirectMemorySize** in the **GC_OPTS** parameter to a larger value based on site requirements and save the configuration.

NOTE

If this alarm is generated, the direct memory size configured for Flume instance cannot meet service requirements. You are advised to change the value of **-XX:MaxDirectMemorySize** to twice the current direct memory size or change the value based on site requirements.

Step 5 Restart the affected services or instances and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

NOTICE

- During the restart, the Flume service is interrupted.
- During the instance restart, if the failover mode of SinkGroup is configured and at least one instance is running properly, the Flume service is not interrupted. Otherwise, the Flume service is interrupted.

Collect the fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **Flume** for the target cluster.

Step 8 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.234 ALM-24008 Flume Server Non Heap Memory Usage Exceeds the Threshold

Alarm Description

The system checks the non-heap memory usage of the Flume service every 60 seconds. This alarm is generated when the non-heap memory usage of the Flume instance exceeds the threshold for 5 consecutive times. This alarm is cleared when the non-heap memory usage is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
24008	Critical (default threshold: 90%) Major (default threshold: 80%)	Quality of service	Tenant plane	Flume	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.

Type	Parameter	Description
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

If the non-heap memory overflows, the service may break down and the Flume instance may be unavailable.

Possible Causes

The non-heap memory of the Flume instance is overused or the non-heap memory is inappropriately allocated.

Handling Procedure

Check non-heap memory usage.

Step 1 Log in to FusionInsight Manager and choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**. On the page that is displayed, locate the row containing **Flume Non-Heap Memory Usage Exceeds the Threshold**, and view the **Location** information. Check the name of the host for which the alarm is generated.

Step 2 On FusionInsight Manager, choose **Cluster** > *Name of the target cluster* > **Services** > **Flume**. On the page that is displayed, click the **Instance** tab. On the displayed tab page, select the role corresponding to the host name for which the alarm is generated and select **Customize** from the drop-down list in the upper right corner of the chart area. Choose **Agent** and select **Flume Non-Heap Memory Resource Percentage**. Then, click **OK**.

Step 3 Check whether the non-heap memory used by Flume reaches the threshold (80% of the maximum non-heap memory by default).

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Service** > **Flume** > **Configuration**. On the page that is displayed, click **All Configurations** and choose **Flume** > **System**. Set **-XX: MaxPermSize** in the **GC_OPTS** parameter to a larger value based on site requirements and save the configuration.

NOTE

If this alarm is generated, the non-heap memory size configured for Flume instance cannot meet service requirements. You are advised to change the value of **-XX:MaxPermSize** to twice the current non-heap memory size or change the value based on site requirements.

Step 5 Restart the affected services or instances and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

NOTICE

- During the restart, the Flume service is interrupted.
- During the instance restart, if the failover mode of SinkGroup is configured and at least one instance is running properly, the Flume service is not interrupted. Otherwise, the Flume service is interrupted.

Collect the fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **Flume** for the target cluster.

Step 8 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.235 ALM-24009 Flume Server Garbage Collection (GC) Duration Exceeds the Threshold

Alarm Description

The system checks the GC duration of the Flume process every 60 seconds. This alarm is generated when the GC duration of the Flume process exceeds the threshold for five consecutive times. This alarm is cleared when the GC duration is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
24009	Critical (default threshold: 12 seconds) Major (default threshold: 10 seconds)	Quality of service	Tenant plane	Flume	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

Flume data transmission efficiency decreases.

Possible Causes

The heap memory of the Flume process is overused or inappropriately allocated, causing frequent occurrence of the GC process.

Handling Procedure

Check the GC duration.

Step 1 Log in to FusionInsight Manager and choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**. On the page that is displayed, locate the row containing **Flume Server GC Duration Exceeds the Threshold**, and view the **Location** information. Check the name of the host for which the alarm is generated.

Step 2 On FusionInsight Manager, choose **Cluster** > *Name of the target cluster* > **Services** > **Flume**. On the page that is displayed, click the **Instance** tab. On the displayed tab page, select the role corresponding to the host name for which the alarm is generated and select **Customize** from the drop-down list in the upper right corner of the chart area. Choose **Agent** and select **Garbage Collection (GC) Duration of Flume**. Then, click **OK**.

Step 3 Check whether the GC duration of the Flume process collected every minute exceeds the threshold (12 seconds by default).

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Service** > **Flume** > **Configuration**. On the page that is displayed, click **All Configurations** and choose **Flume** > **System**. Set **-Xmx** in the **GC_OPTS** parameter to a larger value based on site requirements and save the configuration.

NOTE

If this alarm is generated, the heap memory configured for the Flume instance is insufficient for data transmission. You are advised to change the heap memory to: Channel capacity x Maximum size of a single data record x Number of channels. Note that the value of **xmx** cannot exceed the remaining memory of the node.

Step 5 Restart the affected services or instances and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

NOTICE

- During the restart, the Flume service is interrupted.
- During the instance restart, if the failover mode of SinkGroup is configured and at least one instance is running properly, the Flume service is not interrupted. Otherwise, the Flume service is interrupted.

Collect the fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **Flume** for the target cluster.

Step 8 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.236 ALM-24010 Flume Certificate File Is Invalid or Damaged

Alarm Description

Flume checks whether the Flume certificate file is valid (whether the certificate exists and whether the certificate format is correct) every hour. This alarm is generated when the certificate file is invalid or damaged. This alarm is automatically cleared when the certificate file becomes valid again.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
24010	Major	Error handling	Tenant plane	Flume	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

The Flume client cannot access the Flume server.

Possible Causes

The Flume certificate file is invalid or damaged.

Handling Procedure

View alarm information.

Step 1 Log in to FusionInsight Manager and choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**. On the page that is displayed, locate the row containing **ALM-24010 Flume Certificate File Is Invalid or Damaged**, and view the **Location** information. View the IP address of the instance for which the alarm is generated.

Check whether the certificate file in the system is valid. If it is not, generate a new one.

Step 2 Log in to the node for which the alarm is generated as user **root** and run the **su -omm** command to switch to user **omm**.

Step 3 Run the following command to go to the Flume service certificate directory:

cd ${BIGDATA_HOME}/FusionInsight_Porter_*/install/FusionInsight-Flume-*/flume/conf

Step 4 Run the **ls -l** command to check whether the **flume_sChat.crt** file exists.

- If yes, go to **Step 5**.
- If no, go to **Step 6**.

Step 5 Run the **openssl x509 -in flume_sChat.crt -text -noout** command to check whether certificate details are displayed properly.

- If yes, go to **Step 9**.
- If no, go to **Step 6**.

Step 6 Run the following command to go to the Flume script directory:

cd ${BIGDATA_HOME}/FusionInsight_Porter_*/install/FusionInsight-Flume-*/flume/bin

Step 7 Run the following command to generate a new certificate file. Then check whether the alarm is automatically cleared one hour later.

sh geneJKS.sh -f *Custom certificate password of the Flume role on the server* **-g** *Custom certificate password of the Flume role on the client*

- If yes, go to **Step 8**.
- If no, go to **Step 9**.

NOTE

The custom certificate passwords must meet the following complexity requirements:

- Contain at least four types of uppercase letters, lowercase letters, digits, and special characters.
- Contain 8 to 64 characters.
- Be changed periodically (for example, every three months), and certificates and trust lists are generated again to ensure security.

Step 8 Check whether this alarm is generated again during periodic system check.

- If yes, go to **Step 9**.
- If no, no further action is required.

Collect the fault information.

Step 9 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 10 Expand the **Service** drop-down list, and select **Flume** for the target cluster.

Step 11 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.237 ALM-24011 Flume Certificate File Is About to Expire

Alarm Description

Flume checks whether the Flume certificate file is about to expire every hour. This alarm is generated when the remaining validity period is at most 30 days. This alarm is automatically cleared when the remaining validity period is greater than 30 days.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
24011	Major	Error handling	Tenant plane	Flume	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

Currently, there is no impact on the system.

Possible Causes

The Flume certificate file is about to expire.

Handling Procedure

View alarm information.

Step 1 Log in to FusionInsight Manager and choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**. On the page that is displayed, locate the row containing **ALM-24011 Flume Certificate Is About to Expire**, and view the **Location** information. View the IP address of the instance for which the alarm is generated.

Check whether the certificate file in the system is valid. If it is not, generate a new one.

Step 2 Log in to the node for which the alarm is generated as user **root** and run the **su - omm** command to switch to user **omm**.

Step 3 Run the following command to go to the Flume service certificate directory:

cd ${BIGDATA_HOME}/FusionInsight_Porter_*/install/FusionInsight-Flume-*/flume/conf

Step 4 Run the following command to check the effective time and expiration time of the Flume user certificate:

openssl x509 -noout -text -in flume_sChat.crt

Step 5 Perform **Step 6** to **Step 7** during off-peak hours to update the certificate file as needed.

Step 6 Run the following command to go to the Flume script directory:

cd ${BIGDATA_HOME}/FusionInsight_Porter_*/install/FusionInsight-Flume-*/flume/bin

Step 7 Run the following command to generate a new certificate file. Then check whether the alarm is automatically cleared one hour later.

sh geneJKS.sh -f *Custom certificate password of the Flume role on the server* **-g** *Custom certificate password of the Flume role on the client*

- If yes, go to **Step 9**.
- If no, go to **Step 8**.

NOTE

The custom certificate passwords must meet the following complexity requirements:

- Contain at least four types of uppercase letters, lowercase letters, digits, and special characters.
- Contain 8 to 64 characters.
- Be changed periodically (for example, every three months), and certificates and trust lists are generated again to ensure security.

Step 8 Log in to the Flume node for which the alarm is generated as user **omm** and repeat **Step 6** to **Step 7**. Then, check whether the alarm is automatically cleared one hour later.

- If yes, go to **Step 9**.
- If no, go to **Step 10**.

Step 9 Check whether this alarm is generated again during periodic system check.

- If yes, go to **Step 10**.
- If no, no further action is required.

Collect the fault information.

Step 10 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 11 Expand the **Service** drop-down list, and select **Flume** for the target cluster.

Step 12 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 13 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.238 ALM-24012 Flume Certificate File Has Expired

Alarm Description

Flume checks whether its certificate file in the system has expired every hour. This alarm is generated when the server certificate has expired. This alarm is automatically cleared when the certificate file becomes valid again.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
24012	Major	Error handling	Tenant plane	Flume	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

The Flume client cannot access the Flume server.

Possible Causes

The Flume certificate file has expired.

Handling Procedure

View alarm information.

Step 1 Log in to FusionInsight Manager and choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**. On the page that is displayed, locate the row containing **ALM-24012 Flume Certificate Has Expired**, and view the **Location** information. View the IP address of the instance for which the alarm is generated.

Check whether the certificate file in the system is valid. If it is not, generate a new one.

Step 2 Log in to the node for which the alarm is generated as user **root** and run the **su - omm** command to switch to user **omm**.

Step 3 Run the following command to go to the Flume service certificate directory:

cd ${BIGDATA_HOME}/FusionInsight_Porter_*/install/FusionInsight-Flume-*/flume/conf

Step 4 Run the following command to check the effective time and expiration time of the HA user certificate to determine whether the certificate file is still in the validity period:

openssl x509 -noout -text -in flume_sChat.crt

- If yes, go to **Step 9**.
- If no, go to **Step 5**.

Step 5 Run the following command to go to the Flume script directory:

cd ${BIGDATA_HOME}/FusionInsight_Porter_*/install/FusionInsight-Flume-*/flume/bin

Step 6 Run the following command to generate a new certificate file. Then check whether the alarm is automatically cleared one hour later.

sh geneJKS.sh -f *Custom certificate password of the Flume role on the server* **-g** *Custom certificate password of the Flume role on the client*

- If yes, go to **Step 8**.
- If no, go to **Step 7**.

NOTE

The custom certificate passwords must meet the following complexity requirements:

- Contain at least four types of uppercase letters, lowercase letters, digits, and special characters.
- Contain 8 to 64 characters.
- Be changed periodically (for example, every three months), and certificates and trust lists are generated again to ensure security.

Step 7 Log in to the Flume node for which the alarm is generated as user **omm** and repeat **Step 5** to **Step 6**. Then, check whether the alarm is automatically cleared one hour later.

- If yes, go to **Step 8**.
- If no, go to **Step 9**.

Step 8 Check whether this alarm is generated again during periodic system check.

- If yes, go to **Step 9**.
- If no, no further action is required.

Collect the fault information.

Step 9 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 10 Expand the **Service** drop-down list, and select **Flume** for the target cluster.

Step 11 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.239 ALM-24013 Flume MonitorServer Certificate File Is Invalid or Damaged

Alarm Description

MonitorServer checks whether its certificate file is valid (whether the certificate exists and whether the certificate format is correct) every hour. This alarm is generated when the certificate file is invalid or damaged. This alarm is automatically cleared when the certificate file becomes valid again.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
24013	Major	Error handling	Tenant plane	MonitorServer	Yes

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

The Flume client cannot access the Flume server.

Possible Causes

The MonitorServer certificate file is invalid or damaged.

Handling Procedure

View alarm information.

Step 1 Log in to FusionInsight Manager and choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**. On the page that is displayed, locate the row containing **ALM-24013 MonitorServer Certificate File Is Invalid or Damaged**, and view the **Location** information. View the IP address of the instance for which the alarm is generated.

Check whether the certificate file in the system is valid. If it is not, generate a new one.

Step 2 Log in to the node for which the alarm is generated as user **root** and run the **su - omm** command to switch to user **omm**.

Step 3 Run the following command to go to the MonitorServer certificate file directory:

cd ${BIGDATA_HOME}/FusionInsight_Porter_*/install/FusionInsight-Flume-*/flume/conf

Step 4 Run the **ls -l** command to check whether the **ms_sChat.crt** file exists:

- If yes, go to **Step 5**.
- If no, go to **Step 6**.

Step 5 Run the **openssl x509 -in ms_sChat.crt -text -noout** command to check whether certificate details are displayed.

- If yes, go to **Step 9**.
- If no, go to **Step 6**.

Step 6 Run the following command to go to the Flume script directory:

cd ${BIGDATA_HOME}/FusionInsight_Porter_*/install/FusionInsight-Flume-*/flume/bin

Step 7 Run the following command to generate a new certificate file. Then check whether the alarm is automatically cleared one hour later.

sh geneJKS.sh -m *Custom password of the MonitorServer certificate on the server* **-n** *Custom password of the MonitorServer certificate on the client*

- If yes, go to **Step 8**.
- If no, go to **Step 9**.

NOTE

The custom certificate passwords must meet the following complexity requirements:

- Contain at least four types of uppercase letters, lowercase letters, digits, and special characters.
- Contain 8 to 64 characters.
- Be changed periodically (for example, every three months), and certificates and trust lists are generated again to ensure security.

Step 8 Check whether this alarm is generated again during periodic system check.

- If yes, go to **Step 9**.
- If no, no further action is required.

Collect the fault information.

Step 9 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 10 Select **MonitorServer** in the required cluster for **Service**.

Step 11 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.240 ALM-24014 Flume MonitorServer Certificate Is About to Expire

Alarm Description

MonitorServer checks whether its certificate file is about to expire every hour. This alarm is generated when the remaining validity period is at most 30 days. This alarm is automatically cleared when the remaining validity period is greater than 30 days.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
24014	Major	Error handling	Tenant plane	MonitorServer	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.

Type	Parameter	Description
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

Currently, there is no impact on the system.

Possible Causes

The MonitorServer certificate file is about to expire.

Handling Procedure

View alarm information.

Step 1 Log in to FusionInsight Manager and choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**. On the page that is displayed, locate the row containing **ALM-24014 MonitorServer Certificate Is About to Expire**, and view the **Location** information. View the IP address of the instance for which the alarm is generated.

Check whether the certificate file in the system is valid. If it is not, generate a new one.

Step 2 Log in to the node for which the alarm is generated as user **root** and run the **su - omm** command to switch to user **omm**.

Step 3 Run the following command to go to the MonitorServer certificate file directory:

cd ${BIGDATA_HOME}/FusionInsight_Porter_*/install/FusionInsight-Flume-*/flume/conf

Step 4 Run the following command to check the effective time and expiration time of the MonitorServer user certificate:

openssl x509 -noout -text -in ms_sChat.crt

Step 5 Perform **Step 6** to **Step 7** during off-peak hours to update the certificate file as needed.

Step 6 Run the following command to go to the Flume script directory:

cd ${BIGDATA_HOME}/FusionInsight_Porter_*/install/FusionInsight-Flume-*/flume/bin

Step 7 Run the following command to generate a new certificate file. Then check whether the alarm is automatically cleared one hour later.

sh geneJKS.sh -m *Custom password of the MonitorServer certificate on the server* **-n** *Custom password of the MonitorServer certificate on the client*

- If yes, go to **Step 9**.
- If no, go to **Step 8**.

NOTE

The custom certificate passwords must meet the following complexity requirements:

- Contain at least four types of uppercase letters, lowercase letters, digits, and special characters.
- Contain 8 to 64 characters.
- Be changed periodically (for example, every three months), and certificates and trust lists are generated again to ensure security.

Step 8 Log in to the Flume node for which the alarm is generated as user **omm** and repeat **Step 6** to **Step 7**. Then, check whether the alarm is automatically cleared one hour later.

- If yes, go to **Step 9**.
- If no, go to **Step 10**.

Step 9 Check whether this alarm is generated again during periodic system check.

- If yes, go to **Step 10**.
- If no, no further action is required.

Collect the fault information.

Step 10 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 11 Select **MonitorServer** in the required cluster for **Service**.

Step 12 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 13 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.241 ALM-24015 Flume MonitorServer Certificate File Has Expired

Alarm Description

MonitorServer checks whether its certificate file in the system has expired every hour. This alarm is generated when the server certificate has expired. This alarm is automatically cleared when the server certificate file becomes valid again.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
24015	Major	Error handling	Tenant plane	MonitorServer	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.

Type	Parameter	Description
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

The Flume client cannot access the Flume server.

Possible Causes

The MonitorServer certificate file has expired.

Handling Procedure

View alarm information.

Step 1 Log in to FusionInsight Manager and choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**. On the page that is displayed, locate the row containing **ALM-24015 MonitorServer Certificate Has Expired**, and view the **Location** information. View the IP address of the instance for which the alarm is generated.

Check whether the certificate file in the system is valid. If it is not, generate a new one.

Step 2 Log in to the node for which the alarm is generated as user **root** and run the **su - omm** command to switch to user **omm**.

Step 3 Run the following command to go to the MonitorServer certificate file directory:

cd ${BIGDATA_HOME}/FusionInsight_Porter_*/install/FusionInsight-Flume-*/flume/conf

Step 4 Run the following command to check the effective time and expiration time of the user certificate to determine whether the certificate file is still in the validity period:

openssl x509 -noout -text -in ms_sChat.crt

- If yes, go to **Step 9**.
- If no, go to **Step 5**.

Step 5 Run the following command to go to the Flume script directory:

cd ${BIGDATA_HOME}/FusionInsight_Porter_*/install/FusionInsight-Flume-*/flume/bin

Step 6 Run the following command to generate a new certificate file. Then, check whether the alarm is automatically cleared one hour later.

sh geneJKS.sh -m *Custom password of the MonitorServer certificate on the server* **-n** *Custom password of the MonitorServer certificate on the client*

- If yes, go to **Step 8**.
- If no, go to **Step 7**.

NOTE

The custom certificate passwords must meet the following complexity requirements:

- Contain at least four types of uppercase letters, lowercase letters, digits, and special characters.
- Contain 8 to 64 characters.
- Be changed periodically (for example, every three months), and certificates and trust lists are generated again to ensure security.

Step 7 Log in to the Flume node for which the alarm is generated as user **omm** and repeat **Step 5** to **Step 6**. Then, check whether the alarm is automatically cleared one hour later.

- If yes, go to **Step 8**.
- If no, go to **Step 9**.

Step 8 Check whether this alarm is generated again during periodic system check.

- If yes, go to **Step 9**.
- If no, no further action is required.

Collect fault information.

Step 9 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 10 Select **MonitorServer** in the required cluster for **Service**.

Step 11 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.242 ALM-25000 LdapServer Service Unavailable

Alarm Description

The system checks the LdapServer service status every 30 seconds. This alarm is generated when the system detects that both the active and standby LdapServer services are abnormal.

This alarm is cleared when the system detects that one or two LdapServer services are normal.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
25000	Critical	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

The running status of the component that depends on the LdapServer becomes faulty. As a result, Kerberos authentication fails in the cluster or OS user cache synchronization is abnormal, and component services are abnormal.

Possible Causes

- The node where the LdapServer service locates is faulty.
- The LdapServer process is abnormal.

Handling Procedure

Check whether the nodes where the two SlapdServer instances of the LdapServer service are located are faulty.

Step 1 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **LdapServer** > **Instance** to go to the LdapServer instance page to obtain the host name of the node where the two SlapdServer instances locates.

Step 2 Choose **O&M** > **Alarm** > **Alarms**. On the **Alarm** page of the FusionInsight Manager system, check whether any alarm of **NodeAgent Process Is Abnormal** exists.

- If yes, go to **Step 3**.
- If no, go to **Step 6**.

Step 3 Check whether the host name in the alarm is consistent with the **Step 1** host name.

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 Handle the alarm according to "ALM-12006 NodeAgent Process Is Abnormal".

Step 5 Check whether **LdapServer Service Unavailable** is cleared in the alarm list.

- If yes, no further action is required.
- If no, go to **Step 10**.

Check whether the LdapServer process is normal.

Step 6 Choose **O&M > Alarm > Alarms**. On the **Alarm** page of the FusionInsight Manager system, check whether any alarm of **Process Fault** exists.

- If yes, go to **Step 7**.
- If no, go to **Step 10**.

Step 7 Check whether the service and host name in the alarm are consistent with the LdapServer service and host name.

- If yes, go to **Step 8**.
- If no, go to **Step 10**.

Step 8 Handle the alarm according to "ALM-12007 Process Fault".

Step 9 Check whether **LdapServer Service Unavailable** is cleared in the alarm list.

- If yes, no further action is required.
- If no, go to **Step 10**.

Collect fault information.

Step 10 On the FusionInsight Manager, choose **O&M** > **Log > Download**.

Step 11 Select **LdapServer** in the required cluster from the **Service**.

Step 12 Click the edit button in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 13 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.243 ALM-25004 Abnormal LdapServer Data Synchronization

Alarm Description

The system checks the LdapServer data every 30 seconds. This alarm is generated when the data on the active and standby LdapServers of Manager is inconsistent

for 12 consecutive times. This alarm is cleared when the data on the active and standby LdapServers is consistent.

The system checks the LdapServer data every 30 seconds. This alarm is generated when the LdapServer data in the cluster is inconsistent with that on Manager for 12 consecutive times. This alarm is cleared when the data is consistent.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
25004	Critical	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the details for which the alarm is generated.

Impact on the System

LdapServer data inconsistency occurs because the LdapServer data in Manager is damaged or the LdapServer data in the cluster is damaged. The LdapServer process with damaged data cannot provide services externally, and the authentication functions of Manager and the cluster are affected.

Possible Causes

- The network of the node where the LdapServer process locates is faulty.
- The LdapServer process is abnormal.
- The OS restart damages data on LdapServer.

Handling Procedure

Check whether the network where the LdapServer nodes reside is faulty.

Step 1 On the FusionInsight Manager portal, choose **O&M > Alarm > Alarms**. Record the IP address of HostName in the alarm locating information as IP1 (if multiple alarms exist, record the IP addresses as IP1, IP2, and IP3 respectively).

Step 2 Contact technical support and log in to the nodes corresponding to IP 1. Run the ping command to check whether the IP address of the management plane of the active OMS node can be pinged.

- If yes, go to **Step 4**.
- If no, go to **Step 3**.

Step 3 Contact the network administrator to recover the network and check whether **Abnormal LdapServer Data Synchronization** is cleared.

- If yes, no further action is required.
- If no, go to **Step 4**.

Check whether the LdapServer processes are normal.

Step 4 On the **Alarm** page of FusionInsight Manager, check whether the **OLdap Resource Abnormal** exists.

- If yes, go to **Step 5**.
- If no, go to **Step 7**.

Step 5 Clear the alarm by following the steps provided in "ALM-12004 OLdap Resource Abnormal".

Step 6 Check whether **Abnormal LdapServer Data Synchronization** is cleared in the alarm list.

- If yes, no further action is required.
- If no, go to **Step 7**.

Step 7 On the **Alarm** page of FusionInsight Manager, check whether **Process Faul**t is generated for the LdapServer service.

- If yes, go to **Step 8**.
- If no, go to **Step 10**.

Step 8 Handle the alarm according to "ALM-12007 Process Fault".

Step 9 Check whether **Abnormal LdapServer Data Synchronization** is cleared.

- If yes, no further action is required.
- If no, go to **Step 10**.

Check whether the LdapServer processes are normal.

Step 10 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. Record the IP address of HostName in the alarm locating information as "IP1" (if multiple alarms exist, record the IP addresses as "IP1", "IP2", and "IP3" respectively). Choose **Cluster** > *Name of the desired cluster* > **Services** > **LdapServer** > **Configurations**. Record the port number of LdapServer as "PORT". (If the IP address in the alarm locating information is the IP address of the standby management node, choose **System** > **OMS** > **oldap** > **Modify Configuration** and record the listening port number of LdapServer.)

Step 11 Log in to the nodes corresponding to IP1 as user **omm**.

Step 12 Run the following command to check whether errors are displayed in the queried information.

ldapsearch -H ldaps://*IP1*:*PORT* **-LLL -x -D cn=root,dc=hadoop,dc=com -W -b ou=Peoples,dc=hadoop,dc=com**

After running the command, enter the **LDAP** administrator password. Contact the system administrator to obtain the password.

- If yes, go to **Step 13**.
- If no, go to **Step 15**.

Step 13 Recover the LdapServer and OMS nodes using data backed up before the alarm is generated. For detail, see "Recovering Manager Data" in *MapReduce Service (MRS) 3.3.1-LTS User Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Usage Guide (for Huawei Cloud Stack 8.3.1)*.

NOTE

Use the OMS data and LdapServer data backed up at the same point in time to recover the data. Otherwise, the service and operation may fail. To recover data when services run properly, you are advised to manually back up the latest management data and then recover the data. Otherwise, Manager data produced between the backup point in time and the recovery point in time will be lost.

Step 14 Check whether alarm **Abnormal LdapServer Data Synchronization** is cleared.

- If yes, no further action is required.

- If no, go to **Step 15**.

Collect fault information.

Step 15 On the FusionInsight Manager portal, choose **O&M** > **Log** > **Download**.

Step 16 Select **LdapServer** in the required cluster and **OmsLdapServer** from the **Service**.

Step 17 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 18 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.244 ALM-25005 nscd Service Exception

Alarm Description

The system checks the status of the nscd service every 60 seconds. This alarm is generated when the nscd process fails to be queried for four consecutive times (three minutes) or users in LdapServer cannot be obtained.

This alarm is cleared when the process is restored and users in LdapServer can be obtained.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
25005	Major	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.

Type	Parameter	Description
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Details	Specifies alarm details.

Impact on the System

The alarmed node may not be able to synchronize data from LdapServer. The **id** command may fail to obtain the LDAP data, affecting upper-layer services.

Possible Causes

- The nscd service is not started.
- The network is faulty, and cannot access the LDAP server.
- NameService is abnormal.
- Users cannot be queried because the OS executes commands too slowly.

Handling Procedure

Check whether the nscd service is started.

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Alarms**. Record the IP address of **HostName** in **Location** of the alarm as **IP1** (if multiple alarms exist, record the IP addresses as **IP1**, **IP2**, and **IP3** respectively).

Step 2 Contact the technical support to access the node using IP1 as user **root**. Run the **ps -ef | grep nscd** command on the node and check whether the **/usr/sbin/nscd** process is started.

- If yes, go to **Step 5**.
- If no, go to **Step 3**.

Step 3 Run the **service nscd restart** command as user **root** to restart the nscd service. Then run the **ps -ef | grep nscd** command to check whether the nscd service is started.

- If yes, go to **Step 4**.
- If no, go to **Step 15**.

Step 4 Wait for 5 minutes and run the ps -ef | grep nscd command again as user root. Check whether the service exists.

- If yes, go to **Step 11**.
- If no, go to **Step 15**.

Check whether the network is faulty, and whether the LDAP server can be accessed.

Step 5 Log in to the alarmed node as user **root** and run the **ping** command to check whether the network connectivity between this node and the LdapServer node. is normal.

- If yes, go to **Step 6**.
- If no, contact network administrators to troubleshoot the fault.

Check whether the NameService is normal.

Step 6 Log in to the alarmed node as user **root**. Run the **cat /etc/nsswitch.conf** command to check whether the **passwd**, **group**, **services**, **netgroup**, and **aliases** of NameService are correctly configured.

The correct parameter configurations are as follows:

passwd: **compat ldap**; **group**: **compat ldap**; **services**: **files ldap**; **netgroup**: **files ldap**; **aliases**: **files ldap**

- If yes, go to **Step 7**.
- If no, go to **Step 9**.

Step 7 Log in to the alarmed node as user **root**. Run the **cat /etc/nscd.conf** command to check whether the **enable-cache passwd**, **positive-time-to-live passwd**, **enable-cache group**, and **positive-time-to-live group** in the configuration file are correctly configured.

The correct parameter configurations are as follows:

enable-cache passwd: **yes**; **positive-time-to-live passwd**: **600**; **enable-cache group**: **yes**; **positive-time-to-live group**: **3600**

- If yes, go to **Step 8**.
- If no, go to **Step 10**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 8 Run the **/usr/sbin/nscd -i group** and **/usr/sbin/nscd -i passwd** commands as user **root**. Wait for 2 minutes and run the **id admin** and **id backup/manager** commands to check whether results can be queried.

- If yes, go to **Step 11**.
- If no, go to **Step 15**.

Step 9 Run the **vi /etc/nsswitch.conf** command as user **root**. Correct the configurations in **Step 6** and save the file. Run the **service nscd restart** command to restart the nscd service. Wait for 2 minutes and run the **id admin** and **id backup/manager** commands to check whether results can be queried.

- If yes, go to **Step 11**.
- If no, go to **Step 15**.

Step 10 Run the **vi /etc/nscd.conf** command as user **root**. Correct the configurations in **Step 7** and save the file. Run the **service nscd restart** command to restart the nscd service. Wait for 2 minutes and run the **id admin** and **id backup/manager** commands to check whether results can be queried.

- If yes, go to **Step 11**.
- If no, go to **Step 15**.

Step 11 Log in to the FusionInsight Manager portal. Wait for 5 minutes and check whether the **nscd Service Exception** alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 12**.

Check whether frame freezing occurs when running a command in the operating system.

Step 12 Log in to the faulty node as user **root**, run the **id admin** command, and check whether the command execution takes a long time. If the command execution takes more than 3 seconds, the command execution is deemed to be slow.

- If yes, go to **Step 13**.
- If no, go to **Step 15**.

Step 13 Run the **cat /var/log/messages** command to check whether the nscd frequently restarts or the error information "Can't contact LDAP server" exists.

nscd exception example:

```
Feb 11 11:44:42 10-120-205-33 nscd: nss_ldap: failed to bind to LDAP server ldaps://10.120.205.55:21780: Can't contact LDAP server
Feb 11 11:44:43 10-120-205-33 ntpq: nss_ldap: failed to bind to LDAP server ldaps://10.120.205.55:21780: Can't contact LDAP server
Feb 11 11:44:44 10-120-205-33 ntpq: nss_ldap: failed to bind to LDAP server ldaps://10.120.205.92:21780: Can't contact LDAP server
```

- If yes, go to **Step 14**.
- If no, go to **Step 15**.

Step 14 Run the **vi$BIGDATA_HOME/tmp/random_ldap_ip_order** command to modify the number at the end. If the original number is an odd number, change it to an even number. If the number is an even number, change it to an odd number.

Run the **vi /etc/ldap.conf** command to enter the editing mode, press **Insert** to start editing, and then change the first two IP addresses of the URI configuration item.

After the modification is complete, press **Esc** to exit the editing mode and enter **:wq!** to save the settings and exit.

Run the **service nscd restart** command to restart the nscd service. Wait 5 minutes and run the **id admin** command again. Check whether the command execution is slow.

- If yes, go to **Step 15**.
- If no, log in to other faulty nodes and repeat **Step 12** to **Step 14** to check whether the first LdapServer node in the URI before modifying **/etc/ldap.conf** is faulty. For example, check whether the service IP address is unreachable, the network delay is too long, or other abnormal software is deployed.

Collect the fault information.

Step 15 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 16 Expand the drop-down list next to the **Service** field. In the **Services** dialog box that is displayed, select **LdapClient** for the target cluster.

Step 17 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 18 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.245 ALM-25006 Sssd Service Exception

Alarm Description

The system checks the status of the sssd service every 60 seconds. This alarm is generated when the sssd process fails to be queried for four consecutive times (three minutes) or users in LdapServer cannot be obtained.

This alarm is cleared when the process is restored and users in LdapServer can be obtained.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
25006	Major	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the details for which the alarm is generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

The alarmed node may not be able to synchronize data from LdapServer. The id command may fail to obtain the LDAP data, affecting upper-layer services.

Possible Causes

- The sssd service is not started or is incorrectly started.
- The network is faulty and cannot access the LDAP server.
- NameService is abnormal.
- Users cannot be queried because the OS executes commands too slowly.

Handling Procedure

Check whether the sssd service is correctly started.

Step 1 On the FusionInsight Manager portal, choose **O&M > Alarm > Alarms**. Find the IP address of **HostName** in **Location** of the alarm and record it as IP1 (if multiple alarms exist, record the IP addresses as IP1, IP2, and IP3 respectively).

Step 2 Contact the technical support to access the node using IP1 as user root. Run the **ps -ef | grep sssd** command and check whether the **/usr/sbin/sssd** process is started.

- If the process is started, go to **Step 3**.
- If the process is not started, go to **Step 4**.

Step 3 Check whether the sssd process queried in **Step 2** has three subprocesses.

- If yes, go to **Step 5**.
- If no, go to **Step 4**.

Step 4 Run the **service sssd restart** command as user **root** to restart the sssd service. Then run the **ps -ef | grep sssd** command to check whether the sssd process is normal.

In the normal state, the **/usr/sbin/sssd** process has three subprocesses: **/usr/libexec/sssd/sssd_be**, **/usr/libexec/sssd/sssd_nss**, and **/usr/libexec/sssd/sssd_pam**.

- If it exists, go to **Step 9**.
- If it does not exist, go to **Step 13**.

Check whether the LDAP server can be accessed.

Step 5 Log in to the alarmed node as user **root**. Run the **ping** command to check the network connectivity between this node and the LdapServer node.

- If the network is normal, go to **Step 6**.
- If the network is faulty, contact network administrators to troubleshoot the fault.

Check whether NameService is normal.

Step 6 Log in to the alarmed node as user **root**. Run the **cat /etc/nsswitch.conf** command and check the **passwd** and **group** configurations of NameService.

The correct parameter configurations are as follows: **passwd: compat ldap** and **group: compat ldap**.

- If the configurations are correct, go to **Step 7**.
- If the configurations are incorrect, go to **Step 8**.

Step 7 Run the **/usr/sbin/sss_cache -G** and **/usr/sbin/sss_cache -U** commands as user **root**. Wait for 2 minutes and run the **id admin** and **id backup/manager** commands to check whether results can be queried.

- If results are queried, go to **Step 9**.
- If no result is queried, go to **Step 13**.

Step 8 Run the **vi /etc/nsswitch.conf** command as user **root**. Correct the configurations in **Step 6** and save the file. Run the **service sssd restart** command to restart the sssd service. Wait for 2 minutes and run the **id admin** and **id backup/manager** commands to check whether results can be queried.

- If results are queried, go to **Step 9**.
- If no result is queried, go to **Step 13**.

Step 9 Log in to the FusionInsight Manager portal. Wait for 5 minutes and check whether the **sssd Service Exception** alarm is cleared.

- If the alarm is cleared, no further action is required.
- If the alarm persists, go to **Step 10**.

Check whether frame freezing occurs when running a command in the operating system.

Step 10 Log in to the faulty node as user **root**, run the **id admin** command, and check whether the command execution takes a long time. If the command execution takes more than 3 seconds, the command execution is deemed to be slow.

- If yes, go to **Step 11**.
- If no, go to **Step 13**.

Step 11 Run the **cat /var/log/messages** command to check whether the sssd frequently restarts or the error information **Can't contact LDAP server** exists.

sssd restart example:

```
Feb  7 11:38:16 10-132-190-105 sssd[pam]: Shutting down
Feb  7 11:38:16 10-132-190-105 sssd[nss]: Shutting down
Feb  7 11:38:16 10-132-190-105 sssd[nss]: Shutting down
Feb  7 11:38:16 10-132-190-105 sssd[be[default]]: Shutting down
Feb  7 11:38:16 10-132-190-105 sssd: Starting up
Feb  7 11:38:16 10-132-190-105 sssd[be[default]]: Starting up
Feb  7 11:38:16 10-132-190-105 sssd[nss]: Starting up
Feb  7 11:38:16 10-132-190-105 sssd[pam]: Starting up
```

- If yes, go to **Step 12**.
- If no, go to **Step 13**.

Step 12 Run the **vi $BIGDATA_HOME/tmp/random_ldap_ip_order** command to modify the number at the end. If the original number is an odd number, change it to an even number. If the number is an even number, change it to an odd number.

Run the **vi /etc/sssd/sssd.conf** command to reverse the first two IP addresses of the **ldap_uri** configuration item, save the settings, and exit.

Run the **ps -ef | grep sssd** command to query the ID of the sssd process, kill it, and run the **/usr/sbin/sssd -D -f** command to restart the sssd service. Wait 5 minutes and run the **id admin** command again.

Check whether the command execution is slow.

- If yes, go to **Step 13**.
- If no, log in to other faulty nodes and run **Step 10** to **Step 12**. Collect logs and check whether the first ldapserver node in the ldap_uri before modifying **/etc/sssd/sssd.conf** is faulty. For example, check whether the service IP address is unreachable, the network latency is too long, or other abnormal software is deployed.

Collect fault information.

Step 13 On the FusionInsight Manager portal, choose **O&M** > **Log** > **Download**.

Step 14 Select **LdapClient** in the required cluster from the **Service**.

Step 15 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 16 Contact the technical support and send the collected fault logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.246 ALM-25007 Number of SlapdServer Connections Exceeds the Threshold

Alarm Description

The system checks the number of process connections on the SlapdServer node every 30 seconds and compares the actual number with the threshold. This alarm is generated when the number of process connections exceeds the threshold (**1000** by default) for multiple times (**5** by default).

Its **Trigger Count** is configurable. If **Trigger Count** is set to **1**, this alarm is cleared when the number of process connections is less than or equal to the threshold. If **Trigger Count** is greater than **1**, this alarm is cleared when the number of process connections is less than or equal to 90% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
25007	Major	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Details	Specifies alarm details.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

SlapdServer may respond slowly or become unavailable. Kerberos authentication times out or OS user caches cannot be synchronized. Component services are faulty.

Possible Causes

- There are too many SlapdServer connections.
- The alarm threshold or alarm trigger count is improperly configured.

Handling Procedure

Check whether there are too many SlapdServer process connections.

Step 1 Log in to FusionInsight Manager and choose **Cluster** > **Services** > **LdapServer**.

Step 2 On the LdapServer dashboard page, observe the SlapdServer process connections and decrease the connections based on service requirements.

Figure 1-11 SlapdServer process connections

Step 3 Wait about 2 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 4**.

Check whether the alarm threshold or alarm trigger count is properly configured.

Step 4 On FusionInsight Manager, choose **O&M** > **Alarm** > **Thresholds**, click the name of the desired cluster, choose **LdapServer** > **Other** > **SlapdServer Service Connections**, and check whether the alarm trigger count and alarm threshold are set properly.

- If yes, go to **Step 7**.
- If no, go to **Step 5**.

Step 5 Change the trigger count and alarm threshold based on the actual number of process connections, and apply the changes.

Step 6 Wait 2 minutes and check whether the alarm is automatically cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect fault information.

Step 7 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 8 Expand the **Service** drop-down list, and select **LdapServer** for the target cluster.

Step 9 Specify **Hosts** for collecting logs, which is optional. By default, all hosts are selected.

Step 10 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 11 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.247 ALM-25008 SlapdServer CPU Usage Exceeds the Threshold

Alarm Description

The system checks the CPU usage of the SlapdServer node every 30 seconds and compares the actual usage with the threshold. This alarm is generated when the SlapdServer CPU usage exceeds the threshold for multiple times (**5** by default).

Its **Trigger Count** is configurable. If **Trigger Count** is set to **1**, this alarm is cleared when the SlapdServer CPU usage is less than or equal to the threshold. If **Trigger Count** is greater than **1**, this alarm is cleared when the SlapdServer CPU usage is less than or equal to 90% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
25008	Critical (default threshold: 85%) Major (default threshold: 75%)	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Details	Specifies alarm details.

Impact on the System

SlapdServer may respond slowly or become unavailable. Kerberos authentication times out or OS user caches cannot be synchronized. Component services are faulty.

Possible Causes

- The alarm threshold or alarm trigger count is improperly configured.
- The CPU configuration cannot meet service requirements, and the CPU usage reaches the upper limit.

Handling Procedure

Check whether the alarm threshold or alarm trigger count is properly configured.

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Thresholds**, click the name of the desired cluster, choose **LdapServer** > **Other** > **SlapdServer Service Total CPU Percentage**, and check whether the alarm trigger count and alarm threshold are set properly.

- If yes, go to **Step 4**.
- If no, go to **Step 2**.

Step 2 Change the trigger count and alarm threshold based on the actual CPU usage, and apply the changes.

Step 3 Wait 2 minutes and check whether the alarm is automatically cleared.

- If yes, no further action is required.
- If no, go to **Step 4**.

Check whether the CPU usage reaches the upper limit.

Step 4 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. In the right pane, click this alarm and obtain the host name in **Location**.

Step 5 Choose **Cluster** > **Services** > **LdapServer**, click the **Instance** tab, and click the SlapdServer instance corresponding to the host name in **Step 4**.

Step 6 On the dashboard of the instance, observe the real-time data of the **CPU Usage of a Single SlapdServer Instance** chart for about 5 minutes and check whether the CPU usage exceeds the threshold (**75%** by default) for multiple times.

- If yes, go to **Step 7**.

- If no, go to **Step 9**.

Step 7 Check whether the status of other SlapdServer instances is normal. For details, see **Step 5** to **Step 6**.

- If yes, contact the MRS cluster administrator to evaluate whether to expand the capacity of SlapdServer instances. Then, go to **Step 8**.
- If no, repair the faulty SlapdServer instance and go to **Step 8**.

Step 8 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Collect fault information.

Step 9 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 10 Expand the **Service** drop-down list, and select **LdapServer** for the target cluster.

Step 11 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.248 ALM-25500 KrbServer Service Unavailable

Alarm Description

The system checks the KrbServer service status every 30 seconds. This alarm is generated when the system detects that the KrbServer service is abnormal.

This alarm is cleared when the system detects that the KrbServer service is normal.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
25500	Critical	Quality of service	Tenant plane	FusionInsight Manager	Yes

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

The running status of the component that depends on the KrbServer becomes faulty. As a result, the Kerberos authentication of the cluster fails, and the component services are abnormal.

Possible Causes

- The node where the KrbServer service locates is faulty.
- The OLdap service is abnormal.

Handling Procedure

Check whether the node where the KrbServer service locates is faulty.

Step 1 On the FusionInsight Manager home page, choose **Cluster** > *Name of the desired cluster* > **Services** > **KrbServer** > **Instance** to go to the KrbServer instance page to obtain the host name of the node where the KrbServer service locates.

Step 2 On the **Alarm** page of the FusionInsight Manager system, check whether any alarm of **NodeAgent Process Is Abnormal** exists.

- If yes, go to **Step 3**.
- If no, go to **Step 6**.

Step 3 Check whether the host name in the alarm is consistent with the **Step 1** host name.

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 Handle the alarm according to "ALM-12006 NodeAgent Process Is Abnormal".

Step 5 Check whether **KrbServer Service Unavailable** is cleared in the alarm list.

- If yes, no further action is required.
- If no, go to **Step 6**.

Check whether the OLdap service is normal.

Step 6 On the **Alarm** page of the FusionInsight Manager system, check whether any alarm of **OLdap Resource Abnormal** exists.

- If yes, go to **Step 7**.
- If no, go to **Step 9**.

Step 7 Handle the alarm according to "ALM-12004 OLdap Resource Abnormal".

Step 8 Check whether **KrbServer Service Unavailable** is cleared in the alarm list.

- If yes, no further action is required.
- If no, go to **Step 9**.

Collect fault information.

Step 9 On the FusionInsight Manager, choose **O&M** > **Log > Download**.

Step 10 Select **KrbServer** in the required cluster from the **Service**.

Step 11 Click the edit button in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Related Information

None.

1.3.249 ALM-25501 Too Many KerberosServer Requests

Alarm Description

The system checks the number of requests processed by the KerberosServer node every 30 seconds. This alarm is generated when the number of requests exceeds the threshold for multiple consecutive times (5 by default).

Its **Trigger Count** is configurable. If **Trigger Count** is set to **1**, this alarm is cleared when the number of process connections is less than or equal to the threshold. If **Trigger Count** is greater than **1**, this alarm is cleared when the number of requests is less than or equal to 90% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
25501	Critical (default threshold: 15,000) Major (default threshold: 10,000)	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
New	3.3.1	New alarm	New alarm

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Details	Specifies alarm details.

Impact on the System

KerberosServer responds slowly. As a result, Kerberos authentication times out and component services are in error.

Possible Causes

- There are too many KerberosServer requests.
- The alarm threshold or alarm trigger count is improperly configured.

Handling Procedure

Check whether there are too many KerberosServer requests.

Step 1 Log in to FusionInsight Manager and choose **Cluster** > **Services** > **KrbServer** to go to the KrbServer overview page.

Step 2 Observe the "Total KerberosServer Requests" chart and reduce the number of KerberosServer authentication requests based on the actual service scenario.

If no chart is available, click the drop-down arrow on the right, select **Customize**, select the desired item, and click **OK**.

Figure 1-12 Total KerberosServer requests

Step 3 Wait about 2 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 4**.

Check whether the alarm threshold or alarm trigger count is properly configured.

Step 4 On FusionInsight Manager, choose **O&M** > **Alarm** > **Thresholds**, click the name of the desired cluster, choose **KrbServer** > **Other** > **Total KerberosServer Requests**, and check whether the alarm trigger count and alarm threshold are set properly.

- If yes, go to **Step 7**.
- If no, go to **Step 5**.

Step 5 Change the trigger count and alarm threshold based on the actual number of requests, and apply the changes.

Step 6 Wait 2 minutes and check whether the alarm is automatically cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect fault information.

Step 7 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 8 Expand the **Service** drop-down list, and select **KrbServer** for the target cluster.

Step 9 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.250 ALM-27001 DBService Is Unavailable

Alarm Description

The alarm module checks the DBService status every 30 seconds. This alarm is generated when the system detects that DBService is unavailable.

This alarm is cleared when DBService recovers.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
27001	Critical	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

The database service is unavailable and cannot provide data import and query functions for upper-layer services, which results in service exceptions.

Possible Causes

- The floating IP address does not exist.
- There is no active DBServer instance.
- The active and standby DBServer processes are abnormal.

Handling Procedure

Check whether the floating IP address exists in the cluster environment.

Step 1 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **DBService** > **Instance**.

Step 2 Check whether the active instance exists.

- If yes, go to **Step 3**.
- If no, go to **Step 9**.

Step 3 Select the active DBServer instance and record the IP address.

Step 4 Log in to the host that corresponds to the preceding IP address as user **root**, and run the **ifconfig** command to check whether the floating IP address of DBService exists on the node.

- If yes, go to **Step 5**.
- If no, go to **Step 9**.

Step 5 Run the **ping** *floating IP address* command to check whether the DBService floating IP address can be pinged.

- If yes, go to **Step 6**.
- If no, go to **Step 9**.

Step 6 Log in to the host that corresponds to the DBService floating IP address as user **root**, and run the following command to delete the floating IP address:

ifconfig *interface* **down**

Step 7 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **DBService**. On the displayed page, click **More** > **Restart Service** to restart DBService. Check whether DBService is started successfully.

- If yes, go to **Step 8**.
- If no, go to **Step 9**.

Step 8 Wait about 2 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 14**.

Check the status of the active DBServer instance.

Step 9 Select the DBServer instance whose role status is abnormal and record the IP address.

Step 10 On the **Alarms** page, check whether the **Process Fault** alarm is generated for the DBServer instance on the host corresponding to the preceding IP address.

- If yes, go to **Step 11**.
- If no, go to **Step 19**.

Step 11 Rectify the fault by following the procedure provided in **ALM-12007 Process Fault**.

Step 12 Wait about 5 minutes and check whether the alarm is cleared in the alarm list.

- If yes, no further action is required.
- If no, go to **Step 19**.

Check the status of the active and standby DBServer processes.

Step 13 Log in to the host that corresponds to the IP address of DBService as user **root**, and run the **su - omm** command to switch to user **omm**.

Step 14 Run the **cd ${DBSERVER_HOME}** command to access the installation directory of DBService.

Step 15 Run the **sh sbin/status-dbserver.sh** command to view the status of the active and standby HA processes of DBService. Determine whether the status can be viewed successfully.

```
HAMode
double

NodeName            HostName            HAVersion           StartTime           HAActive
HAAllResOK          HARunPhase
10_5_89_12          host01              V100R001C01         2019-06-13 21:33:09     active
normal              Actived
10_5_89_66          host03              V100R001C01         2019-06-13 21:33:09     standby
normal              Deactived

NodeName            ResName             ResStatus           ResHAStatus         ResType
10_5_89_12          floatip             Normal              Normal              Single_active
10_5_89_12          gaussDB             Active_normal       Normal              Active_standby
10_5_89_66          floatip             Stopped             Normal              Single_active
10_5_89_66          gaussDB             Standby_normal      Normal              Active_standby
```

- If yes, go to **Step 16**.
- If no, go to **Step 19**.

Step 16 Check whether the active and standby HA processes are abnormal.

- If yes, go to **Step 17**.
- If no, go to **Step 19**.

Step 17 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **DBService**. On the displayed page, click **More** > **Restart Service** to restart DBService. Check whether DBService is restarted successfully.

- If yes, go to **Step 18**.
- If no, go to **Step 19**.

Step 18 Wait about 2 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 19**.

Collect fault information.

Step 19 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 20 Expand the **Service** drop-down list, and select **DBService** and **NodeAgent** for the target cluster.

Step 21 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 22 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.251 ALM-27003 DBService Heartbeat Interruption Between the Active and Standby Nodes

Alarm Description

This alarm is generated when the active or standby DBService node has not received heartbeat messages from the peer node for 7 seconds.

This alarm is cleared when the heartbeat recovers.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
27003	Major	Heartbeat	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	Local DBService HA	Specifies a local DBService HA.
	Peer DBService HA	Specifies a peer DBService HA.

Impact on the System

During the DBService heartbeat interruption, only one node can provide the service. If this node is faulty, no standby node is available for failover and the service is unavailable.

Possible Causes

The link between the active and standby DBService nodes is abnormal.

Handling Procedure

Check whether the network between the active and standby DBService servers is normal.

Step 1 In the alarm list on FusionInsight Manager, locate the row that contains the alarm, and click ⌄ to view the IP address of the standby DBService server for which the alarm is generated.

Step 2 Log in to the active DBService server as user **root**.

Step 3 Run the **ping** *heartbeat IP address of the standby DBService* command to check whether the standby DBService server is reachable.

- If yes, go to **Step 6**.
- If no, go to **Step 4**.

Step 4 Contact the network administrator to check whether the network is faulty.

- If yes, go to **Step 5**.
- If no, go to **Step 6**.

Step 5 Rectify the network fault and check whether the alarm is cleared from the alarm list.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select the following services for the target cluster

- DBService

- Controller
- NodeAgent

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.252 ALM-27004 Data Inconsistency Between Active and Standby DBServices

Alarm Description

The system checks the data synchronization status between the active and standby DBServices every 10 seconds. This alarm is generated when the synchronization status cannot be queried for six consecutive times or when the synchronization status is abnormal.

This alarm is cleared when the synchronization is in normal state.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
27004	Critical	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.

Type	Parameter	Description
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Local DBService HA	Specifies a local DBService HA.
	Peer DBService HA	Specifies a peer DBService HA.
	Synchronization of active and standby DBServices	Synchronization rate of active and standby DBService nodes

Impact on the System

When data is not synchronized between the active and standby DBServer and the active instance becomes abnormal, the data may be lost or abnormal.

Possible Causes

- The network between the active and standby nodes is unstable.
- The standby DBService is abnormal.
- The disk space of the standby node is full.
- The CPU usage of the GaussDB process on the active DBService node is high. (You need to locate the fault based on logs.)

Handling Procedure

Check whether the network between the active and standby nodes is normal.

Step 1 On FusionInsight Manager, choose **Cluster** > **Services** > **DBService** > **Instances** to view the service IP address of the standby DBServer instance.

Step 2 Log in to the active DBService node as user **root**.

Step 3 Run the **ping** *heartbeat IP address of the standby DBService* command to check whether the standby DBService node is reachable.

- If yes, go to **Step 6**.
- If no, go to **Step 4**.

Step 4 Contact the network administrator to check whether the network is faulty.

- If yes, go to **Step 5**.
- If no, go to **Step 6**.

Step 5 Rectify the network fault and check whether the alarm is cleared from the alarm list.

- If yes, no further action is required.
- If no, go to **Step 6**.

Check whether the status of the standby DBService is normal.

Step 6 Log in to the standby DBservice node as user **root**.

Step 7 Run the **su - omm** command to switch to user **omm**.

Step 8 Go to the **${DBSERVER_HOME}/sbin** directory and run the **./status-dbserver.sh** command to check whether the GaussDB resource status of the standby DBService is in normal state. In the command output, check whether the following information is displayed in the row where **ResName** is **gaussDB**:

The following is an example:

```
10_10_10_231 gaussDB Standby_normal Normal Active_standby
```

- If yes, go to **Step 9**.
- If no, go to **Step 16**.

Check whether the disk space of the standby node is full.

Step 9 Log in to the standby DBservice node as user **root**.

Step 10 Run the **su - omm** command to switch to user **omm**.

Step 11 Go to the **${DBSERVER_HOME}** directory, and run the following commands to obtain the DBService data directory:

cd ${DBSERVER_HOME}

source .dbservice_profile

echo ${DBSERVICE_DATA_DIR}

Step 12 Run the **df -h** command to check the system disk partition usage.

Step 13 Check whether the DBService data directory space is full.

- If yes, go to **Step 14**.
- If no, go to **Step 16**.

Step 14 Expand the disk capacity of the node by referring to MapReduce Service (MRS) 3.3.1-LTS Physical Machine Cluster Capacity Expansion Guide (for Huawei Cloud Stack 8.3.1).

Step 15 After the disk capacity is expanded, wait 2 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 16**.

Collect fault information.

Step 16 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 17 In the **Service** drop-down list, select **DBService** of the cluster to be operated, select **OS**, **OS Statistics**, and **OS Performance** in the OMS area, and click **OK**.

Step 18 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 19 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.253 ALM-27005 Database Connection Usage Exceeds the Threshold

Alarm Description

The system checks the database connection usage of the DBServer node every 30 seconds and compares the actual database connection usage with the threshold. This alarm is generated when the database connection usage exceeds the threshold for five consecutive times (configurable, five by default).

The trigger count is configurable. When the value is 1 and the data connections are no more than the threshold, the alarm is cleared. When the trigger count is greater than 1 and the data connections are no more than 90% of the threshold, the alarm is cleared.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
27005	Critical (default threshold: 95%) Major (The default threshold: 90%)	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger condition	Specifies the alarm triggering condition.

Impact on the System

Upper-layer services may fail to connect to the DBService database, affecting services.

Possible Causes

- There are too many database connections in use.
- The maximum number of database connections is set improperly.
- The alarm threshold or alarm trigger count is improperly configured.

Handling Procedure

Check whether there are too many database connections in use.

Step 1 On FusionInsight Manager, click **DBService** in the service list on the left. The DBService monitoring page is displayed.

Step 2 View the number of connections used by the database user, as shown in **Figure 1-13**. You can reduce the number of connections based on service requirements.

Figure 1-13 Connections used by the database user

Step 3 Wait 2 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 4**.

Check whether the maximum number of database connections is set properly.

Step 4 Log in to FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Service** > **DBService**, click **Configuration** and then **All Configurations**. Increase the maximum number of database connections allowed based on service requirements. After the modification, click **Save**. On the page that is displayed, click **OK**.

Figure 1-14 Setting maximum database connections

Step 5 After changing the maximum number of database connections, restart DBService (do not restart its upper-layer services).

Procedure: Log in to FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Service** > **DBService**. On the displayed page, click **More** > **Restart Service** in the upper right corner, enter the password of the current login user, and click **OK**. Do not select **Restart upper-layer services**. Click **OK**.

Step 6 Wait 2 minutes and check whether the alarm is automatically cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Check whether the alarm threshold or alarm trigger count is properly configured.

Step 7 Log in to FusionInsight Manager and change the alarm threshold and alarm smoothing times based on the number of database connections. Click **O&M** and choose **Alarm** > **Thresholds** in the navigation pane on the left. On the displayed page, click the name of the desired cluster > **DBService** > **Database** > **Database Connection Usage (DBServer)**. Click the pencil icon next to **Trigger Count** to change the value.

NOTE

If the value of **Trigger Count** exceeds the threshold, the alarm is generated.

Figure 1-15 Setting the alarm trigger count

Click **O&M**, and choose **Alarm** > **Thresholds** in the navigation pane on the left. On the displayed page, click the name of the desired cluster > **DBService** > **Database** > **Database Connection Usage (DBServer)** in the list on the left. Click **Modify** in the **Operation** column. Modify the rule and click **OK**. The modification takes effect immediately.

Figure 1-16 Configuring the alarm threshold

Step 8 Wait 2 minutes and check whether the alarm is automatically cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Collect fault information.

Step 9 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 10 Expand the **Service** drop-down list, and select **DBService** for the target cluster.

Step 11 Specify **Hosts** for collecting logs, which is optional. By default, all hosts are selected.

Step 12 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 13 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.254 ALM-27006 Data Directory Disk Usage Exceeds the Threshold

Alarm Description

The system checks the disk space usage of the data directory on the active DBServer node every 30 seconds and compares the actual disk space usage with the threshold. This alarm is generated when the disk space usage of the data directory exceeds the threshold for five consecutive times (configurable, five by default).

The trigger count is configurable. When the value is 1 and the data directory disk usage is no greater than the threshold, the alarm is cleared. When the trigger count is greater than 1 and the data directory disk usage is smaller than 90% of the threshold, the alarm is cleared.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
27006	Critical (default threshold: 85%) Major (default threshold: 80%)	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	PartitionName	Specifies the disk partition for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the condition for triggering the alarm.

Impact on the System

- The DBService service process cannot provide the API for data writing.
- When the disk space usage of the data directory exceeds 90%, the database enters the read-only mode and "Database Enters the Read-Only Mode" is generated. As a result, service data cannot be written to the database.

Possible Causes

- The alarm threshold is improperly configured.
- The database data volume is too large or the disk configuration cannot meet service requirements. As a result, the disk usage reaches the upper limit.

Handling Procedure

Check whether the threshold is set properly.

Step 1 On FusionInsight Manager, click **O&M** and choose **Alarm** > **Thresholds** in the navigation pane on the left. Click the name of the desired cluster, choose **DBService** > **Database** > **Data Directory Disk Usage**, and check whether the alarm threshold is **80%**.

- If yes, go to **Step 3**.

- If no, go to **Step 2**.

Step 2 Modify the alarm threshold based on the service requirements. For details, see "Configuring the Threshold" in MapReduce Service (MRS) 3.3.1-LTS User Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Usage Guide (for Huawei Cloud Stack 8.3.1).

Step 3 Click **Cluster** and choose the name of the desired cluster > **Service** > **DBService**. On the **Dashboard** page, view the **Data Directory Disk Usage** chart to check whether the disk usage of the data directory is less than the threshold.

- If yes, go to **Step 4**.
- If no, go to **Step 5**.

Step 4 Wait 2 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check whether large files are incorrectly written to the disk.

Step 5 Log in to the active management node as user **omm**.

Step 6 Run the following commands to check whether there are files over 500 MB in the disk of the data directory:

source $DBSERVER_HOME/.dbservice_profile

find "$DBSERVICE_DATA_DIR"/../ -type f -size +500M

- If yes, go to **Step 7**.
- If no, go to **Step 8**.

Step 7 Handle the incorrectly written files and check whether the alarm is cleared 2 minutes later.

- If yes, no further action is required.
- If no, go to **Step 8**.

Collect fault information.

Step 8 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 9 Expand the **Service** drop-down list, and select **DBService** for the target cluster.

Step 10 Specify **Hosts** for collecting logs, which is optional. By default, all hosts are selected.

Step 11 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.255 ALM-27007 Database Enters the Read-Only Mode

Alarm Description

The system checks the disk space usage of the data directory on the active DBServer node every 30 seconds. This alarm is generated when the disk space usage of the data directory exceeds 90%.

This alarm is cleared when the disk space usage of the data directory falls below 80%.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
27007	Critical	Quality of service	Tenant plane	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

- Service data is lost.
- Data cannot be written for upper-layer services and the data is lost.

Possible Causes

The disk configuration cannot meet service requirements. The disk usage reaches the upper limit.

Handling Procedure

Check whether the disk space usage reaches the upper limit.

Step 1 On FusionInsight Manager, choose **Cluster**, click the name of the desired cluster, and choose **Services** > **DBService**.

Step 2 On the **Dashboard** page, view the **Disk Space Usage of the Data Directory** chart to check whether the disk usage of the data directory exceeds 90%.

- If yes, go to **Step 3**.
- If no, go to **Step 13**.

Step 3 Log in to the active management node of the DBServer as user **omm** and run the following commands to check whether the database enters the read-only mode:

source $DBSERVER_HOME/.dbservice_profile

gsql -U omm -W *password* **-d postgres -p 20051**

show default_transaction_read_only;

NOTE

In the preceding command, **password** indicates the password of user **omm** of the DBService database. You can run the **\q** command to exit the database page.

Check whether the value of **default_transaction_read_only** is **on**.

```
POSTGRES=# show default_transaction_read_only;
 default_transaction_read_only
-------------------------------
 on
(1 row)
```

- If yes, go to **Step 4**.
- If no, go to **Step 13**.

Step 4 Run the following commands to open the **dbservice.properties** file:

source $DBSERVER_HOME/.dbservice_profile

vi ${DBSERVICE_SOFTWARE_DIR}/tools/dbservice.properties

Step 5 Change the value of **gaussdb_readonly_auto** to **OFF**. (The default is **ON**.)

Step 6 Run the following command to open the **postgresql.conf** file:

vi ${DBSERVICE_DATA_DIR}/postgresql.conf

Step 7 Delete **default_transaction_read_only = on**.

Step 8 Run the following command for the configuration to take effect:

gs_ctl reload -D ${DBSERVICE_DATA_DIR}

Step 9 Log in to FusionInsight Manager, and Choose **O&M** > **Alarm** > **Alarms**. On the right of the alarm "Database Enters the Read-Only Mode", click **Clear** in the **Operation** column. In the dialog box that is displayed, click **OK** Manually clear the alarm.

Step 10 Log in to the active DBServer node as user **omm**. Run the following commands to check whether files with more than 500 MB are incorrectly written into the disk space of the data directory:

source $DBSERVER_HOME/.dbservice_profile

find "$DBSERVICE_DATA_DIR"/../ -type f -size +500M

- If yes, go to **Step 11**.
- If no, go to **Step 13**.

Step 11 Delete the incorrectly written files based on site requirements.

Step 12 Log in to FusionInsight Manager. Click **Cluster** and choose the name of the desired cluster > **Service** > **DBService**. On the **Dashboard** page, view the **Data Directory Disk Usage** chart to check whether the disk usage is less than 80% of the threshold.

- If yes, no further action is required.
- If no, go to **Step 13**.

Collect fault information.

Step 13 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 14 Expand the **Service** drop-down list, and select **DBService** for the target cluster.

Step 15 Specify **Hosts** for collecting logs, which is optional. By default, all hosts are selected.

Step 16 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 17 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.256 ALM-32000 Solr Service Unavailable

Alarm Description

The system checks the Solr service availability every 30 seconds. This alarm is generated when the system detects that the Solr service is unavailable.

This alarm is cleared when the Solr service recovers.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
32000	Critical	Quality of service	Tenant plane	Solr	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.

Type	Parameter	Description
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

Solr is unavailable, and index data cannot be read or written.

Possible Causes

- The services on which the Solr service depends are abnormal.
- The network connection is interrupted.
- The number of Solr service task requests exceeds the threshold.

Handling Procedure

Check whether the services on which the Solr service depends are running properly.

Step 1 On the FusionInsight Manager portal and click **Cluster** > *Name of the desired cluster* > **Services**.

Step 2 In the service list, check whether the running status of the ZooKeeper services on which the Solr service depends is **Normal**. In security mode, you need to check the running status of KrbServer. In the mean time, if index data is stored on HDFS, you need to check the running status of HDFS.

- If yes, go to **Step 5**.
- If no, go to **Step 3**.

Step 3 Locate an unhealthy service and restart the service.

NOTE

To restart the service, you need to enter the FusionInsight Manager administrator password.

Step 4 Check whether the alarm is cleared from the alarm list.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check whether the network is normal.

Step 5 Choose **Cluster** > *Name of the desired cluster* > **Services** > **Solr** > **Instance** to view the Service plane IP addresses of the two SolrServerAdmin instances.

Step 6 Log in to the server of either SolrServerAdmin instance as user **root**.

Step 7 Run the **ping** *IP address of the other SolrServerAdmin instance* command to check whether the server of other SolrServerAdmin instance is reachable.

- If yes, go to **Step 10**.
- If no, go to **Step 8**.

Step 8 Contact system administrators to rectify network faults.

Step 9 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 10**.

Check whether the number of Solr service task requests exceeds the threshold.

Step 10 Log in to FusionInsight Manager, and choose **Cluster** > *Name of the desired cluster* > **Services** > **Solr** > **Configurations** to go to the Solr configuration page. On the displayed page, click **All Configurations**, search for **SOLR_OVERSEER_QUEUE_MAX_NUMCHILDREN** in the **Search** box, and view the parameter value.

This parameter specifies the maximum length of the task list processed by Solr Overseer.

Step 11 Log in to ZooKeeper, and view the number of tasks in Solr Overseer Queue.

1. Download and install the ZooKeeper client. For details, see "Installing a Client" in *MapReduce Service (MRS) 3.3.1-LTS User Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Usage Guide (for Huawei Cloud Stack 8.3.1).*
2. Log in to the client node as user **root** and run the following commands.

   cd /opt/hadoopclient

   source bigdata_env

   If the cluster uses the Security Mode, you need to perform security authentication.

   kinit admin

zkCli.sh -server *Business IP address of the node where ZooKeeper is located:Port number*(such as 24002)**/solr**

For example: **zkCli.sh-server 192.168.207.5:24002/solr**

3. After a successful login, run **stat /overseer/queue** to view the value of **numChildren** (which specifies the current task number).

```
[zk: 192.168.207.5:24002/solr(CONNECTED) 178] stat /overseer/queue
cZxid = 0x20003458f
ctime = Fri Jul 29 22:16:42 CST 2016
mZxid = 0x20003458f
mtime = Fri Jul 29 22:16:42 CST 2016
pZxid = 0x2000758c9
cversion = 143970
dataVersion = 0
aclVersion = 0
ephemeralOwner = 0x0
dataLength = 0
numChildren = 900
```

4. Check whether the value of **numChildren** is larger than the value of **SOLR_OVERSEER_QUEUE_MAX_NUMCHILDREN**, and the value of **numChildren** will not decrease.

- If yes, ZooKeeper is overloaded and cannot respond to Solr requests in a timely manner, or Solr is overloaded and cannot process tasks in a timely manner. The Solr service is about to become unavailable. Go to **Step 13**.
- If no, go to **Step 12**.

Step 12 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 13**.

Collect fault information.

Step 13 On the FusionInsight Manager portal, choose **O&M** > **Log** > **Download**.

Step 14 Select **Solr** in the required cluster from the **Service** drop-down list box.

Step 15 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 16 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.257 ALM-32002 SolrServerAdmin Heartbeat Interruption Between the Active and Standby Nodes

Alarm Description

This alarm is generated when the SolrServerAdmin active node or standby node does not receive heartbeat messages from the peer for 30 seconds (heartbeat interruption duration configured in keepalive).

This alarm is cleared when the heartbeat recovers.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
32002	Major	Communications	Tenant plane	Solr	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
Modify	3.3.1	Alarm Severity: changed from Minor to Major.	Alarm Severity: Accuracy optimized

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

Only one active SolrServerAdmin node can provide services. If the node is faulty, active/standby switchover cannot be performed.

Possible Causes

- The active or standby SolrServerAdmin instance is in the stopped state.
- The floating network interface used by the abnormal SolrServerAdmin was wrongly configured, so the SolrServerAdmin started failed.
- The link between the active and standby SolrServerAdmin nodes is abnormal.

Handling Procedure

Check the status of the active and standby SolrServerAdmin instances.

Step 1 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services** > **Solr** > **Instance** to check whether the active and standby SolrServerAdmin instances are in the **Normal** state.

- If yes, go to **Step 3**.
- If no, go to **Step 2**.

Step 2 Select a stopped SolrServerAdmin instance and click **Start Instance**. Check whether the alarm is cleared from the alarm list.

- If yes, no further action is required.
- If no, go to **Step 3**.

Check whether the link between the active and standby SolrServerAdmin nodes is abnormal.

Step 3 Choose **Cluster** > *Name of the desired cluster* > **Services** > **Solr** > **Instance** to view the Service plane IP addresses of the two SolrServerAdmin instances.

Step 4 Log in to the server of either SolrServerAdmin instance as user **root**.

Step 5 Run the **ping** *IP address of the other SolrServerAdmin instance* command to check whether the server of other SolrServerAdmin instance is reachable.

- If yes, go to **Step 8**.
- If no, go to **Step 6**.

Step 6 Contact system administrators to rectify network faults.

Step 7 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Check whether any exception message is printed in the log of the node where the abnormal SolrServerAdmin instance resides.

Step 8 Log in to the server of either SolrServerAdmin instance as user **root**.

Step 9 Open the **/var/log/Bigdata/solr/SolrServerAdmin/prestartDetail.log** file and check whether the log file contains **Float ip** *x.x.x.x* **is invalid**.

- If yes, go to **Step 10**.
- If no, go to **Step 12**.

Step 10 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Solr** > **Configurations** > **All Configurations**, search for **SOLRHASERVER_FLOAT_IP**, change the parameter value to the correct floating IP address, save the configuration, and restart the Solr service.

NOTE

Contact the network administrator to obtain the new floating IP address.

Step 11 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 12**.

Collecting Fault Information

Step 12 On the FusionInsight Manager portal, choose **O&M** > **Log** > **Download**.

Step 13 Select the following services in the required cluster from the **Service** drop-down list:

- Solr
- Controller
- NodeAgent

Step 14 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 15 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.258 ALM-32003 Solr Heap Memory Usage Exceeds the Threshold

Alarm Description

The system checks the Solr heap memory usage every 60 seconds. This alarm is generated when the memory usage exceeds the threshold.

When the **Trigger Count** is 1, this alarm is cleared when the Solr heap memory usage is less than or equal to the threshold. When the **Trigger Count** is greater than 1, this alarm is cleared when the Solr heap memory usage is less than or equal to 90% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
32003	Critical (default threshold: 99%) Major (default threshold: 95%)	Quality of service	Tenant plane	Solr	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.

Type	Parameter	Description
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

If the Solr heap memory usage is high, the Solr index data read and write performance may become slow, and the process may restart in serious cases.

Possible Causes

Solr heap memory is insufficient.

Handling Procedure

Delete unnecessary files.

Step 1 Log in to the Solr client as user **root**.

Step 2 Run the following command to go to the installation directory.

cd /opt/hadoopclient

Step 3 Run the following command to import environment variables.

source bigdata_env

Step 4 If the cluster uses a secure version, run the following command to perform security authentication.

kinit solr

Enter the password as prompted. Obtain the password from the administrator.

Step 5 Run the following command to delete the unnecessary collection.

solrctl collection --delete *collection name*

Step 6 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Check the Solr JVM memory usage and configuration.

Step 7 On the FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Solr** > **Configurations**, and click **All Configurations**.

Step 8 In **Search**, enter **GC_OPTS** to check the **GC_OPTS** memory parameter of **Solr->SolrServer**. You can adjust configuration by referring to the Note.

NOTE

Suggestions on configuring the GC parameter of Solr:

- It is recommended that 50% memory be reserved for the Lucence cache and 50% memory for Solr. You are advised to allocate 28 GB (no more than 30 GB) to machines with large memory and confirm that JVM Compressed Oops has been enabled. You can run the following command to check whether the JVM Compressed Oops is enabled after logging in to the Solr client:

  java -server -Xms28G -Xmx28G -XX:+UseConcMarkSweepGC -XX:+UnlockDiagnosticVMOptions -XX:+PrintCompressedOopsMode -version

  If the returned value for Compressed Oops mode is Zero based, it indicates that the JVM Compressed Oops function is enabled and you need to increase the size of the allocated memory. Change 28 GB to 29 GB and check whether the Compressed Oops function is enabled. Try until the allocated memory reaches the maximum for the Compressed Oops function to remain enabled.

  If the returned value for Compressed Oops mode is Non-zero based, it indicates that the JVM Compressed Oops function is disabled and you need to decrease the size of the allocated memory. Change 28 GB to 27 GB and check whether the Compressed Oops function is enabled. Try until the allocated memory reaches the maximum for the Compressed Oops function to remain enabled.
- It is recommended that **-Xms** and **-Xmx** be set to the same value to prevent dynamic adjustment of heap memory size by JVM from affecting the performance.
- If half of the computer memory is less than the number of instances multiplied by 28 GB, allocate the memory by referring to the following:

  Instance memory = (Computer memory x 0.5)/Number of instances on the computer

  For example, if a computer has a memory of 128 GB and has three Solr instances, the value of **GC_OPTS** is: 128 GB x 0.5/3 = 21 GB, and confirm that the JVM Compressed Oops function has been enabled.

Step 9 Modify Solr memory parameters. Click **Save**, and click **OK**.

Step 10 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 11**.

Step 11 On the FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 12 Select **Solr** in the required cluster from the **Service** drop-down list.

Step 13 Click edit button in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 14 Contact the technical support, and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.259 ALM-32005 Down Replicas Exist in Solr

Alarm Description

The system checks all the copy status of a Solr instance every 60 seconds. This alarm is generated when a copy is in the Down state.

The default alarm threshold is 0.

This alarm is cleared when the number of Solr instances in the Down state is less than or equal to 90% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
32005	Critical (default threshold: 100) Major (default threshold: 0)	Quality of service	Tenant plane	Solr	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

If the Solr service replica shard is faulty, the Solr index data read/write performance will be affected.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Possible Causes

There are excessive number of Solr instance copies, and copy status cannot be restored in the specified period of time.

Handling Procedure

Check the default value of SOLR_LEADER_CONFLICT_RESOLVE_WAIT.

Step 1 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services** > **Solr** > **Configurations**, and click **All Configurations**.

Step 2 In **Search**, enter **SOLR_LEADER_CONFLICT_RESOLVE_WAIT** to check the **SOLR_LEADER_CONFLICT_RESOLVE_WAIT** value of **Solr->SolrServer**.

Adjust the configuration in the system.

Step 3 Change the default value of the **SOLR_LEADER_CONFLICT_RESOLVE_WAIT** parameter for the Solr instance whose copy is in the Down state to **43200000** and click **Save**. Then click **OK**.

Step 4 Check whether the alarm is cleared (ensure that this alarm is not generated in 12 hours).

- If yes, no further action is required.
- If no, go to **Step 5**.

Step 5 On the FusionInsight Manager portal, choose **O&M** > **Log** > **Download**.

Step 6 Select **Solr** in the required cluster from the **Service** drop-down list.

Step 7 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 day ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 8 Contact the technical support, and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.260 ALM-32006 Solr Instance GC Time Exceeds the Threshold

Alarm Description

The system detects the garbage collection (GC) time of the Solr instance process every 60 seconds. This alarm is generated when the GC time exceeds the threshold (12000 ms by default).

If Trigger Count is set to 1, and the GC time of the Solr instance process is less than or equal to the threshold, this alarm is cleared. If Trigger Count is set to a value greater than 1, and the GC time of the Solr instance process is less than or equal to 90% of the threshold, this alarm is cleared.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
32006	Critical (default threshold: 30000ms) Major (default threshold: 12000ms)	Quality of service	Tenant plane	Solr	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

If the GC time of the Solr instance process is too long, the Solr index data read/write performance may be affected. In serious cases, the request may time out.

Possible Causes

Service loads of the Solr instance on the node are heavy, or the heap memory is inappropriately allocated. As a result, the process GCs frequently occur.

Handling Procedure

Check the size of the instance heap memory.

Step 1 On the FusionInsight Manager main menu, choose **O&M** > **Alarm** > **Alarms**. Then, find the alarm **Solr Instance GC Time Exceeds the Threshold** in the alarm list, click in the row containing the alarm, and view the information under **Location** to view the IP address of the instance for which the alarm is generated.

Step 2 On the FusionInsight Manager main menu, choose **Cluster** > *Name of the desired cluster* > **Services** > **Solr** > **Instance**. Then, select the instance for which the alarm is generated. Click the drop-down menu in the Chart area and choose **Customize** > **Clear All** > **Garbage Collection** > *Name of the desired instance* **GC Time Stats**, and click **OK** to check whether the GC time exceeds the threshold.

Step 3 On the FusionInsight Manager main menu, choose **Cluster** > *Name of the desired cluster* > **Services** > **Solr**. Then, click **Configurations** on the displayed page.

Step 4 On the **Configurations** tab page, enter **GC_OPTS** in the search box in the upper right corner and click .

GC_OPTS parameters of all instances are displayed.

Step 5 Select the instance whose GC_OPTS value needs to be changed, and check whether the differentiated configuration icon is displayed after the instance value configuration box.

- If yes, go to **Step 6**.
- If no, go to **Step 9**.

Step 6 Click . In the displayed dialog box, click in the right pane and click OK to save the settings.

Step 7 In **Search**, enter **GC_OPTS** to check the **GC_OPTS** memory parameter of **Solr->SolrServer**. You can adjust configuration by referring to the Note.

NOTE

Suggestions on configuring the GC parameter of Solr:

- It is recommended that 50% memory be reserved for the Lucence cache and 50% memory for Solr. You are advised to allocate 28 GB (no more than 30 GB) to machines with large memory and confirm that JVM Compressed Oops has been enabled. You can run the following command to check whether the JVM Compressed Oops is enabled after logging in to the Solr client:

  java -server -Xms28G -Xmx28G -XX:+UseConcMarkSweepGC -XX:+UnlockDiagnosticVMOptions -XX:+PrintCompressedOopsMode -version

  If the returned value for Compressed Oops mode is Zero based, it indicates that the JVM Compressed Oops function is enabled and you need to increase the size of the allocated memory. Change 28 GB to 29 GB and check whether the Compressed Oops function is enabled. Try until the allocated memory reaches the maximum for the Compressed Oops function to remain enabled.

  If the returned value for Compressed Oops mode is Non-zero based, it indicates that the JVM Compressed Oops function is disabled and you need to decrease the size of the allocated memory. Change 28 GB to 27 GB and check whether the Compressed Oops function is enabled. Try until the allocated memory reaches the maximum for the Compressed Oops function to remain enabled.
- It is recommended that **-Xms** and **-Xmx** be set to the same value to prevent dynamic adjustment of heap memory size by JVM from affecting the performance.
- If half of the computer memory is less than the number of instances multiplied by 28 GB, allocate the memory by referring to the following:

  Instance memory = (Computer memory x 0.5)/Number of instances on the computer

  For example, if a computer has a memory of 128 GB and has three Solr instances, the value of **GC_OPTS** is: 128 GB x 0.5/3 = 21 GB and confirm that the JVM Compressed Oops function has been enabled.

Step 8 After the modification, click **Save** in the upper left corner. In the displayed **Save Configuration** dialog box, click **OK**.

Step 9 Restart the affected Solr instance.

Step 10 Check whether the alarm is cleared five minutes later.

- If yes, no further action is required.
- If no, go to **Step 11**.

Collect the fault information.

Step 11 On the FusionInsight Manager main menu, choose **O&M** > **Log** > **Download**.

Step 12 Select **Solr** in the required cluster for **Service**.

Step 13 Click in the upper right corner, and set **Start Date** to a time point 10 minutes earlier than the alarm generation time and **End Date** to a time point 10 minutes later than the alarm generation time. Then, click **Download**.

Step 14 Contact the technical support and provide the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.261 ALM-32007 Solr Has Collections Without Replicas

Alarm Description

The system checks whether collections without replicas exist in Solr every 60 seconds. This alarm is generated when the system detects a collection with no replica in Solr.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
32007	Major	Quality of service	Tenant plane	Solr	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	Index List	Specifies the index list without replicas.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

NOTE

The length of the index list is restricted by the character length. When the content exceeds 256 characters, only some index names can be displayed. For details about how to query the complete index list, see **Handling Procedure**.

Impact on the System

Some Solr index data has only one copy, affecting Solr data reliability. A single node fault may cause data loss.

Possible Causes

No replica is configured or shard replicas are added or deleted when the collections is created.

Handling Procedure

View collections without replicas.

Step 1 On the FusionInsight Manager homepage, choose **O&M** > **Log** > **Online Search**. Enter "Alarm 32007 Collection List" in the **Search Content** text box. Then, select **OMS** > **Agent** for **Service**, the **agent** file for **File**, and **INFO** for **Lowest Log Level**. After the configuration, click **Search**.

Step 2 Select the latest generated logs in the search result and view all collections without replicas. The following is an example.

```
2019-06-13 11:06:00,383 INFO [monitor_60_1_7_SolrServerAdmin] Alarm 32007 Collection List;
{test3=[shard2, shard3, shard1], test1=[shard1]}
com.huawei.fusioninsight.solr.monitor.collector.impl.ReplicaNumCollector.sendRepAlarm(ReplicaNumCollecto
r.java:160)
```

NOTE

As shown in the preceding logs, Collection without replicas are test1 and test3. In test3, shard1, shard2, and shard3 have no replicas. In text1, shard1 has no replicas.

Manually add collection shard replicas.

Step 3 On the FusionInsight Manager homepage, choose **Cluster** > *Name of the desired cluster* > **Services** > **Solr**. Click **SolrServerAdmin** (any one is OK) on the Solr WebUI.

NOTE

By default, the **admin** user does not have the permissions to manage other components. If the page cannot be opened or the displayed content is incomplete when you access the native UI of a component due to insufficient permissions, you can manually create a user with the permissions to manage that component.

Step 4 On the **Solr Admin** page, click the collections without replicas in **Step 2**, expand the desired shard name on the right, and choose **add replica** > **Create Replica** to increase the number of replicas.

Step 5 After adding shard replicas for all collections without setting replicas, manually clear the alarm. Wait for 5 minutes and check whether the alarm is generated again.

- If yes, go to **Step 6**.
- If no, no further action is required.

Collect the fault information.

Step 6 On the FusionInsight Manager homepage, choose **O&M** > **Log** > **Download**.

Step 7 Select **Solr** in the required cluster for **Service**.

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact the technical support and provide the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.262 ALM-32008 Solr Stored Shard Data Volume Exceeds the Threshold

Alarm Description

The system checks the size of data stored on Solr shards every 60 seconds and compares the actual size of data on Solr shards with the threshold. This alarm is

generated when the system detects that the size of data stored on Solr shards exceeds the threshold for a specified number of times (3 times by default).

You can choose **O&M** > **Alarm** > **Thresholds**, click the name of the desired cluster, and choose **Solr** > **Shard** > **Data Volume on Solr Shards** to change the threshold.

This alarm is cleared when **Trigger Count** is **1** and data stored on Solr shards is less than or equal to the threshold. This alarm is cleared when **Trigger Count** is greater than **1** and data stored on Solr shards is less than or equal to 90% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
32008	Critical (default threshold: 83886080 KB) Major (default threshold: 41943040 KB)	Quality of service	Tenant plane	Solr	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.

Type	Parameter	Description
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	Alarm Severity	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

If a large amount of Solr shard data is stored, the read and write performance of Solr index data may be slowed down. When the Solr process is restarted, the restoration speed of shards with a large amount of data is slowed down.

Possible Causes

The number of Solr collection shards is not properly configured. As a result, the size of data stored on Solr shards exceeds the threshold.

Handling Procedure

Check the data size of each shard.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** > *Solr Stored Shard Data Volume Exceeds the Threshold* > **Location**. Check the name of the host for which the alarm is generated.

Step 2 Log in to the host where the client is installed as user **root**. Run **cd** to switch to the client installation directory, and run **source bigdata_env** to configure the environment variables.

If the cluster uses the security mode, perform security authentication.

Run the **kinit***user* command and enter the password as prompted (obtain the password from the MRS cluster administrator).

NOTE

user indicates the Solr user.

Step 3 Run the **curl --negotiate -k -v -u : 'https://*ip:httpport*/solr/admin/cores?action=STATUS&wt=json&indent=on'** command to query details about the data stored on the shards of the current instance.

NOTE

- *ip*: indicates the IP address of the host for which the alarm is reported in the Solr cluster.
- *httpport*: indicates the HTTP port of the Solr instance. On FusionInsight Manager, you can choose **Solr** > **Configurations** > **All Configurations** and search for **SOLR_SEC_PORT** in the search box in the upper right corner of the page and select the required port number based on the instance name. If the cluster uses the normal mode, search for **SOLR_PORT** in the search box.
- In normal mode, delete the security authentication parameter **--negotiate -k -v -u :** and change **https** to **http**.
- The description of parameters in the **curl** command is the same as the preceding command description.

Perform data shard splitting.

Step 4 Determine the shards storing too much data (the configured threshold is exceeded) and run the following command to perform the data shard splitting operation:

curl --negotiate -k -v -u : 'https://*ip:httpport*/solr/admin/collections?action=SPLITSHARD&collection=*collection*&shard=*shard*&async=*request-id*'

NOTE

- ***collection***: indicates the collection where the shard to be split resides.
- ***shard***: shard to be split.
- ***request-id***: specifies the ID of the split request when the request is executed asynchronously. The **async** parameter is optional. If the shard data volume is large and the splitting request takes a long time, you need to use this parameter to execute the shard splitting request asynchronously.
- Shard splitting consumes a large number of I/Os and network resources. Therefore, perform this operation during off-peak hours.

Step 5 Run the following command. If **msg** is **found [*request-id*] in completed tasks** in the command output, the shard splitting is complete.

curl --negotiate -k -v -u : 'https://*ip:httpport*/solr/admin/collections?action=REQUESTSTATUS&requestid=*request-id*'

- If yes, go to **Step 6**.
- If no, continue to wait.

NOTE

request-id: specifies the ID of the asynchronous shard splitting task.

Step 6 After shard splitting, run the following command to delete the original shard:

curl --negotiate -k -v -u : 'https://*ip:httpport*/solr/admin/collections?action=DELETESHARD&shard=*shard*&collection=*collection*'

Step 7 After the shard deletion is complete, check whether the alarm is cleared 5 minutes later.

- If yes, no further action is required.
- If no, go to **Step 8**.

Collect fault information.

Step 8 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 9 Expand the **Service** drop-down list, and select **Solr** for the target cluster.

Step 10 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 11 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.263 ALM-32009 Solr Shard Document Number Exceeds the Threshold

Alarm Description

The system checks the number of documents on each Solr shard every 60 seconds and compares the actual number of documents on each Solr shard with the threshold (0.4 billion by default). This alarm is generated when the number of documents on a Solr shard exceeds the threshold for a specified number of times (3 by default).

You can change the threshold by choosing **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Solr** > **Shard** > **Solr Shard Document Number Exceeds the Threshold**.

This alarm is cleared when the number of times when smoothing is performed is 1 and the number of Solr documents on each shard is less than or equal to the threshold. This alarm is cleared when the number of times when smoothing is performed is greater than 1 and the number of documents on each Solr shard is less than or equal to 90% of the threshold.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
32009	Critical (default threshold: 500,000,000) Major (default threshold: 400,000,000)	Quality of service	Tenant plane	Solr	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	HostName	Specifies the host for which the alarm was generated.
	Alarm Severity	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

If the number of Solr shard documents is too large, the index data read/write performance of Solr may be slowed down. When the Solr process is restarted, the restoration speed of shards with a large amount of data is slowed down.

Possible Causes

The number of Solr collection shards is incorrectly configured, and the number of documents on some shards exceeds the threshold.

Handling Procedure

Check the number of documents on each shard.

Step 1 On the FusionInsight Manager homepage, choose **O&M** > **Alarm** > **Alarms** > *Solr Stored Shard Data Volume Exceeds the Threshold* > **Location**. Check the name of the host for which the alarm is generated.

Step 2 Log in to the host where the client is installed as user **root**. Run **cd** to switch to the client installation directory, and run **source bigdata_env** to configure the environment variables.

If the cluster uses the security mode, perform security authentication.

Run the **kinit***user* command and enter the password as prompted (obtain the password from the MRS cluster administrator).

NOTE

User: indicates the Solr user.

Step 3 Run the **curl --negotiate -k -v -u : 'https://*ip:httpport*/solr/admin/cores?action=STATUS'** command to query details about the number of documents on each shard in the current instance.

NOTE

- *iP*: indicates the IP address of the host for which the alarm is reported in the Solr cluster.
- *httpport*: indicates the HTTP port of the Solr instance. On the FusionInsight Manager homepage, you can choose **Solr** > **Configurations** > **All Configurations** and search for **SOLR_SEC_PORT** in the search box in the upper right corner of the page and select the required port number based on the instance name. If the cluster uses the normal mode, search for **SOLR_PORT** in the search box.
- In normal mode, delete the security authentication parameter **--negotiate -k -v -u :** and change **https** to **http**.
- The description of parameters in the **curl** command is the same as the preceding command description.

Perform data shard splitting.

Step 4 Determine the shards where the document size exceeds the threshold and run the following command to perform the data shard splitting operation:

curl --negotiate -k -v -u : 'https://*ip:httpport*/solr/admin/collections?action=SPLITSHARD&collection=*collection*&shard=*shard&async=request-id*'

NOTE

- ***collection***: indicates the collection where the shard to be split resides.
- ***shard***: Shard to be split.
- ***request-id***: specifies the ID of the split request when the request is executed asynchronously. The **async** parameter is optional. If the shard data volume is large and the splitting request takes a long time, you need to use this parameter to execute the shard splitting request asynchronously.
- Shard splitting consumes a large number of I/Os and network resources. Therefore, perform this operation during off-peak hours.

Step 5 Run the following command. If **msg** is **found [*request-id*] in completed tasks** in the command output, the shard splitting is complete.

curl --negotiate -k -v -u : 'https://*ip:httpport*/solr/admin/collections?action=REQUESTSTATUS&requestid=*request-id*'

- If yes, go to **Step 6**.
- If no, continue to wait.

NOTE

request-id: specifies the ID of the asynchronous shard splitting task.

Step 6 After shard splitting, run the following command to delete the original shard:

curl --negotiate -k -v -u : 'https://*ip:httpport*/solr/admin/collections?action=DELETESHARD&shard=*shard*&collection=*collection*'

Step 7 After the shard deletion is complete, check whether the alarm is cleared 5 minutes later.

- If yes, no further action is required.
- If no, go to **Step 8**.

Collect the fault information.

Step 8 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 9 Expand the **Service** drop-down list, and select **Solr** for the target cluster.

Step 10 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 11 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.264 ALM-32010 Invalid Solr HA Certificate File

Alarm Description

Solr checks whether the HA certificate file is valid (whether the certificate exists and whether its format is correct) in the first health check or at 01:00:00 every day. This alarm is generated when the certificate file is invalid.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
32010	Major	Quality of service	Tenant plane	Solr	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	Alarm Severity	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

Some functions are unavailable.

Possible Causes

The HA certificate file is invalid.

Handling Procedure

View alarm information.

Step 1 Log in to FusionInsight Manager and choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**, locate the row that contains **ALM-32010 Invalid Solr HA Certificate File**, and view the **Location** information. View the IP address of the instance for which the alarm is generated.

Check whether the HA certificate file in the system is valid.

Step 2 Use PuTTY to log in to the host for which the alarm is generated as user **omm**.

Step 3 Run the **cd ${BIGDATA_HOME}/FusionInsight_HD_*/install/FusionInsight-Solr-*/solrhaserver/ha/local/cert** command to go to the directory where the HA certificate is stored.

Step 4 Run the **ls -l** command to check whether the **server.crt** file exists.

- If yes, go to **Step 5**.
- If no, go to **Step 6**.

Step 5 Run the **openssl x509 -in server.crt -text -noout** command and check whether the command output is normal.

- If yes, go to **Step 9**.
- If no, go to **Step 6**.

Step 6 Run the **cd ${BIGDATA_HOME}/FusionInsight_HD_*/install/FusionInsight-Solr-*/bin** command to go to the directory where the Solr script is stored.

Step 7 Run the **sh solr-ha-re-gencert.sh** command to generate a new HA certificate. Then, check whether the alarm is cleared 1 minute later.

- If yes, go to **Step 8**.
- If no, go to **Step 9**.

Step 8 Check whether this alarm is generated again during periodic system check.

- If yes, go to **Step 9**.
- If no, no further action is required.

Collect the fault information.

Step 9 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 10 Select **Solr** in the required cluster for **Service**.

Step 11 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.265 ALM-32011 Solr HA Certificate Is About to Expire

Alarm Description

Solr checks whether the HA certificate file is about to expire in the first health check or at 01:00:00 every day. This alarm is generated when the validity period is less than 30 days.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
32011	Major	Quality of service	Tenant plane	Solr	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	Alarm Severity	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

The user certificate file is about to expire. If the formal file expires, some functions are restricted and cannot be used.

Possible Causes

The HA certificate is about to expire.

Handling Procedure

View alarm information.

Step 1 Log in to FusionInsight Manager and choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**. On the page that is displayed, locate the row containing **ALM-32011 Solr HA Certificate Is About to Expire**, and view the **Location** information. View the IP address of the instance for which the alarm is generated.

Check the validity period of the HA certificate file in the system and generate a new HA certificate file.

Step 2 Use PuTTY to log in to the host for which the alarm is generated as user **omm**.

Step 3 Run the **cd ${BIGDATA_HOME}/FusionInsight_HD_*/install/FusionInsight-Solr-*/solrhaserver/ha/local/cert** command to go to the directory where the HA certificate is stored.

Step 4 Run the **openssl x509 -noout -text -in server.crt** command to query the effective time and due time of the HA certificate.

Step 5 Perform **Step 6** to **Step 7** during off-peak hours to update the certificate file as needed.

Step 6 Run the **cd ${BIGDATA_HOME}/FusionInsight_HD_*/install/FusionInsight-Solr-*/bin** command to go to the directory where the Solr script is stored.

Step 7 Run the **sh solr-ha-re-gencert.sh** command to generate a new HA certificate. Then, check whether the alarm is cleared 1 minute later.

- If yes, go to **Step 9**.
- If no, go to **Step 8**.

Step 8 On the node where the standby SolrServerAdmin instance is located, repeat **Step 6** to **Step 7**. Then, check whether the alarm is cleared 1 minute later.

- If yes, go to **Step 9**.
- If no, go to **Step 10**.

Step 9 Check whether this alarm is generated again during periodic system check.

- If yes, go to **Step 10**.
- If no, no further action is required.

Collect the fault information.

Step 10 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 11 Select **Solr** in the required cluster for **Service**.

Step 12 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 13 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.266 ALM-32012 Solr HA Certificate File Has Expired

Alarm Description

Solr checks whether the HA certificate file has expired in the first health check or at 01:00:00 every day. This alarm is generated when the HA certificate has expired.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
32012	Major	Quality of service	Tenant plane	Solr	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	Alarm Severity	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

Some functions are unavailable.

Possible Causes

The HA certificate file has expired.

Handling Procedure

View alarm information.

Step 1 Log in to FusionInsight Manager and choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**, locate the row that contains **ALM-32012 Solr HA Certificate File Has Expired**, and view the **Location** information. View the IP address of the instance for which the alarm is generated.

Check the validity period of the HA certificate file in the system and generate a new HA certificate file.

Step 2 Use PuTTY to log in to the host for which the alarm is generated as user **omm**.

Step 3 Run the **cd ${BIGDATA_HOME}/FusionInsight_HD_*/install/FusionInsight-Solr-*/solrhaserver/ha/local/cert** command to go to the directory where the HA certificate is stored.

Step 4 Run the **openssl x509 -noout -text -in server.crt** command to query the effective time and due time of the HA certificate and check whether the HA certificate file is valid.

- If yes, go to **Step 9**.
- If no, go to **Step 5**.

Step 5 Run the **cd ${BIGDATA_HOME}/FusionInsight_HD_*/install/FusionInsight-Solr-*/bin** command to go to the directory where the Solr script is stored.

Step 6 Run the **sh solr-ha-re-gencert.sh** command to generate a new HA certificate. Then, check whether the alarm is cleared 1 minute later.

- If yes, go to **Step 8**.
- If no, go to **Step 7**.

Step 7 On the node where the standby SolrServerAdmin instance is located, repeat **Step 5** to **Step 6**. Then, check whether the alarm is cleared 1 minute later.

- If yes, go to **Step 8**.
- If no, go to **Step 9**.

Step 8 Check whether this alarm is generated again during periodic system check.

- If yes, go to **Step 9**.
- If no, no further action is required.

Collect the fault information.

Step 9 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 10 Select **Solr** in the required cluster for **Service**.

Step 11 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.267 ALM-33004 BLU Instance Health Status of Containers Is Abnormal

Alarm Description

The system checks the health status of BLU instances every minute. This alarm is generated when over 50% of deployed BLU instances are abnormal.

This alarm is automatically cleared when the system detects that the BLU instance recovers.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
33004	Minor	Heartbeat	Tenant plane	Containers	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	GroupName	Specifies the name of the group for which the alarm is generated.
	BLU ID	Specifies the ID of a BLU.
	BLU Version	Specifies the BLU version.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	AlarmLevel	Specifies the alarm severity.
Additional Information	Cloud Service	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

If some BLU instances of a BLU role are unhealthy, service functions are not affected, but the service processing capability of the BLU instances may deteriorate. However, if all BLU instances of a BLU role are unhealthy, the services depend on the BLU role become unavailable.

Possible Causes

The causes need to be located by service development and maintenance personnel based on related logs.

Handling Procedure

Collect fault information.

Step 1 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 2 Expand the **Service** drop-down list and select **Containers**.

Step 3 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the hosts to which the role belongs, and click **OK**.

Step 4 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 5 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

1.3.268 ALM-33005 Maximum Number of Concurrent Containers Requests Exceeds the Threshold

Alarm Description

The system checks the maximum number of concurrent Containers requests every 5 minutes and compares the number with the threshold. This alarm is generated when the maximum number of concurrent service requests exceeds the threshold.

This alarm is automatically cleared when the maximum number of concurrent Containers requests is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
33005	Warning	Quality of service	Tenant plane	Containers	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	RegionId	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	RoleName	Specifies the role for which the alarm was generated.
	ApplicationServiceName	Specifies the name of the application for which the alarm is generated.
	Version	Specifies the version for which the alarm is generated.
	Method	Specifies the method for generating the alarm.
	IP	Specifies the IP address for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger condition	Specifies the threshold for triggering the alarm.

Impact on the System

If the maximum number of concurrent Containers requests is too large, the service provider rejects some requests. As a result, the service fails to be called.

Possible Causes

- It takes a long time to process the service logic code.
- The service volume is too large.

Handling Procedure

Check whether the service code processing time is too long.

Step 1 On FusionInsight Manager, choose **Cluster** > **Services** > **Containers**.

Step 2 Choose **SGP Management** > **App Service List**, and click the link of the service for which the alarm is generated to access the service status page.

Step 3 Check whether the provider's processing time is too long.

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 Check whether the processing time of user's upper-layer service logic code is too long.

- If yes, optimize the upper-layer service logic code and execute **Step 5**.
- If no, go to **Step 6**.

Step 5 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Check whether the service volume is too large.

Step 6 On FusionInsight Manager, choose **Cluster** > **Services** > **Containers**, click the **SGP Management** tab, and view charts **Request Number Per Second** and **Response Time** to check whether the data volume remains high.

- If yes, go to **Step 7**.
- If no, go to **Step 9**.

Step 7 Choose **Cluster** > **Services** > **Containers**, and click the **Business Manager** tab. Select the BLU that carries services. On the page that is displayed, click the **BLU Instance** tab and click **Add Instance** to add a BLU instance.

Step 8 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Collect fault information.

Step 9 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 10 Expand the **Service** drop-down list and select **Containers**.

Step 11 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the hosts to which the role belongs, and click **OK**.

Step 12 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 15 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 13 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.269 ALM-33006 Failure Rate of Containers Calls Exceeds the Threshold

Alarm Description

The system checks the failure rate of service calls every 5 minutes and compares the rate with the threshold. This alarm is generated when the failure rate exceeds the threshold.

This alarm is automatically cleared when the failure rate is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
33006	Major	Quality of service	Tenant plane	Containers	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	RegionId	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	ApplicationServiceName	Specifies the name of the application for which the alarm is generated.
	Version	Specifies the version for which the alarm is generated.
	Method	Specifies the method for generating the alarm.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	Side	Specifies the side where the alarm is generated.
	IP	Specifies the IP address for which the alarm is generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger condition	Specifies the threshold for triggering the alarm.

Impact on the System

If the failure rate is too high, the application service fails to be called for many times within 5 minutes. As a result, the service calls be slow or fail.

Possible Causes

- A timeout occurs due to a long network latency.
- The service volume is too large, and the number of concurrent requests exceeds the upper limit.
- The service code is incorrect.

Handling Procedure

Check whether the network latency is too long.

Step 1 Check whether the service for which the alarm is generated is a provider based on the IP address.

- If yes, go to **Step 9**.
- If no, go to **Step 2**.

Step 2 On FusionInsight Manager, choose **Cluster** > **Services** > **Containers**, and click the **SGP Management** tab.

Step 3 Choose **App Service List** and click the link of the service for which the alarm is generated to access the service status page.

Step 4 View the processing time of the service consumer and check whether it is too long.

- If yes, go to **Step 5**.
- If no, go to **Step 9**.

Step 5 View the processing time of the service provider and compare it with that of the consumer to check whether the difference is large.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If yes, check the network configuration, reduce the network latency, and go to **Step 6**.
- If no, go to **Step 7**.

Step 6 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Step 7 Check whether the processing time of user's upper-layer service logic code is too long.

- If yes, optimize the upper-layer service logic code and execute **Step 8**.
- If no, go to **Step 9**.

Step 8 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Check whether the service volume is too large and the number of concurrent requests exceeds the upper limit.

Step 9 On FusionInsight Manager, choose **Cluster** > **Services** > **Containers**, and click the **SGP Management** tab.

Step 10 Click the name of the service for which the alarm is generated to access its **State** page.

Step 11 Check whether the number of concurrent requests exceeds the upper limit.

- If yes, go to **Step 12**.
- If no, go to **Step 14**.

Step 12 Choose **Cluster** > **Services** > **Containers**, and click the **Business Manager** tab. Select the BLU that carries services. On the page that is displayed, click the **BLU Instance** tab and click **Add Instance** to add a BLU instance for the service provider.

Step 13 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 14**.

Check whether the service code is correct.

Step 14 Check whether the upper-layer service code is incorrect.

- If yes, correct the service code and go to **Step 15**.
- If no, go to **Step 16**.

Step 15 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 16**.

Collect fault information.

Step 16 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 17 Expand the **Service** drop-down list and select **Containers**.

Step 18 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the hosts to which the role belongs, and click **OK**.

Step 19 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 20 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 20 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.270 ALM-33007 ALB TPS of Containers Exceeds the Threshold

Alarm Description

This alarm is generated when the ALB TPS exceeds the threshold (**tps.threshold**) set by the cluster administrator in ALB configuration file **alb.properties**.

This alarm is automatically cleared when the ALB TPS is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
33007	Warning	Quality of service	Tenant plane	Containers	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.

Type	Parameter	Description
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	HostName	Specifies the name of the host accommodating the ALB instance for which the alarm is generated.
	Container_ID	Identifies the container accommodating the ALB instance for which the alarm is generated.
	BLU_ID	Identifies the BLU of the ALB instance for which the alarm is generated.
	BLU_Version	Specifies the BLU version of the ALB instance for which the alarm is generated.
	ServerAddress	Specifies the external socket address of the ALB instance for which the alarm is generated.
	TPS_Threshold	Specifies the TPS alarm threshold configured by the administrator.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

ALB request forwarding is slow, and service calls are responded slowly.

Possible Causes

- If the number of requests forwarded by each ALB instance is relatively even, ALB instances may be not enough for external requests.

- If the number of requests forwarded by each ALB instance differs greatly, the TPS of some ALB instances may exceed the threshold.

Handling Procedure

Check whether ALB instances are not enough for external requests if the number of requests forwarded by each ALB instance is relatively even.

Step 1 Check whether the number of requests forwarded to each ALB instance is even based on how external messages are connected to the cluster.

For example, when a forwarder is used to send messages to ALB instances, check the number of messages forwarded by the forwarder to each socket address (one socket address corresponds to one ALB instance).

- If yes, go to **Step 2**.
- If no, go to **Step 6**.

Step 2 Log in to FusionInsight Manager, choose **Cluster** > **Services** > **Containers**, and click the **Business Manager** tab.

Step 3 Choose ALB in the navigation pane and click the ALB name. On the page that is displayed, click **BLU Instance** and check whether there are only a few ALB instances.

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 Click **Add Instance**, select the location of new instance, and click **OK**.

Step 5 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Check whether the TPS of some ALB instances exceeds the threshold if the number of requests forwarded by each ALB instance differs greatly.

Step 6 Resolve this problem based on the actual condition because the policy cannot be modified in the cluster. For example, adjust the forwarding policy of the forwarder to decrease requests sent to overloaded ALB instances (especially those that have received alarms).

Step 7 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Collect fault information.

Step 8 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 9 Expand the **Service** drop-down list and select **Containers**.

Step 10 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the hosts to which the role belongs, and click **OK**.

Step 11 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.271 ALM-33008 Average Latency of Containers Exceeds the Threshold

Alarm Description

The system checks the average latency of service calls every 5 minutes and compares the latency with the threshold. This alarm is generated when the average latency exceeds the threshold.

This alarm is automatically cleared when the average latency is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
33008	Warning	Quality of service	Tenant plane	Containers	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	RegionId	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.

Type	Parameter	Description
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	ApplicationServiceName	Specifies the name of the application for which the alarm is generated.
	Version	Specifies the version for which the alarm is generated.
	Method	Specifies the method for generating the alarm.
	Side	Specifies the side where the alarm is generated.
	IP	Specifies the IP address for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

The BLU service processing becomes slow. As a result, user requests may be stacked, and even upper-layer services may be blocked or unavailable.

Possible Causes

- It takes a long time to process the upper-layer service logic code.
- The service volume is too large.
- The service code is incorrect.

Handling Procedure

Check whether the processing time of the upper-layer service logic code is too long.

Step 1 Check whether the service for which the alarm is generated is a provider based on the IP address.

- If yes, go to **Step 9**.
- If no, go to **Step 2**.

Step 2 On FusionInsight Manager, choose **Cluster** > **Services** > **Containers**, and click the **SGP Management** tab.

Step 3 Choose **App Service List** and click the link of the service for which the alarm is generated to access the service status page.

Step 4 View the processing time of the service consumer and check whether it is too long.

- If yes, go to **Step 5**.
- If no, go to **Step 9**.

Step 5 View the processing time of the service provider and compare it with that of the consumer to check whether the difference is large.

- If yes, check the network configuration, reduce the network latency, and go to **Step 6**.
- If no, go to **Step 7**.

Step 6 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Step 7 Check whether the processing time of user's upper-layer service logic code is too long.

- If yes, optimize the upper-layer service logic code and execute **Step 8**.
- If no, go to **Step 9**.

Step 8 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Check whether the service volume is too large.

Step 9 On FusionInsight Manager, choose **Cluster** > **Services** > **Containers**, and click the **SGP Management** tab.

Step 10 Click the name of the service for which the alarm is generated to access its **State** page.

Step 11 Check whether the number of concurrent requests exceeds the upper limit.

- If yes, go to **Step 12**.
- If no, go to **Step 14**.

Step 12 On FusionInsight Manager, choose **Cluster** > **Services** > **Containers**, and click the **Business Manager** tab. Select the BLU that carries services. On the page that is

displayed, click the **BLU Instance** tab and click **Add Instance** to add a BLU instance for the service provider.

Step 13 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 14**.

Check whether the service code is correct.

Step 14 Check whether the upper-layer service code is incorrect.

- If yes, correct the service code and go to **Step 15**.
- If no, go to **Step 16**.

Step 15 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 16**.

Change the alarm threshold.

Step 16 On FusionInsight Manager, choose **O&M** > **Alarm** > **Thresholds**. On the **Thresholds** page, click the name of the desired cluster, choose **Containers** > **Other** > **Application Service Average Elapse Statistics (SGP)**, and change the alarm threshold based on the actual average latency.

Step 17 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 18**.

Collect fault information.

Step 18 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 19 Expand the **Service** drop-down list and select **Containers**.

Step 20 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the hosts to which the role belongs, and click **OK**.

Step 21 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 22 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.272 ALM-33009 Containers Heap Memory Usage Exceeds the Threshold

Alarm Description

The system checks the heap memory usage of WebContainer instances every 30 seconds. This alarm is generated when the heap memory usage of a WebContainer instance exceeds the threshold (95%).

This alarm is automatically cleared when the heap memory usage is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
33009	Minor	Environment	Tenant plane	Containers	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold for triggering the alarm.

Impact on the System

If the heap memory of Containers is insufficient, memory overflow may occur. As a result, the container instance and the BLU deployed in the container are abnormal, and the alarm "The health status of the BLU instance of the Containers service is abnormal" is reported. This alarm is generated when some BLU instances of a BLU role are unhealthy. Service functions are not affected, but the service processing of the BLU may become slow. If all BLU instances of the BLU role are unhealthy, the service corresponding to the BLU cannot provide services.

Possible Causes

- The alarm threshold or alarm trigger count is improperly configured.
- The WebContainer heap memory is insufficient.

Handling Procedure

Check whether the alarm threshold or alarm trigger count is properly configured.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**, click ⌄ in the row that contains the alarm, and view the host name and role of the instance for which the alarm is generated in **Location**.

Step 2 Choose **O&M** > **Alarm** > **Thresholds**. On the **Thresholds** page, click the name of the desired cluster, choose **Containers** > **Other** > **Heap Mem Usage (WebContainer_*N*)**, and check whether the trigger count and alarm threshold are set properly for the role for which the alarm is generated.

- If yes, go to **Step 5**.
- If no, go to **Step 3**.

Step 3 Change the trigger count and alarm threshold based on the actual heap memory usage, and apply the changes.

Step 4 Wait 2 minutes and check whether the alarm is cleared.

- If yes, no further action is required.

- If no, go to **Step 5**.

Check the heap memory usage of the WebContainer.

Step 5 Choose **Cluster** > **Services** > **Containers** > **Configurations** > **All Configurations**, choose **WebContainer_*N*(Role)** > **Default** of the role for which the alarm is generated, increase the value of **GC_OPTS** as required, click **Save**. Then click **OK** and restart the Containers service.

NOTE

Change the values of **-Xms** and **-Xmx** to twice the current heap memory usage (or adjust the values based on site requirements). The values cannot exceed the remaining memory of the node.

Step 6 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect fault information.

Step 7 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 8 Expand the **Service** drop-down list and select **Containers**.

Step 9 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the hosts to which the role belongs, and click **OK**.

Step 10 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 11 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.273 ALM-33010 Containers Non-Heap Memory Usage Exceeds the Threshold

Alarm Description

The system checks the non-heap memory usage of WebContainer instances every 30 seconds. This alarm is generated when the non-heap memory usage of a WebContainer instance exceeds the threshold (75%).

This alarm is automatically cleared when the non-heap memory usage is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
33010	Minor	Environment	Tenant plane	Containers	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

If the non-heap memory of Containers is insufficient, memory overflow may occur. As a result, the container instance and the BLU deployed in the container are abnormal, and the alarm "The health status of the BLU instance of the Containers service is abnormal" is reported. This alarm is generated when some BLU instances of a BLU role are unhealthy. Service functions are not affected, but the service processing of the BLU may become slow. If all BLU instances of the BLU role are unhealthy, the service corresponding to the BLU cannot provide services.

Possible Causes

- The alarm threshold or alarm trigger count is improperly configured.
- The memory allocated to the WebContainer instance is improper, or the memory of the BLU deployed on the node leaks. As a result, the usage exceeds the threshold.

Handling Procedure

Check whether the alarm threshold or alarm trigger count is properly configured.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**, click ⌄ in the row that contains the alarm, and view the host name and role of the instance for which the alarm is generated in **Location**.

Step 2 Choose **O&M** > **Alarm** > **Thresholds**. On the **Thresholds** page, click the name of the desired cluster, choose **Containers** > **Other** > **Non_Heap Mem Usage (WebContainer_*N*)**, and check whether the trigger count and alarm threshold are set properly for the role for which the alarm is generated.

- If yes, go to **Step 5**.
- If no, go to **Step 3**.

Step 3 Change the trigger count and alarm threshold based on the actual non-heap memory usage, and apply the changes.

Step 4 Wait 2 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check the non-heap memory usage of the WebContainer.

Step 5 Choose **Cluster** > **Services** > **Containers** > **Configurations** > **All Configurations**, choose **WebContainer_*N*(Role)** > **Default** of the role for which the alarm is generated, and check whether the **GC_OPTS** value is set properly.

- If yes, go to **Step 6**.
- If no, go to **Step 7**.

Step 6 Click the **Dashboard** tab. In the upper right corner, click **More** and select **Restart Service**. In the dialog box that is displayed, enter the password to restart the Containers service. Then check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect fault information.

Step 7 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 8 Expand the **Service** drop-down list and select **Containers**.

Step 9 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the hosts to which the role belongs, and click **OK**.

Step 10 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 11 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.274 ALM-33011 Containers Metaspace Usage Exceeds the Threshold

Alarm Description

The system checks the metaspace memory usage of WebContainer instances every 30 seconds. This alarm is generated when the metaspace memory usage of a WebContainer instance exceeds the threshold (75%).

This alarm is automatically cleared when the metaspace memory usage is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
33011	Minor	Environment	Tenant plane	Containers	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	RegionId	Specifies the region where the alarm was generated.

Type	Parameter	Description
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

If the metaspace memory of Containers is insufficient, memory overflow may occur. As a result, the container instance and the BLU deployed in the container are abnormal, and the alarm "The health status of the BLU instance of the Containers service is abnormal" is reported. This alarm is generated when some BLU instances of a BLU role are unhealthy. Service functions are not affected, but the service processing of the BLU may become slow. If all BLU instances of the BLU role are unhealthy, the service corresponding to the BLU cannot provide services.

Possible Causes

- The alarm threshold or alarm trigger count is improperly configured.
- The memory allocated to the WebContainer instance is improper, or the memory of the BLU deployed on the node leaks. As a result, the usage exceeds the threshold.

Handling Procedure

Check whether the alarm threshold or alarm trigger count is properly configured.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**, click ⌄ in the row that contains the alarm, and view the host name and role of the instance for which the alarm is generated in **Location**.

Step 2 Choose **O&M** > **Alarm** > **Thresholds**. On the **Thresholds** page, click the name of the desired cluster, choose **Containers** > **Other** > **MetaSpace Usage (WebContainer_*N*)**, and check whether the trigger count and alarm threshold are set properly for the role for which the alarm is generated.

- If yes, go to **Step 5**.
- If no, go to **Step 3**.

Step 3 Change the trigger count and alarm threshold based on the actual metaspace usage, and apply the changes.

Step 4 Wait 2 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check the WebContainer metaspace usage.

Step 5 Choose **Cluster** > **Services** > **Containers** > **Configurations** > **All Configurations**, choose **WebContainer_*N*(Role)** > **Default** of the role for which the alarm is generated, and check whether the **GC_OPTS** value is set properly.

- If yes, go to **Step 6**.
- If no, go to **Step 7**.

Step 6 Click the **Dashboard** tab. In the upper right corner, click **More** and select **Restart Service**. In the dialog box that is displayed, enter the password to restart the Containers service. Then check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect fault information.

Step 7 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 8 Expand the **Service** drop-down list and select **Containers**.

Step 9 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the hosts to which the role belongs, and click **OK**.

Step 10 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 11 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.275 ALM-33012 Containers' ZooKeeper Client Is Disconnected

Alarm Description

Multiple modules in the FusionInsight RTD cluster contain the ZooKeeper client. This alarm is generated when the ZooKeeper client is disconnected from the ZooKeeper server.

This alarm is automatically cleared when the connection is restored.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
33012	Minor	Communications	Tenant plane	Containers	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	RegionId	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.

Type	Parameter	Description
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	RoleName	Specifies the role for which the alarm is generated.
	HostName	Specifies the host for which the alarm was generated.
	ClientLocation	Specifies the location of the ZooKeeper client.
	ServerAddress	Specifies the ZooKeeper server address.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

If the ZooKeeper client is disconnected, ZooKeeper-dependent functions in the FusionInsight RTD cluster may be unavailable.

Possible Causes

- ZooKeeper is faulty.
- The ZooKeeper client fails to be connected due to a network fault.

Handling Procedure

Check whether ZooKeeper is faulty.

Step 1 On FusionInsight Manager, choose **Cluster** > **Services** > **ZooKeeper** and check whether the ZooKeeper service is running properly.

- If yes, go to **Step 3**.
- If no, go to **Step 2**.

Step 2 Click **More** and select **Restart Service**. In the dialog box that is displayed, enter the password to restart ZooKeeper. After the restart is successful, check whether the alarm is cleared.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If yes, no further action is required.
- If no, go to **Step 3**.

Check whether the ZooKeeper client fails to be connected due to a network fault.

Step 3 Check whether the network between the client and the server is normal and the time is consistent based on the client location and server address in the alarm information.

- If yes, go to **Step 5**.
- If no, go to **Step 4**.

Step 4 Restore the network and adjust the time to ensure that the time difference between the client and server is less than 5 minutes (ignore the time difference for a normal cluster). Wait 5 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Collect fault information.

Step 5 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 6 Expand the **Service** drop-down list and select **Containers**.

Step 7 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the hosts to which the role belongs, and click **OK**.

Step 8 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.276 ALM-35000 FTP-Server Service Unavailable

Alarm Description

The alarm module detects the FTP-Server service status every 180 seconds. This alarm is generated when the alarm module detects that the FTP-Server service is abnormal.

This alarm is cleared when the FTP-Server service recovers and the alarm handling is complete.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
35000	Critical	Quality of service	Tenant plane	FTP-Server	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

When the FTP-Server service is unavailable, files cannot be uploaded or downloaded from the HDFS through FTP.

Possible Causes

- The HDFS service is unavailable.
- The LdapServer service is unavailable.

Handling Procedure

Check the HDFS service status.

Step 1 On FusionInsight Manager, check whether **HDFS Service Unavailable** is generated in the alarm list.

- If yes, clear the alarm by following the steps provided in **ALM-14000 HDFS Service Unavailable**.
- If no, go to **Step 2**.

Check the LdapServer service status.

Step 2 On FusionInsight Manager, check whether **LdapServer Service Unavailable** is generated in the alarm list.

- If yes, clear the alarm by following the steps provided in **ALM-25000 LdapServer Service Unavailable**.
- If no, go to **Step 3**.

Check whether the HDFS/LdapServer service is stopped.

Step 3 In the service list on FusionInsight Manager, check whether the HDFS/LdapServer service is stopped.

- If yes, start the HDFS/LdapServer service.
- If no, go to **Step 4**.

Collect fault information.

Step 4 On FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 5 Select **FTP-Server** in the required cluster from the **Service** drop-down list.

Step 6 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 7 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Related Information

None.

1.3.277 ALM-35001 FTP-Server Heap Memory Usage Exceeds the Threshold

Alarm Description

The system checks the heap memory usage of the FTP-Server service every 60 seconds. The alarm is generated when the heap memory usage of a FTP-Server instance exceeds the threshold for 10 consecutive times. The alarm is cleared when the heap memory usage is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
35001	Critical (default threshold: 95% of the maximum memory) Major (default threshold: 90% of the maximum memory)	Quality of service	Tenant plane	FTP-Server	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

Heap memory overflow may cause service breakdown. As a result, files in HDFS cannot be uploaded or downloaded through FTP.

Possible Causes

The heap memory of the FTP-Server instance is overused or the heap memory is inappropriately allocated.

Handling Procedure

Check heap memory usage.

Step 1 On the FusionInsight Manager portal, choose **O&M** > **Alarm** > **Alarms** > **FTP-Server Heap Memory Usage Exceeds the Threshold** > **Location**. Check the host name of the instance involved in this alarm.

Step 2 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services** > **FTP-Server** > **Instance**. Click the instance for which the alarm is generated to go to the page for the instance. Click the drop-down list in the upper right corner of the chart area, choose **Customize** > **Process** > **FTP-Server Heap Memory Resource Percentage**, and click **OK**.

Step 3 Check whether the used heap memory of FTP-Server reaches the threshold (the default value is 95% of the maximum heap memory) specified for FTP-Server.

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* > **Services** > **FTP-Server** > **Configurations**. Click **All Configurations**, and choose **FTP-Server** > **System**. Increase the value of **FTPSERVER_HEAPSIZE** as required, and click **Save**. Click **OK**.

NOTE

- If this alarm is generated, the heap memory configured for the current FTP-Server instance is insufficient for data transmission. You are advised to open the FTP-Server heap memory resource status monitoring chart (see **Step 2**), and observe the change trend of the heap memory used by FTP-Server in the monitoring chart. Then change the value of **FTPSERVER_HEAPSIZE** to twice the current heap memory usage or to another value to meet site requirements.
- The heap memory cannot exceed the remaining memory of the node where the current instance is located.
- It is recommended that the value of **FTPSERVER_HEAPSIZE** be the same as that of **-Xmx** in **GC_OPTS**. In addition, you need to change the values of the two parameters at the same time and ensure that the value of **-Xms** is smaller than or equal to that of **FTPSERVER_HEAPSIZE**.

Step 5 Restart the affected services or instances and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On the FusionInsight Manager portal, choose **O&M** > **Log** > **Download**.

Step 7 Select **FTP-Server** in the required cluster from the **Service** drop-down list.

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact the technical support and send the collected fault logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.278 ALM-35002 FTP-Server Direct Buffer Usage Exceeds the Threshold

Alarm Description

The system checks the direct memory usage of the FTP-Server service every 30 seconds. The alarm is generated when the direct memory usage of a FTP-Server instance exceeds the threshold for 5 consecutive times. The alarm is cleared when the direct memory usage of FTP-Server is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
35002	Critical (default threshold: 95% of the maximum memory) Major (default threshold: 80% of the maximum memory)	Quality of service	Tenant plane	FTP-Server	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

Direct memory overflow may cause the service to break down and files in the HDFS cannot be uploaded or downloaded through FTP.

Possible Causes

The direct memory of the FTP-Server instance is overused or the direct memory is inappropriately allocated.

Handling Procedure

Check direct memory usage.

Step 1 On the FusionInsight Manager portal, choose **O&M** > **Alarm** > **Alarms** > **FTP-Server Direct Memory Usage Exceeds the Threshold** > **Location**. Check the host name of the instance involved in this alarm.

Step 2 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services** > **FTP-Server** > **Instance**. Click the instance for which the alarm is generated to go to the page for the instance. Click the drop-down list in the upper right corner of the chart area, choose **Customize** > **Process** > **FTP-Server Direct Buffer Usage Statistics**, and click **OK**.

Step 3 Check whether the used direct memory of FTP-Server reaches the threshold (the default value is 80% of the maximum direct memory) specified for FTP-Server.

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* > **Services** > **FTP-Server** > **Configurations**. Click **All Configurations**, and choose **FTP-Server** > **System**. Increase the value of **-XX:MaxDirectMemorySize** in **GC_OPTS** as required, and click **Save**. Click **OK**.

NOTE

If this alarm is generated, the direct memory configured for the current FTP-Server instance is insufficient for the service scenario. You are advised to open the FTP-Server direct memory resource status monitoring chart (see **Step 2**), and observe the change trend of the direct memory used by FTP-Server in the monitoring chart. Then change the value of **-XX:MaxDirectMemorySize** to twice the current direct memory usage or to another value to meet site requirements.

Step 5 Restart the affected services or instances and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On the FusionInsight Manager portal, choose **O&M** > **Log** > **Download**.

Step 7 Select **FTP-Server** in the required cluster from the **Service** drop-down list.

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact the technical support and send the collected fault logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.279 ALM-35003 FTP-Server NonHeap Memory Usage Exceeds the Threshold

Alarm Description

The system checks the non heap memory usage of the FTP-Server service every 30 seconds. The alarm is generated when the non heap memory usage of a FTP-Server instance exceeds the threshold for 5 consecutive times. The alarm is cleared when the non heap memory usage is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
35003	Critical (default threshold: 95% of the maximum memory) Major (default threshold: 80% of the maximum memory)	Quality of service	Tenant plane	FTP-Server	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

NonHeap memory overflow may cause the service to break down and files in HDFS cannot be uploaded or downloaded through FTP.

Possible Causes

The non heap memory of the FTP-Server instance is overused or the non heap memory is inappropriately allocated.

Handling Procedure

Check non heap memory usage.

Step 1 On the FusionInsight Manager portal, choose **O&M** > **Alarm** > **Alarms** > **FTP-Server Non Heap Memory Usage Exceeds the Threshold** > **Location**. Check the host name of the instance involved in this alarm.

Step 2 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services** > **FTP-Server** > **Instance**. Click the instance for which the alarm is generated to go to the page for the instance. Click the drop-down list in the upper right corner of the chart area, choose **Customize** > **Process** > **FTP-Server Non Heap Memory Resource Percentage**, and click **OK.**

Step 3 Check whether the used non heap memory of FTP-Server reaches the threshold (the default value is 80% of the maximum non heap memory) specified for FTP-Server.

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On the FusionInsight Manager portal, choose **Cluster >** *Name of the desired cluster* > **Services** > **FTP-Server** > **Configurations**. Click **All Configurations**, and choose **FTP-Server** > **System**. Increase the value of **-XX: MaxPermSize** in **GC_OPTS** as required, and click **Save**. Click **OK**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

NOTE

If this alarm is generated, the non-heap memory configured for the current FTP-Server instance is insufficient for the service scenario. You are advised to open the FTP-Server non-heap memory resource status monitoring chart (see **Step 2**), and observe the change trend of the non-heap memory used by FTP-Server in the monitoring chart. Then change the value of **-XX:MaxPermSize** to twice the current non-heap memory usage or to another value to meet site requirements.

Step 5 Restart the affected services or instances and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On the FusionInsight Manager portal, choose **O&M** > **Log** > **Download**.

Step 7 Select **FTP-Server** in the required cluster from the **Service** drop-down list.

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact the technical support and send the collected fault logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.280 ALM-35004 FTP-Server Garbage Collection (GC) Time Exceeds the Threshold

Alarm Description

The system checks GC time of the FTP-Server process every 60 seconds. The alarm is generated when GC time of the FTP-Server process exceeds the threshold for 5 consecutive times. The alarm is cleared when GC time is less than the threshold.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
35004	Critical (default threshold: 20000ms) Major (default threshold: 12000ms)	Quality of service	Tenant plane	FTP-Server	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

The efficiency of accessing, uploading, and downloading FTP files is low.

Possible Causes

The heap memory of the FTP-Server instance is overused or the heap memory is inappropriately allocated.

Handling Procedure

Check GC time.

Step 1 On the FusionInsight Manager portal, choose **O&M** > **Alarm** > **Alarms** > **FTP-Server Garbage Collection (GC) Time Exceeds the Threshold** > **Location**. Check the host name of the instance involved in this alarm.

Step 2 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services** > **FTP-Server** > **Instance**. Click the instance for which the alarm is generated to go to the page for the instance. Click the drop-down list in the upper right corner of the chart area, choose **Customize** > **Process** > **Garbage Collection (GC) Duration of FTP-Server**, and click **OK.**

Step 3 Check whether GC time of the FTP-Server process every second exceeds the threshold (default value: **12 seconds**).

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services** > **FTP-Server** > **Configurations**. Click **All Configurations**, and choose **FTP-Server** > **System**. Increase the value of **-Xmx** in **GC_OPTS** as required, and click **Save**. Click **OK**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

NOTE

- If this alarm is generated, the heap memory configured for the current FTP-Server instance is insufficient for data transmission. You are advised to open the FTP-Server heap memory resource status monitoring chart (see **Step 2**), and observe the change trend of the heap memory used by FTP-Server in the monitoring chart. Then change the value of **-Xmx** to twice the current heap memory usage or to another value to meet site requirements.
- You are advised to set **-Xms** and **-Xmx** to the same value to prevent adverse impact on performance when JVM dynamically adjusts the heap memory size.
- You are advised to set **-Xmx** and **FTPSERVER_HEAPSIZE** to the same value and change the values of the parameters at the same time.

Step 5 Restart the affected services or instances and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On the FusionInsight Manager portal, choose **O&M** > **Log** > **Download**.

Step 7 Select **FTP-Server** in the required cluster from the **Service** drop-down list.

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact the technical support and send the collected fault logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.281 ALM-38000 Kafka Service Unavailable

Alarm Description

The system checks the Kafka service status every 30 seconds. This alarm is generated when the Kafka service is unavailable.

This alarm is cleared when the Kafka service recovers.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
38000	Critical	Quality of service	Tenant plane	Kafka	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

The cluster cannot provide the Kafka service, and users cannot perform new Kafka tasks.

Possible Causes

- The KrbServer service is abnormal.(Skip this step if the normal mode is used.)

- The ZooKeeper service is abnormal or does not respond.
- The Broker instance in the Kafka cluster are abnormal.

Handling Procedure

Check the status of the KrbServer service. (Skip this step if the normal mode is used.)

Step 1 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services > KrbServer**.

Step 2 Check whether the running status of the KrbServer service is **Normal**.

- If yes, go to **Step 5**.
- If no, go to **Step 3**.

Step 3 Rectify the fault by following the steps provided in **ALM-25500 KrbServer Service Unavailable**.

Step 4 Perform **Step 2** again.

Check the status of the ZooKeeper cluster.

Step 5 Check whether the running status of the ZooKeeper service is **Normal**.

- If yes, go to **Step 8**.
- If no, go to **Step 6**.

Step 6 If ZooKeeper service is stopped, start it, else rectify the fault by following the steps provided in **ALM-13000 ZooKeeper Service Unavailable**.

Step 7 Perform **Step 5** again.

Check the Broker status.

Step 8 Choose **Cluster** > *Name of the desired cluster* > **Services** > **Kafka** > **Instance** to go to the Kafka instances page.

Step 9 Check whether all instances in **Roles** are running properly.

- If yes, go to **Step 11**.
- If no, go to **Step 10**.

Step 10 Select all Broker instances, choose **More** > **Restart Instance**, and check whether the instances restart successfully.

- If yes, go to **Step 11**.
- If no, go to **Step 13**.

Step 11 Choose **Cluster** > *Name of the desired cluster* > **Services** > **Kafka** to check whether the running status is **Normal**.

- If yes, go to **Step 12**.
- If no, go to **Step 13**.

Step 12 Wait for 30 seconds and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 13**.

Collecting Fault Information

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 13 On the FusionInsight Manager portal, choose **O&M** > **Log** > **Download**.

Step 14 Select **Kafka** in the required cluster from the **Service** drop-down list.

Step 15 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 16 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.282 ALM-38001 Insufficient Kafka Disk Space

Alarm Description

The system checks the Kafka disk usage every 60 seconds and compares the actual disk usage with the threshold. The disk usage has a default threshold. This alarm is generated if the disk usage exceeds the threshold.

To change the threshold, choose **O&M** > **Alarm** > **Thresholds**. In the service list, choose **Kafka** > **Disk** > **Broker Disk Usage (Broker)**.

If the **Trigger Count** is **1**, this alarm is cleared when the usage of the Kafka disk is less than or equal to the threshold. If the **Trigger Count** is greater than **1**, this alarm is cleared when the disk usage is less than or equal to 80% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
38001	Major (default value: 85%) Critical (default value: 90%)	Quality of service	Tenant plane	Kafka	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	PartitionName	Specifies the disk partition for which the alarm is generated.
	Alarm Severity	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

Kafka data write operations fail.

Possible Causes

- The Kafka disk configurations (such as disk count and disk size) are insufficient for the data volume.
- The data retention period is long and historical data occupies large space.
- Services are improperly planned. As a result, data is unevenly distributed and some disks are full.

Handling Procedure

Check the disk configuration of Kafka data.

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Alarms**.

Step 2 In the alarm list, click the alarm and obtain the host name from the **Location** area.

Step 3 Choose **Cluster** > *Name of the desired cluster* > **Hosts**.

Step 4 On the **Hosts** page, click the host name obtained in **Step 2**.

Step 5 Check whether the **Disk** area contains the disk partition name in the alarm.

- If yes, go to **Step 6**.
- If no, manually clear the alarm and no further action is required.

Step 6 In the **Disk** area, check whether the usage of the alarmed partition has reached 100%.

- If yes, handle the alarm by following the instructions in **Related Information**.
- If no, go to **Step 7**.

Check the Kafka data storage duration.

Step 7 Choose **Cluster** > *Name of the desired cluster* > **Services** > **Kafka** > **Configurations** > **All Configurations**.

Step 8 Check whether the value of **disk.adapter.enable** is **true**.

- If yes, go to **Step 10**.
- If no, go to **Step 9**.

Step 9 Set **disk.adapter.enable** to **true**. Check whether the value of **adapter.topic.min.retention.hours** is properly set.

- If yes, go to **Step 10**.
- If no, adjust the data retention period based on service requirements.

NOTICE

If the disk adaptation function is enabled, historical data of topics may be deleted. If the retention period of some topics cannot be adjusted, click **All Configurations** and add the topics to the value of the **disk.adapter.topic.blacklist** parameter.

Step 10 Wait for 10 minutes and check whether the usage of the faulty disk decreases.

- If yes, wait until the alarm is cleared.

- If no, go to **Step 11**.

Check the Kafka data plan.

Step 11 In the **Instance** area, click **Broker**. Click the drop-down menu in the **Chart** area and choose **Customize** to customize monitoring items.

Step 12 In the displayed dialog box, choose **Disk**, select **Broker Disk Usage**, and click **OK**.

The Kafka disk usage information is displayed.

Step 13 View the information in **Step 12** to check whether there is only the disk partition for which the alarm is generated in **Step 2**.

- If yes, go to **Step 14**.
- If no, go to **Step 15**.

Step 14 Perform disk planning and mount a new disk again. Go to the **Instance Configurations** page of the node for which the alarm is generated, modify **log.dirs**, add other disk directories, and restart the Kafka instance by referring to "Kafka Specifications" in MapReduce Service (MRS) 3.3.1-LTS User Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Usage Guide (for Huawei Cloud Stack 8.3.1).

Step 15 Determine whether to shorten the data retention time configured on Kafka based on service requirements and service traffic.

- If yes, go to **Step 16**.
- If the alarm fails to be cleared, go to **Step 17**.

Step 16 Log in to FusionInsight Manager, select **Cluster** > *Name of the desired cluster* > **Services** > **Kafka** > **Configurations**, and click **All Configurations**. In the search box on the right, enter **log.retention.hours**. The value of the parameter indicates the default data retention time of the topic. You can change the value to a smaller one.

NOTE

- For a topic whose data retention time is configured alone, the modification of the data retention time on the Kafka service configuration page does not take effect.
- To modify the data retention time for a topic, use the Kafka client command-line interface (CLI).

  Example: **kafka-configs.sh --bootstrap-server** *<IP address of the Kafka cluster:21007>* **--command-config ../config/client.properties --alter --topic** *Topic name* **--add-config retention.ms=***Storage duration*

Step 17 Check whether partitions are properly configured for topics. For example, if the number of partitions for a topic with a large data volume is smaller than the number of disks, data may be unevenly distributed to the disks and the usage of some disks will reach the upper limit.

NOTE

If you do not know which topics have a large amount of service data, perform the following steps:

1. Log in to an instance node based on the host node information obtained in **2**.
2. Go to the data directory (directory specified by **log.dirs** before the modification in **14**).
3. Check whether there is a topic with partition that uses large disk space.

- If yes, go to **Step 18**.
- If no, go to **Step 19**.

Step 18 On the Kafka client, add partitions to the topics.

kafka-topics.sh --bootstrap-server *<IP address of the Kafka cluster:21007>* **--command-config ../config/client.properties --alter --topic** *Topic name* **--partitions=***Number of new partitions*

NOTE

- You are advised to set the new number of partitions to a multiple of the number of Kafka data disks.
- The step may not quickly clear the alarm, and you need to modify the data retention time in **Step 11** to gradually balance data allocation.

Step 19 Determine whether to perform capacity expansion.

NOTE

You are advised to perform capacity expansion for Kafka when the current disk usage exceeds 80%. For details about scale-out precautions and procedures, see MapReduce Service (MRS) 3.3.1-LTS Physical Machine Cluster Capacity Expansion Guide (for Huawei Cloud Stack 8.3.1).

- If yes, go to **Step 20**.
- If no, go to **Step 21**.

Step 20 Expand the disk capacity and check whether the alarm is cleared after capacity expansion.

- If yes, no further action is required.
- If no, go to **Step 22**.

Step 21 Check whether the alarm is cleared.

- If yes, no further action is required.
- If yes, go to **Step 22**.

Collect fault information.

Step 22 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 23 Expand the **Service** drop-down list, and select **Kafka** for the target cluster.

Step 24 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 25 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

Step 1 Log in to FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Kafka** > **Instances**, stop the Broker instance in the **Restoring** state, and record the management IP address of the node where the instance is deployed and the corresponding **broker.id**. You can click the role name to view the value, on the **Configurations** page, select **All Configurations** and search for the **broker.id** parameter.

Step 2 Log in to the management IP address recorded as the **root** user and run the **df -lh** command to view the mount directory whose disk usage is 100%, for example, **$ {BIGDATA_DATA_HOME}/kafka/data1**.

Step 3 Go to the directory, run the **du -sh *** command to view the size of each file in the directory. Check whether there are files in addition to the files in the **kafka-logs** directory, and determine whether these files can be deleted or migrated.

- If yes, delete or migrate related data and go to **Step 8**.
- If no, go to **Step 4**.

Step 4 Go to the **kafka-logs** directory, run the **du -sh *** command, select a partition folder to be moved. The naming rule is **Topic name-Partition ID**. Record the topic and partition.

Step 5 Modify the **recovery-point-offset-checkpoint** and **replication-offset-checkpoint** files in the **kafka-logs** directory in the same way.

1. Decrease the number in the second line in the file. (To remove multiple directories, the number deducted is equal to the number of files to be removed.)
2. Delete the line where the partition to be removed is. (The line is in "*Topic name Partition ID Offset*" format. Save the data before deletion. The content must be added to the file of the same name in the destination directory.)

Step 6 Modify the **recovery-point-offset-checkpoint** and **replication-offset-checkpoint** files in the destination data directory (for example, **${BIGDATA_DATA_HOME}/kafka/data2/kafka-logs**) in the same way.

- Increase the number in the second line in the file. (To move multiple directories, the number added must be equal to the number of files to be moved.)
- Add the partition to the end of the file. (The line structure is "Topic name Partition ID Offset". You can copy the line data saved in **Step 5**.)

Step 7 Move the partition to the destination directory. After the partition is moved, run the **chown omm:wheel -R** *Partition directory* command to modify the directory owner group for the partition.

Step 8 Log in to FusionInsight Manager and choose **Cluster** > *Name of the desired cluster* > **Services** > **Kafka** > **Instances** to start the stopped Broker instance.

Step 9 Wait for 5 to 10 minutes and check whether the health status of the Broker instance is **Good**.

- If yes, rectify the fault by following the handling suggestion of ALM-38001 Insufficient Kafka Disk Capacity.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If no, contact technical support.

----End

1.3.283 ALM-38002 Kafka Heap Memory Usage Exceeds the Threshold

Alarm Description

The system checks the Kafka service status every 30 seconds. The alarm is generated when the heap memory usage of a Kafka instance exceeds the threshold (95% of the maximum memory) for 10 consecutive times.

When the **Trigger Count** is 1, this alarm is cleared when the heap memory usage is less than or equal to the threshold. When the **Trigger Count** is greater than 1, this alarm is cleared when the heap memory usage is less than or equal to 90% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
38002	Major (default value: 90%) Critical (default value: 95%)	Quality of service	Tenant plane	Kafka	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.

Type	Parameter	Description
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

If the available direct memory of the Kafka service is insufficient, a memory overflow occurs and the broker instance breaks down. As a result, the broker cannot provide read and write services properly.

Possible Causes

The heap memory of the Kafka instance is overused or the heap memory is inappropriately allocated.

Handling Procedure

Check heap memory usage.

Step 1 On the FusionInsight Manager portal, choose **O&M** > **Alarm** > **Alarms** > **Kafka Heap Memory Usage Exceeds the Threshold** > **Location**. Check the host name of the instance involved in this alarm.

Step 2 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services** > **Kafka** > **Instance**. Click the instance for which the alarm is generated to go to the page for the instance. Click the drop-down list in the upper

right corner of the chart area, choose **Customize** > **Process** > **Heap Memory Usage of Kafka**, and click **OK**.

Step 3 Check whether the used heap memory of Kafka reaches 95% of the maximum heap memory specified for Kafka.

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Check the heap memory size configured for Kafka.

Step 4 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services** > **Kafka** > **Configurations** > **All Configurations**> **Broker(Role)** > **Environment**. Increase the value of **KAFKA_HEAP_OPTS** by referring to the Note.

NOTE

- It is recommended that **-Xmx** and **-Xms** be set to the same value.
- You are advised to view **Heap Memory Usage of Kafka** by referring to **Step 2**, and set the value of **KAFKA_HEAP_OPTS** to twice the value of **Heap Memory Used by Kafka.**

Step 5 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On the FusionInsight Manager portal, choose **O&M** > **Log** > **Download**.

Step 7 Select **Kafka** in the required cluster from the **Service** drop-down list.

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.284 ALM-38004 Kafka Direct Memory Usage Exceeds the Threshold

Alarm Description

The system checks the direct memory usage of the Kafka service every 30 seconds. This alarm is generated when the direct memory usage of a Kafka instance exceeds the threshold for 10 consecutive times.

When the **Trigger Count** is 1, this alarm is cleared when the direct memory usage is less than or equal to the threshold. When the **Trigger Count** is greater than 1, this alarm is cleared when the direct memory usage is less than or equal to 90% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
38004	Major (default value: 95%) Critical (default value: 100%)	Quality of service	Tenant plane	Kafka	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

If the available direct memory of the Kafka service is insufficient, a memory overflow occurs and the broker instance breaks down. As a result, the broker cannot provide read and write services properly.

Possible Causes

The direct memory of the Kafka instance is overused or the direct memory is inappropriately allocated.

Handling Procedure

Check the direct memory usage.

Step 1 On the FusionInsight Manager portal, choose **O&M** > **Alarm** > **Alarms** > **Kafka Direct Memory Usage Exceeds the Threshold** > **Location** to check the host name of the instance for which the alarm is generated.

Step 2 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services** > **Kafka** > **Instance**. Click the instance for which the alarm is generated to go to the page for the instance. Click the drop-down menu in the Chart area and choose **Customize** > **Process** > **Kafka Direct Memory Usage**, and click **OK**.

Step 3 Check whether the used direct memory of Kafka reaches 80% of the maximum direct memory specified for Kafka.

- If yes, go to **Step 4**.
- If no, go to **Step 7**.

Check the direct memory size configured for the Kafka.

Step 4 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services** > **Kafka** > **Configurations** > **All Configurations** > **Broker(Role)** > **Environment** to increase the value of **-Xmx** configured in the **KAFKA_HEAP_OPTS** parameter by referring to the Note.

NOTE

- It is recommended that **-Xmx** and **-Xms** be set to the same value.
- You are advised to view **Kafka Direct Memory Usage** by referring to **Step 2**, and set the value of **KAFKA_HEAP_OPTS** to twice the value of **Direct Memory Used by Kafka.**

Step 5 Save the configuration and restart the Kafka service.

Step 6 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect fault information.

Step 7 On the FusionInsight Manager portal, choose **O&M** > **Log** > **Download**.

Step 8 Select **Kafka** in the required cluster from the **Service** drop-down list.

Step 9 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.285 ALM-38005 GC Duration of the Broker Process Exceeds the Threshold

Alarm Description

The system checks the garbage collection (GC) duration of the Broker process every 60 seconds. This alarm is generated when the GC duration exceeds the threshold (12 seconds by default) for 3 consecutive times.

When the **Trigger Count** is 1, this alarm is cleared when the GC duration is less than or equal to the threshold. When the **Trigger Count** is greater than 1, this alarm is cleared when the GC duration is less than or equal to 90% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
38005	Major (default value: 10s) Critical (default value: 12s)	Quality of service	Tenant plane	Kafka	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

A long GC duration of the Broker process may fail to provide read and write services.

Possible Causes

The Kafka GC duration of the node is too long or the heap memory is inappropriately allocated. As a result, GCs occur frequently.

Handling Procedure

Check the GC duration.

Step 1 On the FusionInsight Manager portal, choose **O&M** > **Alarm** > **Alarms** > **GC Duration of the Broker Process Exceeds the Threshold** > **Location**. Check the host name of the instance involved in this alarm.

Step 2 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services** > **Kafka** > **Instance**. Click the instance for which the alarm is generated to go to the page for the instance. Click the drop-down list in the upper right corner of the chart area, choose **Customize** > **Process** > **Broker GC Duration per Minute**, and click **OK**.

Step 3 Check whether the GC duration of the Broker process collected every minute exceeds the threshold (12 seconds by default).

- If yes, go to **Step 4**.
- If no, go to **Step 7**.

Check the direct memory size configured for the Kafka.

Step 4 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services** > **Kafka** > **Configurations** > **All Configurations** > **Broker(Role)** > **Environment** to increase the value of **-Xmx** configured in the **KAFKA_HEAP_OPTS** parameter by referring to the Note.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

NOTE

- It is recommended that **-Xmx** and **-Xms** be set to the same value.
- You are advised to set the value of **KAFKA_HEAP_OPTS** to twice the value of **Direct Memory Used by Kafka.**

  On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services** > **Kafka** > **Instance**. Click the instance for which the alarm is generated to go to the page for the instance. Click the drop-down list in the upper right corner of the chart area and choose **Customize** > **Process** > **Kafka Direct Memory Resource Status** to check the value of **Direct Memory Used by Kafka**.

Step 5 Save the configuration and restart the Kafka service.

Step 6 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect fault information.

Step 7 On the FusionInsight Manager portal, choose **O&M** > **Log** > **Download**.

Step 8 Select **Kafka** in the required cluster from the **Service** drop-down list.

Step 9 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.286 ALM-38006 Percentage of Kafka Partitions That Are Not Completely Synchronized Exceeds the Threshold

Alarm Description

The system checks the percentage of Kafka partitions that are not completely synchronized to the total number of partitions every 60 seconds. This alarm is generated when the percentage exceeds the threshold for 3 consecutive times.

When the **Trigger Count** is 1, this alarm is cleared when the percentage is less than or equal to the threshold. When the **Trigger Count** is greater than 1, this alarm is cleared when the percentage is less than or equal to 90% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
38006	Critical (default threshold: 60%) Major (default threshold: 50%)	Quality of service	Tenant plane	Kafka	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

Too many Kafka partitions that are not completely synchronized affect service reliability. In addition, data may be lost when leaders are switched.

Possible Causes

Some nodes where the Broker instance resides are abnormal or stop running. As a result, replicas of some partitions in Kafka are out of the in-sync replicas (ISR) set.

Handling Procedure

Check Broker instances.

Step 1 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services** > **Kafka** > **Instance**. The Kafka instances page is displayed.

Step 2 Check whether faulty nodes exist among all Broker nodes.

- If yes, record the host name of the node and go to **Step 3**.
- If no, go to **Step 5**.

Step 3 On the FusionInsight Manager portal, click **O&M** > **Alarm** > **Alarms** to check whether the fault described in **Step 2** exists in the alarm information and handle the alarm based on corresponding methods.

Step 4 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services** > **Kafka** > **Instance**. The Kafka instances page is displayed.

Step 5 Check whether stopped nodes exist among all Broker instance.

- If yes, go to **Step 6**.
- If no, go to **Step 7**.

Step 6 Select all stopped Broker instances and click **Start Instance**.

Step 7 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Collect fault information.

Step 8 On the FusionInsight Manager portal, choose **O&M** > **Log** > **Download**.

Step 9 Select **Kafka** in the required cluster from the **Service** drop-down list.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 10 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 11 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.287 ALM-38007 Status of Kafka Default User Is Abnormal

Alarm Description

The system checks the default user of Kafka every 60 seconds. This alarm is generated when the system detects that the user status is abnormal.

Trigger Count is set to **1**. This alarm is cleared when the user status becomes normal.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
38007	Critical	Quality of service	Tenant plane	Kafka	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.

Type	Parameter	Description
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

If the Kafka default user status is abnormal, metadata synchronization between Brokers and interaction between Kafka and ZooKeeper will be affected, affecting service production, consumption, and topic creation and deletion.

Possible Causes

- The Sssd service is abnormal.
- Some Broker instances stop running.

Handling Procedure

Check whether the Sssd service is abnormal.

Step 1 On the FusionInsight Manager portal, choose **O&M** > **Alarm** > **Alarms** > **Status of Kafka Default User Is Abnormal** > **Location** to check the host name of the instance for which the alarm is generated.

Step 2 Find the host information in the alarm information and log in to the host.

Step 3 Run the **id -Gn kafka** command and check whether "No such user" is displayed in the command output.

- If yes, record the host name of the node and go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On the FusionInsight Manager home page, choose **O&M** > **Alarm** > **Alarms**. Check whether there is **Sssd Service Exception** in the alarm information. If there is, handle the alarm based on alarm information.

Check the running status of the Broker instance.

Step 5 On the FusionInsight Manager home page, choose **Cluster** > *Name of the desired cluster* > **Services** > **Kafka** > **Instance**. The Kafka instance page is displayed.

Step 6 Check whether there are stopped nodes on all Broker instances.

- If yes, go to **Step 7**.
- If no, go to **Step 8**.

Step 7 Select all stopped Broker instances and click **Start Instance**.

Step 8 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Collect fault information.

Step 9 On FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 10 In the **Service** area, select **Kafka** in the required cluster.

Step 11 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.288 ALM-38008 Abnormal Kafka Data Directory Status

Alarm Description

The system checks the Kafka data directory status every 60 seconds. This alarm is generated when the system detects that the status of a data directory is abnormal.

Trigger Count is set to **1**. This alarm is cleared when the data directory status becomes normal.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
38008	Major	Quality of service	Tenant plane	Kafka	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	DirName	Specifies the directory name for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

If the Kafka data directory status is abnormal, the current replicas of all partitions in the data directory are brought offline, and the data directory status of multiple nodes is abnormal at the same time. As a result, some partitions may become unavailable.

Possible Causes

- The data directory permission is tampered with.
- The disk where the data directory is located is faulty.

ProcedureHandling Procedure

Check the permission on the faulty data directory.

Step 1 Find the host information in the alarm information and log in to the host.

Step 2 In the alarm information, check whether the data directory and its subdirectories belong to the omm:wheel group.

- If yes, record the host name of the node and go to **Step 4**.
- If no, go to **Step 3**.

Step 3 Restore the owner group of the data directory and its subdirectories to omm:wheel.

- If yes, go to **Step 6**.
- If no, go to **Step 5**.

Check whether the disk where the data directory is located is faulty.

Step 4 In the upper-level directory of the data directory, create and delete files as user **omm**. Check whether data read/write on the disk is normal.

Step 5 Replace or repair the disk where the data directory is located to ensure that data read/write on the disk is normal.

Step 6 On the FusionInsight Manager home page, choose **Cluster** > *Name of the desired cluster* > **Services** > **Kafka** > **Instance**. On the Kafka instance page that is displayed, restart the Broker instance on the host recorded in **Step 2**.

Step 7 After Broker is started, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Collect fault information.

Step 8 On FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 9 In the **Service** area, select **Kafka** in the required cluster.

Step 10 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 11 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.289 ALM-38009 Busy Broker Disk I/Os

Alarm Description

The system checks the I/O status of each Kafka disk every 60 seconds. This alarm is generated when the disk I/O of a Kafka data directory on a broker exceeds the threshold (80% by default).

Its **Trigger Count** is **3**. This alarm is cleared when the disk I/O is lower than the threshold (80% by default).

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
38009	Major	Quality of service	Tenant plane	Kafka	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.

Type	Parameter	Description
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	DataDirectory Name	Specifies the name of the Kafka data directory with frequent disk I/Os.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

The disk partition has frequent I/Os. Data may fail to be written to the Kafka topic for which the alarm is generated.

Possible Causes

- There are many replicas configured for the topic.
- The parameter for batch writing producer's messages is inappropriately configured. The service traffic of this topic is too heavy, and the current partition configuration is inappropriate.

Handling Procedure

Check the number of topic replicas.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. Locate the row that contains this alarm, click ⌄, and view the host name in **Location**.

Step 2 On FusionInsight Manager, choose **Cluster**, click the name of the desired cluster, choose **Services** > **Kafka** > **KafkaTopic Monitor**, search for the topic for which the alarm is generated, and check the number of replicas.

Step 3 Reduce the replication factors of the topic (for example, reduce to **3**) if the number of replicas is greater than 3.

Run the following command on the FusionInsight client to replan the replicas of Kafka topics:

kafka-reassign-partitions.sh --bootstrap-server *<Kafka cluster IP address:21007>* **--command-config ../config/client.properties --reassignment-json-file** *{manual assignment json file path}* **--execute**

For example:

/opt/hadoopclient/Kafka/kafka/bin/kafka-reassign-partitions.sh --bootstrap-server 192.168.0.90:21007,192.168.0.91:21007,192.168.0.92:21007 --command-config /opt/hadoopclient/Kafka/kafka/config/client.properties --reassignment-json-file expand-cluster-reassignment.json --execute

NOTE

In the **expand-cluster-reassignment.json** file, describe the brokers to which the partitions of the topic are migrated in the following format: {"partitions":[{"topic": "*topicName*","partition": 1,"replicas": [1,2,3] }],"version":1}

Step 4 Observe for a period of time and check whether the alarm is cleared. If the alarm persists, go to **Step 5**.

Check the partition planning of the topic.

Step 5 On the **KafkaTopic Monitor** page, view **Topic Input Traffic** in the **Topic Traffic** area of each topic, obtain the topic with the largest value, and check the partitions of this topic as well as information about the host of these partitions.

Step 6 Log in to the host queried in **Step 5** and run the **iostat -d -x** command to check the **%util** value of each disk.

```
:/opt/R3/FusionInsight_Manager/software/packs # iostat -d -x
Linux 3.0.76-0.11-default (189-39-172-162)      06/26/19        _x86_64_

Device:         rrqm/s   wrqm/s     r/s     w/s   rsec/s   wsec/s avgrq-sz avgqu-sz   await  svctm  %util
xvda              0.04    44.44    1.26   21.94    43.62   531.02    24.78     0.03    1.44   0.56   1.30
xvde              0.16   431.84   13.78   82.51   284.32  4115.90    45.70     0.06    1.41   0.64   6.21
```

- If the **%util** value of each disk exceeds the threshold (**80%** by default), expand the Kafka disk capacity. For details, see MapReduce Service (MRS) 3.3.1-LTS Physical Machine Cluster Capacity Expansion Guide (for Huawei Cloud Stack 8.3.1). After the capacity expansion, replan the topic partitions by referring to **Step 3**.
- If the **%util** values of the disks vary greatly, check the disk partition configuration of Kafka. For example, check the value of **log.dirs** in the **$ {BIGDATA_HOME}/FusionInsight_HD_8.3.1/1_14_Broker/etc/server.properties** file.

  Run the following command to view the **Filesystem** information:

  df -h *log.dirs value*

  The command output is as follows.

```
:/opt/R3/FusionInsight_Manager/software/packs # df -h /srv/BigData/kafka/data1/kafka-logs/
Filesystem      Size  Used Avail Use% Mounted on
/dev/xvda2       36G   21G   14G  62% /
:/opt/R3/FusionInsight_Manager/software/packs #
```

- If the partition where Filesystem is located matches the partition with a high **%util** value, plan Kafka partitions on idle disks, configure **log.dirs** as an idle disk directory, and replan topic partitions by referring to **Step 3**. Ensure that the partitions of the topic are evenly distributed to each disk.

Step 7 Observe for a period of time and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, repeat **Step 5** to **Step 6** three times. Then, go to **Step 8**.

Step 8 Observe for a period of time and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Collect fault information.

Step 9 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 10 Expand the **Service** drop-down list, and select **Kafka** for the target cluster.

Step 11 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.290 ALM-38010 Topics with Single Replica

Alarm Description

The system checks the number of replicas of each topic every 60 seconds on the node where the Kafka Controller resides. This alarm is generated when there is one replica for a topic.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
38010	Major	Quality of service	Tenant plane	Kafka	No

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	TopicName	Specifies the list of topics for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

There is the single point of failure (SPOF) risk for topics with only one replica. When the node where the replica resides becomes abnormal, the partition does not have a leader, and services on the topic are affected.

Possible Causes

- The number of replicas for the topic is incorrectly configured.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Handling Procedure

Check the number of replicas for the topic.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**, click ⌄ of this alarm, and view the **TopicName** list in **Location**.

Step 2 Check whether replicas need to be added for the topic for which the alarm is generated.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 On the FusionInsight client, re-plan topic replicas and describe the partition distribution of the topic in the **add-replicas-reassignment.json** file in the following format: {"partitions":[{"topic": "*topic name*","partition": 1,"replicas": [1,2] }],"version":1}. Then, run the following command to add replicas:

kafka-reassign-partitions.sh --bootstrap-server *<Kafka cluster IP address:21007>* **--command-config ../config/client.properties --reassignment-json-file** *{manual assignment json file path}* **--execute**

For example:

/opt/hadoopclient/Kafka/kafka/bin/kafka-reassign-partitions.sh --bootstrap-server 192.168.0.90:21007,192.168.0.91:21007,192.168.0.92:21007 **--command-config /opt/hadoopclient/Kafka/kafka/config/client.properties --reassignment-json-file add-replicas-reassignment.json --execute**

Step 4 Run the following command to check the task execution progress:

kafka-reassign-partitions.sh --bootstrap-server *<Kafka cluster IP address:21007>* **--command-config ../config/client.properties --reassignment-json-file** *{manual assignment json file path}* **--verify**

For example:

/opt/hadoopclient/Kafka/kafka/bin/kafka-reassign-partitions.sh --bootstrap-server 192.168.0.90:21007,192.168.0.91:21007,192.168.0.92:21007 --command-config /opt/hadoopclient/Kafka/kafka/config/client.properties --reassignment-json-file add-replicas-reassignment.json --verify

Step 5 After completing the handling operations or confirming that the alarm has no impact, manually clear the alarm on FusionInsight Manager.

Step 6 After a period of time, check whether the alarm is cleared.

- If it is, no further action is required.
- If it is not, go to **Step 7**.

Collect fault information.

Step 7 On FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 8 In the **Service** area, select **Kafka** in the required cluster.

Step 9 Click ✎ in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact the technical support and send the collected logs.

----End

Alarm Clearance

If the alarm has no impact, manually clear the alarm.

Related Information

None.

1.3.291 ALM-38011 User Connection Usage on Broker Exceeds the Threshold

Alarm Description

The system checks the number of connections of each user on Broker every 30 seconds. This alarm is generated when the connection usage of a user on the Broker exceeds the thresholdfor 5 consecutive times.

The number of times that smoothing is performed is **5**. This alarm is cleared when the connection usage of a user on the Broker is less than the threshold.

The alarm can be automatically cleared. However, if the number of connections of a user suddenly becomes **0** and no connection is created, the alarm cannot be automatically cleared. You need to manually clear it.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
38011	Critical (default threshold: 90%) Major (default threshold: 85%)	Quality of service	Tenant plane	Kafka	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.

Type	Parameter	Description
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	UserName	Specifies the username for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

If the number of connections of a user is excessive, the user cannot create new connections to the Broker.

Possible Causes

- The number of connections (created by a user) used by the client exceeds the preset threshold.
- The threshold for the connection usage does not meet service requirements.

Handling Procedure

Check the number of connections established by the same user on the client.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 1 On the FusionInsight Manager home page, choose **O&M** > **Alarm** > **Alarms** > **User Connection Usage on Broker Exceeds the Threshold**. Check the host name and username of the Broker instance for which the alarm is generated in **Location**.

Step 2 On FusionInsight Manager home page, choose **Cluster** > *Name of the desired cluster* > **Services** > **Kafka** > **Instance**. Click the instance for which the alarm is generated to go to the page for the instance. Click the drop-down list in the upper right corner of the chart area, choose **Customize > Other**, and select **User Connection Usage on Broker**, **Maximum Number of User Connections on Broker**, and **Number of User Connections on Broker** to view the number of the current user connections on the Broker.

Step 3 Observe the number of real-time connections of the current alarm user and check whether the real-time monitoring data of the current user exists.

- If yes, go to **Step 4**.
- If no, the current user has disconnected all connections. You need to clear the alarm manually, and no further action is required.

NOTE

After the alarm user disconnects all connections, the monitoring data of the user disappears. In this case, the alarm will not be automatically cleared. You need to manually clear it.

Step 4 Check whether the user is authorized by the service side.

If yes, go to **Step 7**.

If no, go to **Step 5**.

Step 5 Run the following command on the client to limit the number of connections of the user. There are two configuration rules based on the following commands:

1. For the specific Broker and user, run the following command:

   kafka-configs.sh --bootstrap-server *<broker ip:port>* **--alter --add-config 'max.connections.per.user.overrides=[***<username>***:***<connection.number>***]' --entity-type brokers --entity-name** *<broker.id>* **--command-config Kafka/kafka/config/producer.properties**

   NOTE

   For unauthorized users, confirm with the service side to reduce the maximum number of connections of an unauthorized user or set the maximum number of connections to **0**.

   In the command, you need to specify the IP address and port number of Broker, set values of configuration items, and specify the **brokerId** and **username**. Here, the user refers to the authorized Kerberos user.

   The configuration updated using the command line tool can take effect dynamically. The configuration becomes invalid after the service is restarted. To make the configuration take effect after the restart, choose **Cluster** > *Name of the desired cluster* > **Services** > **Kafka** > **Configurations** > **All Configurations**> **Broker** > **Server** on the FusionInsight Manager home page and update the configuration to **max.connections.per.user.overrides**.

2. For the specific use and default Broker (that is, all Broker instances in the cluster), run the following command:

   kafka-configs.sh --bootstrap-server *<broker ip:port>* **--alter --add-config 'max.connections.per.user.overrides=[***<username>***:***<connection.number>***]' --**

entity-type brokers ---entity-default --command-config Kafka/kafka/config/client.properties

Example:

kafka-configs.sh --bootstrap-server 10.153.3.26:21007 --alter --add-config 'max.connections.per.user.overrides=[showcase:4]' --entity-type brokers --entity-name 1 --command-config Kafka/kafka/config/client.properties

Step 6 Check whether the maximum number of connections is **0** and whether the number of connections of the current user decreases or remains unchanged according to **Step 2**.

- If yes, manually clear the alarm and no further action is required.
- If no, go to **Step 7**.

Step 7 Check whether the number of real-time connections and connection usage of the current user are sharply increased when they are compared with historical data, and whether have exceeded the specified maximum number of connections.

- If yes, go to **Step 8**.
- If no, go to **Step 9**.

NOTE

If there is an obvious increase after the comparison and the maximum number of connections has reached the preset value, the connections of the user may be abnormal. You need to confirm with the service party.

Check whether the number of user connections meets service requirements.

Step 8 Check whether the number of connections of the user meets service requirements.

- If yes, go to **Step 9**.
- If no, contact the service party to rectify the fault.

NOTE

If the number of user connections is abnormal, contact the service party to rectify the fault from the following aspects:

- Check whether new services are added so that the number of user connections increases sharply.
- Check whether handle leakage occurs on the code at the service side.

Step 9 Consider whether to increase the maximum number of connections of the user.

- If yes, go to **Step 10**.
- If no, go to **Step 12**.

Step 10 Increase the maximum number of connections based on the service requirements. Set the number of connections of the user on the Kafka client. For details, see **Step 5**.

Step 11 Wait for several minutes and then check whether the alarm is automatically cleared.

- If yes, go to **Step 12**.
- If no, go to **Step 2**.

Step 12 Determine whether to add the user to the whitelist based on service requirements on the service side.

- If yes, go to **Step 13**.
- If no, go to **Step 15**.

NOTE

To add a user to the whitelist, you need to restart the Kafka service. However, this operation will cause service interruption and affect service running. Therefore, you must confirm with the service side before performing this operation.

Step 13 On the FusionInsight Manager home page, choose **Cluster** > *Name of the desired cluster* > **Services** > **Kafka** > **Configurations** > **All Configurations** > **Broker(Role)** > **Server** to add the user to the **max.connections.per.user.whitelist** configuration item.

Step 14 Restart the service for the modification to take effect. In addition, you need to manually clear the alarm, and no further action is required.

Collect the fault information.

Step 15 On the FusionInsight Manager homepage, choose **O&M** > **Log** > **Download**.

Step 16 Expand the **Service** drop-down list, and select **Kafka** for the target cluster.

Step 17 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 18 Contact the technical support and send the collected fault logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.292 ALM-39000 AOF Persistence Exception

Alarm Description

The system checks the Redis cluster service status every 5 seconds. This alarm is generated when Redis fails to perform AOF file writes.

This alarm is cleared when the Redis performs AOF file writes successfully.

This alarm can be automatically cleared.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
39000	Major	Quality of service	Tenant plane	Redis	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

Redis persistency exceptions reduce data integrity and may cause data loss during Redis restart or restart failure.

Possible Causes

- The disk permission is abnormal, the space is insufficient, or the disk is faulty.
- During Redis persistency, Fork subprocesses need to perform data persistency. If the memory or the number of available processes is not enough, Fork subprocesses fail to perform data persistency and an exception occurs.

  NOTE

  It is recommended that the memory usage of the Redis be no more than 60% of the system memory.

Handling Procedure

Check the disk permission and status.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. In the real-time alarm list, click ⌄ next to this alarm and view the hostname and role name corresponding to the alarm in **Location**.

Step 2 Choose **Cluster** > *Name of the desired cluster* > **Services** > **Redis** > **Instance**.

Step 3 Select the instance whose hostname is that displayed in **Location** in alarm details, and record the IP address and hostname.

Step 4 Log in to the host where the preceding IP address is obtained as user **root**.

Step 5 Go to the disk directory where Redis data is stored and run the **ll** command to check whether the user permission is 700 and whether the user is **omm:wheel**.

The default work directory is **${BIGDATA_DATA_HOME}/redis/***<role name>*.

- If yes, go to **Step 8**.
- If no, go to **Step 6**.

Step 6 Modify the permission of the faulty disk. For example, if the faulty disk is **Redis_1**, run the following commands:

chown omm:wheel Redis_1

chmod 700 Redis_1

Step 7 Use redis-cli to run the **BGREWRITEAOF** command and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Step 8 Run the **df** command to check the available disk space of the Redis work directory is enough.

- If yes, go to **Step 9**.
- If no, go to **Step 10**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 9 Stop the Redis instance for which the alarm is generated, replace the disk with a disk with larger capacity, restart the instance. Use the redis-cli tool to run the **BGREWRITEAOF** command, and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 10**.

Check the number of processes.

Step 10 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** to check whether the "Process Usage Exceeds the Threshold" alarm is reported.

- If yes, go to **Step 11**.
- If no, go to **Step 12**.

Step 11 Clear the alarm by referring to the alarm help of ALM-12061 Process Usage Exceeds the Threshold. Use the redis-cli tool to run the **BGREWRITEAOF** command, and check whether "AOF Persistence Exception" is cleared.

- If yes, no further action is required.
- If no, go to **Step 12**.

Collect fault information.

Step 12 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 13 Expand the **Service** drop-down list, and select **Redis** for the target cluster.

Step 14 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 15 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.293 ALM-39001 RDB Persistence Exception

Alarm Description

The system checks the Redis cluster service status every 5 seconds. This alarm is generated when Redis fails to perform RDB file writes.

This alarm is cleared when Redis performs RDB file writes successfully.

This alarm can be automatically cleared.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
39001	Major	Quality of service	Tenant plane	Redis	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

Redis persistency exceptions reduce data integrity and may cause data loss during Redis restart or restart failure.

Possible Causes

- The disk permission is abnormal, the space is insufficient, or the disk is faulty.
- During Redis persistency, Fork subprocesses need to perform data persistency. If the memory is insufficient or the number of available processes is insufficient, Fork subprocesses fail to perform data persistency and an exception occurs.

  NOTE

  It is recommended that the memory usage of the Redis be no more than 60% of the system memory.

Handling Procedure

Check the disk permission and status.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. In the real-time alarm list, click ⌄ next to this alarm and view the hostname and role name corresponding to the alarm in **Location**.

Step 2 Choose **Cluster** > *Name of the desired cluster* > **Services** > **Redis** > **Instance**.

Step 3 Select the instance whose hostname is that displayed in **Location** in alarm details, and record the IP address and hostname.

Step 4 Log in to the host where the preceding IP address is obtained as user **root**.

Step 5 Go to the disk directory where Redis data is stored and run the **ll** command to check whether the user permission is 700 and whether the user is **omm:wheel**.

The default work directory is **${BIGDATA_DATA_HOME}/redis/***<role name>*.

- If yes, go to **Step 8**.
- If no, go to **Step 6**.

Step 6 Modify the permission of the faulty disk. For example, if the faulty disk is **Redis_1**, run the following commands:

chown omm:wheel Redis_1

chmod 700 Redis_1

Step 7 Use redis-cli to run the **BGSAVE** command and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Step 8 Run the **df** command to check the available disk space of the Redis work directory is enough.

- If yes, go to **Step 9**.

- If no, go to **Step 10**.

Step 9 Stop the Redis instance for which the alarm is generated, replace the disk with a disk with larger capacity, restart the instance. Use the redis-cli tool to run the **BGSAVE** command, and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 10**.

Check the number of processes.

Step 10 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** to check whether the "Process Usage Exceeds the Threshold" alarm is reported.

- If yes, go to **Step 11**.
- If no, go to **Step 12**.

Step 11 Clear the alarm by referring to the alarm help of ALM-12061 Process Usage Exceeds the Threshold. Use the redis-cli tool to run the **BGSAVE** command, and check whether "RDB Persistence Exception" is cleared.

- If yes, no further action is required.
- If no, go to **Step 12**.

Collect fault information.

Step 12 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 13 Expand the **Service** drop-down list, and select **Redis** for the target cluster.

Step 14 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 15 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.294 ALM-39002 Abnormal Redis Cluster

Alarm Description

The system periodically checks the Redis cluster service every 30 seconds. This alarm is generated when the system detects that the cluster is abnormal.

This alarm is cleared when the Redis cluster service becomes available.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
39002	Critical	Quality of service	Tenant plane	Redis	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RedisClusterName	Specifies the name of the Redis logical cluster for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

If the Redis cluster is offline, the Redis cluster service is unavailable and cannot provide services for components that use caches.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Possible Causes

At least one instance in the Redis cluster is faulty.

Handling Procedure

Check the process status of each instance in the Redis cluster.

Step 1 In the FusionInsight Manager alarm list, click next to the alarm. Obtain the name of the cluster for which the alarm is generated from **Location**.

Step 2 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services**, choose **Redis**, and then click **Redis Manager**. Select the cluster name obtained in **Step 1**, go to the **Redis Cluster Status** page, and record the cluster instances.

Step 3 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services**, choose **Redis**, and then click **Instance**. Select the instance obtained in **Step 2** in the **Instances** tab, and choose **More** > **Restart Instance** to restart the abnormal instance. Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 4**.

Step 4 Rectify the fault by referring to the alarm help of **ALM-39010 Redis Instance Connections Are Abnormal**. Then, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Collect fault information.

Step 5 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 6 Expand the **Service** drop-down list, and select **Redis** for the target cluster.

Step 7 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 8 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

1.3.295 ALM-39004 Redis Service Unavailable

Alarm Description

The system checks the services on which Redis depends every 30 seconds. This alarm is generated when the functions of a service on which Redis depends are unavailable.

This alarm is cleared when the services on which Redis depends are restored.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
39004	Critical	Quality of service	Tenant plane	Redis	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

The Redis service functions are abnormal, and operations cannot be performed on the Redis cluster on FusionInsight Manager. As a result, Redis cannot provide services for components that use the cache service.

Possible Causes

- The services on which Redis depends are abnormal.
  - The DBService service is abnormal.
  - The KrbServer service is abnormal.
  - The LdapServer service is abnormal.
- The redis_1 process is faulty.
- The Redis process is faulty.

Handling Procedure

Check whether the services on which Redis depends are normal.

NOTE

Redis in normal mode is related to DBService only during startup. Go to **Step 7** to handle the alarm.

Step 1 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** to check whether DBService, KrbServer, and LdapServer are stopped.

- If yes, start them and go to **Step 2**.
- If no, go to **Step 3**.

Step 2 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. In the alarm list, check whether the **Redis Service Unavailable** alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 3**.

Step 3 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. In the alarm list, check whether the **KrbServer Service Unavailable**, **LdapServer Service Unavailable**, or **DBService Service Unavailable** alarm exists

- If yes, go to **Step 4**.
- If no, go to **Step 7**.

Step 4 Handle the alarm by following the instructions provided in the alarm help. After all alarms are cleared, check whether this alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Check whether the redis_1 process is normal.

Step 5 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. In the alarm list, check whether the alarm whose role name is **redis_1** exists.

- If yes, rectify the fault by referring to the alarm help based on the alarm ID. Then, check whether the alarm is cleared.
- If no, go to **Step 9**.

Step 6 Check whether **redis_1** is restarted. On FusionInsight Manager, click in the upper right corner to go to the task management center. Select **Restart Instance** and click to check whether the task details contain the **redis_1** instance.

- If yes, go to **Step 9**.
- If no, go to **Step 7**.

Check whether the Redis process is normal.

Step 7 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. In the alarm list, check whether any process fault alarm exists.

- If yes, go to **Step 8**.
- If no, go to **Step 9**.

Step 8 Rectify the fault by following the procedure for handling **ALM-12007 Process Fault**. Then, check whether this alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Collect the fault information.

Step 9 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 10 Expand the **Service** drop-down list, and select **Redis** for the target cluster.

Step 11 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.296 ALM-39005 Single Master Redis Instance

Alarm Description

The system checks the Redis cluster service status every 30 seconds. This alarm is generated when a master instance in the Redis cluster does not have a slave instance.

This alarm is cleared when the slave instance of the master instance recovers.

This alarm can be cleared automatically.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
39005	Major	Quality of service	Tenant plane	Redis	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	RedisClusterName	Indicates the name of the Redis logical cluster for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

The cluster is running properly. However, if the master instance is abnormal, no slave instance can take over the services and the cluster becomes unavailable.

Possible Causes

The Redis instance is abnormal.

Handling Procedure

Check the abnormal Redis instance.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. In the alarm list, click ⌄ next to the alarm. Obtain the hostname, role name, and cluster name for which the alarm is generated from **Location Information**.

Step 2 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Redis** > **Redis Manager**.

Step 3 In the cluster instance list, find out the abnormal instance.

Step 4 Choose **Cluster** > *Name of the desired cluster* > **Services** > **Redis** > **Instances**, select the abnormal instance, and restart it.

Step 5 Check whether this alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Step 6 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** to check whether alarm "Redis Instance Connections Are Abnormal" is reported.

- If yes, go to **Step 7**.
- If no, go to **Step 8**.

Step 7 Rectify the fault by referring to the alarm help **ALM-39010 Redis Instance Connections Are Abnormal**. Then, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Collect fault information.

Step 8 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 9 Expand the **Service** drop-down list, and select **Redis** for the target cluster.

Step 10 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 11 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.297 ALM-39006 Too Many Redis Master Instances Are on the Same Host

Alarm Description

The system checks the Redis cluster service status every 30 seconds. In a Redis cluster, more than half of master instances are running on the same node. This alarm is generated when this node is faulty and the cluster cannot be restored.

This alarm is cleared when the cluster recovers, that is, the failover is complete and the status is stable.

This alarm can be cleared automatically.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
39006	Major	Quality of service	Tenant plane	Redis	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.

Type	Parameter	Description
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RedisClusterName	Specifies the name of the Redis logical cluster for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

If this alarm occurs, the cluster will be unavailable.

Possible Causes

Some master instances are abnormal. Their slave instances become master instances.

Handling Procedure

Find out abnormal instances.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. In the real-time alarm list, click ⌄ next to the alarm to view the hostname, role name, and cluster name of the slave instance for which the alarm is generated.

Step 2 Choose **Cluster** > *Name of the desired cluster* > **Services** > **Redis** > **Redis Manager**.

Step 3 Click the cluster for which the alarm is generated and view the instance status to find out the abnormal instance.

Step 4 Choose **Cluster** > *Name of the desired cluster* > **Services** > **Redis** > **Instances**, select the abnormal instance, and restart it.

Step 5 Check whether this alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **Redis** for the target cluster.

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.298 ALM-39007 Inconsistent Maximum Memory Configurations on Redis Master and Slave Instances

Alarm Description

The system checks the Redis cluster service status every 30 seconds. This alarm is generated when the maximum memory configurations of a pair of master and slave Redis instances in the cluster is inconsistent.

This alarm is cleared when the maximum memory configurations are consistent or the slave instance is lost.

This alarm can be cleared automatically.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
39007	Major	Quality of service	Tenant plane	Redis	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RedisClusterName	Specifies the name of the Redis logical cluster for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

Redis cluster failover may fail because the memory for the slave instance is insufficient.

Possible Causes

Configuration errors exist or the configuration is not synchronized between the master and slave instances after the cluster is installed.

Handling Procedure

Check the instance configuration.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. In the real-time alarm list, click next to the alarm to view the hostname, role name, and cluster name of the slave instance for which this alarm is generated.

Step 2 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Redis** > **Redis Manager**.

Step 3 View the instance details of the cluster and record the hostname and role name of the master instance corresponding to the slave instance.

Step 4 Choose **Cluster** > *Name of the desired cluster* > **Services** > **Redis** > **Instances**, click the target instance in the **Instance** column, click **Instance Configurations**, and check whether the **maxmemory** values of the master and slave instances are the same.

- If yes, go to **Step 6**.
- If no, go to **Step 5**.

Step 5 Change the **maxmemory** value of the Redis instances to the same value, click **Save**, and then click **OK**. Restart the Redis instances and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **Redis** for the target cluster.

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.299 ALM-39008 Uneven Slot Distribution of Redis Master Instances

Alarm Description

The system checks the Redis cluster status every 30 seconds. This alarm is generated when the slots of master instances are unevenly distributed.

You can scale in the cluster or perform a balance operation on the cluster management page to balance the slots.

This alarm is automatically cleared after the slots are balanced.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
39008	Minor	Quality of service	Tenant plane	Redis	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RedisClusterName	Specifies the name of the Redis logical cluster for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

The load is unbalanced. The memory usage of some instances reaches the upper limit. As a result, the instances cannot provide services.

Possible Causes

- The disk permission is abnormal, the space is insufficient, or the disk is faulty.
- The cluster scale-out, scale-in, or balance operation is abnormal.

Handling Procedure

Check the disk permission and status.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. Check whether the alarm **Redis AOF Persistence Exception** or **Redis RDB Persistence Exception** is reported.

- If yes, go to **Step 2**.
- If no, go to **Step 3**.

Step 2 Clear the alarm by referring to the alarm handling procedure in **ALM-39000 AOF Persistence Exception** or **ALM-39001 RDB Persistence Exception**. Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 3**.

Check the instance status.

Step 3 Log in to FusionInsight Manager. In the real-time alarm list, click next to the row that contains the alarm. In the **Location** area, check the hostname, role name, and cluster name of the slave instance that sends the alarm.

Step 4 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Redis** > **Redis Manager**.

Step 5 Click the cluster for which the alarm is generated and view the instance status.

Step 6 Ensure that all instances are in position. Click **Balance** in the **Operation** column of the Redis cluster name.

Step 7 In **Balance Redis Cluster**, enter the system administrator password and click **OK**.

NOTE

- If an instance is not in position and cannot be restored, scale in the cluster to remove the instance and its master instance.
- During cluster scale-out, scale-in, or balance, ensure that the Redis cluster is not busy or it does not provide services externally. Otherwise, the operation may fail.

Step 8 Check whether this alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Collect fault information.

Step 9 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 10 Expand the **Service** drop-down list, and select **Redis** for the target cluster.

Step 11 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.300 ALM-39009 Redis Slot Migration Exception

Alarm Description

The system checks the Redis cluster service status every 30 seconds. This alarm is generated when an exception occurs during the Redis cluster scale-out, scale-in, and balance.

You can rectify the fault on the cluster management page.

This alarm is automatically cleared when the fault is fixed.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
39009	Critical	Quality of service	Tenant plane	Redis	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.

Type	Parameter	Description
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RedisClusterName	Specifies the name of the Redis logical cluster for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

The access of some keys is lost, and some cluster data is lost.

Possible Causes

The Redis cluster scale-out, scale-in, or balance operation is abnormal.

Handling Procedure

Restore the Redis cluster.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. In the real-time alarm list, click ⌄ next to the alarm. Obtain the name of the cluster for which the alarm is generated from **Location**.

Step 2 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Redis** > **Redis Manager**.

Step 3 Click **Repair** in the **Operation** column of the target Redis cluster.

Step 4 In the displayed dialog box, enter the password of the current administrator. After the fault is rectified, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Collect fault information.

Step 5 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 6 Expand the **Service** drop-down list, and select **Redis** for the target cluster.

Step 7 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 8 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.301 ALM-39010 Redis Instance Connections Are Abnormal

Alarm Description

This alarm is generated when connections between instances in the Redis cluster are abnormal in the scenario where the monitoring module monitors the Redis cluster status in a 30-second period.

This alarm can be automatically cleared after the instance connections are normal.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
39010	Major	Quality of service	Tenant plane	Redis	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.

Type	Parameter	Description
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RedisClusterName	Specifies the name of the Redis logical cluster for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

If connections between instances in the Redis cluster are abnormal, the related instances will fail to provide services for the external systems.

Possible Causes

- The disk permission is abnormal, the space is insufficient, or the disk is faulty.
- The installation directory permission is abnormal.
- The network is faulty.

Handling Procedure

Check the disk working status.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. Check whether the alarm **Redis AOF Persistence Exception** or **Redis RDB Persistence Exception** exists.

- If yes, go to **Step 2**.
- If no, go to **Step 3**.

Step 2 Clear the alarm by referring to the alarm handling procedure in **ALM-39000 AOF Persistence Exception** or **ALM-39001 RDB Persistence Exception**. Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 3**.

Check the permission of the cluster installation directory.

Step 3 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. In the real-time alarm list, click ⌄ next to this alarm and view the Redis instance and role name corresponding to the alarm in **Location**.

Step 4 Log in to the host where the preceding IP address is obtained as user **root**.

Step 5 Go to the Redis installation directory and check whether the permission of the files in the installation directory is **700** and whether the user is **omm:wheel**.

- If yes, go to **Step 8**.
- If no, go to **Step 6**.

Step 6 Modify the permission of the faulty directory. For example, if the faulty directory is **Redis_1**, run the following commands:

chown -R omm:wheel Redis_1

chmod -R 700 Redis_1

Step 7 Check whether the alarm is cleared in the alarm list.

- If yes, no further action is required.
- If no, go to **Step 8**.

Check network faults.

Step 8 Use redis-cli to log in to the recorded IP address and port.

- Logging in to the client

  cd *Redis client installation directory*

  source bigdata_env

  kinit *Login username* (For a cluster in security mode, change the password upon the first login. For a cluster in normal mode, you do not need to run this command.)

- Connecting to the Redis cluster

  redis-cli -h *IP* **-p** *port*

  Check whether the login is successful.

  – If yes, go to **Step 9**.
  – If no, go to **Step 11**.

NOTE

- If channel encryption is enabled for Redis, run the **redis-cli -h** *IP* **-p** *port* **--tls** command.
- To enable SSL channel encryption for Redis, log in to Manager, click **Cluster**, and choose **Services** > **Redis**. On the displayed page, click **Configurations** and then **All Configurations**, search for **REDIS_SSL_ON**, and set this parameter to **true**. Channel encryption encrypts data during data transfer but affects performance. Do not enable this function (set **REDIS_SSL_ON** to **false**) when Redis does not contain important or sensitive data.

Step 9 Run the **cluster mynode** command to check whether it is executed successfully.

- If yes, go to **Step 10**.
- If no, go to **Step 11**.

Step 10 The intermittent network disconnection or Redis cluster access overloads may cause temporary connection exception. It will be automatically recovered after a period of time. If the alarm persists for a long time, go to **Step 11**.

Collect the fault information.

Step 11 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 12 Expand the **Service** drop-down list, and select **Redis** for the target cluster.

Step 13 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 14 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.302 ALM-39011 Exceeded Redis Instance Memory Usage

Alarm Description

The alarm module monitors the Redis cluster status in a 30-second period. This alarm is generated when the instance memory usage of the Redis cluster exceeds the preset threshold (80%) for three consecutive times.

This alarm is cleared automatically when the memory usage becomes lower than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
39011	Major	Quality of service	Tenant plane	Redis	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RedisClusterName	Specifies the name of the Redis logical cluster for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

As services increase, the Redis memory usage will reach the upper limit at any time. As a result, the Redis instance cannot provide services.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Possible Causes

The amount of stored Redis service data is about to exceed the maximum memory usage configured for the instance.

Handling Procedure

Check the instance memory usage.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. In the alarm list, click the alarm. In **Location** and **Additional Information**, check the information about the Redis instance for which the alarm is generated, including the instance IP address and port information.

Step 2 On any node in the cluster, run the following commands to log in to the queried IP address:

- Logging in to the client

  cd *Redis client installation directory*

  source bigdata_env

  kinit *Login username* (For a cluster in security mode, change the password upon the first login. For a cluster in normal mode, you do not need to run this command.)

- Connecting to the Redis cluster

  redis-cli -h *IP* **-p** *port*

  NOTE

  If channel encryption is enabled for Redis, run the **redis-cli -h** *IP* **-p** *port* **--tls** command.

  To enable SSL channel encryption for Redis, log in to Manager, click **Cluster**, and choose **Services** > **Redis**. On the displayed page, click **Configurations** and then **All Configurations**, search for **REDIS_SSL_ON**, and set this parameter to **true**. Channel encryption encrypts data during data transfer but affects performance. Do not enable this function (set **REDIS_SSL_ON** to **false**) when Redis does not contain important or sensitive data.

Step 3 Run the **info memory** command to check the value of **used_memory_human**.

Step 4 Log in to FusionInsight Manager, choose **Cluster**, click the name of the desired cluster, click **Redis**, and then **Configurations**. Check the value of **maxmemory** for the instance group based on the port number, and modify the parameter value as required. Then, save the modification and restart the instance.

Step 5 Wait for a period of time and then check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect the fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **Redis** for the target cluster.

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.303 ALM-39012 Excessive Redis Client Connections

Alarm Description

The system checks the Redis cluster status every 5 seconds. This alarm is generated when the number of Redis client connections is greater than the product of the client connection threshold (85% by default) and the maximum number of client connections (10,000 by default).

This alarm is cleared when the number of Redis client connections is less than the product of the client connection threshold and the maximum number of client connections. This alarm can be automatically cleared.

NOTICE

Typically, this alarm is generated because client connection leakage occurs. You can adjust the maximum number of client connections according to the handling procedure to temporarily avoid risks. Check the code on the service side to eliminate risks.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
39012	Major	Quality of service	Tenant plane	Redis	Yes

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

The system rejects connection requests. As a result, the service is unavailable.

Possible Causes

Excessive connection pools need to be established on the client due to service requirements.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Handling Procedure

Step 1 Log in to FusionInsight Manager, choose **Cluster** > **Services** > **Redis**. On the page that is displayed, click the **Configurations** tab then the **All Configurations** sub-tab. On this sub-tab page, click **Client**. Set **maxclients** to a larger value, for example, **20000**, based on service requirements. Then click **Save**.

NOTE

The value of **maxclients** is limited by the number of file handles of the operating system. You can log in to the node where the Redis instance resides and run the **cat /proc/sys/fs/file-max** command to check the number of file handles. The value of **maxclients** must be less than the number of file handles of the operating system minus 32.

Step 2 Choose **Cluster** > **Services** > **Redis**. On the page that is displayed, click **More** and select **Restart Service** to restart the Redis service. Check whether the Redis instance can be successfully restarted.

- If yes, go to **Step 5**.
- If no, go to **Step 4**.

Step 3 Choose **O&M** > **Alarm** > **Alarms**. In the real-time alarm list, click ⌄ in the row containing the alarm, and click the link next to **HostName** in **Location**. Record the service IP address on the page that is displayed.

Step 4 Use the service IP address to log in to the node where the Redis client is installed as the Redis service user. The user must have the Redis management permission.

1. Log in to the client.

   cd *Redis client installation directory*

   source bigdata_env

   kinit *Redis service user* (For a cluster in security mode, you need to run this command to change the password upon your first login. For a cluster in normal mode, you do not need to run this command.)

2. Connect to and configure the Redis cluster.
   - Redis cluster with SSL channel encryption disabled:

     redis-cli -h *IP* **-p** *port* **--cluster call** *IP.port* **config set maxclients** *20000*
   - Redis cluster with SSL channel encryption enabled:

     redis-cli -h *IP* **-p** *port* **--cluster call** *IP.port* **config set maxclients** *20000* **--tls**

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

NOTE

- To check whether SSL channel encryption has been enabled for a Redis cluster, perform the following steps:

  Log in to FusionInsight Manager, choose **Cluster** > **Services** > **Redis**. On the page that is displayed, click the **Configurations** tab then the **All Configurations** sub-tab. On this sub-tab page, search for **REDIS_SSL_ON**. If its value is **true**, SSL channel encryption has been enabled for Redis. Otherwise, SSL channel encryption has not been enabled for Redis.

- *port* indicates the port number of the Redis instance.

  The port number of a Redis instance is calculated as follows: 22400 + *Instance ID* – 1.

  To obtain the instance ID, log in to FusionInsight Manager and choose **Cluster** > **Services** > **Redis**. On the page that is displayed, click **Redis Manager**. On this page, click the target Redis cluster name.

  For example, in the Redis cluster, the port number of the Redis instance that corresponds to the role **R1** port is 22400 (22400 + 1 – 1 = 22400).

Step 5 Wait for a while and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list. In the **Services** dialog box that is displayed, select **Redis** under the target cluster name, and click **OK**.

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.304 ALM-39013 Abnormal Synchronization Between the Active and Standby Redis Nodes

Alarm Description

The system checks the Redis cluster status every 5 seconds. This alarm is generated when the synchronization between the active and standby Redis nodes is abnormal.

This alarm is automatically cleared when the synchronization between the active and standby Redis nodes becomes normal. This alarm can be cleared automatically.

NOTE

During the restart of a service or instance, the synchronization between the active and standby Redis nodes is abnormal for a short period of time. As a result, this alarm is automatically cleared.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
39013	Major	Quality of service	Tenant plane	Redis	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

The standby Redis instance cannot be synchronized. If the active Redis instance is abnormal, the standby instance becomes the active instance, and data is lost.

Possible Causes

- The value of **client-output-buffer-limit-replica** does not match the service usage.
- The value of **cluster-node-timeout** does not match the service usage.

Handling Procedure

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. In the real-time alarm list, click ⌄ in the row containing this alarm and view the role name and instance IP address in **Location**.

Step 2 Choose **Cluster** > **Services** > **Redis**. On the page that is displayed, click the **Instance** tab. On this tab page, select the Redis instance for which the alarm is generated. On the **Dashboard** tab page that is displayed, click **redis** in the log area to view the instance log and check whether the following information exists in the log after the alarm is generated:

```
[warning] I/O error trying to sync with MASTER: connection lost
```

- If yes, go to **Step 3**.
- If no, go to **Step 6**.

Step 3 Choose **Cluster** > **Services** > **Redis**. On the page that is displayed, click the **Configuration** tab then the **All Configurations** sub-tab. On this sub-tab page, click **Redis(Service)**, select **Client**, set **client-output-buffer-limit-replica** to a larger value based on service requirements, and click **Save**. Then, restart the service for the settings to take effect. After the service is restarted, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 4**.

Step 4 Click **Cluster**, choose **Services** > **Redis**, and click **Instance** to check whether the number of Redis instances exceeds **400**.

- If yes, go to **Step 5**.
- If no, go to **Step 6**.

Step 5 Click **Cluster**, choose **Services** > **Redis**, click **Configurations**, and then **All Configurations**. Click **Redis(Service)** and select **Cluster**, change the value of **cluster-node-timeout** to **25000**, and click **Save**. Restart the service for the settings to take effect. After the service is restarted, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

NOTE

You can change the value of **cluster-node-timeout** based on service requirements. It is recommended that the value be less than or equal to **25000**. If the value is too large, the active/standby switchover will be slow.

Collect the fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list. In the **Services** dialog box that is displayed, select **Redis** under the target cluster name, and click **OK**.

Step 8 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the hosts to which the role belongs, and click **OK**.

Step 9 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.305 ALM-41007 RTDService Unavailable

Alarm Description

The system checks the RTDService service status every 60 seconds. This alarm is generated when all RTDService services are abnormal and the RTDService service is unavailable.

This alarm is cleared when the RTDService service becomes normal.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
41007	Critical	Quality of service	Tenant plane	RTDService	Yes

Alarm Parameters

Type	Name	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	Host Name	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

RTDService cannot provide services for external systems. The RTD console cannot be accessed, and functions such as modifying tenants and event sources are unavailable.

Possible Causes

- The disk or memory usage exceeds 90%.
- The RTDService process is faulty.

Handling Procedure

Check the disk and memory usage.

Step 1 On FusionInsight Manager, choose O&M > Alarm > RTDService Service Unavailable to view and record the host name reported in Location Info.

Step 2 Click Host, view the node corresponding to the host for which the alarm is generated, and log in to the faulty node as the **root** user.

Step 3 Run the **df -h** command to check whether the disk space usage exceeds 90%.

- If yes, clear the space and go to **Step 4**.
- If no, go to **Step 5**.

Step 4 Wait for 10 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Step 5 Run the **free -m** command to check whether the memory usage exceeds 90%.

NOTE

The memory usage is calculated as follows: Actual memory usage (values in the -/+ buffers/cache row and used column) divided by total.

```
[root@xxx FusionInsight_RTD_xxx]# free -m
             total        used        free      shared  buff/cache   available
Mem:         64263        7140       22633        5485       34490       46393
Swap:            0           0           0
```

- If yes, expand the memory capacity and go to **Step 6**.
- If no, go to **Step 7**.

Step 6 Wait for 10 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Check the RTDService process.

Step 7 Log in to the node corresponding to the host for which the alarm is generated as the **root** user.

Step 8 Perform to check whether the RTDService process exists.

ps -aux | grep tomcat | grep RTDServer

- If yes, record the PID and go to **Step 10**.

- If no, log in to FusionInsight Manager and choose **Cluster** > **Services** > **RTDService**. On the page that is displayed, choose **More** > **Restart Service** to restart the RTDService service. Then, go to **Step 9**.

Step 9 Wait for 10 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, run the **Step 8** command again to query the RTDService process. If the process still does not exist, go to **Step 12**.

Step 10 Run the following command to check whether the process status is **D**:

cat /proc/*pid*/status |grep -i state

- If yes, run the **reboot** command to restart the host. Then, go to **Step 11**.
- If no, go to **Step 12**.

Step 11 Wait for 10 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 12**.

Collect fault information.

Step 12 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 13 Select **RTDService** for **Service** and click **OK**.

Step 14 In the **Hosts** area, select the host where the role is located.

Step 15 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 16 Contact O&M personnel/Technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.306 ALM-43001 Spark Service Unavailable

Alarm Description

The system checks the Spark service status every 300 seconds. This alarm is generated when the Spark service is unavailable.

This alarm is cleared when the Spark service recovers.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43001	Critical	Error handling	Tenant plane	Spark	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

The Spark tasks submitted by users fail to be executed.

Possible Causes

- The KrbServer service is abnormal.
- The LdapServer service is abnormal.
- The ZooKeeper service is abnormal.
- The HDFS service is abnormal.
- The Yarn service is abnormal.
- The corresponding Hive service is abnormal.
- The Spark assembly package is abnormal.
- The NameNode memory is insufficient.
- The memory of the Spark process is insufficient.

Handling Procedure

If the alarm is caused due to the abnormal Spark assembly package, wait about 10 minutes, and the alarm will be automatically cleared.

Check whether any service unavailability alarms have been generated for the services that Spark depends on.

Step 1 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**.

Step 2 Check whether the following alarms exist in the alarm list:

- ALM-25500 KrbServer Service Unavailable
- ALM-25000 LdapServer Service Unavailable
- ALM-13000 ZooKeeper Service Unavailable
- ALM-14000 HDFS Service Unavailable
- ALM-18000 Yarn Service Unavailable
- ALM-16004 Hive Service Unavailable

NOTE

If the multi-instance function is enabled for the cluster and multiple Spark services are installed, check the Spark service for which the alarm is generated based on the value of **ServiceName** in **Location** and check whether the corresponding Hive service is faulty. The mapping between Spark and Hive follows the following rule: Spark corresponds to Hive, Spark1 corresponds to Hive1, and so on.

- If yes, go to **Step 3**.
- If no, go to **Step 4**.

Step 3 Handle the alarms by following the instructions provided in the alarm help.

After those alarms are cleared, wait a few minutes and check whether this alarm is cleared.

- If yes, no further action is required.

- If no, go to **Step 4**.

Check whether the NameNode memory is insufficient.

Step 4 Check whether the NameNode memory is insufficient.

- If yes, go to **Step 5**.
- If no, go to **Step 6**.

Step 5 Restart the NameNode to release the memory. Then, check whether this alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Check whether the memory of the Spark process is insufficient.

Step 6 Check whether the memory of the Spark process is insufficient due to memory-related modifications.

- If yes, go to **Step 7**.
- If no, go to **Step 8**.

Step 7 Ensure that the memory of the Spark process is sufficient or expand the cluster capacity. Then, check whether this alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Collect fault information.

Step 8 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 9 Expand the **Service** drop-down list, and select the following services for the target cluster (Hive is determined based on **ServiceName** in the alarm location information):

- KrbServer
- LdapServer
- ZooKeeper
- HDFS
- Yarn
- Hive

Step 10 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 11 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.307 ALM-43006 Heap Memory Usage of the JobHistory Process Exceeds the Threshold

Alarm Description

The system checks the heap memory usage of the JobHistory process every 30 seconds. A major alarm is reported when the heap memory usage is greater than 95% of the maximum memory. A minor alarm is reported when the usage is greater than 85% and less than 95% of the maximum memory.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43006	Major (default threshold: 95% of the maximum memory) Major (default threshold: 85% of the maximum memory)	Quality of service	Tenant plane	Spark	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

If the direct memory usage of the JobHistory process is too high, the performance deteriorates, and the process even becomes unavailable due to memory overflow. When it is unavailable, execution records of Spark tasks cannot be queried.

Possible Causes

The heap memory of the JobHistory process is overused or the heap memory is inappropriately allocated.

Handling Procedure

Check the heap memory usage.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** and select the alarm whose ID is **43006**. Check the role name and the IP address of the host where the alarm is generated in **Location**.

Step 2 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Spark** > **Instance**. Click the JobHistory that reported the alarm to go to the **Dashboard** page. Click the drop-down list in the upper right corner of the chart area, and choose **Customize** > **Memory** > **JobHistory Memory Usage**

Statistics > **OK**. Check whether the heap memory used by the process reaches the maximum heap memory threshold (95% by default).

- If yes, go to **Step 3**.
- If no, go to **Step 7**.

Step 3 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Spark** > **Instance**. Click the JobHistory that reported the alarm to go to the **Dashboard** page. Click the drop-down list in the upper right corner of the chart area, and choose **Customize** > **Memory** > **Heap Memory Statistics for the heap memory of the JobHistory process** > **OK**. Based on the alarm generation time, check the values of the used heap memory of the process in the corresponding period and obtain the maximum value.

Step 4 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > Spark > **Configurations**, click **All Configurations**, and select **JobHistory** > **Default**. The default value of **SPARK_DAEMON_MEMORY** is **4G**. You can change the value based on the ratio of the maximum JobHistory heap memory usage to the threshold specified by **JobHistoryHeap Memory Usage Statistics (JobHistory)** in the alarm period. If the alarm persists after the parameter value is changed, increase the value by 0.5 times. If the alarm is generated frequently, increase the value by one time.

NOTE

On FusionInsight Manager, you can choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Spark** > **Memory** > **Spark Heap Memory Usage Statistics (Spark)** to view the threshold.

Step 5 Restart all JobHistory instances.

Step 6 Check whether the alarm is cleared 10 minutes later.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect fault Information.

Step 7 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 8 Expand the **Service** drop-down list, and select **Spark** for the target cluster.

Step 9 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.308 ALM-43007 Non-Heap Memory Usage of the JobHistory Process Exceeds the Threshold

Alarm Description

The system checks the non-heap memory usage of the JobHistory process every 30 seconds. A major alarm is reported when the non-heap memory usage is greater than 95% of the maximum memory. A minor alarm is reported when the usage is greater than 85% and less than 95% of the maximum memory.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43007	Major (default threshold: 95% of the maximum memory) Major (default threshold: 85% of the maximum memory)	Quality of service	Tenant plane	Spark	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

If the non-heap memory usage of the JobHistory process is too high, the performance deteriorates, and the process even becomes unavailable due to memory overflow. When it is unavailable, execution records of Spark tasks cannot be queried.

Possible Causes

The non-heap memory of the JobHistory process is overused or the non-heap memory is inappropriately allocated.

Handling Procedure

Check non-heap memory usage.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** and select the alarm whose ID is **43007**. Check the role name and the IP address of the host where the alarm is generated in **Location**.

Step 2 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Spark** > **Instance**. Click the JobHistory that reported the alarm to go to the **Dashboard** page. Click the drop-down list in the upper right corner of the chart area, and choose **Customize** > **Memory** > **JobHistory Memory Usage Statistics** > **OK**. Check whether the non-heap memory used by the process reaches the maximum non-heap memory threshold (95% by default).

- If yes, go to **Step 3**.
- If no, go to **Step 7**.

Step 3 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Spark** > **Instance**. Click the JobHistory that reported the alarm to go to the **Dashboard** page. Click the drop-down list in the upper right corner of the chart area, and choose **Customize** > **Memory** > **Statistics for the non-heap memory of the JobHistory process** > **OK**. Based on the alarm generation time, check the values of the used non-heap memory of the process in the corresponding period and obtain the maximum value.

Step 4 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > Spark > **Configurations**, click **All Configurations**, select **Default**, and change the value of **-XX:MaxMetaspaceSize** in the **SPARK_DAEMON_JAVA_OPTS** parameter based on the ratio of the maximum non-heap memory usage to the threshold specified by **JobHistory Non-Heap Memory Usage Statistics (JobHistory)** in the alarm period.

NOTE

On FusionInsight Manager, you can choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Spark** > **Memory** > **Spark Non-Heap Memory Usage Statistics (Spark)** to view the threshold.

Step 5 Restart all JobHistory instances.

Step 6 Check whether the alarm is cleared 10 minutes later.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect fault Information.

Step 7 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 8 Expand the **Service** drop-down list, and select **Spark** for the target cluster.

Step 9 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.309 ALM-43008 Direct Memory Usage of the JobHistory Process Exceeds the Threshold

Alarm Description

The system checks the direct memory usage of the JobHistory process every 30 seconds. A major alarm is reported when the direct memory usage is greater than 95% of the maximum memory. A minor alarm is reported when the usage is greater than 85% and less than 95% of the maximum memory.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43008	Major (default threshold: 95% of the maximum memory) Major (default threshold: 85% of the maximum memory)	Quality of service	Tenant plane	Spark	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

If the direct memory usage of the JobHistory process is too high, the performance deteriorates, and the process even becomes unavailable due to memory overflow. When it is unavailable, execution records of Spark tasks cannot be queried.

Possible Causes

The direct memory of the JobHistory process is overused or the direct memory is inappropriately allocated.

Handling Procedure

Check the direct memory usage.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** and select the alarm whose ID is **43008**. Check the role name and the IP address of the host where the alarm is generated in **Location**.

Step 2 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Spark** > **Instance**. Click the JobHistory that reported the alarm to go to the **Dashboard** page. Click the drop-down list in the upper right corner of the chart area, and choose **Customize** > **Memory** > **JobHistory Memory Usage Statistics** > **OK**. Check whether the direct memory used by the process reaches the maximum direct memory threshold (95% by default).

- If yes, go to **Step 3**.
- If no, go to **Step 7**.

Step 3 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Spark** > **Instance**. Click the JobHistory that reported the alarm to go to the **Dashboard** page. Click the drop-down list in the upper right corner of the chart area, and choose **Customize** > **Direct Memory of JobHistory** > **OK**. Based on the alarm generation time, check the values of the used direct memory of the process in the corresponding period and obtain the maximum value.

Step 4 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Spark** > **Configurations** > **All Configurations** > **JobHistory** > **Default**. You can change the value of **XX:MaxDirectMemorySize** (the default value is 512 MB) in the **SPARK_DAEMON_JAVA_OPTS** parameter based on the ratio of the maximum direct memory used by the JobHistory process to the threshold specified by **JobHistory Direct Memory Usage Statistics (JobHistory)** in the alarm period. If the alarm persists after the parameter value is changed, increase the value by 0.5 times. If the alarm is generated frequently, double the rate. It is recommended that the rate be less than or equal to the value of the **SPARK_DAEMON_MEMORY** parameter.

NOTE

On FusionInsight Manager, you can choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Spark** > **Memory** > **JobHistory Non-Heap Memory Usage Statistics (JobHistory)** to view the threshold.

Step 5 Restart all JobHistory instances.

Step 6 Check whether the alarm is cleared 10 minutes later.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect fault Information.

Step 7 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 8 Expand the **Service** drop-down list, and select **Spark** for the target cluster.

Step 9 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.310 ALM-43009 JobHistory Process GC Duration Exceeds the Threshold

Alarm Description

The system checks the GC duration of JobHistory every 60 seconds. A major alarm is reported when the GC duration exceeds 12 seconds for three consecutive times. A minor alarm is reported when the duration exceeds 9.6 seconds for three consecutive times. To change the threshold, choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Spark** > **GC Time** > **JobHistory Total GC time**. This alarm is cleared when the JobHistory GC duration is shorter than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43009	Minor (default threshold: 9.6 seconds for three consecutive times) Minor (default threshold: 12 seconds for three consecutive times)	Quality of service	Tenant plane	Spark	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

The process performance deteriorates, and the process can even be unavailable. Historical execution records of Spark tasks cannot be queried.

Possible Causes

The heap memory of the JobHistory process is overused or inappropriately allocated, causing frequent occurrence of the GC process.

Handling Procedure

Check the GC duration.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** and select the alarm whose ID is **43009**. Check the role name and the IP address of the host where the alarm is generated in **Location**.

Step 2 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Spark** > **Instance** and click the JobHistory for which the alarm is generated to enter the **Dashboard** page. Click the drop-down menu in the Chart area and choose **Customize** > **GC Time** > **Garbage Collection (GC) Time of JobHistory** from the drop-down list box in the upper right corner and click **OK** to

check whether the GC duration is longer than the threshold (default value: 12 seconds).

- If yes, go to **Step 3**.
- If no, go to **Step 6**.

Step 3 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > Spark > **Configurations**, click **All Configurations**, and select **Default**. Increase the value of **SPARK_DAEMON_MEMORY** (4 GB by default) by 0.5 times if this alarm is generated occasionally. Double the value if the alarm is reported frequently.

Step 4 Restart all JobHistory instances.

Step 5 Check whether the alarm is cleared 10 minutes later.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault Information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **Spark** for the target cluster.

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.311 ALM-43010 Heap Memory Usage of the JDBCServer Process Exceeds the Threshold

Alarm Description

The system checks the heap memory usage of the JDBCServer processes every 30 seconds.

A major alarm is reported when the usage is greater than 85% and less than 95% of the maximum memory. A critical alarm is reported when the usage is greater than the 95% of the maximum memory.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43010	Major (default threshold: 85% of the maximum memory) Critical (default threshold: 95% of the maximum memory.)	Quality of service	Tenant plane	Spark	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

If the heap memory usage of the JDBCServer process is too high, the performance deteriorates, and even memory overflow occurs. As a result, the JDBCServer process is unavailable, and Spark JDBC tasks are slow or fail to run.

Possible Causes

The heap memory of the JDBCServer process is overused or the heap memory is inappropriately allocated.

Handling Procedure

Check the heap memory usage.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** and select the alarm whose ID is **43010**. Check the role name and the IP address of the host where the alarm is generated in **Location**.

Step 2 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Spark** > **Instance**. Click the JDBCServer that reported the alarm to go to the **Dashboard** page. Click the drop-down list in the upper right corner of the chart area, and choose **Customize** > **JDBCServer Memory Usage Statistics** > **OK**. Check whether the heap memory used by the process reaches the maximum heap memory threshold (95% by default).

- If the threshold is reached, go to **Step 3**.
- If the threshold is not reached, go to **Step 7**.

Step 3 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Spark** > **Instance**. Click the JDBCServer that reported the alarm to go to the **Dashboard** page. Click the drop-down list in the upper right corner of the chart area, and choose **Customize** > **Statistics for the heap memory of the JDBCServer process** > **OK**. Based on the alarm generation time, check the values of the used heap memory of the process in the corresponding period and obtain the maximum value.

Step 4 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Spark** > **Configurations** > **All Configurations** > **JDBCServer** > **Performance**. The default value of the **SPARK_DRIVER_MEMORY** parameter is 4 GB. You can change the value based on the ratio of the maximum heap memory

used by the JDBCServer process to the threshold specified by **JDBCServer Heap Memory Usage Statistics (JDBCServer)** in the alarm period. If the alarm persists after the parameter value is changed, increase the value by 0.5 times. If the alarm is generated frequently, increase the value by one time. In the case of large service volume and high service concurrency, you are advised to add instances.

NOTE

On FusionInsight Manager, you can choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Spark** > **Memory** > **JDBCServer Heap Memory Usage Statistics (JDBCServer)** to view the threshold.

Step 5 Restart all JDBCServer instances.

Step 6 Check whether the alarm is cleared 10 minutes later.

- If yes, no further action is required.
- If the threshold is not reached, go to **Step 7**.

Collect fault Information.

Step 7 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 8 Expand the **Service** drop-down list, and select **Spark** for the target cluster.

Step 9 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.312 ALM-43011 Non-Heap Memory Usage of the JDBCServer Process Exceeds the Threshold

Alarm Description

The system checks the non-heap memory usage of the JDBCServer process every 30 seconds.

A major alarm is reported when the usage is greater than 85% and less than 95% of the maximum memory. A critical alarm is reported when the usage is greater than 95% of the maximum memory.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43011	Major (default threshold: 85% of the maximum memory) Critical (default threshold: 95% of the maximum memory.)	Quality of service	Tenant plane	Spark	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

If the non-heap memory usage of the JDBCServer process is too high, the performance deteriorates, and even memory overflow occurs. As a result, the JDBCServer process is unavailable, and Spark JDBC tasks are slow or fail to run.

Possible Causes

The non-heap memory of the JDBCServer process is overused or the non-heap memory is inappropriately allocated.

Handling Procedure

Check non-heap memory usage.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** and select the alarm whose ID is **43011**. Check the role name and the IP address of the host where the alarm is generated in **Location**.

Step 2 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Spark** > **Instance**. Click the JDBCServer that reported the alarm to go to the **Dashboard** page. Click the drop-down list in the upper right corner of the chart area, and choose **Customize** > **JDBCServer Memory Usage Statistics** > **OK**. Check whether the non-heap memory used by the process reaches the maximum non-heap memory threshold (95% by default).

- If yes, go to **Step 3**.
- If the threshold is not reached, go to **Step 7**.

Step 3 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Spark** > **Instance**. Click the JDBCServer that reported the alarm to go to the **Dashboard** page. Click the drop-down list in the upper right corner of the chart area, and choose **Customize** > **Statistics for the non-heap memory of the JDBCServer process** > **OK**. Based on the alarm generation time, check the values of the used non-heap memory of the process in the corresponding period and obtain the maximum value.

Step 4 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Spark** > **Configurations** > **All Configurations** > **JDBCServer** > **Performance**. You can change the value of **XX:MaxMetaspaceSize** in the **spark.driver.extraJavaOptions** parameter based on the ratio of the maximum

non-heap memory used by the JDBCServer process to the threshold specified by **JDBCServerNon-Heap Memory Usage Statistics (JDBCServer)** in the alarm period.

NOTE

On FusionInsight Manager, you can choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Spark** > **Memory** > **JDBCServer Non-Heap Memory Usage Statistics (JDBCServer)** to view the threshold.

Step 5 Restart all JDBCServer instances.

Step 6 Check whether the alarm is cleared 10 minutes later.

- If yes, no further action is required.
- If the threshold is not reached, go to **Step 7**.

Collect fault Information.

Step 7 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 8 Expand the **Service** drop-down list, and select **Spark** for the target cluster.

Step 9 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.313 ALM-43012 Direct Memory Usage of the JDBCServer Process Exceeds the Threshold

Alarm Description

The system checks the direct memory usage of the JDBCServer process every 30 seconds. A major alarm is reported if the usage is greater than 85% but less than 95% of the maximum memory. A critical alarm is reported if the usage is greater than 95% of the maximum memory.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43012	Major (default threshold: 85% of the maximum memory) Critical (default threshold: 95% of the maximum memory.)	Quality of service	Tenant plane	Spark	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

If the direct memory usage of the JDBCServer process is too high, the performance deteriorates, and even memory overflow occurs. As a result, the JDBCServer process is unavailable, and Spark JDBC tasks are slow or fail to run.

Possible Causes

The direct memory of the JDBCServer process is overused or the direct memory is inappropriately allocated.

Handling Procedure

Check the direct memory usage.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** and select the alarm whose ID is **43012**. Check the role name and the IP address of the host where the alarm is generated in **Location**.

Step 2 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Spark** > **Instance**. Click the JDBCServer that reported the alarm to go to the **Dashboard** page. Click the drop-down list in the upper right corner of the chart area, and choose **Customize** > **JDBCServer Memory Usage Statistics** > **OK**. Check whether the direct memory used by the process reaches the maximum direct memory threshold.

- If yes, go to **Step 3**.
- If no, go to **Step 7**.

Step 3 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Spark** > **Instance**. Click the JDBCServer that reported the alarm to go to the **Dashboard** page. Click the drop-down list in the upper right corner of the chart area, and choose **Customize** > **Direct Memory of JDBCServer** > **OK**. Based on the alarm generation time, check the values of the used direct memory of the process in the corresponding period and obtain the maximum value.

Step 4 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Spark** > **Configurations** > **All Configurations** > **JDBCServer** > **Performance**. You can change the value of **XX:MaxDirectMemorySize** (the default value is 512 MB) in the **spark.driver.extraJavaOptions** parameter based on the ratio of the maximum direct memory used by the JDBCServer process to

the threshold specified by **JDBCServerDirect Memory Usage Statistics (JDBCServer)** in the alarm period. If the alarm persists after the parameter value is changed, increase the value by 0.5 times. If the alarm is generated frequently, increase the value by one time. It is recommended that the parameter value be less than or equal to the value of **SPARK_DRIVER_MEMORY**. In the case of large service volume and high service concurrency, you are advised to add instances.

NOTE

On FusionInsight Manager, you can choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Spark** > **Memory** > **JDBCServer Non-Heap Memory Usage Statistics (JDBCServer)** to view the threshold.

Step 5 Restart all JDBCServer instances.

Step 6 Check whether the alarm is cleared 10 minutes later.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect fault information.

Step 7 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 8 Expand the **Service** drop-down list, and select **Spark** for the target cluster.

Step 9 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.314 ALM-43013 JDBCServer Process GC Duration Exceeds the Threshold

Alarm Description

The system checks the GC duration of JDBCServer every 60 seconds. A critical alarm is reported when the GC duration exceeds 12 seconds for three consecutive times. A major alarm is reported when the duration exceeds 9.6 seconds for three consecutive times. To change the threshold, choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Spark** > **GC Time** > **JDBCServer Total GC time**. This alarm is cleared when the JDBCServer GC duration is shorter than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43013	Major (default threshold: 9.6 seconds for three consecutive times) Critical (default threshold: 12 seconds for three consecutive times)	Quality of service	Tenant plane	Spark	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

If the GC duration exceeds the threshold, the performance of the JDBCServer process deteriorates, and the process can even be unavailable. As a result, Spark JDBC tasks are slow or fail to run.

Possible Causes

The heap memory of the JDBCServer process is overused or inappropriately allocated, causing frequent occurrence of the GC process.

Handling Procedure

Check the GC duration.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** and select the alarm whose ID is **43013**. Check the role name and the IP address of the host where the alarm is generated in **Location**.

Step 2 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Spark** > **Instance** and click the JDBCServer for which the alarm is generated to enter the **Dashboard** page. Click the drop-down menu in the Chart area and choose **Customize** > **GC Time** > **Garbage Collection (GC) Time of JDBCServer** from the drop-down list box in the upper right corner and click **OK** to check whether the GC time is longer than the threshold (default value: 12 seconds).

- If yes, go to **Step 3**.
- If no, go to **Step 6**.

Step 3 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > Spark > **Configurations**, click **All Configurations**, and select **JDBCServer** > **Default**. The default value of **SPARK_DRIVER_MEMORY** is **4G**. If the alarm persists after the parameter value is changed, increase the value by 0.5 times. Double the value if the alarm is reported frequently. In the case of large service volume and high service concurrency, you are advised to add instances.

Step 4 Restart all JDBCServer instances.

Step 5 Check whether the alarm is cleared 10 minutes later.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault Information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **Spark** for the target cluster.

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.315 ALM-43017 JDBCServer Process Full GC Times Exceeds the Threshold

Alarm Description

The system checks the number of JDBCServer Full GC times every 60 seconds. A critical alarm is reported when the number exceeds 12 for three consecutive times. A major alarm is reported when the number exceeds 12 x 0.8 (rounded down) for three consecutive times. You can change the threshold by choosing **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Spark** > **GC Number** > **Full GC Number of JDBCServer**. This alarm is cleared when the Full GC times of the JDBCServer process is less than or equal to the threshold. This alarm is cleared when the Full GC times of the JDBCServer process is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43017	Major (default threshold: 9 for three consecutive times) Critical (default threshold: 12 for three consecutive times)	Quality of service	Tenant plane	Spark	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

If the full GC times exceeds the threshold, the performance of the JDBCServer process deteriorates, and the process can even be unavailable. As a result, Spark JDBC tasks are slow or fail to run.

Possible Causes

The heap memory of the JDBCServer process is overused or inappropriately allocated, causing frequent occurrence of the full GC process.

Handling Procedure

Check the Full GC times.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** and select the alarm whose ID is **43017**. Check the role name and the IP address of the host where the alarm is generated in **Location**.

Step 2 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Spark** > **Instance** and click the JDBCServer for which the alarm is generated to enter the **Dashboard** page. Click the drop-down menu in the chart area and choose **Customize** > **Full GC Number of JDBCServer** from the drop-down list box in the upper right corner and click **OK** to check whether the full GC times is larger than the threshold (default value: 12).

- If yes, go to **Step 3**.
- If no, go to **Step 6**.

Step 3 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Spark** > **Configurations** > **All Configurations** > **JDBCServer** > **Performance**. The default value of the **SPARK_DRIVER_MEMORY** is 4 GB. You can increase the value by 0.5 times if this alarm is generated occasionally. Double the value if the alarm is reported frequently. In the case of large service volume and high service concurrency, you are advised to add instances.

Step 4 Restart all JDBCServer instances.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 5 Check whether the alarm is cleared 10 minutes later.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **Spark** for the target cluster.

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.316 ALM-43018 JobHistory Process Full GC Times Exceeds the Threshold

Alarm Description

The system checks the number of JobHistory Full GC times every 60 seconds. A major alarm is reported when the number exceeds 12 for three consecutive times. A minor alarm is reported when the number exceeds 12 x 0.8 (rounded down) for three consecutive times. You can change the threshold by choosing **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Spark** > **GC Number** > **Full GC Number of JobHistory**. This alarm is cleared when the Full GC times of the process is less than or equal to the threshold. This alarm is cleared when the Full GC times of the JobHistory process is less than or equal to the threshold.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43018	Minor (default threshold: 9 for three consecutive times) Major (default threshold: 12 for three consecutive times)	Quality of service	Tenant plane	Spark	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

The process performance deteriorates, and the process can even be unavailable. Historical execution records of Spark tasks cannot be queried.

Possible Causes

The heap memory of the JobHistory process is overused or inappropriately allocated, causing frequent occurrence of the full GC process.

Handling Procedure

Check the Full GC times.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** and select the alarm whose ID is **43018**. Check the role name and the IP address of the host where the alarm is generated in **Location**.

Step 2 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Spark** > **Instance** and click the JobHistory for which the alarm is generated to enter the **Dashboard** page. Click the drop-down menu in the chart area and choose **Customize** > **Full GC Number of JobHistory** from the drop-down list box in the upper right corner and click **OK** to check whether the full GC times is larger than the threshold (default value: 12).

- If yes, go to **Step 3**.
- If no, go to **Step 6**.

Step 3 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Spark** > **Configurations** > **All Configurations** > **JobHistory** > **Default**. The default value of the **SPARK_DAEMON_MEMORY** is 4 GB. You can increase the value by 0.5 times if this alarm is generated occasionally. Double the value if the alarm is reported frequently.

Step 4 Restart all JobHistory instances.

Step 5 Check whether the alarm is cleared 10 minutes later.

- If yes, no further action is required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If no, go to **Step 6**.

Collect fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **Spark** for the target cluster.

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.317 ALM-43019 Heap Memory Usage of the IndexServer Process Exceeds the Threshold

Alarm Description

The system checks the heap memory usage of the IndexServer process every 30 seconds. A major alarm is reported if the usage is greater than 85% but less than 95% of the maximum memory. A critical alarm is reported if the usage is greater than 95% of the maximum memory.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43019	Major (default threshold: 85% of the maximum memory) Critical (default threshold: 95% of the maximum memory.)	Quality of service	Tenant plane	Spark	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

If the heap memory usage of the IndexServer process is too high, the performance deteriorates, and even memory overflow occurs. As a result, the IndexServer process is unavailable, and Carbon tasks with indexing enabled are slow or fail to run.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Possible Causes

The heap memory of the IndexServer process is overused or the heap memory is inappropriately allocated.

Handling Procedure

Check the heap memory usage.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** and select the alarm whose ID is **43019**. Check the role name and the IP address of the host where the alarm is generated in **Location**.

Step 2 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Spark** > **Instance**. Click the IndexServer that reported the alarm to go to the **Dashboard** page. Click the drop-down list in the upper right corner of the chart area, and choose **Customize** > **IndexServer Memory Usage Statistics** > **OK**. Check whether the heap memory used by the process reaches the maximum heap memory threshold (95% by default).

- If the threshold is reached, go to **Step 3**.
- If the threshold is not reached, go to **Step 7**.

Step 3 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Spark** > **Instance**. Click the IndexServer that reported the alarm to go to the **Dashboard** page. Click the drop-down list in the upper right corner of the chart area, and choose **Customize** > **Statistics for the heap memory of the IndexServer process** > **OK**. Based on the alarm generation time, check the values of the used heap memory of the process in the corresponding period and obtain the maximum value.

Step 4 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Spark** > **Configurations** > **All Configurations** > **IndexServer** > **Performance**. The default value of the **SPARK_DRIVER_MEMORY** parameter is 4 GB. You can change the value based on the ratio of the maximum heap memory used by the IndexServer process to the threshold specified by **IndexServer Heap Memory Usage Statistics (IndexServer)** in the alarm period. If the alarm persists after the parameter value is changed, increase the value by 0.5 times. If the alarm is generated frequently, increase the value by one time.

NOTE

On FusionInsight Manager, you can choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Spark** > **Memory** > **IndexServer Heap Memory Usage Statistics (IndexServer)** to view the threshold.

Step 5 Restart all IndexServer instances.

Step 6 Check whether the alarm is cleared 10 minutes later.

- If the alarm is cleared, no further action is required.
- If the alarm is not cleared, go to **Step 7**.

Collect fault information.

Step 7 On FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 8 Expand the **Service** drop-down list, and select **Spark** for the target cluster.

Step 9 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.318 ALM-43020 Non-Heap Memory Usage of the IndexServer Process Exceeds the Threshold

Alarm Description

The system checks the non-heap memory usage of the IndexServer process every 30 seconds. A major alarm is reported if the usage is greater than 85% but less than 95% of the maximum memory. A critical alarm is reported if the usage is greater than 95% of the maximum memory.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43020	Major (default threshold: 85% of the maximum memory) Critical (default threshold: 95% of the maximum memory.)	Quality of service	Tenant plane	Spark	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.

Type	Parameter	Description
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

If the non-heap memory usage of the IndexServer process is too high, the performance deteriorates, and even memory overflow occurs. As a result, the IndexServer process is unavailable, and Carbon tasks with indexing enabled are slow or fail to run.

Possible Causes

The non-heap memory of the IndexServer process is overused or the non-heap memory is inappropriately allocated.

Handling Procedure

Check non-heap memory usage.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** and select the alarm whose ID is **43020**. Check the role name and the IP address of the host where the alarm is generated in **Location**.

Step 2 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Spark** > **Instance**. Click the IndexServer that reported the alarm to go to the **Dashboard** page. Click the drop-down list in the upper right corner of the chart area, and choose **Customize** > **IndexServer Memory Usage Statistics** > **OK**. Check whether the non-heap memory used by the process reaches the maximum non-heap memory threshold (95% by default).

- If the threshold is reached, go to **Step 3**.
- If the threshold is not reached, go to **Step 7**.

Step 3 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Spark** > **Instance**. Click the IndexServer that reported the alarm to go to the **Dashboard** page. Click the drop-down list in the upper right corner of the chart area, and choose **Customize** > **Statistics for the non-heap memory of the IndexServer process** > **OK**. Based on the alarm generation time, check the values of the used non-heap memory of the process in the corresponding period and obtain the maximum value.

Step 4 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Spark** > **Configurations** > **All Configurations** > **IndexServer** > **Performance**. You can change the value of **XX:MaxMetaspaceSize** in the **spark.driver.extraJavaOptions** parameter based on the ratio of the maximum non-heap memory used by the IndexServer process to the threshold specified by **IndexServerNon-Heap Memory Usage Statistics (IndexServer)** in the alarm period.

NOTE

On FusionInsight Manager, you can choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Spark** > **Memory** > **IndexServer Non-Heap Memory Usage Statistics (IndexServer)** to view the threshold.

Step 5 Restart all IndexServer instances.

Step 6 Check whether the alarm is cleared 10 minutes later.

- If the alarm is cleared, no further action is required.
- If the alarm is not cleared, go to **Step 7**.

Collect fault information.

Step 7 On FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 8 Expand the **Service** drop-down list, and select **Spark** for the target cluster.

Step 9 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.319 ALM-43021 Direct Memory Usage of the IndexServer Process Exceeds the Threshold

Alarm Description

The system checks the direct memory usage of the IndexServer process every 30 seconds. A major alarm is reported if the usage is greater than 85% but less than 95% of the maximum memory. A critical alarm is reported if the usage is greater than 95% of the maximum memory.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43021	Major (default threshold: 85% of the maximum memory) Critical (default threshold: 95% of the maximum memory.)	Quality of service	Tenant plane	Spark	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.

Type	Parameter	Description
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

If the direct memory usage of the IndexServer process is too high, the performance deteriorates, and even memory overflow occurs. As a result, the IndexServer process is unavailable, and Carbon tasks with indexing enabled are slow or fail to run.

Possible Causes

The direct memory of the IndexServer process is overused or the direct memory is inappropriately allocated.

Handling Procedure

Check direct memory usage.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** and select the alarm whose ID is **43021**. Check the role name and the IP address of the host where the alarm is generated in **Location**.

Step 2 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Spark** > **Instance**. Click the IndexServer that reported the alarm to go to the **Dashboard** page. Click the drop-down list in the upper right corner of the chart area, and choose **Customize** > **IndexServer Memory Usage Statistics** > **OK**. Check whether the direct memory used by the process reaches the maximum direct memory threshold.

- If the threshold is reached, go to **Step 3**.
- If the threshold is not reached, go to **Step 7**.

Step 3 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Spark2x** > **Instance**. Click the IndexServer that reported the alarm to go to the **Dashboard** page. Click the drop-down list in the upper right corner of the chart area, and choose **Customize** > **Memory** > **Direct Memory of IndexServer** > **OK**. Based on the alarm generation time, check the values of the used direct memory of the process in the corresponding period and obtain the maximum value.

Step 4 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Spark** > **Configurations** > **All Configurations** > **IndexServer** > **Performance**. You can change the value of **XX:MaxDirectMemorySize** (the default value is 512 MB) in the **spark.driver.extraJavaOptions** parameter based on the ratio of the maximum direct memory used by the IndexServer process to the threshold specified by **IndexServer Direct Memory Usage Statistics (IndexServer)** in the alarm period. If the alarm persists after the parameter value is changed, increase the value by 0.5 times. If the alarm is generated frequently, increase the value by one time.

NOTE

On FusionInsight Manager, you can choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Spark** > **Memory** > **IndexServer Non-Heap Memory Usage Statistics (IndexServer)** to view the threshold.

Step 5 Restart all IndexServer instances.

Step 6 Check whether the alarm is cleared 10 minutes later.

- If the alarm is cleared, no further action is required.
- If the alarm is not cleared, go to **Step 7**.

Collect fault information.

Step 7 On FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 8 Expand the **Service** drop-down list, and select **Spark** for the target cluster.

Step 9 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.320 ALM-43022 IndexServer Process GC Time Exceeds the Threshold

Alarm Description

The system checks the GC duration of IndexServer every 60 seconds. A critical alarm is reported when the GC duration exceeds 12 seconds for three consecutive times. A major alarm is reported when the duration exceeds 12 x 0.8 seconds for three consecutive times. To change the threshold, choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Spark** > **GC Time** > **IndexServer Total GC time**. This alarm is cleared when the IndexServer GC duration is shorter than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43022	Major (default threshold: 9.6 seconds for three consecutive times) Critical (default threshold: 12 seconds for three consecutive times)	Quality of service	Tenant plane	Spark	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

If the GC duration exceeds the threshold, the performance of the IndexServer process deteriorates, and the process can even be unavailable. As a result, Carbon tasks with indexing enabled are slow or fail to run.

Possible Causes

The heap memory of the IndexServer process is overused or inappropriately allocated, causing frequent occurrence of the GC process.

Handling Procedure

Check the GC time.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** and select the alarm whose ID is **43022**. Check the role name and the IP address of the host where the alarm is generated in **Location**.

Step 2 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Spark** > **Instance** and click the IndexServer for which the alarm is generated to enter the **Dashboard** page. Click the drop-down menu in the Chart area and choose **Customize** > **GC Time** > **Garbage Collection (GC) Time of IndexServer** from the drop-down list box in the upper right corner and click **OK** to check whether the GC time is longer than the threshold (default value: 12 seconds).

- If the threshold is reached, go to **Step 3**.
- If the threshold is not reached, go to **Step 6**.

Step 3 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Spark** > **Configurations** > **All Configurations** > **IndexServer** > **Default**. The default value of the **SPARK_DRIVER_MEMORY** is 4 GB. You can increase the value 1.5 times to its default. If this alarm is still generated occasionally after the adjustment, increase the value by 0.5 times. Double the value if the alarm is reported frequently.

Step 4 Restart all IndexServer instances.

Step 5 Check whether the alarm is cleared 10 minutes later.

- If the alarm is cleared, no further action is required.
- If the alarm is not cleared, go to **Step 6**.

Collect fault information.

Step 6 On FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **Spark** for the target cluster.

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.321 ALM-43023 IndexServer Process Full GC Number Exceeds the Threshold

Alarm Description

The system checks the number of IndexServer Full GC times every 60 seconds. A critical alarm is reported when the number exceeds 12 for three consecutive times.

A major alarm is reported when the number exceeds 12 x 0.8 (rounded down) for three consecutive times. You can change the threshold by choosing **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Spark** > **GC Number** > **Full GC Number of IndexServer**. This alarm is cleared when the Full GC times of the JDBCServer process is less than or equal to the threshold. This alarm is cleared when the Full GC times of the IndexServer process is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43023	Minor (default threshold: 9 for three consecutive times) Critical (default threshold: 12 for three consecutive times)	Quality of service	Tenant plane	Spark	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

If the GC times exceeds the threshold, the performance of the IndexServer process deteriorates, and the process can even be unavailable. As a result, Carbon tasks with indexing enabled are slow or fail to run.

Possible Causes

The heap memory of the IndexServer process is overused or inappropriately allocated, causing frequent occurrence of the full GC process.

Handling Procedure

Check the number of Full GCs.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** and select the alarm whose ID is **43023**. Check the role name and the IP address of the host where the alarm is generated in **Location**.

Step 2 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Spark** > **Instance** and click the IndexServer for which the alarm is generated to enter the **Dashboard** page. Click the drop-down menu in the chart area and choose **Customize** > **Full GC Number of IndexServer** from the drop-down list box in the upper right corner and click **OK** to check whether the full GC times is larger than the threshold (default value: 12).

- If the threshold is reached, go to **Step 3**.
- If the threshold is not reached, go to **Step 6**.

Step 3 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Spark** > **Configurations** > **All Configurations** > **IndexServer** > **Performance**. The default value of the **SPARK_DRIVER_MEMORY** is 4 GB. You can increase the value by 0.5 times if this alarm is generated occasionally. Double the value if the alarm is reported frequently. In the case of large service volume and high service concurrency, you are advised to add instances.

Step 4 Restart all IndexServer instances.

Step 5 Check whether the alarm is cleared 10 minutes later.

- If the alarm is cleared, no further action is required.
- If the alarm is not cleared, go to **Step 6**.

Collect fault information.

Step 6 On FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **Spark** for the target cluster.

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.322 ALM-43028 JDBCServer Process Session Overload

Alarm Description

This alarm is generated when the JDBCServer process forwards requests and triffic control is triggered due to insufficient session resources. In this case, too many requests are sent to the JDBCServer process, exceeding the processing capability of the JDBCServer process.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43028	Minor (default threshold: 9 for three consecutive times) Critical (default threshold: 12 for three consecutive times)	Quality of service	Tenant plane	Spark	No

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	Alarm Severity	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

Requests that cannot be processed are responded with a failure message.

Possible Causes

The JDBCServer process on the node is overloaded.

Handling Procedure

Check the source of the requests for connecting to the JDBCServer service.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** and select the alarm whose ID is **43028**. Check the role name and the IP address of the host where the alarm is generated in **Location**.

Step 2 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Spark** > **Instances**, click the JDBCServer for which this alarm is generated, and click **dbcserver-audit** in the **Log** column on the left.

Step 3 Click the download button in the lower left corner to download the logs to the local PC.

Step 4 Search for **UserIP** in the logs, collect statistics on the IP addresses of the clients that submit a large number of requests, and limit the traffic of these clients to reserve resources for other clients.

Collect fault information.

Step 5 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 6 Expand the **Service** drop-down list, and select **Spark** for the target cluster.

Step 7 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 8 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm needs to be cleared manually.

Related Information

None.

1.3.323 ALM-43200 Elasticsearch Service Unavailable

Alarm Description

The system checks the Elasticsearch service availability every 60 seconds. This alarm is generated when the system detects that the Elasticsearch service is unavailable. This alarm is cleared when the Elasticsearch service recovers.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43200	Critical	Quality of service	Tenant plane	Elasticsearch	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

The Elasticsearch service is unavailable, and index data cannot be read or written.

Possible Causes

- The network connection is abnormal.
- The component service that Elasticsearch depends on is not available.
- The EsMaster instance is abnormal.

Handling Procedure

Check whether the network is normal.

Step 1 Click **Cluster** > *Name of the desired cluster* > **Services** > **Elasticsearch** > **Instance** on the FusionInsight Manager to view the service plane IP address of the EsMaster instance.

Step 2 Log in to the server where any EsMaster instance resides as user **root**.

Step 3 Run the **ping** *IP address of other EsMaster instance* command to check whether the servers of other EsMaster instances are reachable.

- If yes, go to **Step 6**.
- If no, go to **Step 4**.

Step 4 Contact the system administrator to rectify network faults.

Step 5 Check whether the alarm is cleared from the alarm list.

- If yes, no further action is required.
- If no, go to **Step 6**.

Check Server that Elasticsearch depends on is normal.

Step 6 Choose **Cluster** > *Name of the desired cluster* > **Services** > **ZooKeeper** to check whether the health of the ZooKeeper service is normal. And check if can connect to ZooKeeper service. Specific operations can refer to the ZooKeeper operating documentation. And if the cluster is in the security mode, check the KrbServer running state is normal.

- If yes, go to **Step 8**.
- If no, please repair the failed service to make sure the service is normal.

Step 7 Check whether the alarm is cleared from the alarm list.

- If yes, no further action is required.
- If no, go to **Step 8**.

Check whether EsMaster instances are running properly.

Step 8 Choose **Cluster** > *Name of the desired cluster* > **Services** > **Elasticsearch** > **Instance** to check whether EsMaster instances are healthy.

- If yes, no further action is required.
- If no, go to **Step 9**.

Step 9 Locate the EsMaster instance whose **Running Status** is not **Normal** and choose **More** > **Restart Instance** to restart instance.

NOTE

You need to enter the administrator password for FusionInsight Manager to restart an instance.

Step 10 Check whether the alarm is cleared from the alarm list.

- If yes, no further action is required.
- If no, go to **Step 11**.

Collect fault information.

Step 11 On the FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 12 Select **Elasticsearch** in the required cluster from the **Service** list.

Step 13 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 14 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.324 ALM-43201 Heap Memory Usage of Elasticsearch Exceeds the Threshold

Alarm Description

The system checks the elasticsearch heap memory usage every 60 seconds. This alarm is generated when the heap memory usage exceeds the threshold.

When the number of smoothing times is 1, this alarm is cleared when the elasticsearch heap memory usage is less than or equal to the threshold.When the number of smoothing times is greater than 1, this alarm is cleared when the elasticsearch heap memory usage is less than or equal to 90% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43201	Major (default threshold: 90%) Critical (default threshold: 95%)	Quality of service	Tenant plane	Elasticsearch	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

If the Elasticsearch heap memory usage is too high, the read and write performance of Elasticsearch index data may be affected. In serious cases, the process may restart.

Possible Causes

Elasticsearch memory is insufficient.

Handling Procedure

Delete invalid indexes.

Step 1 Check whether the Elasticsearch cluster is in the security mode.

Specifically, on FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Elasticsearch**. On the displayed page, click **Configurations**. Search for **ELASTICSEARCH_SECURITY_ENABLE**, and check whether the parameter can be queried and its value is **true**.

- If yes, go to **Step 2**.
- If no, go to **Step 3**.

Step 2 If the security mode is used, configure the permission for running the curl command.

For details, see section "Preparing the Environment" in "Curl Command Usage for Linux" in *MapReduce Service (MRS) 3.3.1-LTS User Guide (for Huawei Cloud Stack*

8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Usage Guide (for Huawei Cloud Stack 8.3.1).

Step 3 Log in to a host where Elasticsearch resides as user **root**.

Step 4 Run the **curl -XGET --tlsv1.2 --negotiate -k -v -u : 'https://***ip:httpport***/_cat/indices?v'** command to query the index details in the current cluster.

NOTE

- In this command, replace **ip** with the IP address of any node in the cluster.
- Replace **httpport** with the HTTP port number of the Elasticsearch instance, which is specified by **SERVER_PORT**. To obtain the parameter value, on FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Elasticsearch**. On the displayed page, choose **Configurations** > **All Configurations** and search for **SERVER_PORT**.
- In common mode, delete the security authentication parameter **--tlsv1.2 --negotiate -k -v -u**, and change **https** to **http**.
- These rules also apply to the following curl commands.

Step 5 Run the **curl -XDELETE --tlsv1.2 --negotiate -k -v -u : 'https://***ip:httpport***/***indexname***'** command to delete unnecessary indexes.

NOTE

Deleting a file or folder is a high-risk operation. Ensure that the file or folder is no longer required before performing this operation.

Check the JVM memory usage and adjust system configurations.

Step 6 On the FusionInsight Manager portal, choose **Cluster** >*Name of the desired cluster* > **Services** > **Elasticsearch** > **Configurations > All Configurations.**

Step 7 In the upper right corner of the Configuration page, enter **GC_OPTS** in the search box and click . The **GC_OPTS** parameters of all instances are displayed.

Step 8 Select the instance whose **GC_OPTS** value needs to be changed, and check whether the differentiated configuration icon is displayed after the instance value configuration box.

- If yes, go to **Step 9**.
- If no, go to **Step 10**.

Step 9 Click . In the displayed dialog box, click in the right pane and click **OK** to save the settings.

Step 10 Adjust the values of **-Xms** and **-Xmx** of the **GC_OPTS** parameter by referring to the Note.

NOTE

Suggestions on configuring the GC parameter of Elasticsearch:

- It is recommended that 50% memory be reserved for the Lucence cache and 50% memory for Solr. You are advised to allocate 30 GB (no more than 31 GB) to machines with large memory. Confirm that the JVM Compressed Oops function has been enabled. You can run the following command to check:

  java -server -Xms28G -Xmx28G -XX:+UseConcMarkSweepGC -XX:+UnlockDiagnosticVMOptions -XX:+PrintCompressedOopsMode -version

  If the returned value for Compressed Oops mode is Zero based, it indicates that the JVM Compressed Oops function is enabled and you need to increase the size of the allocated memory. Change 28 GB to 29 GB and check whether the Compressed Oops function is enabled. Try until the allocated memory reaches the maximum for the Compressed Oops function to remain enabled.

  If the returned value for Compressed Oops mode is Non-zero based, it indicates that the JVM Compressed Oops function is disabled and you need to decrease the size of the allocated memory. Change 28 GB to 27 GB and check whether the Compressed Oops function is enabled. Try until the allocated memory reaches the maximum for the Compressed Oops function to remain enabled.
- It is recommended that **-Xms** and **-Xmx** be set to the same value to prevent dynamic adjustment of heap memory size by JVM from affecting the performance.
- If half of the computer memory is less than the number of instances multiplied by 30 GB, allocate the memory by referring to the following:

  Instance memory = (Computer memory x 0.5)/Number of instances on the computer

  For example, if a computer has a memory of 128 GB and has three Elasticsearch instances, the value of **GC_OPTS** is: 128 GB x 0.5/3 = 21 GB and confirm that the JVM Compressed Oops function has been enabled.

Step 11 Modify Elasticsearch memory parameters and click **Save** and **OK**.

Step 12 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Elasticsearch**. On the displayed page, click **Instance**, select the instances whose **Configuration Status** is **Expired**, and restart the instances.

Step 13 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 14**.

Collect fault information.

Step 14 On the FusionInsight Manager, choose **O&M** > **Log > Download**.

Step 15 Select **Elasticsearch** in the required cluster from the **Service** list.

Step 16 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 17 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.325 ALM-43202 Indices in the Yellow State Exist in Elasticsearch

Alarm Description

The system checks all indices status of all Elasticsearch every 60 seconds. This alarm is generated when an index is in the Yellow state.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43202	Major	Quality of service	Tenant plane	Elasticsearch	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
Modify	3.3.1	Alarm Severity: changed from Minor to Major.	Alarm Severity: Accuracy optimized

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	List of indices in the yellow state	Specifies the list of indices in yellow state in Elasticsearch.

NOTE

The length of the index list is restricted by the character length. When the content exceeds 256 characters, only some index names can be displayed. To query the complete index list, perform the following steps:

On the FusionInsight Manager homepage, choose **O&M** > **Log** > **Online Search**. Enter "alarm 43202" in the **Search Content** text box. Then, select **OMS** > **Agent** for **Service**, the **pluginmonitor** file for **File**, and **ERROR** for **Lowest Log Level**. After the configuration, click **Search**.

Select the latest log in the search result and view the complete list of indices in yellow state. For example:

```
2020-04-01 05:05:00,550 ERROR [monitor_300_1_6_EsMaster] Send alarm 43202. The Elasticsearch cluster has
indexes in the Yellow state, List of indexes in the Yellow state is [post_20200328, log_20200331]
com.huawei.hadoop.elasticsearch.monitor.collector.impl.ReplicaNumCollector.sendDownStateShardAlarm(ReplicaNum
Collector.java:182)
```

Impact on the System

The replicai shards of some Elasticsearch indexes are faulty, which may slow down the read/write performance of Elasticsearch index data.

Possible Causes

The replica shards of some Elasticsearch instances are not allocated.

Handling Procedure

Check whether all instances are normal.

Step 1 Choose **Cluster** > *Name of the desired cluster* > **Services** > **Elasticsearch** > **Instance** page, check whether all instances are in normal state.

- If yes, go to **Step 4**.
- If no, go to **Step 2**.

Step 2 Select instances whose **Running Status** is not **Normal**. Choose **Restart Instance** from the drop-down list of **More**.

NOTE

When restarting the instance, you need enter the password of the FusionInsight Manager administrator.

Step 3 Check whether the alarm is cleared from the alarm list.

- If yes, no further action is required.
- If yes, go to **Step 4**.

Step 4 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Elasticsearch**. Click **Resource**. On the displayed page, check indexes with **Health Status** set to **yellow** in the **Index Information** area. Record the index names and number of replicas.

Step 5 Check whether the Elasticsearch cluster is in the security mode.

Specifically, on FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Elasticsearch**. On the displayed page, click **Configurations**. Search for **ELASTICSEARCH_SECURITY_ENABLE**, and check whether the parameter can be queried and its value is **true**.

- If yes, go to **Step 6**.
- If no, go to **Step 7**.

Step 6 If the security mode is used, configure the permission for running the curl command.

For details, see section "Preparing the Environment" in "Curl Command Usage for Linux" in *MapReduce Service (MRS) 3.3.1-LTS User Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Usage Guide (for Huawei Cloud Stack 8.3.1)*.

Step 7 Run the curl command to set the replica number.

curl -XPUT --tlsv1.2 --negotiate -k -v -u : 'https://*ip:httpport/index/***_settings' -H 'Content-Type: application/json' -d'{"number_of_replicas": "0"}'**

NOTE

- ip: The IP address of any node in the Elasticsearch cluster.
- httpport: The HTTP port number of the Elasticsearch instance, which is specified by **SERVER_PORT**. To obtain the parameter value, on FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Elasticsearch**. On the displayed page, choose **Configurations** > **All Configurations** and search for **SERVER_PORT**.
- index: Name of the index for which the number of copies needs to be reset.
- In common mode, delete the security authentication parameter **--tlsv1.2 --negotiate -k -v -u**, and change **https** to **http**.
- These rules also apply to the following curl commands.

Step 8 10 minutes later, check whether the alarm is cleared.

- If yes, go to **Step 9**.
- If no, go to **Step 10**.

Step 9 Run the curl command to set the replica number to the original value. 10 minutes later, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 10**.

Collect fault information.

Step 10 On the FusionInsight Manager choose **O&M** > **Log > Download**.

Step 11 Select **Elasticsearch** in the required cluster from the **Service** list.

Step 12 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 13 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.326 ALM-43203 Indices in the Red State Exist in Elasticsearch

Alarm Description

The system checks all indices status of all Elasticsearch every 60 seconds. This alarm is generated when an index is in the Red state.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43203	Critical	Quality of service	Tenant plane	Elasticsearch	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
Modify	3.3.1	Alarm Severity: changed from Major to Critical.	Alarm Severity: Accuracy optimized

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	List of indices in the red state	Specifies the list of indices in red state in Elasticsearch.

NOTE

The length of the index list is restricted by the character length. When the content exceeds 256 characters, only some index names can be displayed. To query the complete index list, perform the following steps:

1. On the FusionInsight Manager homepage, choose **O&M** > **Log** > **Online Search**.
2. Enter "alarm 43203" in the **Search Content** text box. Then, select **OMS** > **Agent** for **Service**, the **pluginmonitor** file for **File**, and **ERROR** for **Lowest Log Level**. After the configuration, click **Search**.
3. Select the latest log in the search result and view the complete list of indices in red state. For example:
   2020-07-10 14:34:00,508 ERROR [monitor_60_1_18_EsMaster] Send alarm 43203. The Elasticsearch cluster has indexes in the Red state, List of indexes in the Red state is [**myindex292,myindex200**]

Impact on the System

The primary shards of some Elasticsearch indexes are faulty, and the faulty indexes cannot be read or written.

Possible Causes

The primary shard of Elasticsearch is missing.

Handling Procedure

Check whether all the instances are normal.

Step 1 Specifically, log in to FusionInsight Manager, and choose **Cluster** > *Name of the desired cluster* > **Services** > **Elasticsearch**. On the displayed page, click **Instance** and check whether all instances are in normal state.

- If yes, go to **Step 4**.
- If no, go to **Step 2**.

Step 2 Select instances whose running status is not **Normal** and choose **Restart Instance** from the drop-down list of **More**.

NOTE

When restarting the instance, you need enter the password of the FusionInsight Manager administrator.

Step 3 Check whether the alarm is cleared from the alarm list.

- If yes, no further action is required.
- If yes, go to **Step 4**.

Step 4 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Elasticsearch**.

Step 5 Click **Resource**. On the displayed page, check indexes with **Health Status** set to **red** in the **Index Information** area.

Step 6 Check whether the index is an invalid index.

- If yes, go to **Step 7**.
- If no, go to **Step 11**.

Step 7 Check whether the Elasticsearch cluster is in the security mode.

Specifically, on FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Elasticsearch**. On the displayed page, click **Configurations**. Search for **ELASTICSEARCH_SECURITY_ENABLE**, and check whether the parameter can be queried and its value is **true**.

- If yes, go to **Step 8**.
- If no, go to **Step 9**.

Step 8 If the security mode is used, configure the permission for running the curl command.

For details, see section "Preparing the Environment" in "Curl Command Usage for Linux" in *MapReduce Service (MRS) 3.3.1-LTS User Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Usage Guide (for Huawei Cloud Stack 8.3.1)*.

Step 9 Delete the invalid index.

curl -XDELETE --tlsv1.2 --negotiate -k -v -u : 'https://*ip:httpport***/** *index name*'

NOTE

- In this command, replace **ip** with the IP address of any node in the cluster.
- Replace **httpport** with the HTTP port number of the Elasticsearch instance, which is specified by **SERVER_PORT**. To obtain the parameter value, on FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Elasticsearch**. On the displayed page, choose **Configurations** > **All Configurations** and search for **SERVER_PORT**.
- Replace **index name** with the name of the index to be deleted.
- In common mode, delete the security authentication parameter **--tlsv1.2 --negotiate -k -v -u**, and change **https** to **http**.
- Deleting a file or folder is a high-risk operation. Ensure that the file or folder is no longer required before performing this operation.

Step 10 5 minutes later, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 11**.

Collect fault information.

Step 11 On the FusionInsight Manager, choose **O&M**> **Log** > **Download**.

Step 12 Select **Elasticsearch** in the required cluster from the **Service** list.

Step 13 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 14 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.327 ALM-43204 GC Duration of the Elasticsearch Process Exceeds the Threshold

Alarm Description

The system checks the garbage collection (GC) duration of the Elasticsearch process every 60s. This alarm is generated when the GC duration exceeds the threshold.

If **Trigger Count** is set to **1**, and the GC duration of the Elasticsearch process is less than or equal to the threshold, this alarm is cleared. If **Trigger Count** is greater than **1**, and the GC duration of the Elasticsearch process is less than or equal to 90% of the threshold, this alarm is cleared.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43204	Major (default threshold: 30000ms) Critical (default threshold: 60000ms)	Quality of service	Tenant plane	Elasticsearch	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

If the GC time of the Elasticsearch instance process is too long, the index data read/write performance of Elasticsearch may be affected, and the request may time out.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Possible Causes

Service load of the Elasticsearch instance on the node is high or the heap memory is not properly configured. As a result, GC frequently occurs.

Handling Procedure

Check the configured heap memory.

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm > Alarms**, and check the location information of this alarm. Check the IP address of the instance for which the alarm is generated.

Step 2 On the FusionInsight Manager home page, choose **Cluster** > *Name of the desired cluster* > **Services** > **Elasticsearch**. On the displayed page, click **Instance** and Click the drop-down menu in the Chart area and choose **Customize** > **Clear All** > **Garbage Collection** > **EsMaster GC Time Stats**, and click **OK**. Check whether the GC duration is greater than the threshold.

Step 3 Choose **Cluster** > *Name of the desired cluster* > **Services** > **Elasticsearch**. On the displayed page, click **Configurations**.

Step 4 In the upper right corner of the Configuration page, enter GC_OPTS in the search box and click . The GC_OPTS parameter values of all instances are displayed.

Step 5 Select the instance whose GC_OPTS value needs to be changed, and check whether the differentiated configuration icon is displayed after the instance value configuration box.

- If yes, go to **Step 6**.
- If no, go to **Step 7**.

Step 6 Click . In the displayed dialog box, click in the right pane and click **OK** to save the settings.

Step 7 Adjust the values of **-Xms** and **-Xmx** of the **GC_OPTS** parameter by referring to the Note.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

NOTE

Suggestions on configuring the GC parameter of Elasticsearch:

- It is recommended that 50% memory be reserved for the Lucence cache and 50% memory for Solr. You are advised to allocate 30 GB (no more than 31 GB) to machines with large memory. Confirm that the JVM Compressed Oops function has been enabled. You can run the following command to check:

  java -server -Xms28G -Xmx28G -XX:+UseConcMarkSweepGC -XX:+UnlockDiagnosticVMOptions -XX:+PrintCompressedOopsMode -version

  If the returned value for Compressed Oops mode is Zero based, it indicates that the JVM Compressed Oops function is enabled and you need to increase the size of the allocated memory. Change 28 GB to 29 GB and check whether the Compressed Oops function is enabled. Try until the allocated memory reaches the maximum for the Compressed Oops function to remain enabled.

  If the returned value for Compressed Oops mode is Non-zero based, it indicates that the JVM Compressed Oops function is disabled and you need to decrease the size of the allocated memory. Change 28 GB to 27 GB and check whether the Compressed Oops function is enabled. Try until the allocated memory reaches the maximum for the Compressed Oops function to remain enabled.
- It is recommended that **-Xms** and **-Xmx** be set to the same value to prevent dynamic adjustment of heap memory size by JVM from affecting the performance.
- If half of the computer memory is less than the number of instances multiplied by 30 GB, allocate the memory by referring to the following:

  Instance memory = (Computer memory x 0.5)/Number of instances on the computer

  For example, if a computer has a memory of 128 GB and has three Elasticsearch instances, the value of **GC_OPTS** is: 128 GB x 0.5/3 = 21 GB, and Confirm that the JVM Compressed Oops function has been enabled.

Step 8 After the modification, click **Save** in the upper left corner. In the **Save Configuration** dialog box displayed, click **OK**.

Step 9 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Elasticsearch**. On the displayed page, click **Instance**, select the instances whose **Configuration Status** is **Expired**, and restart the instances.

Step 10 Five minutes later, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 11**.

Collect fault information.

Step 11 On FusionInsight Manager, and choose **O&M** > **Log** > **Download**.

Step 12 Select **Elasticsearch** in the required cluster for **Service**.

Step 13 Click in the upper right corner. In the displayed dialog box, set **Start Date** and **End Date** to 10 minutes before and after the alarm generation time respectively and click **OK**. Then, click **Download**.

Step 14 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.328 ALM-43205 Elasticsearch Stored Shard Data Volume Exceeds the Threshold

Alarm Description

The system checks the volume of shard data stored in Elasticsearch every 60 seconds and compares the volume with the threshold. This alarm is generated when the system detects that the volume exceeds the threshold for multiple consecutive times (three times by default).

The threshold can be changed by choosing **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Elasticsearch** > **Shard** > **Elasticsearch Shard Data Volume (EsMaster)**.

If **Trigger Count** is set to **1**, and the volume of shard data stored in Elasticsearch is less than or equal to the threshold, this alarm is cleared. If **Trigger Count** is greater than **1**, and the volume of shard data stored in Elasticsearch is less than or equal to 90% of the threshold, this alarm is cleared.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43205	Major (default threshold: 41943040KB) Critical (default threshold: 83886080KB)	Quality of service	Tenant plane	Elasticsearch	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

A large amount of data is stored in Elasticsearch shards, which may slow down the read and write performance of Elasticsearch index data. When the Elasticsearch process is restarted, the restoration of a large amount of data slows down.

Possible Causes

The number of index shards is incorrectly configured. As a result, the stored shard data volume exceeds the threshold.

Handling Procedure

Check the stored shard data volume

Step 1 Check whether the Elasticsearch cluster is in the security mode.

Specifically, on FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Elasticsearch**. On the displayed page, click **Configurations**. In the upper right corner of the configuration page, search for **ELASTICSEARCH_SECURITY_ENABLE** and check whether the parameter can be queried and its value is **true**.

- If yes, go to **Step 2**.
- If no, go to **Step 3**.

Step 2 If the security mode is used, configure the permission for running the **curl** command.

For details, see section "Preparing the Environment" in "Curl Command Usage for Linux" in *MapReduce Service (MRS) 3.3.1-LTS User Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Usage Guide (for Huawei Cloud Stack 8.3.1)*.

Step 3 Log in to any node where Elasticsearch resides as user **root**.

Step 4 Run the following command to query the stored shard data volume of the current cluster: **curl -XGET --tlsv1.2 --negotiate -k -v -u : 'https://***ip:httpport***/_cat/shards?v&s=store:desc'**

NOTE

- In this command, replace **ip** with the IP address of any node in the cluster.
- Replace **httpport** with the HTTP port number of the Elasticsearch instance, which is specified by **SERVER_PORT**. To obtain the parameter value, on FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Elasticsearch**. On the displayed page, choose **Configurations** > **All Configurations** and search for **SERVER_PORT**.
- In normal mode, delete the security authentication parameter **--tlsv1.2 --negotiate -k -v -u:** and change **https** to **http**.

Step 5 Obtain the index with a large amount of shard data. You are advised to plan the index again as follows:

- Method 1: Stop writing data to the index and plan a new index to store the written data.
- Method 2: Migrate data in the index in which stored shard data volume exceeds the threshold to the planned new index, and delete the old index.

NOTE

Deleting a file or folder is a high-risk operation. Ensure that the file or folder is no longer required before performing this operation.

Step 6 After the index planning is complete, Five minutes after the index planning is complete, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect fault information.

Step 7 On FusionInsight Manager, and choose **O&M** > **Log** > **Download**.

Step 8 Select **Elasticsearch** in the required cluster for **Service**.

Step 9 Click in the upper right corner. In the displayed dialog box, set **Start Date** and **End Date** to 10 minutes before and after the alarm generation time respectively and click **OK**. Then, click **Download**.

Step 10 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.329 ALM-43206 Elasticsearch Shard Document Number Exceeds the Threshold

Alarm Description

The system checks the number of documents in Elasticsearch shards every 60 seconds and compares the number with the threshold. This alarm is generated when the system detects that the number exceeds the threshold for multiple consecutive times (three times by default).

The threshold can be changed by choosing **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Elasticsearch** > **Shard** > **Elasticsearch Shard Document Number (EsMaster)**.

If **Trigger Count** is set to **1**, and the number of documents in Elasticsearch shards is less than or equal to the threshold, this alarm is cleared. If **Trigger Count** is greater than **1**, and the number of documents in Elasticsearch shards is less than or equal to 90% of the threshold, this alarm is cleared.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43206	Major (default threshold: 100000000) Critical (default threshold: 150000000)	Quality of service	Tenant plane	Elasticsearch	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

If the number of Elasticsearch shard documents is too large, the read and write performance of Elasticsearch index data may be affected. When the Elasticsearch process is restarted, the restoration speed of shards with a large amount of data may be slow.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Possible Causes

The configuration of Elasticsearch index shard number is inappropriate.

Handling Procedure

Check the number of documents in shards.

Step 1 Check whether the Elasticsearch cluster is in the security mode.

Specifically, on FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Elasticsearch**. On the displayed page, click **Configurations**. Search for **ELASTICSEARCH_SECURITY_ENABLE**, and check whether the parameter can be queried and its value is **true**.

- If yes, go to **Step 2**.
- If no, go to **Step 3**.

Step 2 If the security mode is used, configure the permission for running the **curl** command.

For details, see section "Preparing the Environment" in "Curl Command Usage for Linux" in *MapReduce Service (MRS) 3.3.1-LTS User Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Usage Guide (for Huawei Cloud Stack 8.3.1)*.

Step 3 Log in to any node where Elasticsearch resides as user **root**.

Step 4 Run the following command to query the stored shard documents volume of the current cluster: **curl -XGET --tlsv1.2 --negotiate -k -v -u : 'https://*ip:httpport*/_cat/shards?v&s=docs:desc'**

NOTE

- In this command, replace **ip** with the IP address of any node in the cluster.
- Replace **httpport** with the HTTP port number of the Elasticsearch instance, which is specified by **SERVER_PORT**. To obtain the parameter value, on FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Elasticsearch**. On the displayed page, choose **Configurations** > **All Configurations** and search for **SERVER_PORT**.
- In normal mode, delete the security authentication parameter **--tlsv1.2 --negotiate -k -v -u :**, and change **https** to **http**.

Step 5 Obtain the indexes with a large number of shard documents and plan the index again as follows:

- Method 1: Stop writing data to the index and plan a new index to store the written data.
- Method 2: Migrate the data in the index whose number of shard documents exceeds the threshold to the planned index, and delete the old index.

NOTE

Deleting a file or folder is a high-risk operation. Ensure that the file or folder is no longer required before performing this operation.

Step 6 After the index planning is complete, Five minutes after the index planning is complete, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect fault information.

Step 7 On FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 8 Select **Elasticsearch** in the required cluster for **Service**.

Step 9 Click in the upper right corner. In the displayed dialog box, set **Start Date** and **End Date** to 10 minutes before and after the alarm generation time respectively and click **OK**. Then, click **Download**.

Step 10 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.330 ALM-43207 Elasticsearch Has Indexes Without Replicas

Alarm Description

The system checks whether there are indexes without replicas in Elasticsearch every 10 minutes. This alarm is generated when there are.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43207	Major	Quality of service	Tenant plane	Elasticsearch	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
Modify	3.3.1	Clearance Rules: changed from manual clearance to automatic clearance.	Clearance Rules: Optimized

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Index List	Specifies the index list without replicas.

Impact on the System

Some index data of Elasticsearch has only one copy, which affects the data reliability of Elasticsearch. If a single node is faulty, data may be lost.

Possible Causes

No replica is configured when an index is created, or the number of index replicas is modified and not restored.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Handling Procedure

Check indexes.

Step 1 Check whether the Elasticsearch cluster is in the security mode.

Specifically, on FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Elasticsearch**. On the displayed page, click **Configurations**. Search for **ELASTICSEARCH_SECURITY_ENABLE**, and check whether the parameter can be queried and its value is **true**.

- If yes, go to **Step 2**.
- If no, go to **Step 3**.

Step 2 If the security mode is used, configure the permission for running the **curl** command.

For details, see section "Preparing the Environment" in "Curl Command Usage for Linux" in *MapReduce Service (MRS) 3.3.1-LTS User Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Usage Guide (for Huawei Cloud Stack 8.3.1)*.

Step 3 Log in to any node where Elasticsearch resides as user **root**.

Step 4 Run the following command to query index information in the current cluster:

curl -XGET --tlsv1.2 --negotiate -k -v -u : 'https://*ip:httpport***/_cat/indices?v&pretty'**

```
health status index   uuid                   pri rep docs.count docs.deleted store.size pri.store.size
green  open   test    s8wOFxAARtKkhEGSc5vgEQ   3   0          0            0      1.5kb          783b
```

NOTE

- In this command, replace **ip** with the IP address of any node in the cluster.
- Replace **httpport** with the HTTP port number of the Elasticsearch instance, which is specified by **SERVER_PORT**. To obtain the parameter value, on FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Elasticsearch**. On the displayed page, choose **Configurations** > **All Configurations** and search for **SERVER_PORT**.
- In normal mode, delete the security authentication parameter **--tlsv1.2 --negotiate -k -v -u:** and change **https** to **http**.
- These rules also apply to the following curl commands.

Step 5 Obtain the index not configured with replicas and configure index replicas as follows:

1. Run the following command to configure the number of index replicas:

   curl -XPUT --tlsv1.2 --negotiate -k -v -u : 'https://*ip:httpport***/***index***/_settings' -H 'Content-Type: application/json' -d'{ "number_of_replicas": 1 }'**

2. Run the following command to query indexes in the cluster and ensure that replicas are configured for the index.

   curl -XGET --tlsv1.2 --negotiate -k -v -u : 'https://*ip:httpport***/_cat/indices?v&pretty'**

```
health status index   uuid                   pri rep docs.count docs.deleted store.size pri.store.size
green  open   test    s8wOFxAARtKkhEGSc5vgEQ   3   1          0            0      1.5kb          783b
```

NOTE

- In this command, replace **index** with the index not configured with replicas in the cluster. Regular expression match is supported, and * indicates all indexes.
- Replace **number_of_replicas** with the number of index replicas. The value **1** is recommended.

Step 6 Manually clear the alarm.

Collect fault information.

Step 7 On FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 8 Select **Elasticsearch** in the required cluster for **Service**.

Step 9 Click in the upper right corner. In the displayed dialog box, set **Start Date** and **End Date** to 10 minutes before and after the alarm generation time respectively and click **OK**. Then, click **Download**.

Step 10 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.331 ALM-43208 Elasticsearch Data Directory Usage Exceeds the Threshold

Alarm Description

The system checks the Elasticsearch data directory usage every 60 seconds and compares the usage with the threshold. This alarm is generated when the system detects that the usage exceeds the threshold for multiple consecutive times (three times by default).

The threshold can be changed by choosing **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Elasticsearch** > **Data Directory Usage**.

If **Trigger Count** is set to **1**, and the Elasticsearch data directory usage is less than or equal to the threshold, this alarm is cleared. If **Trigger Count** is greater than **1**, and the Elasticsearch data directory usage is less than or equal to 90% of the threshold, this alarm is cleared.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43208	Major (default threshold: 90%) Critical (default threshold: 80%)	Quality of service	Tenant plane	Elasticsearch	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

The remaining space of the Elasticsearch data directory is insufficient, and new data cannot be written.

Possible Causes

The service data volume exceeds the cluster storage capacity.

Handling Procedure

Delete invalid indexes.

Step 1 Check whether the Elasticsearch cluster is in the security mode.

>Specifically, on FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Elasticsearch**. On the displayed page, click **Configurations**. Search for **ELASTICSEARCH_SECURITY_ENABLE**, and check whether the parameter can be queried and its value is **true**.

- If yes, go to **Step 2**.
- If no, go to **Step 3**.

Step 2 If the security mode is used, configure the permission for running the curl command.

For details, see section "Preparing the Environment" in "Curl Command Usage for Linux" in *MapReduce Service (MRS) 3.3.1-LTS User Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Usage Guide (for Huawei Cloud Stack 8.3.1)*.

Step 3 Log in to any node where Elasticsearch resides as user **root**.

Step 4 Run the **curl -XGET --tlsv1.2 --negotiate -k -v -u : 'https:**//*ip:httpport*/**_cat/indices?v&pretty'** command to query indexes in the cluster.

NOTE

- In this command, replace **ip** with the IP address of any node in the cluster.
- Replace **httpport** with the HTTP port number of the Elasticsearch instance, which is specified by **SERVER_PORT**. To obtain the parameter value, on FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Elasticsearch**. On the displayed page, choose **Configurations** > **All Configurations** and search for **SERVER_PORT**.
- In normal mode, delete the security authentication parameter **--tlsv1.2 --negotiate -k -v -u :** and change **https** to **http**.
- The rules also apply to the following **curl** commands.

Step 5 Run the **curl -XDELETE --tlsv1.2 --negotiate -k -u : "https://***ip:httpport/index***"** command to delete invalid or expired indexes if there are.

NOTE

- In this command, replace **index** with the index planned to be deleted in the cluster. Regular expression match is supported, and * indicates all indexes.
- Deleting a file or folder is a high-risk operation. Ensure that the file or folder is no longer required before performing this operation.

Step 6 Five minutes later, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Expand the cluster capacity.

Step 7 Expand the Elasticsearch cluster capacity by following instructions in *MapReduce Service (MRS) 3.3.1-LTS Physical Machine Cluster Component Migration Guide (for Huawei Cloud Stack 8.3.1)*.

Collect fault information.

Step 8 On FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 9 Select **Elasticsearch** in the required cluster for **Service**.

Step 10 Click in the upper right corner. In the displayed dialog box, set **Start Date** and **End Date** to 10 minutes before and after the alarm generation time respectively and click **OK**. Then, click **Download**.

Step 11 Contact the technical support and send the collected logs.

----End

Alarm Clearance

This alarm must be manually cleared after the fault is rectified.

Related Information

None.

1.3.332 ALM-43209 Total Number of Elasticsearch Instance Shards Exceeds the Threshold

Alarm Description

The system checks the total number of Elasticsearch instance shards every 60 seconds and compares the number with the threshold. This alarm is generated when the system detects that the number exceeds the threshold for multiple consecutive times (three times by default).

The threshold can be changed by choosing **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Elasticsearch** > **Shard** > **Number Of Shard**.

If **Trigger Count** is set to **1**, and the total number of Elasticsearch instance shards is less than or equal to the threshold, this alarm is cleared. If **Trigger Count** is greater than **1**, and the total number of Elasticsearch instance shards is less than or equal to 90% of the threshold, this alarm is cleared.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43209	Major (default threshold: 400) Critical (default threshold: 500)	Quality of service	Tenant plane	Elasticsearch	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

If the total number of Elasticsearch shards is too large, the index data read/write performance of Elasticsearch may be affected, and the shard restoration speed may be slow when the Elasticsearch process is restarted.

Possible Causes

The configuration of the Elasticsearch index shard number is inappropriate.

Handling Procedure

Check the total number of Elasticsearch instance shards.

Step 1 Check whether the Elasticsearch cluster is in the security mode.

Specifically, on FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Elasticsearch**. On the displayed page, click **Configurations**. Search for **ELASTICSEARCH_SECURITY_ENABLE**, and check whether the parameter can be queried and its value is **true**.

- If yes, go to **Step 2**.

- If no, go to **Step 3**.

Step 2 If the security mode is used, configure the permission for running the **curl** command.

For details, see section "Preparing the Environment" in "Curl Command Usage for Linux" in *MapReduce Service (MRS) 3.3.1-LTS User Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Usage Guide (for Huawei Cloud Stack 8.3.1)*.

Step 3 Log in to any node where Elasticsearch resides as user **root**.

Step 4 Run the **curl -XGET --tlsv1.2 --negotiate -k -v -u : 'https://*ip:httpport*/_cat/allocation?v'** command to query the total number of instance shards in the cluster.

NOTE

- In this command, replace **ip** with the IP address of any node in the cluster.
- Replace **httpport** with the HTTP port number of the Elasticsearch instance, which is specified by **SERVER_PORT**. To obtain the parameter value, on FusionInsight Manager, choose **Cluster** > **Services** > **Elasticsearch**. On the displayed page, choose **Configurations** > **All Configurations** and search for **SERVER_PORT**.
- In normal mode, delete the security authentication parameter **--tlsv1.2 --negotiate -k -v -u :** and change **https** to **http**.

Step 5 Use either of the following methods:

- Method 1: Delete the indexes that are no longer used in the cluster.
- Method 2: Change the threshold of the total number of instance shards.

NOTE

If you change the threshold to be greater than 500, modify **cluster.routing.allocation.total_shards_per_node** at the same time. The modification takes effect immediately without restarting the Elasticsearch service.

Step 6 Five minutes later, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect fault information.

Step 7 On FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 8 Select **Elasticsearch** in the required cluster for **Service**.

Step 9 Click in the upper right corner. In the displayed dialog box, set **Start Date** and **End Date** to 10 minutes before and after the alarm generation time respectively and click **OK**. Then, click **Download**.

Step 10 Contact the technical support and send the collected logs.

----End

Alarm Clearance

This alarm will be automatically cleared after the fault is rectified.

Related Information

None.

1.3.333 ALM-43210 Total Number of Elasticsearch Shards Exceeds the Threshold

Alarm Description

The system checks the total number of Elasticsearch shards every 60 seconds and compares the number with the threshold. This alarm is generated when the system detects that the number exceeds the threshold for multiple consecutive times (five times by default).

The threshold can be changed by choosing **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Elasticsearch** > **Replica Quantity Statistics**> **Total shard number**.

If **Trigger Count** is set to **1**, and the total number of Elasticsearch shards is less than or equal to the threshold, this alarm is cleared. If **Trigger Count** is greater than **1**, and the total number of Elasticsearch shards is less than or equal to 90% of the threshold, this alarm is cleared.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43210	Major (default threshold: 70000) Critical (default threshold: 90000)	Quality of service	Tenant plane	Elasticsearch	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold triggering the alarm. If the current indicator value exceeds this threshold, the alarm is generated.

Impact on the System

If the total number of shards in the Elasticsearch cluster is too large, the index data read/write performance of Elasticsearch may be affected, and the shard restoration speed may be slow when the Elasticsearch service is restarted.

Possible Causes

The configuration of the Elasticsearch index shard number is inappropriate.

Handling Procedure

Check the total number of Elasticsearch shards.

Step 1 Check whether the Elasticsearch cluster is in the security mode.

Specifically, on FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Elasticsearch**. On the displayed page, click **Configurations**.

Search for **ELASTICSEARCH_SECURITY_ENABLE**, and check whether the parameter can be queried and its value is **true**.

- If yes, go to **Step 2**.
- If no, go to **Step 3**.

Step 2 If the security mode is used, configure the permission for running the **curl** command.

For details, see section "Preparing the Environment" in "Curl Command Usage for Linux" in *MapReduce Service (MRS) 3.3.1-LTS User Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Usage Guide (for Huawei Cloud Stack 8.3.1)*.

Step 3 Log in to any node where Elasticsearch resides as user **root**.

Step 4 Run the **curl -XGET --tlsv1.2 --negotiate -k -v -u : 'https://*ip:httpport*/_cat/indices?v'** command to query the index details in the current cluster.

NOTE

- In this command, replace **ip** with the IP address of any node in the cluster.
- Replace **httpport** with the HTTP port number of the Elasticsearch instance, which is specified by **SERVER_PORT**. To obtain the parameter value, on FusionInsight Manager, choose **Cluster** > **Services** > **Elasticsearch**. On the displayed page, choose **Configurations** > **All Configurations** and search for **SERVER_PORT**.
- In normal mode, delete the security authentication parameter **--tlsv1.2 --negotiate -k -v -u :** and change **https** to **http**.

Step 5 Use either of the following methods:

- Method 1: Delete the indexes that are no longer used in the cluster.
- Method 2: Change the threshold of the total number of shards.

Step 6 Five minutes later, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect fault information.

Step 7 On FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 8 Select **Elasticsearch** in the required cluster for **Service**.

Step 9 Click in the upper right corner. In the displayed dialog box, set **Start Date** and **End Date** to 10 minutes before and after the alarm generation time respectively and click **OK**. Then, click **Download**.

Step 10 Contact the technical support and send the collected logs.

----End

Alarm Clearance

This alarm will be automatically cleared after the fault is rectified.

Related Information

None.

1.3.334 ALM-43600 GraphBase Service Unavailable

Alarm Description

The system checks the GraphBase service status every 60 seconds. This alarm is generated when LoadBalancer or GraphServer cannot provide services properly.

This alarm is cleared when either the LoadBalancer or GraphServer service is normal and the system considers that GraphBase recovers.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43600	Critical	Error handling	Tenant plane	GraphBase	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

The GraphServer service cannot be used.

Possible Causes

- The LoadBalancer service is not started.
- The GraphServer service is not started.
- The LoadBalancer node is abnormal.
- The GraphServer node is abnormal.
- The service on which GraphBase depends is abnormal.

Handling Procedure

Check whether the node where GraphBase is deployed is normal.

Step 1 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **GraphBase** > **Instance**.

Step 2 Check whether the status of LoadBalancer and GraphServer is **Good**.

- If yes, go to **Step 5**.
- If no, go to **Step 3**.

Step 3 Select the faulty instance, choose **More** > **Restart Instance**, and check whether the instance is successfully started.

- If yes, go to **Step 6**.
- If no, go to **Step 4**.

Step 4 Check whether the value of **loadbalancer.floatip** is correct.

- If yes, go to **Step 7**.
- If no, go to **Step 5**.

Step 5 Reconfigure the parameter value and restart the GraphBase service.

Step 6 Wait for one minute and check whether the alarm is cleared.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If yes, no further action is required.
- If no, go to **Step 7**.

Check the status of DBService, Yarn, HBase, Spark, Zookeeper, Elasticsearch and Kafka.

Step 7 Log in to FusionInsight Manager and choose **Cluster** > *Name of the desired cluster* > **Service**.

Step 8 Check whether the status of DBService, Yarn, HBase, Spark, Zookeeper, Elasticsearch, and Kafka services is **Good**.

- If yes, go to **Step 12**.
- If no, go to **Step 9**.

Step 9 Click a component whose status is **Not started** or **Startup failed**.

Step 10 In the **Instances** tab, select the faulty instance, choose **More** > **Restart Instance**, and check whether the instance can be started successfully.

- If yes, go to **Step 11**.
- If no, go to **Step 12**.

Step 11 Wait for one minute and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 12**.

Collect fault information.

Step 12 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 13 In the **Service** area, select the following nodes of the desired cluster.

- If the fault is caused by GraphBase, select GraphBase.
- If the fault is caused by services on which GraphBase depends, select the faulty services and the GraphBase service. (The corresponding hosts are automatically selected once you select the services.)

Step 14 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 15 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.335 ALM-43605 Number of Real-Time Requests on a GraphBase Node Exceeds the Threshold

Alarm Description

The system checks the status of GraphBase service every 60 seconds. This alarm is generated when the number of query requests to the GraphBase client exceeds the configured threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43605	Major	Quality of service	Tenant plane	GraphBase	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

- Too many connections are maintained for the requests and the network resources are limited. As a result, the communications between services may be abnormal.
- The GraphBase service may be unavailable.

Possible Causes

- The client is requested too frequently.
- The threshold is too low.

Handling Procedure

Check the number of real-time requests on the GraphServer node.

Step 1 On FusionInsight Manager, click O&M, and choose **Alarm** > **Thresholds** in the navigation pane on the left. Click the name of the desired cluster > **GraphBase** and view the threshold of **GraphServer Real-Time Requests**.

Step 2 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** and select the alarm whose ID is **43605**. Check the role name and the IP address of the host where the alarm is generated in **Location**.

Step 3 On the FusionInsight Manager homepage, choose **Cluster** > *Name of the desired cluster* > **Service** > **GraphBase** > **Instance**. Click the GraphServer where the alarm is reported. On the dashboard page that is displayed, expand the drop-down list box in the upper right corner of the graph area, choose **Customize** > **GraphServer Real-Time Requests**, and click **OK** to check whether the number of the requests exceeds the threshold.

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On FusionInsight Manager, click O&M, and choose **Alarm** > **Thresholds** in the navigation pane on the left. Click the name of the desired cluster > **GraphBase** and reset the threshold of **GraphServer Real-Time Requests**.

Step 5 Wait for one minute and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Step 6 Stop sending any requests for creating, deleting, updating, or querying relationships.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Wait for one minute and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect fault information.

Step 7 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 8 Expand the **Service** drop-down list, and select **GraphBase** for the target cluster.

Step 9 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.336 ALM-43607 Nginx Fault in GraphBase

Alarm Description

The system checks the Nginx service of GraphBase every 30 seconds. This alarm is generated when the Nginx service of GraphBase is abnormal during the HA health check.

This alarm is cleared when the Nginx service becomes normal during the HA health check.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43607	Major	Error handling	Tenant plane	GraphBase	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

- The active and standby LoadBalancers of GraphBase may be switched over.
- The GraphBase service may be unavailable.

Possible Causes

The Ngnix service is not running properly.

Handling Procedure

Check whether the node where GraphBase is deployed is normal.

Step 1 On FusionInsight Manager, select the alarm whose ID is **43607**, and view the IP address of the instance in location information.

Step 2 Log in to the node for which the alarm is generated as user **root**.

Step 3 Go to the **${BIGDATA_HOME}/FusionInsight_GraphBase_*/install/FusionInsight-GraphBase-*/miner/ha/module/hacom/script/** directory and run the **sh status_ha.sh** script to check whether Nginx of the active Manager is normal. Specifically, check whether the following information is displayed in the line where **ResName** of the active management node is **nginx**:

```
ngnix  Normal  Normal   Single_active
```

- If yes, go to **Step 5**.
- If no, go to **Step 4**.

Step 4 Contact the network administrator to check whether the network is faulty.

- If yes, rectify the network fault and go to **Step 5**.
- If no, go to **Step 6**.

Step 5 Wait for 5 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 In the **Service** area, select the following nodes of the desired cluster.

- If the fault is caused by GraphBase, select GraphBase.
- If the fault is caused by services on which GraphBase depends, select the faulty services and the GraphBase service. (The corresponding hosts are automatically selected once you select the services.)

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.337 ALM-43608 Floating IP Address of GraphBase Is Faulty

Alarm Description

The system checks the floating IP address of GraphBase every 30 seconds. This alarm is generated when the floating IP address of GraphBase is abnormal during HA health check.

This alarm is cleared when the floating IP address of GraphBase becomes normal during HA health check.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43608	Major	Error handling	Tenant plane	GraphBase	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

- If the GraphBase floating IP address is abnormal, users cannot log in to and use FusionInsight Manager.
- The active and standby LoadBalancers of GraphBase may be switched over.
- The GraphBase service may be unavailable.

Possible Causes

The floating IP address is abnormal.

Handling Procedure

Check whether the node where GraphBase is deployed is normal.

Step 1 On the FusionInsight Manager homepage, choose **Cluster** > *Name of the desired cluster* > **Service** > **GraphBase** > **Configuration** > **All Configurations**, and search for **loadbalancer.floatip**.

Step 2 Check whether the value of **loadbalancer.floatip** can be pinged.

- If yes, go to **Step 3**.
- If no, go to **Step 4**.

Step 3 Wait for 5 minutes, and check whether this alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 4**.

Step 4 On FusionInsight Manager, select the alarm whose ID is **43608**, and view the IP address of the instance in location information.

Step 5 Log in to the node for which the alarm is generated as user **root**.

Step 6 Go to the **${BIGDATA_HOME}/FusionInsight_GraphBase_*/install/FusionInsight-GraphBase-*/miner/ha/module/hacom/script/** directory and run the **sh status_ha.sh** script to check whether the floating IP address of the active Manager is normal. Specifically, check whether the following information is displayed in the line where **ResName** of the active management node is **floatip**:

The following is an example:

```
floatip  Normal  Normal   Single_active
```

- If yes, go to **Step 8**.
- If no, go to **Step 7**.

Step 7 Contact the network administrator to check whether the network is faulty.

- If yes, rectify the fault and go to **Step 8**.
- If no, go to **Step 9**.

Step 8 Wait for 5 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Collect fault information.

Step 9 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 10 Expand the **Service** drop-down list, and select **GraphBase** for the target cluster.

Step 11 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.338 ALM-43609 TaskManager of GraphBase Is Faulty

Alarm Description

The system checks TaskManager service of GraphBase every 30 seconds. This alarm is generated when the TaskManager service of GraphBase is abnormal during the HA health check.

This alarm is cleared when the TaskManager service of GraphBase becomes normal during the HA health check.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43609	Major	Error handling	Tenant plane	GraphBase	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

- The active and standby LoadBalancers of GraphBase may be switched over.
- The GraphBase service may be unavailable.

Possible Causes

The Tomcat service is abnormal.

Handling Procedure

Check whether the node where GraphBase locates is normal.

Step 1 On FusionInsight Manager, select the alarm whose ID is **43609**, and view the IP address of the instance in location information.

Step 2 Log in to the node for which the alarm is generated as user **root**.

Step 3 Go to the **${BIGDATA_HOME}/FusionInsight_GraphBase_*/install/FusionInsight-GraphBase-*/miner/ha/module/hacom/script/** directory and run the **sh status_ha.sh** script to check whether TaskManager of the active Manager is normal. Specifically, check whether the following information is displayed in the line where **ResName** of the active management node is **taskmanager**:

The following are two examples:

```
taskmanager   Normal  Normal   Single_active
```

- If yes, go to **Step 5**.
- If no, go to **Step 4**.

Step 4 Contact the network administrator to check whether the network is faulty.

- If yes, rectify the fault and go to **Step 5**.
- If no, go to **Step 6**.

Step 5 Wait for 5 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect the fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 In the **Service** area, select the following nodes of the desired cluster.

- If the fault is caused by GraphBase, select GraphBase.
- If the fault is caused by services on which GraphBase depends, select the faulty services and the GraphBase service. (The corresponding hosts are automatically selected once you select the services.)

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.339 ALM-43610 GC Time of the Old-Generation GraphServer Process Exceeds the Threshold

Alarm Description

The system checks the GC time of the old-generation GraphBase service every 30 seconds. This alarm is generated when the GC time of the old-generation

GraphBase service exceeds the threshold (the GC time exceeds 5 seconds for three consecutive times by default). On the FusionInsight Manager homepage, choose **O&M** > **Alarm** > **Threshold Configuration** > *Name of the desired cluster* > **GraphBase** > **GC Time** > **GC Time of the Old-Generation GraphServer Process** to change the threshold. This alarm is cleared when the GC time of the old-generation GraphBase service is less than or equal to the threshold.

NOTE

If the multi-instance function is enabled in the cluster and multiple HBase services are installed, determine the GraphBase service for which the alarm is generated based on the value of **ServiceName** in **Location Information** of the alarm. For example, if the GraphBase1 service is unavailable, the service name displayed in **Location Information** is **GraphBase1** and the operation object in the handling procedure is changed to **GraphBase1**.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43610	Major	Quality of service	Tenant plane	GraphBase	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

If the GC time of the old-generation GraphServer exceeds the threshold, the GraphBase interface cannot be accessed normally.

Possible Causes

The memory of GraphBase instances on the node is overused, the heap memory is inappropriately allocated, or a large number of I/O operations exist in GraphBase. As a result, GCs occur frequently.

Handling Procedure

Check the GC time.

Step 1 On the FusionInsight Manager homepage, choose **O&M** > **Alarm** > **Threshold Configuration** > *Name of the desired cluster* > **GraphBase** > **GC Time** > **GC Time of the Old-Generation GraphServer Process** to view the threshold.

Step 2 On the FusionInsight Manager homepage, choose **Cluster** > *Name of the Desired cluster* > **Service** > **GraphBase**. Click the drop-down list in the upper right corner of the graph area, choose **Customize** > **GC Time of the Old-Generation GraphServer Process**, and click **OK** to check whether the threshold is exceeded.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 On the FusionInsight Manager homepage, choose **O&M** > **Alarm** > **Threshold Setting** > *Name of the desired cluster* > **GraphBase** > **GC Time** > **GC Time of the Old-Generation GraphServer Process** to set the parameter to a new value.

Step 4 Wait for one minute and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Step 5 Stop sending any requests for creating, deleting, updating, or querying relationships.

Wait for one minute and check whether the alarm is cleared.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect the fault information.

Step 6 On the FusionInsight Manager homepage, choose **O&M** > **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **GraphBase** for the target cluster.

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.340 ALM-43611 Number of GC Times of the Old-Generation GraphServer Process Exceeds the Threshold

Alarm Description

The system checks the number of GC times of the old-generation GraphBase service every 30 seconds. This alarm is generated when the number of GC times of the old-generation GraphBase service exceeds the threshold (the number of GC times exceeds 5 seconds for three consecutive times by default). On the FusionInsight Manager homepage, choose **O&M** > **Alarm** > **Threshold Configuration** > *Name of the desired cluster* > **GraphBase** > **GC Count** > **Number of GC Times of the Old-Generation GraphServer Process**. This alarm is cleared when the number of GC times of the old-generation GraphBase service is less than or equal to the threshold.

NOTE

If the multi-instance function is enabled in the cluster and multiple HBase services are installed, determine the GraphBase service for which the alarm is generated based on the value of **ServiceName** in **Location Information** of the alarm. For example, if the GraphBase1 service is unavailable, the service name displayed in **Location Information** is **GraphBase1** and the operation object in the handling procedure is changed to **GraphBase1**.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43611	Major	Quality of service	Tenant plane	GraphBase	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

If the number of GC times of the old-generation GraphServer exceeds the threshold, the GraphBase interface cannot be accessed normally.

Possible Causes

The memory of GraphBase instances on the node is overused, the heap memory is inappropriately allocated, or a large number of I/O operations exist in GraphBase. As a result, GCs occur frequently.

Handling Procedure

Check the number of GC times.

Step 1 On the FusionInsight Manager homepage, choose **O&M** > **Alarm** > **Threshold Configuration** > *Name of the desired cluster* > **GraphBase** > **GC Count** > **Number of GC Times of the Old-Generation GraphServer Process**.

Step 2 On the FusionInsight Manager homepage, choose **Cluster** > *Name of the Desired cluster* > **Service** > **GraphBase**. Click the drop-down list in the upper right corner of the graph area, choose **Customize** > **Number of GC Times of the Old-Generation GraphServer Process**, and click **OK** to check whether the threshold is exceeded.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 On the FusionInsight Manager homepage, choose **O&M** > **Alarm** > **Threshold Configuration** > *Name of the desired cluster* > **GraphBase** > **GC Count** > **Number of GC Times of the Old-Generation GraphServer Process** to reset the threshold.

Step 4 Wait for one minute and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Step 5 Stop sending any requests for creating, deleting, updating, or querying relationships.

Wait for one minute and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect the fault information.

Step 6 On the FusionInsight Manager homepage, choose **O&M** > **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **GraphBase** for the target cluster.

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.341 ALM-43612 GC Duration of the Young-Generation GraphServer Process Exceeds the Threshold

Alarm Description

The system checks the GC time of the young-generation GraphBase service every 30 seconds. This alarm is generated when the GC time of the young-generation GraphBase service exceeds the threshold (the GC time exceeds 5 seconds for three consecutive times by default). On the FusionInsight Manager homepage, choose **O&M** > **Alarm** > **Threshold Configuration** > *Name of the desired cluster* > **GraphBase** > **GC Time** > **GC Time of the Young-Generation GraphServer Process** to change the threshold. This alarm is cleared when the GC time of the young-generation GraphBase service is less than or equal to the threshold.

NOTE

If the multi-instance function is enabled in the cluster and multiple HBase services are installed, determine the GraphBase service for which the alarm is generated based on the value of **ServiceName** in **Location Information** of the alarm. For example, if the GraphBase1 service is unavailable, the service name displayed in **Location Information** is **GraphBase1** and the operation object in the handling procedure is changed to **GraphBase1**.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43612	Major	Quality of service	Tenant plane	GraphBase	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

If the GC time of the young-generation GraphServer exceeds the threshold, the GraphBase interface cannot be accessed normally.

Possible Causes

The memory of GraphBase instances on the node is overused, the heap memory is inappropriately allocated, or a large number of I/O operations exist in GraphBase. As a result, GCs occur frequently.

Handling Procedure

Check the GC time.

Step 1 On the FusionInsight Manager homepage, choose **O&M** > **Alarm** > **Threshold Configuration** > *Name of the desired cluster* > **GraphBase** > **GC Time** > **GC Time of the Young-Generation GraphServer Process** to view the threshold.

Step 2 On the FusionInsight Manager homepage, choose **Cluster** > *Name of the Desired cluster* > **Service** > **GraphBase**. Click the drop-down list in the upper right corner

of the graph area, choose **Customize** > **GC Time of the Young-Generation GraphServer Process**, and click **OK** to check whether the threshold is exceeded.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 On the FusionInsight Manager homepage, choose **O&M** > **Alarm** > **Threshold Configuration** > *Name of the desired cluster* > **GraphBase** > **GC Time** > **GC Time of the Young-Generation GraphServer Process** to view the threshold.

Step 4 Wait for one minute and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Step 5 Stop sending any requests for creating, deleting, updating, or querying relationships.

Wait for one minute and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect the fault information.

Step 6 On the FusionInsight Manager homepage, choose **O&M** > **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **GraphBase** for the target cluster.

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.342 ALM-43613 Number of GC Times of the Young-Generation GraphServer Process Exceeds the Threshold

Alarm Description

The system checks the number of GC times of the young-generation GraphBase service every 30 seconds. This alarm is generated when the number of GC times of the young-generation GraphBase service exceeds the threshold (the number of GC times exceeds 5 seconds for three consecutive times by default). On the FusionInsight Manager homepage, choose **O&M** > **Alarm** > **Threshold Configuration** > *Name of the desired cluster* > **Service** > **GraphBase** > **GC Time** >

Number of GC Times of the Young-Generation GraphServer Process. This alarm is cleared when the number of GC times of the young-generation GraphBase service is less than or equal to the threshold.

NOTE

If the multi-instance function is enabled in the cluster and multiple HBase services are installed, determine the GraphBase service for which the alarm is generated based on the value of **ServiceName** in **Location Information** of the alarm. For example, if the GraphBase1 service is unavailable, the service name displayed in **Location Information** is **GraphBase1** and the operation object in the handling procedure is changed to **GraphBase1**.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43613	Major	Quality of service	Tenant plane	GraphBase	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

If the number of GC times of the young-generation GraphServer process exceeds the threshold, the GraphBase interface cannot be accessed normally.

Possible Causes

The memory of GraphBase instances on the node is overused, the heap memory is inappropriately allocated, or a large number of I/O operations exist in GraphBase. As a result, GCs occur frequently.

Handling Procedure

Check the number of GC times.

Step 1 On the FusionInsight Manager homepage, choose **O&M** > **Alarm** > **Threshold Configuration** > *Name of the desired cluster* > **GraphBase** > **GC Time** > **Number of GC Times of the Young-Generation GraphServer Process**.

Step 2 On the FusionInsight Manager homepage, choose **Cluster** > *Name of the Desired cluster* > **Service** > **GraphBase**. Click the drop-down list in the upper right corner of the graph area, choose **Customize** > **Number of GC Times of the Young-Generation GraphServer Process**, and click **OK** to check whether the threshold is exceeded.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 On the FusionInsight Manager homepage, choose **O&M** > **Alarm** > **Threshold Configuration** > *Name of the desired cluster* > **GraphBase** > **GC Time** > **Number of GC Times of the Young-Generation GraphServer Process** to reset the threshold.

Step 4 Wait for one minute and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Step 5 Stop sending any requests for creating, deleting, updating, or querying relationships.

Wait for one minute and check whether the alarm is cleared.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect the fault information.

Step 6 On the FusionInsight Manager homepage, choose **O&M** > **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **GraphBase** for the target cluster.

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.343 ALM-43614 Time Spent on a GraphBase Path Query Request Exceeds the Threshold

Alarm Description

The system checks the status of GraphBase service every 30 seconds. This alarm is generated when the time Spent on a path query request on the GraphBase client from the GraphServer node exceeds the configured threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43614	Major	Quality of service	Tenant plane	GraphBase	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.

Type	Parameter	Description
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

- If the requested content is too large or the request is frequently sent, the system is delayed. As a result, the communication between services may be abnormal.
- The GraphBase service may be unavailable.

Possible Causes

- The content requested by the client is too large or the request is frequently sent.
- The threshold is configured too low.

Handling Procedure

Check the time spent on a real-time path query request on the GraphServer node.

Step 1 On the FusionInsight Manager homepage, choose **O&M** > **Alarm** > **Threshold Configuration** > *Name of desired the cluster* > **GraphBase** to view the threshold of **Response Time for a Path Query on GraphServer**.

Step 2 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** and select the alarm whose ID is **43614**. Check the role name and the IP address of the host where the alarm is generated in **Location**.

Step 3 On the FusionInsight Manager homepage, choose **Cluster** > *Name of the desired cluster* > **Service** > **GraphBase** > **Instance**. Click the GraphServer where the alarm is reported. On the dashboard page that is displayed, expand the drop-down list box in the upper right corner of the graph area, choose **Customize** > **Response Time for a Path Query on GraphServer**, and click **OK** to check whether the query time of the current path exceeds the threshold.

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On the FusionInsight Manager homepage, choose **O&M** > **Alarm** > **Threshold Configuration** > *Name of desired cluster* > **GraphBase** to update the threshold of **Response Time for a Path Query on GraphServer**.

Step 5 Wait for one minute and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Step 6 Stop sending any requests for creating, deleting, updating, or querying relationships.

Wait for one minute and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect the fault information.

Step 7 On the FusionInsight Manager homepage, choose **O&M** > **Log** > **Download**.

Step 8 Expand the **Service** drop-down list, and select **GraphBase** for the target cluster.

Step 9 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.344 ALM-43615 Time Spent on a Line Expansion Query Request in GraphBase Exceeds the Threshold

Alarm Description

The system checks the status of GraphBase service every 30 seconds. This alarm is generated when the time Spent on a line expansion query request on the GraphBase client from the GraphServer node exceeds the configured threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43615	Major	Quality of service	Tenant plane	GraphBase	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

- If the requested content is too large or the request is frequently sent, the system is delayed. As a result, the communication between services may be abnormal.
- The GraphBase service may be unavailable.

Possible Causes

- The content requested by the client is too large or the request is frequently sent.
- The threshold is too low.

Handling Procedure

Check the time spent on a real-time line expansion query request on the GraphServer node.

Step 1 On the FusionInsight Manager homepage, choose **O&M** > **Alarm** > **Threshold Configuration** > *Name of the desired cluster* > **GraphBase** to view the threshold of **Response Time for a Line Expansion Query on GraphServer**.

Step 2 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** and select the alarm whose ID is **43615**. Check the role name and the IP address of the host where the alarm is generated in **Location**.

Step 3 On the FusionInsight Manager homepage, choose **Cluster** > *Name of the desired cluster* > **Service** > **GraphBase** > **Instance**. Click the GraphServer where the alarm is reported. On the **Dashboard** page that is displayed, expand the drop-down list box in the upper right corner of the graph area, choose **Customize** > **Response Time for a Line Expansion Query on GraphServer**, and click **OK** to check whether the query time of the current path exceeds the threshold.

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On the FusionInsight Manager homepage, choose **O&M** > **Alarm** > **Threshold Configuration** > *Name of the desired cluster* > **GraphBase** to update the threshold of **Response Time for a Line Expansion Query on GraphServer**.

Step 5 Wait for one minute and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 6 Stop sending any requests for creating, deleting, updating, or querying relationships.

Wait for one minute and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect the fault information.

Step 7 On the FusionInsight Manager homepage, choose **O&M** > **Log** > **Download**.

Step 8 Expand the **Service** drop-down list, and select **GraphBase** for the target cluster.

Step 9 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.345 ALM-43616 GraphBase-related Yarn Jobs Are Abnormal

Alarm Description

The system checks Yarn jobs related to GraphBase every 30 seconds. This alarm is generated when a failed Yarn job is found.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43616	Minor	Error handling	Tenant plane	GraphBase	No

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	TaskType	Specifies the job type of an asynchronous Yarn job.
	TaskId	Specifies the ID of the Yarn task that fails to be executed.

Impact on the System

- Operations performed in GraphBase may fail.
- The GraphBase service may be unavailable.
- After the fault is rectified, you need to execute the task again.

Possible Causes

Required parameter configuration for Yarn jobs is incorrect.

Handling Procedure

Check GraphBase-related Yarn jobs.

Step 1 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Service** > **Yarn** > **ResourceManager(Active)**. On the Yarn web UI, analyze the cause of the Yarn task failure.

NOTE

By default, the **admin** user does not have the permissions to manage other components. If the page cannot be opened or the displayed content is incomplete when you access the native UI of a component due to insufficient permissions, you can manually create a user with the permissions to manage that component.

Step 2 Find the failure cause and submit Yarn jobs again to check whether new Yarn jobs can be successfully executed.

- If yes, click **Clear** in the **Operation** column of the alarm to manually clear the alarm.
- If no, go to **Step 3**.

Step 3 If the new Yarn jobs submitted fail to be executed, download the fault logs and analyze the cause.

Collect the fault information.

Step 4 On the FusionInsight Manager homepage, choose **O&M** > **Log** > **Download**.

Step 5 Expand the **Service** drop-down list, and select **GraphBase** for the target cluster.

Step 6 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 7 Contact technical support and provide the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system does not automatically clear this alarm and you need to manually clear the alarm.

Related Information

None.

1.3.346 ALM-43617 Number of Waiting Queues for Real-Time Data Import to GraphBase Exceeds the Threshold

Alarm Description

The system checks whether the number of waiting queues imported to GraphBase in real time exceeds the threshold every 30 seconds. This alarm is generated when the number of waiting queues exceeds the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43617	Minor	Quality of service	Tenant plane	GraphBase	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	TaskId	Specifies the ID of a Yarn job.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

- As a result, real-time data import is blocked and the import time becomes longer.
- The real-time data import may be suspended.

Possible Causes

- The imported data size is too large and the configuration for data import is improper.
- The threshold is too low. The default value is **100**.

Handling Procedure

Check whether the number of waiting queues for real-time data import exceeds the threshold.

Step 1 On the FusionInsight Manager homepage, choose **Cluster** > *Name of the desired cluster* > **Service** > **Yarn** > **ResourceManager(Active)**. On the Yarn web UI, check the GraphBase-related SparkStreaming Yarn jobs.

NOTE

By default, the **admin** user does not have the permissions to manage other components. If the page cannot be opened or the displayed content is incomplete when you access the native UI of a component due to insufficient permissions, you can manually create a user with the permissions to manage that component.

Step 2 Click **ApplicationMaster** on the Yarn job page to go to the Spark job page.

Step 3 Click **Streaming** to view the status of the suspended queues.

Step 4 Enable the client not to send other Yarn tasks that are imported in real time. After a period of time, check whether the alarm is automatically cleared. If the alarm is cleared, the blocked queue is restored.

Step 5 If the queues are still suspended, download fault logs to analyze the cause. On FusionInsight Manager, choose **O&M** > **Alarm** > **Threshold Configuration** > *Name of the desired cluster* > **GraphBase** > **Threshold** to set the threshold of **graphStreaming Real-time import waiting queue**.

Step 6 Wait for one minute and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect the fault information.

Step 7 On the FusionInsight Manager homepage, choose **O&M** > **Log** > **Download**.

Step 8 Expand the **Service** drop-down list, and select **GraphBase** for the target cluster.

Step 9 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm. No manual operation is required.

Related Information

None.

1.3.347 ALM-43618 GraphServer Heap Memory Usage Exceeds the Threshold

Alarm Description

The system checks the heap memory usage of the GraphServer service every 30 seconds. This alarm is generated when the system detects that the heap memory usage of a GraphServer instance exceeds the threshold (90% of the maximum memory) for five consecutive periods (smoothing is performed for 5 times).

The alarm is cleared when the heap memory usage is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43618	Major	Quality of service	Tenant plane	GraphBase	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

If the heap memory usage of the GraphServer is too high, the performance of submitting and running GraphServer jobs may be affected, or the GraphServer service may break down due to memory overflow.

Possible Causes

The heap memory of the GraphServer instance is overused or the heap memory is inappropriately allocated. As a result, the usage exceeds the threshold.

Handling Procedure

Check the heap memory usage.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarm** > **ALM-43618 GraphServer Heap Memory Usage Exceeds the Threshold** > **Location Information**. View the IP address of the instance for which the alarm is generated.

Step 2 On the FusionInsight Manager homepage, choose **Cluster** > *Name of the desired cluster* > **Service** > **GraphBase** > **Instance** > **GraphServer** (corresponding to the IP address of the instance for which this alarm is generated) > **GraphServer Heap Memory Usage Statics**. check the heap memory usage.

Step 3 Check whether the heap memory used by GraphServer reaches 90% of the maximum heap memory (default threshold) configured for GraphServer.

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On the FusionInsight Manager homepage, choose **Cluster** > *Name of the desired cluster* > **Service** > **GraphBase** > **Configuration** > **All Configurations** > **GraphServer** > **System**. Change the value of **GC_OPTS** as described in the following note.

NOTE

Change the value of **GC_OPTS** as follows:

The default values of **-Xmx** and **-Xms** are **-Xmx30720M -Xms30720M**. When you increase the parameter values, you are advised to set **-Xmx** and **-Xms** to the same value. For example, increase them by **2048M** using **-Xmx32768M -Xms32768M**. It is recommended that the value be less than or equal to 50% of the host memory of the node and the maximum value be less than or equal to 32 GB.

Step 5 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect the fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **GraphBase** for the target cluster.

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.348 ALM-43619 Invalid GraphBase HA Certificate Files

Alarm Description

GraphBase checks whether the HA certificate files are valid (whether the certificate exists and whether its format is correct) in the first health check or at 01:00:00 every day. This alarm is generated when the certificate file is invalid.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43619	Major	Quality of service	Tenant plane	GraphBase	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

The HA root certificate file or HA user certificate file has expired. As a result, functions are restricted and cannot be used.

Possible Causes

The HA root certificate file or HA user certificate file is invalid.

Handling Procedure

View alarm information.

Step 1 Log in to FusionInsight Manager and choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**, and locate the row that contains **ALM-43619 Invalid GraphBase HA Certificate Files**. Check the host name in the location information and the file name in the additional information. Use PuTTY to log in to the host where the alarm is generated as user **omm**.

- If the file name displayed in additional information is **root-ca.crt**, go to **Step 2**.
- If the file name displayed in additional information is **server.crt**, go to **Step 10**.

Check whether the HA root certificate file in the system is valid.

Step 2 Run the **cd ${BIGDATA_HOME}/FusionInsight_GraphBase_*/install/FusionInsight-GraphBase-*/miner/ha/local/cert** command to go to the directory where the HA certificate is stored.

Step 3 Run the **ls -l** command to check whether the **root-ca.crt** file exists.

- If yes, go to **Step 4**.
- If no, go to **Step 16**.

Step 4 Run the **openssl x509 -in root-ca.crt -text -noout** command and check whether the command output is normal.

- If yes, go to **Step 16**.
- If no, go to **Step 5**.

Step 5 In the alarm list on FusionInsight Manager, check whether **ALM-12054 Invalid Certificate File** is reported.

- If yes, go to **Step 6**.
- If no, go to **Step 7**.

Step 6 Clear the alarm according to the handling procedure of **ALM-12054 Invalid Certificate File**.

Step 7 Run the **cp ${NODE_AGENT_HOME}/security/cert/subcert/certFile/ca.crt root-ca.crt** and **cp ${NODE_AGENT_HOME}/security/cert/subcert/certFile/ca.key root-ca.pem** commands to copy the HA root certificate again. Run the **rm ${BIGDATA_HOME}/FusionInsight_GraphBase_*/install/FusionInsight-GraphBase-*/miner/bin/CHECK_FLAG** command. Wait for 1 minute and check whether the alarm with the same additional information is cleared.

- If yes, go to **Step 8**.

- If no, go to **Step 16**.

Step 8 Log in to the node where the other LoadBalancer instance is deployed as user **omm** and repeat **Step 2** to **Step 7**.

Step 9 Check whether the alarm with the same additional information is generated again during the periodic check.

- If yes, go to **Step 16**.
- If no, no further action is required.

Check whether the HA user certificate file in the system is valid.

Step 10 Run the **cd ${BIGDATA_HOME}/FusionInsight_GraphBase_*/install/FusionInsight-GraphBase-*/miner/ha/local/cert** command to go to the directory where the HA certificate is stored.

Step 11 Run the **ls -l** command to check whether the **server.crt** file exists.

- If yes, go to **Step 12**.
- If no, go to **Step 13**.

Step 12 Run the **openssl x509 -in server.crt -text -noout** command and check whether the command output is normal.

- If yes, go to **Step 16**.
- If no, go to **Step 13**.

Step 13 Run the **cd ${BIGDATA_HOME}/FusionInsight_GraphBase_*/install/FusionInsight-GraphBase-*/miner/bin** command to go to the directory where the miner script is stored.

Step 14 Run the **sh miner-ha-re-gencert.sh** command to generate a new HA certificate. Then, check whether the alarm with the same additional information is cleared 1 minute later.

- If yes, go to **Step 15**.
- If no, go to **Step 16**.

Step 15 Check whether the alarm with the same additional information is generated again during the periodic check.

- If yes, go to **Step 16**.
- If no, no further action is required.

Collect the fault information.

Step 16 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 17 Select **GraphBase** in the required cluster for **Service**.

Step 18 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 19 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.349 ALM-43620 GraphBase HA Certificates Are About to Expire

Alarm Description

GraphBase checks whether HA certificate files are about to expire in the first health check or at 01:00:00 every day. This alarm is generated when the validity period is less than 30 days.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43620	Major	Quality of service	Tenant plane	GraphBase	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

Currently, there is no impact on the system.

Possible Causes

The HA root certificate file or HA user certificate file is about to expire.

Handling Procedure

View alarm information.

Step 1 Log in to FusionInsight Manager and choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**, and locate the row that contains **ALM-43620 GraphBase HA Certificates Are About to Expire** Check the host name in the location information and the file name in additional information. Use PuTTY to log in to the host where the alarm is generated as user **omm**.

- If the file name displayed in additional information is **root-ca.crt**, go to **Step 2**.
- If the file name displayed in additional information is **server.crt**, go to **Step 10**.

Check whether the HA root certificate file in the system is valid. If it is not, generate new HA certificate files.

Step 2 Run the **cd ${BIGDATA_HOME}/FusionInsight_GraphBase_*/install/FusionInsight-GraphBase-*/miner/ha/local/cert** command to go to the HA certificate directory.

Step 3 Run the **openssl x509 -noout -text -in root-ca.crt** command to query the effective time and due time of the HA root certificate.

Step 4 Perform **Step 5** to **Step 9** during off-peak hours to update HA certificate files as needed.

Step 5 In the alarm list on FusionInsight Manager, check whether the **ALM-12055 Certificate File About to Expire** alarm is generated.

- If yes, go to **Step 6**.
- If no, go to **Step 7**.

Step 6 Clear the alarm according to the handling procedure of **ALM-12055 Certificate File About to Expire**.

Step 7 Run the **cp ${NODE_AGENT_HOME}/security/cert/subcert/certFile/ca.crt root-ca.crt** and **cp ${NODE_AGENT_HOME}/security/cert/subcert/certFile/ca.key root-ca.pem** commands to copy the HA root certificate again. Run the **rm ${BIGDATA_HOME}/FusionInsight_GraphBase_*/install/FusionInsight-GraphBase-*/miner/bin/CHECK_FLAG** command. Wait for 1 minute and check whether the alarm with the same additional information is cleared.

- If yes, go to **Step 8**.
- If no, go to **Step 18**.

Step 8 Log in to the node where the other LoadBalancer instance is deployed as user **omm** and repeat **Step 2** to **Step 7**.

Step 9 Check whether the alarm with the same additional information is generated again during the periodic check.

- If yes, go to **Step 18**.
- If no, no further action is required.

Check whether the HA user certificate file in the system is valid. If it is not, generate new HA certificate files.

Step 10 Use PuTTY to log in to the host for which the alarm is generated as user **omm**.

Step 11 Run the **cd ${BIGDATA_HOME}/FusionInsight_GraphBase_*/install/FusionInsight-GraphBase-*/miner/ha/local/cert** command to go to the HA certificate directory.

Step 12 Run the **openssl x509 -noout -text -in server.crt** command to query the effective time and due time of the HA user certificate.

Step 13 Perform **Step 14** to **Step 15** update the HA certificate during off-peak hours as required.

Step 14 Run the **cd ${BIGDATA_HOME}/FusionInsight_GraphBase_*/install/FusionInsight-GraphBase-*/miner/bin** command to go to the directory where the miner script is stored.

Step 15 Run the **sh miner-ha-re-gencert.sh** command to generate a new HA certificate. Then, check whether the alarm is cleared 1 minute later.

- If yes, go to **Step 17**.
- If no, go to **Step 16**.

Step 16 On the node where the standby LoadBalancer instance is located, repeat **Step 14** to **Step 15**. Then, check whether the alarm is cleared 1 minute later.

- If yes, go to **Step 17**.
- If no, go to **Step 18**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 17 Check whether this alarm is generated again during periodic system check.

- If yes, go to **Step 18**.
- If no, no further action is required.

Collect the fault information.

Step 18 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 19 Select **GraphBase** in the required cluster for **Service**.

Step 20 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 21 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.350 ALM-43621 GraphBase HA Certificate Files Have Expired

Alarm Description

GraphBase checks whether HA certificate files have expired in the first health check or at 01:00:00 every day. This alarm is generated when the HA certificate has expired.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43621	Major	Quality of service	Tenant plane	GraphBase	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

The HA root certificate file or HA user certificate file has expired. As a result, functions are restricted and cannot be used.

Possible Causes

The HA root certificate file or HA user certificate file has expired.

Handling Procedure

View alarm information.

Step 1 Log in to FusionInsight Manager and choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**, and locate the row that contains **ALM-43621**

GraphBase HA Certificate Files Have Expired Check the host name in the location information and the file name in additional information. Use PuTTY to log in to the host where the alarm is generated as user **omm**.

- If the file name displayed in additional information is **root-ca.crt**, go to **Step 2**.
- If the file name displayed in additional information is **server.crt**, go to **Step 9**.

Check whether the HA root certificate file in the system is valid. If it is not, generate new HA certificate files.

Step 2 Run the **cd ${BIGDATA_HOME}/FusionInsight_GraphBase_*/install/FusionInsight-GraphBase-*/miner/ha/local/cert** command to go to the directory where the HA certificate is stored.

Step 3 Run the **openssl x509 -noout -text -in root-ca.crt** command to query the effective time and due time of the HA root certificate and check whether the file is valid.

- If yes, go to **Step 15**.
- If no, go to **Step 4**.

Step 4 In the alarm list on FusionInsight Manager, check whether **ALM-12054 Invalid Certificate File** is reported.

- If yes, go to **Step 5**.
- If no, go to **Step 6**.

Step 5 Clear the alarm according to the handling procedure of **ALM-12054 Invalid Certificate File**.

Step 6 Run the **cp ${NODE_AGENT_HOME}/security/cert/subcert/certFile/ca.crt root-ca.crt** and **cp ${NODE_AGENT_HOME}/security/cert/subcert/certFile/ca.key root-ca.pem** commands to copy the HA root certificate again. Run the **rm ${BIGDATA_HOME}/FusionInsight_GraphBase_*/install/FusionInsight-GraphBase-*/miner/bin/CHECK_FLAG** command. Wait for 1 minute and check whether the alarm with the same additional information is cleared.

- If yes, go to **Step 7**.
- If no, go to **Step 15**.

Step 7 Log in to the node where the other LoadBalancer instance is deployed as user **omm** and repeat **Step 2** to **Step 6**.

Step 8 Check whether the alarm with the same additional information is generated again during the periodic check.

- If yes, go to **Step 15**.
- If no, no further action is required.

Check whether the HA user certificate file in the system is valid. If it is not, generate new HA certificate files.

Step 9 Run the **cd ${BIGDATA_HOME}/FusionInsight_GraphBase_*/install/FusionInsight-GraphBase-*/miner/ha/local/cert** command to go to the directory where the HA certificate is stored.

Step 10 Run the **openssl x509 -noout -text -in server.crt** command to query the effective time and due time of the HA user certificate and check whether the file is valid.

- If yes, go to **Step 15**.
- If no, go to **Step 11**.

Step 11 Run the **cd ${BIGDATA_HOME}/FusionInsight_GraphBase_*/install/FusionInsight-GraphBase-*/miner/bin** command to go to the directory where the miner script is stored.

Step 12 Run the **sh miner-ha-re-gencert.sh** command to generate a new HA certificate. Then, check whether the alarm is cleared 1 minute later.

- If yes, go to **Step 14**.
- If no, go to **Step 13**.

Step 13 On the node where the standby LoadBalancer instance is located, repeat **Step 11** to **Step 12**. Then, check whether the alarm is cleared 1 minute later.

- If yes, go to **Step 14**.
- If no, go to **Step 15**.

Step 14 Check whether this alarm is generated again during periodic system check.

- If yes, go to **Step 15**.
- If no, no further action is required.

Collect the fault information.

Step 15 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 16 Select **GraphBase** in the required cluster for **Service**.

Step 17 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 18 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.351 ALM-43850 KMS Service Unavailable

Alarm Description

The system checks the KMS service status every 60 seconds. This alarm is generated when the KMS service is unavailable.

This alarm is cleared when the KMS service recovers.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43850	Critical	Quality of service	Tenant plane	KMS	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

KMS cannot provide the encryption key management service. If you cannot obtain the key, data cannot be encrypted or decrypted, and services encrypted or decrypted using KMS fail.

Possible Causes

- The ZooKeeper service is abnormal.
- The KMSWebServer instance is abnormal.

Handling Procedure

Check the KMSWebServer status.

Step 1 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **ZooKeeper**, and check whether the service running status is normal.

- If yes, go to **Step 3**.
- If no, go to **Step 2**.

Step 2 Rectify the fault by following the instructions in the help information of "ALM-13000 ZooKeeper Service Unavailable" and check whether the ZooKeeper running status is normal.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services**> **KMS**. On the**Dashboard** tab, check whether there is a node configured with the KMSWebServer role in the normal running status.

- If yes, go to **Step 4**.
- If no, go to **Step 5**.

Step 4 choose **O&M** > **Alarm** > **Alarms**, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Collect fault information.

Step 5 On FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 6 In the **Service** area, select the following services of the desired cluster.

- ZooKeeper
- KrbServer

Step 7 Click **OK**.

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact the technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm. You do not need to manually clear it.

Related Information

None.

1.3.352 ALM-43853 KMS Process Is Abnormal

Alarm Description

The KMSWebServer process checks the process status every 20 seconds. This alarm is generated when the process status is abnormal and does not recover for a long time.

This alarm is cleared when the process status recovers.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
43853	Major	Quality of service	Tenant plane	KMS	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
New	3.3.1	New alarm	New alarm

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

If the process status is abnormal, the process cannot provide services properly. As a result, the entire service may become abnormal.

Possible Causes

The host responds slowly to I/O (disk I/O and network I/O) requests and some processes are in the D state and Z state. The process may also be suspended and enter the T state.

Handling Procedure

Check whether the process is in the D, Z, or T state.

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Alarms**. Wait for about 10 minutes and check whether the alarm is automatically cleared.

- If the alarm is not in the list, no further action is required.
- If the alarm is in the list, view the alarm details and record the IP address of the host where the alarm is generated. Run the command in **Step 2**.

Step 2 Log in to the host where the alarm is generated as the **root** user and run the **su - omm** command to switch to the **omm** user.

Step 3 Run the following command to check the process state:

ps ww -eo stat,cmd| grep -w Dproc_kms | grep -v grep | awk '{print$1}'

Step 4 Check whether the command output contains any abnormal state (D, Z, or T).

- If the output contains any abnormal state, go to **Step 5**.
- If the output does not contain abnormal states, go to **Step 7**.

Step 5 Switch to user **root** and run the **reboot** command to restart the host for which the alarm is generated. (Restarting a host is risky. Ensure that the service process is normal after the restart.)

Step 6 Wait 5 minutes and check whether the alarm is cleared.

- If the alarm is cleared, no further action is required.
- If the alarm fails to be cleared, go to **Step 7**.

Collect fault information.

Step 7 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 8 Expand the drop-down list next to the **Service** field. In the **Services** dialog box that is displayed, select **KMS** for the target cluster.

Step 9 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.353 ALM-45000 HetuEngine Service Unavailable

Alarm Description

The system checks the HetuEngine service status every 300 seconds. This alarm is generated when the HetuEngine service is unavailable.

This alarm is cleared when the HetuEngine service recovers.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45000	Critical	Error handling	Tenant plane	HetuEngine	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

FusionInsight Manager cannot be used to perform operations on the HetuEngine cluster, and HetuEngine functions are unavailable.

Possible Causes

- The KrbServer service is abnormal.
- The ZooKeeper service is abnormal.
- The HDFS service is abnormal.
- The Yarn service is abnormal.
- The DBService service is abnormal.
- The Hive service is abnormal.
- There is no HetuEngine HSBroker instance that is running properly.

Handling Procedure

Check the KrbServer service status.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarm**.

Step 2 In the alarm list, check whether the "ALM-25500 KrbServer Service Unavailable" alarm is generated.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 Clear "ALM-25500 KrbServer Service Unavailable" according to the alarm help.

Step 4 In the alarm list, check whether the alarm "ALM-45000 HetuEngine Service Unavailable" is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check the ZooKeeper service status.

Step 5 In the alarm list, check whether the alarm "ALM-12007 Process Fault" is generated.

- If yes, go to **Step 6**.
- If no, go to **Step 9**.

Step 6 In the alarm list, click ⌄ in the row that contains the "Process Fault" alarm. Check whether the name of the service for which the alarm is generated is ZooKeeper in **Location Information**.

- If yes, go to **Step 7**.
- If no, go to **Step 9**.

Step 7 Clear "ALM-12007 Process Fault" according to the alarm help.

Step 8 In the alarm list, check whether the alarm "ALM-45000 HetuEngine Service Unavailable" is cleared.

- If yes, no further action is required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If no, go to **Step 9**.

Check the HDFS service status.

Step 9 In the alarm list, check whether the "ALM-14000 HDFS Service Unavailable" alarm is generated.

- If yes, go to **Step 10**.
- If no, go to **Step 12**.

Step 10 Clear "ALM-14000 HDFS Service Unavailable" according to the alarm help.

Step 11 In the alarm list, check whether the "ALM-45000 HetuEngine Service Unavailable" alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 12**.

Check the YARN service status.

Step 12 In the alarm list, check whether the "ALM-18000 YARN Service Unavailable" alarm is generated.

- If yes, go to **Step 13**.
- If no, go to **Step 15**.

Step 13 Clear "ALM-18000 YARN Service Unavailable" according to the alarm help.

Step 14 In the alarm list, check whether the "ALM-45000 HetuEngine Service Unavailable" alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 15**.

Check the DBService service status.

Step 15 In the alarm list, check whether the "ALM-27001 DBService Service Unavailable" alarm is generated.

- If yes, go to **Step 16**.
- If no, go to **Step 18**

Step 16 Clear "ALM-27001 DBService Service Unavailable" according to the alarm help.

Step 17 In the alarm list, check whether the "ALM-45000 HetuEngine Service Unavailable" alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 18**.

Check the Hive service status.

Step 18 In the alarm list, check whether the "ALM-16004 Hive Service Unavailable" alarm is generated.

- If yes, go to **Step 19**.
- If no, go to **Step 21**.

Step 19 Clear "ALM-16004 Hive Service Unavailable" according to the alarm help.

Step 20 In the alarm list, check whether the "ALM-45000 HetuEngine Service Unavailable" alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 21**.

Check whether there is no HetuEngine HSBroker instance that is running properly.

Step 21 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **HetuEngine**. On the page that is displayed, click the **Instance** tab.

Step 22 **Check whether there is no HSBroker instance that is running properly.**

- If yes, select the instance whose running status is not good, click **More** > **Restart Instance** in the **Operation** column to restart the instance, and go to **Step 23**.
- If no, go to **Step 24**.

Step 23 In the alarm list, check whether the "ALM-45000 HetuEngine Service Unavailable" alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 24**.

Check the network connection between HetuEngine and ZooKeeper, HDFS, YARN, DBService, and Hive.

Step 24 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **HetuEngine**. On the page that is displayed, click the **Instance** tab.

Step 25 Click the host name in the **HSBroker** row and record the management IP address in the **Basic Information** area.

Step 26 Log in to the host where HSBroker resides as user **omm** using the IP address obtained in **Step 25**.

Step 27 Run the **ping** command to check whether the network connection between the host where HSBroker resides and the hosts where ZooKeeper, HDFS, Yarn, DBService, and Hive reside is in the normal state.

- If yes, go to **Step 30**.
- If no, go to **Step 28**.

Step 28 Contact the network administrator to restore the network.

Step 29 In the alarm list, check whether the "ALM-45000 HetuEngine Service Unavailable" alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 30**.

Collect fault information.

Step 30 On FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 31 Expand the **Service** drop-down list. In the **Services** dialog box that is displayed, select **HetuEngine** under the target cluster name, and click **OK**.

Step 32 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the hosts to which the role belongs, and click **OK**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 33 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 34 Contact technical support and provide the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None.

1.3.354 ALM-45001 Faulty HetuEngine Compute Instances

Alarm Description

The system checks the HetuEngine compute instance status every 60 seconds. This alarm is generated when the HetuEngine compute instance is faulty.

This alarm is cleared when all faulty HetuEngine compute instances are restored.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45001	Critical	Quality of service	Tenant plane	HetuEngine	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

SQL tasks submitted to the faulty compute instance of HetuEngine fail to be executed.

Possible Causes

- The HDFS service is abnormal.
- The Yarn service is abnormal.
- Yarn queue resources are insufficient.
- The process of compute instances is faulty.

Handling Procedure

Check the HDFS service status.

Step 1 In the alarm list, check whether the "ALM-14000 HDFS Service Unavailable" alarm is generated.

- If yes, go to **Step 2**.
- If no, go to **Step 4**.

Step 2 Clear "ALM-14000 HDFS Service Unavailable" according to the alarm help.

Step 3 In the alarm list, check whether this alarm is cleared.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If yes, no further action is required.
- If no, go to **Step 4**.

Check the YARN service status.

Step 4 In the alarm list, check whether the "ALM-18000 YARN Service Unavailable" alarm is generated.

- If yes, go to **Step 5**.
- If no, go to **Step 7**.

Step 5 Clear "ALM-18000 YARN Service Unavailable" according to the alarm help.

Step 6 In the alarm list, check whether this alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Check the YARN queue resource status.

Step 7 In the alarm list, check whether the "ALM-18022 Insufficient YARN Queue Resources" alarm is generated.

- If yes, go to **Step 8**.
- If no, go to **Step 10**.

Step 8 Clear "ALM-18022 Insufficient YARN Queue Resources" according to the alarm help.

Step 9 In the alarm list, check whether this alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 10**.

Check the HetuEngine compute instance status.

Step 10 Log in to FusionInsight Manager as an administrator who can access the HetuEngine web UI and choose **Cluster** > **Services** > **HetuEngine**.

Step 11 In the **Basic Information** area on the **Dashboard** tab page, click the link next to **HSConsole WebUI** to access the HSConsole page.

Step 12 On the compute instance page, check whether any compute instances are in the **FAULT** state.

- If yes, go to **Step 13**.
- If no, go to **Step 14**.

Step 13 In the **Operation** column, click **Start** and wait until the instance is started.

Step 14 In the alarm list, check whether this alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 15**.

Collect fault information.

Step 15 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 16 Expand the **Service** drop-down list, select **HetuEngine** for the target cluster, and click **OK**.

Step 17 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the hosts to which the role belongs, and click **OK**.

Step 18 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 19 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.355 ALM-45003 HetuEngine QAS Disk Capacity Is Insufficient

Alarm Description

The system checks the HetuEngine QAS disk usage every 60 seconds and compares the actual disk usage with the threshold. The disk usage has a default threshold. This alarm is generated if the disk usage exceeds the threshold.

To change the threshold, choose **O&M** > **Alarm** > **Thresholds**. In the service list, choose **HetuEngine** > **Disk** > **QAS Disk Usage (QAS)**.

If the **Trigger Count** is **1**, this alarm is cleared when the usage of the HetuEngine QAS disk is less than or equal to the threshold. If the **Trigger Count** is greater than **1**, this alarm is cleared when the disk usage is less than or equal to 80% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45003	Critical (default threshold: 95%) Major (default threshold: 80%)	Quality of service	Tenant plane	HetuEngine	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	PartitionName	Specifies the disk partition for which the alarm is generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

Data cannot be written to the HetuEngine QAS disk. SQL diagnosis and materialized view recommendation of HetuEngine SQL O&M are unavailable.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Possible Causes

- The alarm threshold is improperly configured.
- The configuration of the HetuEngine QAS disk cannot meet service requirements. The disk usage reaches the upper limit.

Handling Procedure

Check whether the threshold is set properly.

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Thresholds**. In the service list, choose **HetuEngine** > **Disk** > **QAS Disk Usage (QAS)**. Check whether the alarm threshold is set properly. The default threshold is 80% of the disk capacity. You can change the threshold as required.

- If the threshold is set properly, go to **Step 4**.
- If the threshold is not set properly, go to **Step 2**.

Step 2 Click **Modify** in the **Operation** column to modify and save the alarm threshold as required.

Step 3 Wait 2 minutes and check whether the alarm is cleared.

- If the alarm is cleared, no further action is required.
- If the alarm is not cleared, go to **Step 4**.

Check whether the disk usage reaches the upper limit.

Step 4 Expand the alarm information, view the information in the **Location** area, and check the role name and host name of the QAS disk where the alarm is generated.

Step 5 Choose **Cluster** > **Services** > **HetuEngine** and click **Instance**. On the displayed page, click the QAS role name in the alarm information. On the instance page that is displayed, click **Chart** and check whether the QAS disk usage in the **QAS Disk Usage** chart exceeds the threshold (80% of the disk capacity by default).

- If the disk usage reaches the upper limit, go to **Step 6**.
- If the disk usage does not reaches the upper limit, go to **Step 9**.

Step 6 Log in to the host of the node where the QAS instance reporting the alarm is located as the **root** user.

Step 7 Run the following command to go to the QAS data directory and delete temporary files as required:

cd ${BIGDATA_DATA_HOME}/hetuengine/qas

NOTICE

Deleting temporary files affects the latest QAS execution result but does not affect subsequent results.

Step 8 Wait 2 minutes and check whether the alarm is cleared.

- If the alarm is cleared, no further action is required.

- If the alarm fails to be cleared, go to **Step 9**.

Collect fault information.

Step 9 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 10 Expand the **Service** drop-down list, select **HetuEngine** for the target cluster, and click **OK**.

Step 11 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the hosts to which the role belongs, and click **OK**.

Step 12 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 13 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.356 ALM-45004 Tasks Stacked on HetuEngine Compute Instance

Alarm Description

The system checks the number of running tasks on a HetuEngine compute instance every 30 seconds. This alarm is generated when the number of running tasks is greater than 50.

This alarm is cleared when the number of tasks running on the HetuEngine compute instance is no more than 50.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45004	Major	Quality of service	Tenant plane	HetuEngine	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
New	3.3.1	New alarm	New alarm

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Running Queries Backlog	Specifies the tenant name of the compute instance for which the alarm is generated and how much the threshold is exceeded.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

The performance of the compute instance deteriorates and the SQL response becomes slow.

Possible Causes

- The compute instance specification is too small.
- Large SQL tasks occupy too many compute resources. No resource is available for other tasks, and the compute instance cannot respond quickly. As a result, tasks are stacked.

Handling Procedure

Check whether compute instance resources are properly configured.

Step 1 Log in to FusionInsight Manager as an administrator who can access the HetuEngine web UI.

Step 2 Choose **O&M** > **Alarm** > **Alarms** > **Tasks Stacked on HetuEngine Compute Instance**, check the **Additional Information** of the alarm, and view and record the tenant name for which the alarm is generated.

Step 3 Choose **Cluster** > **Services** > HetuEngine. In the **Basic Information** area in the **Dashboard** tab, click the link next to **HSConsole Web UI**. The HSConsole page is displayed.

Step 4 On the **Compute Instance** page, click **Configure** in the **Operation** column of the tenant to which the compute instance belongs. Check whether the resource configured for the compute instance is proper. (The the minimum resources are used by default. You can adjust the configuration based on the site requirements.)

- If yes, go to **Step 8**.
- If no, go to **Step 5**.

Step 5 Return to the compute instance list, click **Stop Instances** in the **Operation** column, and stop instances as prompted.

NOTICE

Tasks submitted to the stopped compute instances will be will interrupted.

Step 6 Click **Configure**, add resources to the target compute instance based on the site requirements, and click **OK**. Click **Start Instances** and start instances as prompted.

Step 7 Wait 2 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Check whether there are large SQL tasks.

Step 8 On the **Compute Instances** page, expand the instances of the tenant and click **LINK** in the **WebUI** column of a compute instance to view the status of all tasks.

Step 9 In the **Sort** column, select **Execution Time** to sort the running tasks and check whether there are tasks that have been running for hours.

- If yes, go to **Step 10**.
- If no, go to **Step 12**.

Step 10 End the tasks that have been running for a long time based on service requirement and optimize the service SQL statements.

Step 11 Wait 2 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 12**.

Collect fault information.

Step 12 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 13 Expand the **Service** drop-down list, select **HetuEngine** for the target cluster, and click **OK**.

Step 14 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the hosts to which the role belongs, and click **OK**.

Step 15 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 16 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.357 ALM-45005 CPU Usage of HetuEngine Compute Instance Exceeded the Threshold

Alarm Description

The system checks the average CPU usage of HetuEngine compute instances every 30 seconds. This alarm is generated when the average CPU usage of the instances is greater than 90%.

This alarm is cleared when the CPU usage of the HetuEngine compute instances is no more than 90%.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45005	Major	Quality of service	Tenant plane	HetuEngine	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
New	3.3.1	New alarm	New alarm

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Cpu Usage Exceeds The Threshold	Specifies the tenant name of the compute instance for which the alarm is generated and how much the threshold is exceeded.

Impact on the System

The performance of the compute instances deteriorates and the response to SQL statements becomes slow.

Possible Causes

- The compute instance specification is too small.
- Large SQL tasks occupy too many compute resources. No resource is available for other tasks, and the compute instance cannot respond quickly. As a result, tasks are stacked.

Handling Procedure

Check whether compute instance resources are properly configured.

Step 1 Log in to FusionInsight Manager as an administrator who can access the HetuEngine web UI.

Step 2 Choose **O&M** > **Alarm** > **Alarms** > **Tasks Stacked on HetuEngine Compute Instance**, check the **Additional Information** of the alarm, and view and record the tenant name for which the alarm is generated.

Step 3 Choose **Cluster** > **Services** > HetuEngine. In the **Basic Information** area in the **Dashboard** tab, click the link next to **HSConsole Web UI**. The HSConsole page is displayed.

Step 4 On the **Compute Instance** page, click **Configure** in the **Operation** column of the tenant to which the compute instance belongs. Check whether the resource configured for the compute instance is proper. (The the minimum resources are used by default. You can adjust the configuration based on the site requirements.)

- If yes, go to **Step 8**.
- If no, go to **Step 5**.

Step 5 Return to the compute instance list, click **Stop Instances** in the **Operation** column, and stop instances as prompted.

NOTICE

Tasks submitted to the stopped compute instances will be will interrupted.

Step 6 Click **Configure**, add resources to the target compute instance based on the site requirements, and click **OK**. Click **Start Instances** and start instances as prompted.

Step 7 Wait 2 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Check whether there are large SQL tasks.

Step 8 On the **Compute Instances** page, expand the instances of the tenant and click **LINK** in the **WebUI** column of a compute instance to view the status of all tasks.

Step 9 In the **Sort** column, select **Execution Time** to sort the running tasks and check whether there are tasks that have been running for hours.

- If yes, go to **Step 10**.
- If no, go to **Step 12**.

Step 10 End the tasks that have been running for a long time based on service requirement and optimize the service SQL statements.

Step 11 Wait 2 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 12**.

Collect fault information.

Step 12 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 13 Expand the **Service** drop-down list, select **HetuEngine** for the target cluster, and click **OK**.

Step 14 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the hosts to which the role belongs, and click **OK**.

Step 15 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 16 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.358 ALM-45006 Memory Usage of a HetuEngine Compute Instance Exceeded the Threshold

Alarm Description

The system checks the memory usage of HetuEngine compute instances every 30 seconds. This alarm is generated when the memory usage of the instance is greater than 80%.

This alarm is cleared when the memory usage of the HetuEngine compute instance is no more than 80%.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45006	Major	Quality of service	Tenant plane	HetuEngine	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
New	3.3.1	New alarm	New alarm

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Memory Usage Exceeds The Threshold	Specifies the tenant name of the compute instance for which the alarm is generated and how much the threshold is exceeded.

Impact on the System

The performance of the compute instance deteriorates and the response to service SQL statements becomes slow.

Possible Causes

- The compute instance specification is too small.
- Large SQL tasks occupy too many compute resources. No resource is available for other tasks, and the compute instance cannot respond quickly. As a result, tasks are stacked.

Handling Procedure

Check whether compute instance resources are properly configured.

Step 1 Log in to FusionInsight Manager as an administrator who can access the HetuEngine web UI.

Step 2 Choose **O&M** > **Alarm** > **Alarms** > **Tasks Stacked on HetuEngine Compute Instance**, check the **Additional Information** of the alarm, and view and record the tenant name for which the alarm is generated.

Step 3 Choose **Cluster** > **Services** > HetuEngine. In the **Basic Information** area in the **Dashboard** tab, click the link next to **HSConsole Web UI**. The HSConsole page is displayed.

Step 4 On the **Compute Instance** page, click **Configure** in the **Operation** column of the tenant to which the compute instance belongs. Check whether the resource configured for the compute instance is proper. (The the minimum resources are used by default. You can adjust the configuration based on the site requirements.)

- If yes, go to **Step 8**.
- If no, go to **Step 5**.

Step 5 Return to the compute instance list, click **Stop Instances** in the **Operation** column, and stop instances as prompted.

NOTICE

Tasks submitted to the stopped compute instances will be will interrupted.

Step 6 Click **Configure**, add resources to the target compute instance based on the site requirements, and click **OK**. Click **Start Instances** and start instances as prompted.

Step 7 Wait 2 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Check whether there are large SQL tasks.

Step 8 On the **Compute Instances** page, expand the instances of the tenant and click **LINK** in the **WebUI** column of a compute instance to view the status of all tasks.

Step 9 In the **Sort** column, select **Execution Time** to sort the running tasks and check whether there are tasks that have been running for hours.

- If yes, go to **Step 10**.
- If no, go to **Step 12**.

Step 10 End the tasks that have been running for a long time based on service requirement and optimize the service SQL statements.

Step 11 Wait 2 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 12**.

Collect fault information.

Step 12 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 13 Expand the **Service** drop-down list, select **HetuEngine** for the target cluster, and click **OK**.

Step 14 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the hosts to which the role belongs, and click **OK**.

Step 15 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 16 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.359 ALM-45007 Number of Workers of a HetuEngine Compute Instance Is Less Than the Threshold

Alarm Description

The system checks the number of Workers of a HetuEngine compute instance every 60 seconds. This alarm is generated when the number of Workers is less than 80% of the initial value.

This alarm is cleared when the number of Workers running on the HetuEngine compute instance is no less than 80% of the initial value.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45007	Major	Quality of service	Tenant plane	HetuEngine	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
New	3.3.1	New alarm	New alarm

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.

Type	Parameter	Description
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Worker Less Threshold	Specifies the tenant name of the compute instance for which the alarm is generated and how much the threshold is exceeded.

Impact on the System

The performance of the compute instance deteriorates and the SQL response becomes slow.

Possible Causes

- YARN queue resources are insufficient.
- A large number of tasks are running, causing OMM memory overflow on Worker nodes. As a result, the number of Worker nodes decreases.

Handling Procedure

Check whether YARN resource queue resources are sufficient.

Step 1 Log in to FusionInsight Manager as an administrator who can access the HetuEngine web UI.

Step 2 Choose **O&M** > **Alarm** > **Alarms** > **Number of Workers of a HetuEngine Compute Instance Is Less Than the Threshold**, check the **Additional**

Information of the alarm, and view and record the tenant name for which the alarm is generated.

Step 3 Click **Tenant Resources**, select the tenant of the compute instance, and check whether the resource quota of the tenant is sufficient.

- If yes, go to **Step 6**.
- If no, go to **Step 4**.

Step 4 Increase the maximum percentage of the tenant's resources based on the actual usage.

Step 5 Wait 5 to 10 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Check whether there is a large number of running tasks.

Step 6 Choose **Cluster** > **Services** > **HetuEngine**.

Step 7 In the **Basic Information** area on the **Dashboard** tab page, click the link next to **HSConsole Web UI** to access the HSConsole page.

Step 8 On the **Compute Instances** page, expand the instances of the tenant and click **LINK** in the **WebUI** column of a compute instance to view the status of all tasks.

Step 9 Check whether the number of running tasks exceeds 50.

- If yes, go to **Step 10**.
- If no, go to **Step 12**.

Step 10 Reduce the number of jobs submitted at a time or add compute instance resources based on service requirements.

Step 11 Wait 5 to 10 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 12**.

Collect fault information.

Step 12 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 13 Expand the **Service** drop-down list, select **HetuEngine** for the target cluster, and click **OK**.

Step 14 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the hosts to which the role belongs, and click **OK**.

Step 15 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 16 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.360 ALM-45179 Number of Failed OBS readFully API Calls Exceeds the Threshold

Alarm Description

The system checks whether the number of failed OBS readFully API calls exceeds the threshold every 30 seconds. This alarm is generated when the number of failed API calls exceeds the threshold.

This alarm is automatically cleared when the number of failed OBS readFully API calls is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45179	Minor	Error handling	Tenant plane	meta	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

Certain upper-layer big data computing tasks will fail to execute.

Possible Causes

An execution exception or severe timeout occurs on the OBS server.

Handling Procedure

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Thresholds**. On the **Thresholds** page, choose **meta** > **Number of failed calls to the OBS readFully interface**. In the right pane, set **Threshold** or **Trigger Count** to a larger value as required.

Step 2 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 3**.

Step 3 Contact OBS technical support to check whether the OBS service is normal.

- If yes, go to **Step 4**.
- If no, contact OBS technical support to restore the OBS service.

Collect fault information.

Step 4 On FusionInsight Manager, choose **Cluster** > **Services** > **meta**. On the page that is displayed, click the **Chart** tab. On this tab page, select **OBS data read operation** in the **Chart Category** area. In the **Number of failed calls to the OBS readFully**

interface-All Instances chart, view the host name of the instance that has the maximum number of failed OBS readFully API calls. For example, the host name is **node-ana-corevpeO003**.

Step 5 Choose **O&M** > **Log** > **Download** and select **meta** and **meta** under it for **Service**.

Step 6 Select the host obtained in **Step 4** for **Hosts**.

Step 7 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time respectively. Then, click **Download**.

Step 8 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.361 ALM-45180 Number of Failed OBS read API Calls Exceeds the Threshold

Alarm Description

The system checks whether the number of failed OBS read API calls exceeds the threshold every 30 seconds. This alarm is generated when the number of failed API calls exceeds the threshold.

This alarm is automatically cleared when the number of failed OBS read API calls is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45180	Minor	Error handling	Tenant plane	meta	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

Certain upper-layer big data computing tasks will fail to execute.

Possible Causes

An execution exception or severe timeout occurs on the OBS server.

Handling Procedure

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Thresholds**. On the **Thresholds** page, choose **meta** > **Number of failed calls to the OBS read interface**. In the right pane, set **Threshold** or **Trigger Count** to a larger value as required.

Step 2 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 3**.

Step 3 Contact OBS technical support to check whether the OBS service is normal.

- If yes, go to **Step 4**.
- If no, contact OBS technical support to restore the OBS service.

Collect fault information.

Step 4 On FusionInsight Manager, choose **Cluster** > **Services** > **meta**. On the page that is displayed, click the **Chart** tab. On this tab page, select **OBS data read operation** in the **Chart Category** area. In the **Number of failed calls to the OBS read interface-All Instances** chart, view the host name of the instance that has the maximum number of failed OBS read API calls. For example, the host name is **node-ana-corevpeO003**.

Step 5 Choose **O&M** > **Log** > **Download** and select **meta** and **meta** under it for **Service**.

Step 6 Select the host obtained in **Step 4** for **Hosts**.

Step 7 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time respectively. Then, click **Download**.

Step 8 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.362 ALM-45181 Number of Failed OBS write API Calls Exceeds the Threshold

Alarm Description

The system checks whether the number of failed OBS write API calls exceeds the threshold every 30 seconds. This alarm is generated when the number of failed API calls exceeds the threshold.

This alarm is automatically cleared when the number of failed OBS write API calls is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45181	Minor	Error handling	Tenant plane	meta	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.

Type	Parameter	Description
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

Certain upper-layer big data computing tasks will fail to execute.

Possible Causes

An execution exception or severe timeout occurs on the OBS server.

Handling Procedure

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Thresholds**. On the **Thresholds** page, choose **meta** > **Number of failed calls to the OBS write interface**. In the right pane, set **Threshold** or **Trigger Count** to a larger value as required.

Step 2 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 3**.

Step 3 Contact OBS technical support to check whether the OBS service is normal.

- If yes, go to **Step 4**.
- If no, contact OBS technical support to restore the OBS service.

Collect fault information.

Step 4 On FusionInsight Manager, choose **Cluster** > **Services** > **meta**. On the page that is displayed, click the **Chart** tab. On this tab page, select **OBS data write operation** in the **Chart Category** area. In the **Number of failed calls to the OBS write interface-All Instances** chart, view the host name of the instance that has the maximum number of failed OBS write API calls. For example, the host name is **node-ana-corevpeO003**.

Step 5 Choose **O&M** > **Log** > **Download** and select **meta** and **meta** under it for **Service**.

Step 6 Select the host obtained in **Step 4** for **Hosts**.

Step 7 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time respectively. Then, click **Download**.

Step 8 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.363 ALM-45182 Number of Throttled OBS Operations Exceeds the Threshold

Alarm Description

The system checks whether the number of throttled OBS operations exceeds the threshold every 30 seconds. This alarm is generated when the number of throttled OBS operations exceeds the threshold.

This alarm is automatically cleared when the number of throttled OBS operations is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45182	Minor	Error handling	Tenant plane	meta	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

Certain upper-layer big data computing tasks will fail to execute.

Possible Causes

The frequency of requesting OBS APIs is too high.

Handling Procedure

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Thresholds**. On the **Thresholds** page, choose **meta** > **Number of Throttled OBS Operations**. In the right pane, set **Threshold** or **Trigger Count** to a larger value as required.

Step 2 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 3**.

Step 3 Contact OBS technical support to check whether the OBS service is normal.

- If yes, go to **Step 4**.
- If no, contact OBS technical support to restore the OBS service.

Collect fault information.

Step 4 On FusionInsight Manager, choose **Cluster** > **Services** > **meta**. On the page that is displayed, click the **Chart** tab. On this tab page, select **OBS Throttled** in the **Chart Category** area. In the **Number of Throttled OBS Operations-All Instances** chart, view the host name of the instance that has the maximum number of throttled OBS API calls. For example, the host name is **node-ana-coreUQqJ0002**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 5 Choose **O&M** > **Log** > **Download** and select **meta** and **meta** under it for **Service**.

Step 6 Select the host obtained in **Step 4** for **Hosts**.

Step 7 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time respectively. Then, click **Download**.

Step 8 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.3.364 ALM-45183 Total Number of FileNotFoundException Errors Reported by OBS Exceeds the Threshold

Alarm Description

The system checks whether the number of FileNotFoundException errors reported by OBS exceeds the threshold every 30 seconds. This alarm is generated when the number exceeds the threshold.

This alarm is automatically cleared when the number of FileNotFoundException errors reported by OBS is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45183	Minor	Error handling	Tenant plane	meta	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

Cluster components fail to access OBS. For systems with decoupled storage and compute, some computing tasks in the cluster may fail to be executed.

Possible Causes

The OBS object to be accessed by the task does not exist.

Handling Procedure

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Thresholds**. On the **Thresholds** page, choose **meta** > **OBS Exception** > **Total Number of OBS FileNotFoundException Errors**. In the right pane, set **Threshold** or **Trigger Count** to a larger value as required.

Step 2 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 3**.

Collect fault information.

Step 3 On FusionInsight Manager, choose **Cluster** > **Services** > **meta**. On the page that is displayed, click the **Chart** tab. On this page, choose **OBS Exception** in the **Chart Category** area. In the **Number of OBS FileNotFoundException Errors-All Instances** chart, view the host name of the instance that has the maximum number of OBS FileNotFoundException errors. For example, the host name is **node-ana-coreUQqJ0002**.

Step 4 Choose **O&M** > **Log** > **Download** and select **meta** and **meta** under it for **Service**.

Step 5 Select the host obtained in **Step 3** for **Hosts**.

Step 6 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time respectively. Then, click **Download**.

Step 7 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.3.365 ALM-45184 Total Number of OBSIllegalArgumentException Errors Reported by OBS Exceeds the Threshold

Alarm Description

The system checks whether the number of OBSIllegalArgumentException errors reported by OBS exceeds the threshold every 30 seconds. This alarm is generated when the number exceeds the threshold.

This alarm is automatically cleared when the number of OBSIllegalArgumentException errors reported by OBS is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45184	Minor	Error handling	Tenant plane	meta	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

Cluster components fail to access OBS. For systems with decoupled storage and compute, some computing tasks in the cluster may fail to be executed.

Possible Causes

The input parameter is invalid. For example, the field is too long or contains invalid characters.

Handling Procedure

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Thresholds**. On the **Thresholds** page, choose **meta** > **OBS Exception** > **Total Number of OBSIllegalArgumentException Errors**. In the right pane, set **Threshold** or **Trigger Count** to a larger value as required.

Step 2 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 3**.

Collect fault information.

Step 3 On FusionInsight Manager, choose **Cluster** > **Services** > **meta**. On the page that is displayed, click the **Chart** tab. On this page, choose **OBS Exception** in the **Chart Category** area. In the **Number of OBSIllegalArgumentException Errors-All Instances** chart, view the host name of the instance that has the maximum number of OBSIllegalArgumentException errors. For example, the host name is **node-ana-coreUQqJ0002**.

Step 4 Choose **O&M** > **Log** > **Download** and select **meta** and **meta** under it for **Service**.

Step 5 Select the host obtained in **Step 3** for **Hosts**.

Step 6 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time respectively. Then, click **Download**.

Step 7 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.3.366 ALM-45185 Total Number of AccessControlException Errors Reported by OBS Exceeds the Threshold

Alarm Description

The system checks whether the number of AccessControlException errors reported by OBS exceeds the threshold every 30 seconds. This alarm is generated when the number exceeds the threshold.

This alarm is automatically cleared when the number of AccessControlException errors reported by OBS is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45185	Minor	Error handling	Tenant plane	meta	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

Cluster components fail to access OBS. For systems with decoupled storage and compute, some computing tasks in the cluster may fail to be executed.

Possible Causes

The AK/SK obtained by the task does not have the permission to access some OBS paths.

Handling Procedure

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Thresholds**. On the **Thresholds** page, choose **meta** > **OBS Exception** > **Total Number of OBS AccessControlException Errors**. In the right pane, set **Threshold** or **Trigger Count** to a larger value as required.

Step 2 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 3**.

Collect fault information.

Step 3 On FusionInsight Manager, choose **Cluster** > **Services** > **meta**. On the page that is displayed, click the **Chart** tab. On this page, choose **OBS Exception** in the **Chart Category** area. In the **Number of OBS AccessControlException Errors-All Instances** chart, view the host name of the instance that has the maximum number of OBS AccessControlException errors. For example, the host name is **node-ana-coreUQqJ0002**.

Step 4 Choose **O&M** > **Log** > **Download** and select **meta** and **meta** under it for **Service**.

Step 5 Select the host obtained in **Step 3** for **Hosts**.

Step 6 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time respectively. Then, click **Download**.

Step 7 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.3.367 ALM-45186 Total Number of OBSMethodNotAllowedException Errors Reported by OBS Exceeds the Threshold

Alarm Description

The system checks whether the number of OBSMethodNotAllowedException errors reported by OBS exceeds the threshold every 30 seconds. This alarm is generated when the number exceeds the threshold.

This alarm is automatically cleared when the number of OBSMethodNotAllowedException errors reported by OBS is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45186	Minor	Error handling	Tenant plane	meta	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

Cluster components fail to access OBS. For systems with decoupled storage and compute, some computing tasks in the cluster may fail to be executed.

Possible Causes

The specified method is not allowed against the given resource.

Handling Procedure

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Thresholds**. On the **Thresholds** page, choose **meta** > **OBS Exception** > **Total Number of OBSMethodNotAllowedException Errors**. In the right pane, set **Threshold** or **Trigger Count** to a larger value as required.

Step 2 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 3**.

Collect fault information.

Step 3 On FusionInsight Manager, choose **Cluster** > **Services** > **meta**. On the page that is displayed, click the **Chart** tab. On this page, choose **OBS Exception** in the **Chart Category** area. In the **Number of OBSMethodNotAllowedException Errors-All Instances** chart, view the host name of the instance that has the maximum number of OBSMethodNotAllowedException errors. For example, the host name is **node-ana-coreUQqJ0002**.

Step 4 Choose **O&M** > **Log** > **Download** and select **meta** and **meta** under it for **Service**.

Step 5 Select the host obtained in **Step 3** for **Hosts**.

Step 6 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time respectively. Then, click **Download**.

Step 7 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.3.368 ALM-45187 Total Number of OBSFileConflictException Errors Reported by OBS Exceeds the Threshold

Alarm Description

The system checks whether the number of OBSFileConflictException errors reported by OBS exceeds the threshold every 30 seconds. This alarm is generated when the number exceeds the threshold.

This alarm is automatically cleared when the number of OBSFileConflictException errors reported by OBS is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45187	Minor	Error handling	Tenant plane	meta	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

Cluster components fail to access OBS. For systems with decoupled storage and compute, some computing tasks in the cluster may fail to be executed.

Possible Causes

A conflicting operation is being performed on this resource, for example, a concurrent rename operation.

Handling Procedure

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Thresholds**. On the **Thresholds** page, choose **meta** > **OBS Exception** > **Total Number of OBSFileConflictException Errors**. In the right pane, set **Threshold** or **Trigger Count** to a larger value as required.

Step 2 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 3**.

Collect fault information.

Step 3 On FusionInsight Manager, choose **Cluster** > **Services** > **meta**. On the page that is displayed, click the **Chart** tab. On this page, choose **OBS Exception** in the **Chart Category** area. In the **Number of OBSFileConflictException Errors-All Instances** chart, view the host name of the instance that has the maximum number of OBSFileConflictException errors. For example, the host name is **node-ana-coreUQqJ0002**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 4 Choose **O&M** > **Log** > **Download** and select **meta** and **meta** under it for **Service**.

Step 5 Select the host obtained in **Step 3** for **Hosts**.

Step 6 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time respectively. Then, click **Download**.

Step 7 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.3.369 ALM-45188 Total Number of OBSIOException Errors Reported by OBS Exceeds the Threshold

Alarm Description

The system checks whether the number of OBSIOException errors reported by OBS exceeds the threshold every 30 seconds. This alarm is generated when the number exceeds the threshold.

This alarm is automatically cleared when the number of OBSIOException errors reported by OBS is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45188	Minor	Error handling	Tenant plane	meta	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

Cluster components fail to access OBS. For systems with decoupled storage and compute, some computing tasks in the cluster may fail to be executed.

Possible Causes

The OBS server is abnormal.

Handling Procedure

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Thresholds**. On the **Thresholds** page, choose **meta** > **OBS Exception** > **Total Number of OBSIOException Errors**. In the right pane, set **Threshold** or **Trigger Count** to a larger value as required.

Step 2 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 3**.

Collect fault information.

Step 3 On FusionInsight Manager, choose **Cluster** > **Services** > **meta**. On the page that is displayed, click the **Chart** tab. On this page, choose **OBS Exception** in the **Chart Category** area. In the **Number of OBSIOException Errors-All Instances** chart, view the host name of the instance that has the maximum number of OBSIOException errors. For example, the host name is **node-ana-coreUQqJ0002**.

Step 4 Choose **O&M** > **Log** > **Download** and select **meta** and **meta** under it for **Service**.

Step 5 Select the host obtained in **Step 3** for **Hosts**.

Step 6 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time respectively. Then, click **Download**.

Step 7 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.3.370 ALM-45189 Total Number of EOFException Errors Reported by OBS Exceeds the Threshold

Alarm Description

The system checks whether the number of EOFException errors reported by OBS exceeds the threshold every 30 seconds. This alarm is generated when the number exceeds the threshold.

This alarm is automatically cleared when the number of EOFException errors reported by OBS is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45189	Minor	Error handling	Tenant plane	meta	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

Cluster components fail to access OBS. For systems with decoupled storage and compute, some computing tasks in the cluster may fail to be executed.

Possible Causes

The requested range cannot be obtained.

Handling Procedure

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Thresholds**. On the **Thresholds** page, choose **meta** > **OBS Exception** > **Total Number of OBS EOFException Errors**. In the right pane, set **Threshold** or **Trigger Count** to a larger value as required.

Step 2 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 3**.

Collect fault information.

Step 3 On FusionInsight Manager, choose **Cluster** > **Services** > **meta**. On the page that is displayed, click the **Chart** tab. On this page, choose **OBS Exception** in the **Chart Category** area. In the **Number of OBS EOFException Errors-All Instances** chart, view the host name of the instance that has the maximum number of OBS EOFException errors. For example, the host name is **node-ana-coreUQqJ0002**.

Step 4 Choose **O&M** > **Log** > **Download** and select **meta** and **meta** under it for **Service**.

Step 5 Select the host obtained in **Step 3** for **Hosts**.

Step 6 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time respectively. Then, click **Download**.

Step 7 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.3.371 ALM-45190 Total Number of Other OBS Exceptions Exceeds the Threshold

Alarm Description

The system checks whether the number of other OBS exceptions exceeds the threshold every 30 seconds. This alarm is generated when the number exceeds the threshold.

This alarm is automatically cleared when the number of other OBS exceptions is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45190	Minor	Error handling	Tenant plane	meta	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

Cluster components fail to access OBS. For systems with decoupled storage and compute, some computing tasks in the cluster may fail to be executed.

Possible Causes

OBSA throws an exception. For details about the cause, see related logs.

Handling Procedure

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Thresholds**. On the **Thresholds** page, choose **meta** > **OBS Exception** > **Total Number of Other OBS Exceptions**. In the right pane, set **Threshold** or **Trigger Count** to a larger value as required.

Step 2 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 3**.

Collect fault information.

Step 3 On FusionInsight Manager, choose **Cluster** > **Services** > **meta**. On the page that is displayed, click the **Chart** tab. On this page, choose **OBS Exception** in the **Chart Category** area. In the **Number of Other OBS Exceptions-All Instances** chart, view the host name of the instance that has the maximum number of other OBS exceptions. For example, the host name is **node-ana-coreUQqJ0002**.

Step 4 Choose **O&M** > **Log** > **Download** and select **meta** and **meta** under it for **Service**.

Step 5 Select the host obtained in **Step 3** for **Hosts**.

Step 6 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time respectively. Then, click **Download**.

Step 7 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.3.372 ALM-45191 Failed to Obtain ECS Metadata

Alarm Description

Before calling an ECS API to obtain the AK/SK information for the first time, Meta calls an ECS API first to obtain and cache the metadata. Then, it updates the cache every day. This alarm is generated when an API fails to be called for three consecutive times.

This alarm is cleared when Meta successfully calls the ECS API to obtain metadata.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45191	Major	Error handling	Tenant plane	meta	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

For systems with decoupled storage and compute, the cluster cannot obtain the latest temporary AK/SK because it fails to obtain the metadata. As a result, the cluster fails to access OBS, and component services cannot be provided.

Possible Causes

- The meta role of the MRS cluster is abnormal.
- The cluster has been bound to an agency and accessed OBS, but it has been unbound from the agency currently.

Handling Procedure

Check the status of the meta role.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**, click ⌄ in the row of this alarm, and view the host name of the instance for which the alarm is generated in **Location**.

Step 2 On FusionInsight Manager of the cluster, choose **Cluster** > **Services** > **meta**. On the page that is displayed, click the **Instance** tab, and check whether the meta role corresponding to the host for which the alarm is generated is normal.

- If yes, go to **Step 5**.
- If no, go to **Step 3**.

Step 3 Select the abnormal role, click **More**, and select **Restart Instance** to restart the abnormal meta role.

Step 4 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Step 5 Log in to the host obtained in **Step 1** and check whether the **/var/log/Bigdata/meta/mrs-meta.log** file contains error information. If yes, rectify the fault based on the log information.

Step 6 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Rebind the cluster to an agency.

Step 7 Log in to the MRS console.

Step 8 In the navigation pane on the left, choose **Clusters** > **Active Clusters**. On the page that is displayed, click the cluster name to go to its dashboard. Then, check whether the cluster is bound to an agency in the O&M management area.

- If yes, go to **Step 10**.
- If no, go to **Step 9**.

Step 9 Click **Manage Agency**. On the page that is displayed, rebind the cluster to an agency. Then check whether the alarm is cleared a few minutes later.

- If yes, no further action is required.
- If no, go to **Step 10**.

Collect fault information.

Step 10 On FusionInsight Manager of the active cluster, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 11 Expand the **Service** drop-down list, select **meta** for the target cluster, and click **OK**.

Step 12 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 13 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.373 ALM-45192 Failed to Obtain the IAM Security Token

Alarm Description

Meta calls an ECS API to obtain the AK/SK information. If permissions are set for users, Meta also needs to call an IAM API to obtain the security token. This alarm is generated when Meta fails to call the IAM API for three consecutive times.

This alarm is cleared when Meta successfully calls the IAM API.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45192	Major	Error handling	Tenant plane	meta	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

For systems with decoupled storage and compute, the cluster cannot obtain the latest security token. Users with fine-grained permissions may fail to access OBS and cannot use component services.

Possible Causes

- The meta role of the MRS cluster is abnormal.
- The IAM service is abnormal.

Handling Procedure

Check the status of the meta role.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**, click ⌄ in the row of this alarm, and view the host name of the instance for which the alarm is generated in **Location**.

Step 2 On FusionInsight Manager of the cluster, choose **Cluster** > **Services** > **meta**. On the page that is displayed, click the **Instance** tab, and check whether the meta role corresponding to the host for which the alarm is generated is normal.

- If yes, go to **Step 5**.
- If no, go to **Step 3**.

Step 3 Select the abnormal role, click **More**, and select **Restart Instance** to restart the abnormal meta role.

Step 4 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Step 5 Log in to the host obtained in **Step 1** and check whether the **/var/log/Bigdata/meta/mrs-meta.log** file contains error information. If yes, rectify the fault based on the log information.

Step 6 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect fault information.

Step 7 On FusionInsight Manager of the active cluster, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 8 Expand the **Service** drop-down list, select **meta** for the target cluster, and click **OK**.

Step 9 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.374 ALM-45275 Ranger Service Unavailable

Alarm Description

The alarm module checks the Ranger service status every 180 seconds. This alarm is generated if the Ranger service is abnormal.

This alarm is cleared after the Ranger service recovers.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45275	Critical	Error handling	Tenant plane	Ranger	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.

Type	Parameter	Description
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

The native UI of Ranger cannot be accessed, and policies cannot be created, modified, or deleted.

Possible Causes

- The DBService service on which Ranger depends is abnormal.
- The KrbServer service on which Ranger depends is abnormal.
- The LdapServer service on which Ranger depends is abnormal.
- The RangerAdmin role instance is abnormal.

Handling Procedure

Check the DBService process status.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. On the displayed page, check whether the ALM-27001 DBService Service Unavailable alarm is reported.

- If yes, go to **Step 2**.
- If no, go to **Step 3**.

Step 2 Rectify the DBService service fault by following the handling procedure of **ALM-27001 DBService Service Unavailable**. After the DBService alarm is cleared, check whether the **Ranger Service Unavailable** alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 3**.

Check the KrbServer status.

Step 3 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. On the page that is displayed, check whether **ALM-25500 KrbServer Service Unavailable** is reported.

- If yes, go to **Step 4**.
- If no, go to **Step 5**.

Step 4 Rectify the KrbServer service fault by following the handling procedure of **ALM-25500 KrbServer Service Unavailable**. After the KrbServer alarm is cleared, check whether the **Ranger Service Unavailable** alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check the LdapServer status.

Step 5 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. On the page that is displayed, check whether **ALM-12004 OLdap Resource Abnormal** is reported.

- If yes, go to **Step 6**.
- If no, go to **Step 7**.

Step 6 Rectify the LdapServer service fault by following the handling procedure of **ALM-12004 OLdap Resource Abnormal**. After the LdapServer alarm is cleared, check whether the **Ranger Service Unavailable** alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Check all RangerAdmin instances.

Step 7 Log in to the node where the RangerAdmin instance is located as user **omm** and run the **ps -ef|grep "proc_rangeradmin"** command to check whether the RangerAdmin process exists on the current node.

- If yes, go to **Step 8**.
- If no, restart the faulty RangerAdmin instance or Ranger service and go to **Step 7**.

Step 8 In the alarm list, check whether the **Ranger Service Unavailable** alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Collect the fault information.

Step 9 On FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 10 Expand the **Service** drop-down list, and select **Ranger** for the target cluster.

Step 11 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact technical support and provide the collected logs.

----End

Alarm Clearance

After the fault that triggers the alarm is rectified, the alarm is automatically cleared.

Related Information

None.

1.3.375 ALM-45276 Abnormal RangerAdmin Status

Alarm Description

The alarm module checks the RangerAdmin service status every 60 seconds. This alarm is generated if RangerAdmin is unavailable.

This alarm is automatically cleared after the RangerAdmin service recovers.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45276	Major	Error handling	Tenant plane	Ranger	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.

Type	Parameter	Description
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

If the status of a RangerAdmin is abnormal, access to the Ranger native UI is not affected. If there are two abnormal RangerAdmin instances, the Ranger native UI cannot be accessed and operations such as creating, modifying, and deleting policies are unavailable.

Possible Causes

The RangerAdmin port is not started.

Handling Procedure

Check the port process.

Step 1 In the alarm list on FusionInsight Manager, locate the row that contains the alarm, and click ⌄ to view the name of the host for which the alarm is generated.

Step 2 Log in to the node where the RangerAdmin instance is located as user **omm**. Run the **ps -ef|grep "proc_rangeradmin" | grep -v grep | awk -F ' ' '{print $2}'** command to obtain ***pid*** of the RangerAdmin process, and run the **netstat -anp| grep *pid* | grep LISTEN** command to check whether the RangerAdmin process listens to port 21401 in the security mode and port 21400 in standard mode.

- If yes, go to **Step 4**.
- If no, restart the faulty RangerAdmin instance or Ranger service and go to **Step 3**.

Step 3 In the alarm list, check whether the "Abnormal RangerAdmin Status" alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 4**.

Collect the fault information.

Step 4 On FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 5 Expand the **Service** drop-down list, and select **Ranger** for the target cluster.

Step 6 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 7 Contact technical support and provide the collected logs.

----End

Alarm Clearance

After the fault that triggers the alarm is rectified, the alarm is automatically cleared.

Related Information

None.

1.3.376 ALM-45277 RangerAdmin Heap Memory Usage Exceeds the Threshold

Alarm Description

The system checks the heap memory usage of the RangerAdmin service every 60 seconds. This alarm is generated when the system detects that the heap memory usage of the RangerAdmin instance exceeds the threshold (95% of the maximum memory) for 10 consecutive times. This alarm is cleared when the heap memory usage is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45277	Major	Quality of service	Tenant plane	Ranger	Yes

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

If the heap memory overflows, the service may break down. As a result, the native UI of Ranger cannot be accessed, and policies cannot be created, modified, or deleted.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Possible Causes

The heap memory usage of the RangerAdmin instance is high or the heap memory is improperly allocated.

Handling Procedure

Check the heap memory usage.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** > **ALM-45277 RangerAdmin Heap Memory Usage Exceeds the Threshold**. Check the location information of the alarm and view the host name of the instance for which the alarm is generated.

Step 2 On FusionInsight Manager, choose **Cluster** > **Services** > **Ranger** > **Instance**. Select the role corresponding to the host name of the instance for which the alarm is generated. Click the drop-down list in the upper right corner of the chart area and choose **Customize** > **CPU and Memory** > **RangerAdmin Heap Memory Usage**. Click **OK**.

Step 3 Check whether the heap memory used by RangerAdmin reaches the threshold (95% of the maximum heap memory by default).

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On FusionInsight Manager, choose **Cluster** > **Services** > **Ranger** > **Instance** > **RangerAdmin** > **Instance Configuration**. Click **All Configurations**, and choose **RangerAdmin** > **System**. Increase the value of **-Xmx** in the **GC_OPTS** parameter based on the site requirements and save the configuration.

NOTE

If this alarm is generated, the heap memory configured for RangerAdmin cannot meet the heap memory required by the RangerAdmin process. You are advised to check the heap memory usage of RangerAdmin and change the value of **-Xmx** in **GC_OPTS** to the twice of the heap memory used by RangerAdmin. The value can be changed based on the actual service scenario. For details, see **Step 2**.

Step 5 Restart the affected services or instances and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect the fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **Ranger** for the target cluster.

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.377 ALM-45278 RangerAdmin Direct Memory Usage Exceeds the Threshold

Alarm Description

The system checks the direct memory usage of the RangerAdmin service every 60 seconds. This alarm is generated when the direct memory usage of the RangerAdmin instance exceeds the threshold (80% of the maximum memory) for five consecutive times. This alarm is cleared when the direct memory usage of RangerAdmin is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45278	Major	Quality of service	Tenant plane	Ranger	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

If the direct memory overflows, the service may break down. As a result, the native UI of Ranger cannot be accessed, and policies cannot be created, modified, or deleted.

Possible Causes

The direct memory of the RangerAdmin instance is overused or the direct memory is inappropriately allocated. As a result, the memory usage exceeds the threshold.

Handling Procedure

Check the direct memory usage.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** > **ALM-45278 RangerAdmin Direct Memory Usage Exceeds the Threshold**. Check the location information of the alarm and view the host name of the instance for which the alarm is generated.

Step 2 On FusionInsight Manager, choose **Cluster** > **Services** > **Ranger** > **Instance**. Select the role corresponding to the host name of the instance for which the alarm is generated. Click the drop-down list in the upper right corner of the chart area and choose **Customize** > **CPU and Memory** > **RangerAdmin Direct Memory Usage**. Click **OK**.

Step 3 Check whether the direct memory used by RangerAdmin reaches the threshold (80% of the maximum direct memory by default).

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On FusionInsight Manager, choose **Cluster** > **Services** > **Ranger** > **Instance** > **RangerAdmin** > **Instance Configuration**. Click **All Configurations**, and choose **RangerAdmin** > **System**. Increase the value of **-XX:MaxDirectMemorySize** in the **GC_OPTS** parameter based on the site requirements and save the configuration.

NOTE

If this alarm is generated, the direct memory configured for RangerAdmin cannot meet the direct memory required by the RangerAdmin process. You are advised to check the direct memory usage of RangerAdmin and change the value of **-XX:MaxDirectMemorySize** in **GC_OPTS** to the twice of the direct memory used by RangerAdmin. You can change the value based on the actual service scenario. For details, see **Step 2**.

Step 5 Restart the affected services or instances and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect the fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **Ranger** for the target cluster.

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.378 ALM-45279 RangerAdmin Non-Heap Memory Usage Exceeds the Threshold

Alarm Description

The system checks the non-heap memory usage of the RangerAdmin service every 60 seconds. This alarm is generated when the non-heap memory usage of the RangerAdmin instance exceeds the threshold (80% of the maximum memory) for five consecutive times. This alarm is cleared when the non-heap memory usage is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45279	Major	Quality of service	Tenant plane	Ranger	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

If the non-heap memory overflows, the service may break down. As a result, the native UI of Ranger cannot be accessed, and policies cannot be created, modified, or deleted.

Possible Causes

The non-heap memory usage of the RangerAdmin instance is high or the non-heap memory is improperly allocated.

Handling Procedure

Check non-heap memory usage.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** > **ALM-45279 RangerAdmin Non-Heap Memory Usage Exceeds the Threshold**. Check the location information of the alarm and view the host name of the instance for which the alarm is generated.

Step 2 On FusionInsight Manager, choose **Cluster** > **Services** > **Ranger** > **Instance**. Select the role corresponding to the host name of the instance for which the alarm is generated. Click the drop-down list in the upper right corner of the chart area and choose **Customize** > **CPU and Memory** > **RangerAdmin Non-Heap Memory Usage**. Click **OK**.

Step 3 Check whether the non-heap memory used by RangerAdmin reaches the threshold (80% of the maximum non-heap memory by default).

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On FusionInsight Manager, choose **Cluster** > **Services** > **Ranger** > **Instance** > **RangerAdmin** > **Instance Configuration**. Click **All Configurations**, and choose **RangerAdmin** > **System**. Set **-XX: MaxPermSize** in the **GC_OPTS** parameter to a larger value based on site requirements and save the configuration.

NOTE

If this alarm is generated, the non-heap memory size configured for the RangerAdmin instance cannot meet the non-heap memory required by the RangerAdmin process. You are advised to change the value of **-XX:MaxPermSize** in **GC_OPTS** to the twice of the current non-heap memory usage or change the value based on the site requirements.

Step 5 Restart the affected services or instances and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect the fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **Ranger** for the target cluster.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.379 ALM-45280 RangerAdmin GC Duration Exceeds the Threshold

Alarm Description

The system checks the GC duration of the RangerAdmin process every 60 seconds. This alarm is generated when the GC duration of the RangerAdmin process exceeds the threshold for five consecutive times. This alarm is cleared when the GC duration is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45280	Critical (default threshold: 20000ms) Major (default threshold: 12000ms)	Quality of service	Tenant plane	Ranger	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.

Type	Parameter	Description
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

The RangerAdmin responds slowly to requests for creating, modifying, and deleting policies.

Possible Causes

The heap memory of the RangerAdmin instance is overused or the heap memory is inappropriately allocated. As a result, GCs occur frequently.

Handling Procedure

Check the GC duration.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** > **ALM-45280 RangerAdmin GC Duration Exceeds the Threshold**. Check the location information of the alarm and view the host name of the instance for which the alarm is generated.

Step 2 On FusionInsight Manager, choose **Cluster** > **Services** > **Ranger** > **Instance**. Select the role corresponding to the host name of the instance for which the alarm is generated and click the drop-down list in the upper right corner of the chart area. Choose **Customize** > **GC** > **RangerAdmin GC Duration**. Click **OK**.

Step 3 Check whether the GC duration of the RangerAdmin process collected every minute exceeds the threshold (12 seconds by default).

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On FusionInsight Manager, choose **Cluster** > **Services** > **Ranger** > **Instance** > **RangerAdmin** > **Instance Configuration**. Click **All Configurations**, and choose **RangerAdmin** > **System**. Increase the value of **-Xmx** in the **GC_OPTS** parameter based on the site requirements and save the configuration.

NOTE

If this alarm is generated, the heap memory configured for RangerAdmin cannot meet the heap memory required by the RangerAdmin process. You are advised to check the heap memory usage of RangerAdmin and change the value of **-Xmx** in **GC_OPTS** to the twice of the heap memory used by RangerAdmin. The value can be changed based on the actual service scenario. For details, see **Step 2**.

Step 5 Restart the affected services or instances and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect the fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **Ranger** for the target cluster.

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.380 ALM-45281 UserSync Heap Memory Usage Exceeds the Threshold

Alarm Description

The system checks the heap memory usage of the UserSync service every 60 seconds. This alarm is generated when the system detects that the heap memory usage of the UserSync instance exceeds the threshold (95% of the maximum memory) for 10 consecutive times. This alarm is cleared when the heap memory usage is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45281	Major	Quality of service	Tenant plane	Ranger	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

The service may break down. Ranger cannot synchronize LDAP user information.

Possible Causes

The heap memory usage of the UserSync instance is high or the heap memory is improperly allocated.

Handling Procedure

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** > **ALM-45281 UserSync Heap Memory Usage Exceeds the Threshold**. Check the location information of the alarm and view the host name of the instance for which the alarm is generated.

Step 2 On FusionInsight Manager, choose **Cluster** > **Services** > **Ranger** > **Instance**. Select the role corresponding to the host name of the instance for which the alarm is generated. Click the drop-down list in the upper right corner of the chart area and choose **Customize** > **CPU and Memory** > **UserSync Heap Memory Usage**. Click **OK**.

Step 3 Check whether the heap memory used by UserSync reaches the threshold (95% of the maximum heap memory by default).

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On FusionInsight Manager, choose **Cluster** > **Services** > **Ranger** > **Instance** > **UserSync** > **Instance Configuration**. Click **All Configurations**, and choose **UserSync** > **System**. Increase the value of **-Xmx** in the **GC_OPTS** parameter based on the site requirements and save the configuration.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

NOTE

If this alarm is generated, the heap memory configured for UserSync cannot meet the heap memory required by the UserSync process. You are advised to change the **-Xmx** value of **GC_OPTS** to twice that of the heap memory used by UserSync. You can change the value based on the actual service scenario. For details about how to check the UserSync heap memory usage, see **Step 2**.

Step 5 Restart the affected services or instances and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect the fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **Ranger** for the target cluster.

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.381 ALM-45282 UserSync Direct Memory Usage Exceeds the Threshold

Alarm Description

The system checks the direct memory usage of the UserSync service every 60 seconds. This alarm is generated when the direct memory usage of the UserSync instance exceeds the threshold (80% of the maximum memory) for five consecutive times. This alarm is cleared when the UserSync direct memory usage is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45282	Major	Quality of service	Tenant plane	Ranger	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

The service may break down. Ranger cannot synchronize LDAP user information.

Possible Causes

The direct memory of the UserSync instance is overused or the direct memory is inappropriately allocated. As a result, the memory usage exceeds the threshold.

Handling Procedure

Check the direct memory usage.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** > **ALM-45282 UserSync Direct Memory Usage Exceeds the Threshold**. Check the location information of the alarm. Check the name of the instance host for which the alarm is generated.

Step 2 On FusionInsight Manager, choose **Cluster** > **Services** > **Ranger** > **Instance**. Select the role corresponding to the host name of the instance for which the alarm is generated. Click the drop-down list in the upper right corner of the chart area and choose **Customize** > **CPU and Memory** > **UserSync Direct Memory Usage**. Click **OK**.

Step 3 Check whether the direct memory used by the UserSync reaches the threshold (80% of the maximum direct memory by default).

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On FusionInsight Manager, choose **Cluster** > **Services** > **Ranger** > **Instance** > **UserSync** > **Instance Configuration**. Click **All Configurations**, and choose **UserSync** > **System**. Increase the value of **-XX:MaxDirectMemorySize** in the **GC_OPTS** parameter based on the site requirements and save the configuration.

NOTE

If this alarm is generated, the direct memory configured for UserSync cannot meet the direct memory required by the UserSync process. You are advised to check the direct memory usage of UserSync and change the value of **-XX:MaxDirectMemorySize** in **GC_OPTS** to the twice of the direct memory used by UserSync. You can change the value based on the actual service scenario. For details, see **Step 2**.

Step 5 Restart the affected services or instances and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect the fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **Ranger** for the target cluster.

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Related Information

None.

1.3.382 ALM-45283 UserSync Non-Heap Memory Usage Exceeds the Threshold

Alarm Description

The system checks the non-heap memory usage of the UserSync service every 60 seconds. This alarm is generated when the non-heap memory usage of the UserSync instance exceeds the threshold (80% of the maximum memory) for five consecutive times. This alarm is cleared when the non-heap memory usage is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45283	Major	Quality of service	Tenant plane	Ranger	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

The service may break down. Ranger cannot synchronize LDAP user information.

Possible Causes

The non-heap memory of the UserSync process is overused or the non-heap memory is inappropriately allocated.

Handling Procedure

Check non-heap memory usage.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** > **ALM-45283 UserSync Non-Heap Memory Usage Exceeds the Threshold**. Check the location information of the alarm and view the host name of the instance for which the alarm is generated.

Step 2 On FusionInsight Manager, choose **Cluster** > **Services** > **Ranger** > **Instance**. Select the role corresponding to the host name of the instance for which the alarm is generated. Click the drop-down list in the upper right corner of the chart area and choose **Customize** > **CPU and Memory** > **UserSync Non-Heap Memory Usage**. Click **OK**.

Step 3 Check whether the non-heap memory used by UserSync reaches the threshold (80% of the maximum non-heap memory by default).

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On FusionInsight Manager, choose **Cluster** > **Services** > **Ranger** > **Instance** > **UserSync** > **Instance Configuration**. Click **All Configurations**, and choose **UserSync** > **System**. Set **-XX: MaxPermSize** in the **GC_OPTS** parameter to a larger value based on site requirements and click **Save** to save the configuration.

NOTE

If this alarm is generated, the non-heap memory size configured for the UserSync instance cannot meet the non-heap memory required by the UserSync process. You are advised to change the **-XX:MaxPermSize** value of **GC_OPTS** to twice that of the current non-heap memory size or change the value based on the site requirements.

Step 5 Restart the affected services or instances and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect the fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **Ranger** for the target cluster.

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.383 ALM-45284 UserSync Garbage Collection (GC) Time Exceeds the Threshold

Alarm Description

The system checks the GC duration of the UserSync process every 60 seconds. This alarm is generated when the GC duration of the UserSync process exceeds the threshold for five consecutive times. This alarm is cleared when the GC duration is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45284	Critical (default threshold: 20000ms) Major (default threshold: 12000ms)	Quality of service	Tenant plane	Ranger	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

If UserSync responds slowly, Ranger cannot synchronize LDAP user information quickly.

Possible Causes

The heap memory of the UserSync instance is overused or the heap memory is inappropriately allocated. As a result, GCs occur frequently.

Handling Procedure

Check the GC time.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** > **ALM-45284 UserSync Garbage Collection (GC) Time Exceeds the Threshold**. Check the location information of the alarm and view the host name of the instance for which the alarm is generated.

Step 2 On FusionInsight Manager, choose **Cluster** > **Services** > **Ranger** > **Instance**. Select the role corresponding to the host name of the instance for which the alarm is generated and click the drop-down list in the upper right corner of the chart area. Choose **Customize** > **GC** > **UserSync GC Duration**. Click **OK**.

Step 3 Check whether the GC duration of the UserSync process collected every minute exceeds the threshold (12 seconds by default).

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On FusionInsight Manager, choose **Cluster** > **Services** > **Ranger** > **Instance** > **UserSync** > **Instance Configuration**. Click **All Configurations**, and choose **UserSync** > **System**. Increase the value of **-Xmx** in the **GC_OPTS** parameter based on the site requirements and save the configuration.

NOTE

If this alarm is generated, the heap memory configured for UserSync cannot meet the heap memory required by the UserSync process. You are advised to change the value of **-Xmx** in **GC_OPTS** to the twice that of the heap memory used by UserSync. You can change the value based on the actual service scenario. For details about how to check the UserSync heap memory usage, see **Step 2**.

Step 5 Restart the affected services or instances and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect the fault information.

Step 6 On FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **Ranger** for the target cluster.

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

After the fault that triggers the alarm is rectified, the alarm is automatically cleared.

Related Information

None.

1.3.384 ALM-45285 TagSync Heap Memory Usage Exceeds the Threshold

Alarm Description

The system checks the heap memory usage of the TagSync service every 60 seconds. This alarm is generated when the heap memory usage of the TagSync instance exceeds the threshold (95% of the maximum memory) for 10 consecutive times. This alarm is cleared when the heap memory usage is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45285	Major	Quality of service	Tenant plane	Ranger	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.

Type	Parameter	Description
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

The service may break down. TagSync is unavailable for Ranger.

Possible Causes

The heap memory usage of the TagSync instance is high or the heap memory is improperly allocated.

Handling Procedure

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** > **ALM-45285 TagSync Heap Memory Usage Exceeds the Threshold**. Check the location information of the alarm and view the host name of the instance for which the alarm is generated.

Step 2 On FusionInsight Manager, choose **Cluster** > **Services** > **Ranger** > **Instance**. Select the role corresponding to the host name of the instance for which the alarm is generated. Click the drop-down list in the upper right corner of the chart area and choose **Customize** > **CPU and Memory** > **TagSync Heap Memory Usage**. Click **OK**.

Step 3 Check whether the heap memory used by TagSync reaches the threshold (95% of the maximum heap memory by default).

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On FusionInsight Manager, choose **Cluster** > **Services** > **Ranger** > **Instance** > **TagSync** > **Instance Configuration**. Click **All Configurations** and choose **TagSync** > **System**. Increase the value of **-Xmx** in the **GC_OPTS** parameter based on the site requirements and save the configuration.

NOTE

If this alarm is generated, the heap memory configured for TagSync cannot meet the heap memory required by the TagSync process. You are advised to change the **-Xmx** value of **GC_OPTS** to twice that of the heap memory used by TagSync. You can change the value based on the actual service scenario. For details about how to check the TagSync heap memory usage, see **Step 2**.

Step 5 Restart the affected services or instances and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect the fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **Ranger** for the target cluster.

Step 8 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

1.3.385 ALM-45286 TagSync Direct Memory Usage Exceeds the Threshold

Alarm Description

The system checks the direct memory usage of the TagSync service every 60 seconds. This alarm is generated when the direct memory usage of the TagSync instance exceeds the threshold (80% of the maximum memory) for five consecutive times. This alarm is cleared when the TagSync direct memory usage is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45286	Major	Quality of service	Tenant plane	Ranger	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

The service may break down. TagSync is unavailable for Ranger.

Possible Causes

The direct memory of the TagSync instance is overused or the direct memory is inappropriately allocated. As a result, the memory usage exceeds the threshold.

Handling Procedure

Check the direct memory usage.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** > **ALM-45286 TagSync Direct Memory Usage Exceeds the Threshold**. Check the location information of the alarm and view the host name of the instance for which the alarm is generated.

Step 2 On FusionInsight Manager, choose **Cluster** > **Services** > **Ranger** > **Instance**. Select the role corresponding to the host name of the instance for which the alarm is generated. Click the drop-down list in the upper right corner of the chart area and choose **Customize** > **CPU and Memory** > **TagSync Direct Memory Usage**. Click **OK**.

Step 3 Check whether the direct memory used by the TagSync reaches the threshold (80% of the maximum direct memory by default).

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On FusionInsight Manager, choose **Cluster** > **Services** > **Ranger** > **Instance** > **TagSync** > **Instance Configuration**. Click **All Configurations** and choose **TagSync** > **System**. Increase the value of **-XX:MaxDirectMemorySize** in the **GC_OPTS** parameter based on the site requirements and save the configuration.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

NOTE

If this alarm is generated, the direct memory configured for TagSync cannot meet the direct memory required by the TagSync process. You are advised to check the direct memory usage of TagSync and change the value of **-XX:MaxDirectMemorySize** in **GC_OPTS** to the twice of the direct memory used by TagSync. You can change the value based on the actual service scenario. For details, see **Step 2**.

Step 5 Restart the affected services or instances and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect the fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **Ranger** for the target cluster.

Step 8 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.386 ALM-45287 TagSync Non-Heap Memory Usage Exceeds the Threshold

Alarm Description

The system checks the non-heap memory usage of the TagSync service every 60 seconds. This alarm is generated when the non-heap memory usage of the TagSync instance exceeds the threshold (80% of the maximum memory) for five consecutive times. This alarm is cleared when the non-heap memory usage is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45287	Major	Quality of service	Tenant plane	Ranger	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

The service may break down. TagSync is unavailable for Ranger.

Possible Causes

The non-heap memory of the TagSync process is overused or the non-heap memory is inappropriately allocated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Handling Procedure

Check non-heap memory usage.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** > **ALM-45287 TagSync Non-Heap Memory Usage Exceeds the Threshold**. Check the location information of the alarm and view the host name of the instance for which the alarm is generated.

Step 2 On FusionInsight Manager, choose **Cluster** > **Services** > **Ranger** > **Instance**. Select the role corresponding to the host name of the instance for which the alarm is generated. Click the drop-down list in the upper right corner of the chart area and choose **Customize** > **CPU and Memory** > **TagSync Non-Heap Memory Usage**. Click **OK**.

Step 3 Check whether the non-heap memory used by TagSync reaches the threshold (80% of the maximum non-heap memory by default).

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On FusionInsight Manager, choose **Cluster** > **Services** > **Ranger** > **Instance** > **TagSync** > **Instance Configuration**. Click **All Configurations** and choose **TagSync** > **System**. Set **-XX: MaxPermSize** in the **GC_OPTS** parameter to a larger value based on site requirements and save the configuration.

NOTE

If this alarm is generated, the non-heap memory size configured for the TagSync instance cannot meet the non-heap memory required by the TagSync process. You are advised to change the **-XX:MaxPermSize** value of **GC_OPTS** to twice that of the current non-heap memory size or change the value based on the site requirements.

Step 5 Restart the affected services or instances and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect the fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **Ranger** for the target cluster.

Step 8 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.387 ALM-45288 TagSync Garbage Collection (GC) Time Exceeds the Threshold

Alarm Description

The system checks the GC duration of the TagSync process every 60 seconds. This alarm is generated when the GC duration of the TagSync process exceeds the threshold for five consecutive times. This alarm is cleared when the GC duration is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45288	Critical (default threshold: 20000ms) Major (default threshold: 12000ms)	Quality of service	Tenant plane	Ranger	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

TagSync is unavailable for Ranger.

Possible Causes

The heap memory of the TagSync instance is overused or the heap memory is inappropriately allocated. As a result, GCs occur frequently.

Handling Procedure

Check the GC duration.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** > **ALM-45288 TagSync Garbage Collection (GC) Time Exceeds the Threshold**. Check the location information of the alarm and view the host name of the instance for which the alarm is generated.

Step 2 On FusionInsight Manager, choose **Cluster** > **Services** > **Ranger** > **Instance**. Select the role corresponding to the host name of the instance for which the alarm is generated and click the drop-down list in the upper right corner of the chart area. Choose **Customize** > **GC** > **TagSync GC Duration**. Click **OK**.

Step 3 Check whether the GC duration of the TagSync process collected every minute exceeds the threshold (12 seconds by default).

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On FusionInsight Manager, choose **Cluster** > **Services** > **Ranger** > **Instance** > **TagSync** > **Instance Configuration**. Click **All Configurations** and choose **TagSync** > **System**. Increase the value of **-Xmx** in the **GC_OPTS** parameter based on the site requirements and save the configuration.

NOTE

If this alarm is generated, the heap memory configured for TagSync cannot meet the heap memory required by the TagSync process. You are advised to change the **-Xmx** value of **GC_OPTS** to twice that of the heap memory used by TagSync. You can change the value based on the actual service scenario. For details about how to check the TagSync heap memory usage, see **Step 2**.

Step 5 Restart the affected services or instances and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect the fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **Ranger** for the target cluster.

Step 8 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.388 ALM-45289 PolicySync Heap Memory Usage Exceeds the Threshold

Alarm Description

The system checks the heap memory usage of the PolicySync service every 60 seconds. This alarm is generated when the heap memory usage of the PolicySync instance exceeds the threshold (95% of the maximum memory) for 10 consecutive times. This alarm is cleared when the heap memory usage is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45289	Major	Quality of service	Tenant plane	Ranger	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

The service may break down. Ranger cannot connect to LakeFormation.

Possible Causes

The heap memory of the PolicySync instance is overused or the heap memory is inappropriately allocated.

Handling Procedure

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Alarms** > **ALM-45289 PolicySync Heap Memory Usage Exceeds the Threshold**. Check the location information of the alarm and view the host name of the instance for which the alarm is generated.

Step 2 On FusionInsight Manager, choose **Cluster** > **Services** > **Ranger** > **Instance**. Select the role corresponding to the host name of the instance for which the alarm is generated. Click the drop-down list in the upper right corner of the chart area and choose **Customize** > **CPU and Memory** > **PolicySync Heap Memory Usage**. Click **OK**.

Step 3 Check whether the heap memory used by PolicySync reaches the threshold (95% of the maximum heap memory by default).

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On FusionInsight Manager, choose **Cluster** > **Services** > **Ranger** > **Instance** > **PolicySync**. Click **Instance Configuration** and then **All Configurations**, and choose **PolicySync** > **System**. Set **-Xmx** in the **GC_OPTS** parameter to a larger value based on site requirements and save the configuration.

NOTE

If this alarm is generated, the heap memory configured for PolicySync cannot meet the heap memory required by the PolicySync process. You are advised to change the value of **-Xmx** in **GC_OPTS** to twice that of the heap memory used by PolicySync. You can change the value based on the actual service scenario. Refer to **Step 2** to view the PolicySync heap memory usage.

Step 5 Restart the affected services or instances and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **Ranger** for the target cluster.

Step 8 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.389 ALM-45290 PolicySync Direct Memory Usage Exceeds the Threshold

Alarm Description

The system checks the direct memory usage of the PolicySync service every 60 seconds. This alarm is generated when the direct memory usage of the PolicySync instance exceeds the threshold (90% of the maximum memory) for five consecutive times. This alarm is cleared when the PolicySync direct memory usage is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45290	Major	Quality of service	Tenant plane	Ranger	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

The service may break down. Ranger cannot connect to LakeFormation.

Possible Causes

The direct memory of the PolicySync process is overused or the direct memory is inappropriately allocated.

Handling Procedure

Check the direct memory usage.

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Alarms** > **ALM-45290 PolicySync Direct Memory Usage Exceeds the Threshold**. Check the location information of the alarm and view the host name of the instance for which the alarm is generated.

Step 2 On FusionInsight Manager, choose **Cluster** > **Services** > **Ranger** > **Instance**. Select the role corresponding to the host name of the instance for which the alarm is generated. Click the drop-down list in the upper right corner of the chart area and choose **Customize** > **CPU and Memory** > **PolicySync Direct Memory Usage**. Click **OK**.

Step 3 Check whether the direct memory used by the PolicySync reaches the threshold (90% of the maximum direct memory by default).

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On FusionInsight Manager, choose **Cluster** > **Services** > **Ranger** > **Instance** > **PolicySync**. Click **Instance Configuration** and then **All Configurations**, and choose **PolicySync** > **System**. Set **-XX:MaxDirectMemorySize** in the **GC_OPTS** parameter to a larger value based on site requirements and save the configuration.

NOTE

If this alarm is generated, the direct memory configured for PolicySync cannot meet the direct memory required by the PolicySync process. You are advised to check the direct memory usage of PolicySync and change the value of **-XX:MaxDirectMemorySize** in **GC_OPTS** to the twice of the direct memory used by PolicySync. You can change the value based on the actual service scenario. Refer to **Step 2** to view the TokenServer direct memory usage.

Step 5 Restart the affected services or instances and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **Ranger** for the target cluster.

Step 8 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.390 ALM-45291 PolicySync Non-Heap Memory Usage Exceeds the Threshold

Alarm Description

The system checks the non-heap memory usage of the PolicySync service every 60 seconds. This alarm is generated when the non-heap memory usage of the PolicySync instance exceeds the threshold (90% of the maximum memory) for five consecutive times. This alarm is cleared when the non-heap memory usage is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45291	Major	Quality of service	Tenant plane	Ranger	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

The service may break down. Ranger cannot connect to LakeFormation.

Possible Causes

The non-heap memory of the PolicySync instance is overused or the non-heap memory is inappropriately allocated.

Handling Procedure

Check non-heap memory usage.

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Alarms** > **ALM-45291 PolicySync Non-Heap Memory Usage Exceeds the Threshold**. Check the location information of the alarm and view the host name of the instance for which the alarm is generated.

Step 2 On FusionInsight Manager, choose **Cluster** > **Services** > **Ranger** > **Instance**. Select the role corresponding to the host name of the instance for which the alarm is generated. Click the drop-down list in the upper right corner of the chart area and choose **Customize** > **CPU and Memory** > **PolicySync Non-Heap Memory Usage**. Click **OK**.

Step 3 Check whether the non-heap memory used by PolicySync reaches the threshold (90% of the maximum heap memory by default).

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On FusionInsight Manager, choose **Cluster** > **Services** > **Ranger** > **Instance** > **PolicySync**. Click **Instance Configuration** and then **All Configurations**, and choose **PolicySync** > **System**. Set **-XX: MaxPermSize** in the **GC_OPTS** parameter to a larger value based on site requirements and save the configuration.

NOTE

If this alarm is generated, the non-heap memory size configured for the PolicySync instance cannot meet the non-heap memory required by the PolicySync process. You are advised to change the value of **-XX:MaxPermSize** in **GC_OPTS** to twice that of the current non-heap memory size or change the value based on site requirements.

Step 5 Restart the affected services or instances and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **Ranger** for the target cluster.

Step 8 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.391 ALM-45292 PolicySync GC Duration Exceeds the Threshold

Alarm Description

The system checks the GC duration of the PolicySync process every 60 seconds. This alarm is generated when the GC duration of the PolicySync process exceeds the threshold for five consecutive times. This alarm is cleared when the GC duration is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45292	Critical (default threshold: 20000 ms) Major (default threshold: 12000 ms)	Quality of service	Tenant plane	Ranger	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.

Type	Parameter	Description
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

Ranger cannot connect to LakeFormation.

Possible Causes

The heap memory of the PolicySync process is overused or inappropriately allocated, causing frequent occurrence of the GC process.

Handling Procedure

Check the GC duration.

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Alarms** > **ALM-45292 PolicySync GC Duration Exceeds the Threshold**. Check the location information of the alarm and view the host name of the instance for which the alarm is generated.

Step 2 On FusionInsight Manager, choose **Cluster** > **Services** > **Ranger** > **Instance**. Select the role corresponding to the host name of the instance for which the alarm is

generated and click the drop-down list in the upper right corner of the chart area. Choose **Customize** > **GC** > **PolicySync GC Duration**. Click **OK**.

Step 3 Check whether the GC duration of the PolicySync process collected every minute exceeds the threshold (12 seconds by default).

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On FusionInsight Manager, choose **Cluster** > **Services** > **Ranger** > **Instance** > **PolicySync**. Click **Instance Configuration** and then **All Configurations**, and choose **PolicySync** > **System**. Set **-Xmx** in the **GC_OPTS** parameter to a larger value based on site requirements and save the configuration.

NOTE

If this alarm is generated, the heap memory configured for PolicySync cannot meet the heap memory required by the PolicySync process. You are advised to change the value of **-Xmx** in **GC_OPTS** to twice that of the heap memory used by PolicySync. You can change the value based on the actual service scenario. Refer to **Step 2** to view the PolicySync heap memory usage.

Step 5 Restart the affected services or instances and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **Ranger** for the target cluster.

Step 8 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.392 ALM-45293 Ranger User Synchronization Exception

Alarm Description

The system checks synchronization status of the UserSync process every 5 minutes. This alarm is generated when a synchronization exception occurs. This alarm is cleared when user synchronization becomes normal.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45293	Major	Quality of service	Tenant plane	Ranger	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
New	3.3.1	New alarm	New alarm

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the trigger condition, that is, an exception occurs during Ranger user synchronization.

Impact on the System

Unsynchronized users cannot access the native Ranger page and set permission policies for other users. As a result, some users may fail to access services that require Ranger permissions.

Possible Causes

The RangerAdmin instance is abnormal.

The UserSync instance is abnormal.

The LDAP service is abnormal.

Handling Procedure

Check whether the UserSync is abnormal.

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Alarms** > **ALM-45293 Ranger User Synchronization Exception**. Check the location information of the alarm and view the host name of the instance for which the alarm is generated.

Step 2 On FusionInsight Manager, choose **Cluster** > **Services** > **Ranger** > **Instance**, select the UserSync instance on the host for which the alarm is generated, and check whether the instance status is abnormal.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 On FusionInsight Manager, choose **Cluster** > **Services** > **Ranger**, click **Instances**, and click **UserSync**. On the displayed page, click **More** > **Restart Instance**, or restart the Ranger service.

Step 4 Check whether the alarm is cleared in 5 to 10 minutes.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check whether the RangerAdmin is abnormal.

Step 5 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** to check whether alarm "ALM-45276 Abnormal RangerAdmin Status" is reported.

- If yes, go to **Step 6**.
- If no, go to **Step 8**.

Step 6 Rectify the fault by following the handling procedure of "ALM-45276 Abnormal RangerAdmin Status".

Step 7 Check whether the alarm is cleared in 5 to 10 minutes.

- If yes, no further action is required.
- If no, go to **Step 8**.

Check whether the LDAP service is abnormal.

Step 8 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** to check whether alarm "ALM-25000 LdapServer Service Unavailable" is reported.

- If yes, go to **Step 9**.
- If no, go to **Step 11**.

Step 9 Clear the alarm according to the handling procedure of "ALM-25000 LdapServer Service Unavailable".

Step 10 Check whether the alarm is cleared in 5 to 10 minutes.

- If yes, no further action is required.
- If no, go to **Step 11**.

Collect fault information.

Step 11 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 12 Expand the **Service** drop-down list, and select **Ranger** for the target cluster.

Step 13 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 14 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.393 ALM-45294 RangerKMS Process Is Abnormal

Alarm Description

The RangerKMS process checks the process status every 20 seconds. This alarm is generated when the process status is abnormal and does not recover for a long time.

This alarm is cleared when the process status recovers.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45294	Major	Quality of service	Tenant plane	Ranger	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
New	3.3.1	New alarm	New alarm

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

If the process status is abnormal, the process cannot provide services properly. As a result, the entire service may become abnormal.

Possible Causes

The host responds slowly to I/O (disk I/O and network I/O) requests and some processes are in the D state and Z state. The process may also be suspended and enter the T state.

Handling Procedure

Check whether the process is in the D, Z, or T state.

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Alarms**. Wait for about 10 minutes and check whether the alarm is automatically cleared.

- If the alarm is not in the list, no further action is required.
- If the alarm is in the list, view the alarm details and record the IP address of the host where the alarm is generated. Run the command in **Step 2**.

Step 2 Log in to the host where the alarm is generated as the **root** user and run the **su - omm** command to switch to the **omm** user.

Step 3 Run the following command to check the process state:

ps ww -eo stat,cmd| grep -w Dproc_rangerkms | grep -v grep | awk '{print$1}'

Step 4 Check whether the command output contains any abnormal state (D, Z, or T).

- If the output contains any abnormal state, go to **Step 5**.
- If the output does not contain abnormal states, go to **Step 7**.

Step 5 Switch to user **root** and run the **reboot** command to restart the host for which the alarm is generated. (Restarting a host is risky. Ensure that the service process is normal after the restart.)

Step 6 Wait 5 minutes and check whether the alarm is cleared.

- If the alarm is cleared, no further action is required.
- If the alarm fails to be cleared, go to **Step 7**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Collect fault information.

Step 7 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 8 Expand the drop-down list next to the **Service** field. In the **Services** dialog box that is displayed, select **Ranger** for the target cluster.

Step 9 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.394 ALM-45425 ClickHouse Service Unavailable

Alarm Description

The alarm module checks the ClickHouseServer instance status every 60 seconds. This alarm is generated when the alarm module detects that all instances of a ClickHouseServer shard are abnormal.

This alarm is cleared when the system detects that any instance of the ClickHouseServer shard is restored and the alarm is handled.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45425	Critical	Quality of service	Tenant plane	ClickHouse	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.

Type	Parameter	Description
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

FusionInsight Manager cannot be used to perform cluster operations on the ClickHouse service, and ClickHouse service functions are unavailable.

Possible Causes

- The ZooKeeper service is unavailable.
- The configuration information in the **metrika.xml** file in the component configuration directory of the faulty ClickHouse instance is inconsistent with configuration of that ClickHouse instance in ZooKeeper.

Handling Procedure

The ZooKeeper service is unavailable.

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Alarms**. In the alarm list, check whether alarm **ALM-13000 ZooKeeper Service Unavailable** exists.

- If yes, go to **Step 2**.
- If no, go to **Step 3**.

Step 2 Handle alarm **ALM-13000 ZooKeeper Service Unavailable** according to the alarm help. In the alarm list, check whether alarm **ALM-45425 ClickHouse Service Unavailable** is cleared.

- If yes, no further action is required.
- If no, go to **Step 3**.

Check whether the configuration in metrika.xml of the ClickHouse instance is correct.

Step 3 Log in to FusionInsight Manager, choose **Cluster** > **Services** > **ClickHouse**, click the **Instance** tab, and check whether there is any abnormal ClickHouse instance based on the alarm information.

- If yes, go to **Step 4**.
- If no, go to **Step 11**.

Step 4 Log in to the host where the ClickHouse service is abnormal and ping the IP address of another normal ClickHouse instance node to check whether the network connection is normal.

- If yes, go to **Step 5**.
- If no, contact the network administrator to repair the network.

Step 5 Log in to the node where the client is installed as the client installation user and run the following commands:

cd *{Client installation path}*

source bigdata_env

- For a cluster with Kerberos authentication enabled (security mode):

  kinit *Component service user*

  clickhouse client --host *IP address of the ClickHouseServer instance for which the alarm is reported* **--port** 21427 **--secure**

- For a cluster with Kerberos authentication disabled (normal mode):

  clickhouse client --host *IP address of the ClickHouseServer instance for which the alarm is reported* **--user** *Username* **--password --port** 21423

Run the following command to query the value of **macros.id**:

select substitution from system.macros where macro='id';

Step 6 Log in to the host where the ZooKeeper client is located and log in to the ZooKeeper client.

Switch to the client installation directory.

Example: **cd /opt/hadoopclient**

Run the following command to configure environment variables:

source bigdata_env

Run the following command to authenticate the user (skip this step for a cluster in normal mode):

kinit *Component service user*

Run the following command to log in to the client tool:

zkCli.sh -server *Service IP address of the node where the ZooKeeper instance resides*: *Client port*

Step 7 Run the following command to check whether the ClickHouse cluster topology information can be obtained:

get /clickhouse/config/*macros.id* *value in* ***Step 5*****/metrika.xml**

- If yes, go to **Step 8**.
- If no, go to **Step 11**.

Step 8 Log in to the host where the ClickHouse instance is abnormal and go to the configuration directory of the ClickHouse instance.

cd ${BIGDATA_HOME}**/FusionInsight_ClickHouse_***Version***/**x_x_**ClickHouseServer/etc**

cat metrika.xml

Step 9 Check whether the cluster topology information on ZooKeeper obtained in **Step 7** is the same as that in the **metrika.xml** file in the component configuration directory in **Step 8**.

- If yes, check whether the alarm is cleared. If the alarm persists, go to **Step 11**.
- If no, go to **Step 10**.

Step 10 On FusionInsight Manager, choose **Cluster** > **Services** > **ClickHouse**, click **More**, and select **Synchronize Configuration**. Then, check whether the service status is normal and whether the alarm is cleared 5 minutes later.

- If yes, no further action is required.
- If no, go to **Step 11**.

Collect fault information.

Step 11 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 12 Expand the **Service** drop-down list, and select **ClickHouse** for the target cluster.

Step 13 Expand the **Hosts** drop-down list and select the target hosts.

Step 14 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 15 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.395 ALM-45426 ClickHouse Service Quantity Quota Usage in ZooKeeper Exceeds the Threshold

Alarm Description

The alarm module checks the quota usage of the ClickHouse service in the ZooKeeper every 60 seconds. This alarm is generated when the alarm module detects that the usage exceeds the threshold (90%).

This alarm is cleared when the system detects that the usage is lower than the threshold and the alarm is cleared.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45426	Critical (default threshold: 95%) Major (default threshold: 90%)	Quality of service	Tenant plane	ClickHouse	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

After the ZooKeeper quantity quota of the ClickHouse service exceeds the threshold, you cannot perform cluster operations on the ClickHouse service on FusionInsight Manager. As a result, the ClickHouse service cannot be used.

Possible Causes

- When table data is created, inserted, or deleted, the ClickHouse creates znodes on ZooKeeper nodes. As the service volume increases, the number of znodes may exceed the configured threshold.
- No quota limit is set for the metadata directory **/clickhouse** of ClickHouse in ZooKeeper.

Handling Procedure

Check the number of znodes created by ClickHouse on ZooKeeper.

Step 1 Log in to the host where the ZooKeeper client is located and log in to the ZooKeeper client.

Switch to the client installation directory.

Example: **cd /opt/hadoopclient**

Run the following command to configure environment variables:

source bigdata_env

Run the following command to authenticate the user (skip this step in common mode):

kinit *Component service user*

Run the following command to log in to the client tool:

zkCli.sh -server *service IP address of the node where the ZooKeeper role instance locates:client port*

Step 2 Run the following command to check the quota used by the ClickHouse in the ZooKeeper and check whether the quota information is correctly set:

listquota /clickhouse

```
absolute path is /zookeeper/quota/clickhouse
Quota for path /clickhouse does not exist.
```

If the preceding information indicates that the quota configuration is incorrect, go to **Step 3**.

If no, go to **Step 5**.

Step 3 Log in to FusionInsight Manager and choose **Cluster** > **Services** > **ZooKeeper**. On the displayed page, click **Configurations** and click **All Configurations**. On this sub-tab page, search for **quotas.auto.check.enable** to check whether its value is **true**.

If the value is not **true**, change the value to **true** and click **Save**.

Step 4 On FusionInsight Manager, choose **Cluster** > **Services** > **ClickHouse**, click **More**, and select **Synchronize Configuration**. After the synchronization is successful, go to **Step 1**.

Step 5 Run the following command and check whether the ratio of the **count** value of **Output stat** to the **count** value of **Output quota** in the command output is greater than **0.9**:

listquota /clickhouse

```
absolute path is /zookeeper/quota/clickhouse
Output quota for /clickhouse count=200000,bytes=1000000000
Output stat for /clickhouse count=2667,bytes=60063
```

In the preceding information, the **count** value of **Output stat** is **2667**, and the **count** value of **Output quota** is **200000**.

- If yes, go to **Step 6**.
- If no, check whether the alarm is cleared 5 minutes later. If the alarm persists, go to **Step 8**.

Step 6 On FusionInsight Manager, choose **Cluster** > **Services** > **ClickHouse**. Click **Configurations** and then **All Configurations**. Search for **clickhouse.zookeeper.quota.node.count**, set it to a value twice the **count** of **Output stat** in **Step 5**. Do not use a value larger than 6000000. Otherwise, there will be high risks. Exercise caution when setting this parameter.

Step 7 Restart the ClickHouse instance for which the alarm is generated, and check whether the alarm is cleared 5 minutes later.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If yes, no further action is required.
- If no, perform **Step 6** again, and check whether the alarm is cleared 5 minutes later. If the alarm persists, go to **Step 8**.

Collect the fault information.

Step 8 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 9 Expand the **Service** drop-down list, and select **ClickHouse** for the target cluster.

Step 10 Choose the corresponding host form the host list.

Step 11 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.396 ALM-45427 ClickHouse Service Capacity Quota Usage in ZooKeeper Exceeds the Threshold

Alarm Description

The alarm module checks the quota usage of the ClickHouse service in the ZooKeeper every 60 seconds. This alarm is generated when the alarm module detects that the usage exceeds the threshold (90%).

This alarm is cleared when the system detects that the usage is lower than the threshold and the alarm is cleared.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45427	Critical (default threshold: 95%) Major (default threshold: 90%)	Quality of service	Tenant plane	ClickHouse	Yes

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

After the ZooKeeper capacity quota of the ClickHouse service exceeds the threshold, you cannot perform cluster operations on the ClickHouse service on FusionInsight Manager. As a result, the ClickHouse service cannot be used.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Possible Causes

- When table data is created, inserted, or deleted, ClickHouse creates znodes on ZooKeeper nodes. As the service volume increases, the capacity of znodes may exceed the configured threshold.
- No quota limit is set for the metadata directory **/clickhouse** of ClickHouse in ZooKeeper.

Handling Procedure

Check the znode capacity of the ClickHouse in the ZooKeeper.

Step 1 Log in to the host where the ZooKeeper client is located and log in to the ZooKeeper client.

Switch to the client installation directory.

Example: **cd /opt/hadoopclient**

Run the following command to configure environment variables:

source bigdata_env

Run the following command to authenticate the user (skip this step in common mode):

kinit *Component service user*

Run the following command to log in to the client tool:

zkCli.sh -server *service IP address of the node where the ZooKeeper role instance locates*:*client port*

Step 2 Run the following command to check the quota used by the ClickHouse in the ZooKeeper and check whether the quota information is correctly set:

listquota /clickhouse

```
absolute path is /zookeeper/quota/clickhouse
Quota for path /clickhouse does not exist.
```

- If the preceding information indicates that the quota configuration is incorrect, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 Log in to FusionInsight Manager and choose **Cluster** > **Services** > **ZooKeeper**. On the displayed page, click **Configurations** and click **All Configurations**. On this sub-tab page, search for **quotas.auto.check.enable** to check whether its value is **true**.

If the value is not **true**, change the value to **true** and click **Save**.

Step 4 On FusionInsight Manager, choose **Cluster** > **Services** > **ClickHouse**, click **More**, and select **Synchronize Configuration**. After the synchronization is successful, go to **Step 1**.

Step 5 Run the following command and check whether the ratio of the **bytes** value of **Output stat** to the **bytes** value of **Output quota** in the command output is greater than **0.9**:

listquota /clickhouse

```
absolute path is /zookeeper/quota/clickhouse
Output quota for /clickhouse count=200000,bytes=1000000000
Output stat for /clickhouse count=2667,bytes=60063
```

In the preceding information, the **bytes** value of **Output stat** is **60063**, and the **bytes** value of **Output quota** is **1000000000**.

- If yes, go to **Step 6**.
- If no, check whether the alarm is cleared 5 minutes later. If the alarm persists, go to **Step 8**.

Step 6 On FusionInsight Manager, choose **Cluster** > **Services** > **ClickHouse**. Click **Configurations** and then **All Configurations**. Search for **clickhouse.zookeeper.quota.size**, set it to a value twice the **bytes** of **Output stat** in **Step 5**. Do not use a value larger than 6000000. Otherwise, there will be high risks. Exercise caution when setting this parameter.

Step 7 Restart the ClickHouse instance for which the alarm is generated, and check whether the alarm is cleared 5 minutes later.

- If yes, no further action is required.
- If no, perform **Step 6** again, and check whether the alarm is cleared 5 minutes later. If the alarm persists, go to **Step 8**.

Collect the fault information.

Step 8 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 9 Expand the **Service** drop-down list, and select **ClickHouse** for the target cluster.

Step 10 Choose the corresponding host form the host list.

Step 11 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.397 ALM-45428 ClickHouse Disk I/O Exception

Description

This alarm is generated when the alarm module detects EIO or EROFS errors during ClickHouse read and write every 60 seconds.

Attribute

Alarm ID	Alarm Severity	Auto Clear
45428	Major (default)	No

Parameters

Name	Meaning
Source	Specifies the cluster for which the alarm is generated.
ServiceName	Specifies the service for which the alarm is generated.
RoleName	Specifies the role for which the alarm is generated.
HostName	Specifies the host for which the alarm is generated.

Impact on the System

- ClickHouse fails to read and write data. The INSERT, SELECT, and CREATE operations on the local tables may be abnormal. Distributed tables are not affected.
- Services are affected, and I/O operations fail.

Possible Causes

The disk is aged or has bad sectors.

Procedure

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** > **ALM-45428 ClickHouse Disk I/O Exception**. Check the role name and the IP address of the host where the alarm is generated in **Location**.

Step 2 Use PuTTY to log in to the node for which the fault is generated as user **root**.

Step 3 Run the **df -h** command to check the mount directory and find the disk mounted to the faulty directory.

Step 4 Run the **smartctl -a /dev/sd*** command to check disks.

- If **SMART Health Status: OK** is displayed, as shown in the following figure, the disk is healthy. In this case, go to **Step 6**.

```
=== START OF READ SMART DATA SECTION ===
SMART Health Status: OK

Current Drive Temperature:     26 C
Drive Trip Temperature:        60 C

Manufactured in week 50 of year 2018
Specified cycle count over device lifetime:  10000
Accumulated start-stop cycles:  25
Specified load-unload count over device lifetime:  300000
Accumulated load-unload cycles:  356
Elements in grown defect list: 0
```

- If the number following **Elements in grown defect list** is not 0, as shown in the following figure, the disk may have bad sectors. If **SMART Health Status: FAILURE** is displayed, the disk is in the sub-health state. In this case, contact O&M personnel and to **Step 5**.

```
=== START OF READ SMART DATA SECTION ===
SMART Health Status: FAILURE PREDICTION THRESHOLD EXCEEDED: ascq=0x5 [asc=5d, ascq=5]

Current Drive Temperature:     30 C
Drive Trip Temperature:        60 C

Manufactured in week 50 of year 2018
Specified cycle count over device lifetime:  10000
Accumulated start-stop cycles:  28
Specified load-unload count over device lifetime:  300000
Accumulated load-unload cycles:  354
Elements in grown defect list: 5344

Vendor (Seagate) cache information
```

Step 5 After the fault is rectified, manually clear the alarm on FusionInsight Manager and check whether the alarm is generated again during the periodic check.

- If yes, go to **Step 6**.
- If no, no further action is required.

Collect fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **ClickHouse** for the target cluster.

Step 8 Expand the **Hosts** drop-down list and select the target hosts.

Step 9 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearing

If the alarm has no impact, manually clear the alarm.

Related Information

None

1.3.398 ALM-45429 Table Metadata Synchronization Failed on the Added ClickHouse Node

Alarm Description

This alarm is generated when the local table corresponding to the distributed table fails to be created during ClickHouse capacity expansion.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45429	Major	Quality of service	Tenant plane	ClickHouse	No

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

The distributed table fails to be queried.

Possible Causes

A node is stopped or faulty during capacity expansion.

Handling Procedure

Step 1 On FusionInsight Manager, choose **Cluster** > **Services** > **ClickHouse** > **Instance**.

Step 2 Check whether an instance is stopped, decommissioned, or faulty.

- If yes, go to **Step 3**.
- If no, go to **Step 4**.

Step 3 Start the instance or rectify the instance fault until all instances are running properly.

Step 4 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**, locate this alarm and the faulty host based on the location information.

Step 5 Log in to the faulty host as user **omm**.

Step 6 Run the following commands to initialize environment variables:

```
source ${BIGDATA_HOME}/FusionInsight_ClickHouse_*/*_*_ClickHouseServer/etc/ENV_VARS
source ${BIGDATA_HOME}/FusionInsight_ClickHouse_*/*_*_ClickHouseServer/etc/clickhouse-env.sh
export CLICKHOUSE_CONF_DIR=${CLICKHOUSE_CONF_DIR}
```

Step 7 Run the following command to run the metadata synchronization tool to synchronize metadata from the existing node to the faulty node:

```
sh ${BIGDATA_HOME}/FusionInsight_ClickHouse_*/install/FusionInsight-ClickHouse-*/clickhouse/sbin/clickhouse-create-meta.sh true
```

Step 8 Run the following command to view the log information and check whether the metadata has been synchronized:

```
vim /var/log/Bigdata/clickhouse/clickhouseServer/start.log
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If the synchronization is complete, go to **Step 9**.
- If the synchronization fails, go to **Step 10**.

Step 9 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. In the **Alarm ID** column, locate the corresponding alarm and click **Clear** in the **Operation** column. In the displayed dialog box, click **OK** to manually clear the alarm.

Collect fault information.

Step 10 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 11 Expand the **Service** drop-down list, select **ClickHouse** for the target cluster, and click **OK**.

Step 12 Expand the **Hosts** drop-down list and select the target hosts.

Step 13 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 14 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm needs to be manually cleared after the fault is rectified.

Related Information

None.

1.3.399 ALM-45430 Permission Metadata Synchronization Failed on the Added ClickHouse Node

Alarm Description

This alarm is generated when user and permission information fails to be synchronized during ClickHouse capacity expansion.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45430	Major	Quality of service	Tenant plane	ClickHouse	No

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

The created user does not have operation permissions on the node.

Possible Causes

A node is stopped or faulty during capacity expansion.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Handling Procedure

Step 1 On FusionInsight Manager, choose **Cluster** > **Services** > **ClickHouse** > **Instance**.

Step 2 Check whether an instance is stopped, decommissioned, or faulty.

- If yes, go to **Step 3**.
- If no, go to **Step 4**.

Step 3 Start the instance or rectify the instance fault until all instances are running properly.

Step 4 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**, locate this alarm and the faulty host based on the location information.

Step 5 Log in to the faulty host as user **omm**.

Step 6 Run the following commands to initialize environment variables:

source ${BIGDATA_HOME}/FusionInsight_ClickHouse_*/*_*_ClickHouseServer/etc/ENV_VARS

source ${BIGDATA_HOME}/FusionInsight_ClickHouse_*/*_*_ClickHouseServer/etc/clickhouse-env.sh

export CLICKHOUSE_CONF_DIR=${CLICKHOUSE_CONF_DIR}

Step 7 Run the following command to run the metadata synchronization tool to synchronize metadata from the existing node to the faulty node:

sh ${BIGDATA_HOME}/FusionInsight_ClickHouse_*/install/FusionInsight-ClickHouse-*/clickhouse/sbin/clickhouse-create-meta.sh true

Step 8 Run the following command to view the log information and check whether the metadata has been synchronized:

vim /var/log/Bigdata/clickhouse/clickhouseServer/start.log

If the synchronization is complete, go to **Step 9**.

If the synchronization fails, go to **Step 10**.

Step 9 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. In the **Alarm ID** column, locate the corresponding alarm and click **Clear** in the **Operation** column. In the displayed dialog box, click **OK** to manually clear the alarm.

Collect fault information.

Step 10 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 11 Expand the **Service** drop-down list, select **ClickHouse** for the target cluster, and click **OK**.

Step 12 Expand the **Hosts** drop-down list and select the target hosts.

Step 13 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 14 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm needs to be manually cleared after the fault is rectified.

Related Information

None.

1.3.400 ALM-45431 Improper ClickHouse Instance Distribution for Topology Allocation

Alarm Description

The ClickHouseServer instance distribution does not meet the topology allocation requirements.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45431	Critical	Quality of service	Tenant plane	ClickHouse	No

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

Some ClickHouseServer instances are unavailable.

Possible Causes

During installation or capacity expansion, the number of instances or allocation mode does not meet the topology requirements.

Handling Procedure

Step 1 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**, locate the row that contains the alarm, and analyze the cause based on **Location** and **Additional Information**.

Step 2 Handle the alarm based on the additional alarm information and handling method in the following table.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Additional Information	Description	Handling Method
n ClickHouseServer instances should be added to other AZ.	This alarm is generated when a single cluster is deployed in cross-AZ DR mode. The ClickHouseServer instance deployment does not meet the cross-AZ DR topology allocation requirements. As a result, some instances cannot work properly.	1. On FusionInsight Manager, choose **Cluster** > **Services** > **ClickHouse**, click the **Instance** tab, locate the row that contains the alarm, view the host name in **Location**, and find the AZ for which the alarm is generated in the AZ column based on the host name. 2. On the **Instance** page, click **Add Instance** to add *n* ClickHouseServer instances to other AZs except the AZ where the alarm is generated.
n ClickHouseServer instances should be added.	This alarm is generated when a non-single-cluster is deployed in the default deployment mode of cross-AZ DR. The number of ClickHouseServer instances in the cluster is less than an even number. As a result, some instances cannot work properly.	1. Determine the number (*n*) of ClickHouseServer instances to be added based on the alarm information. 2. On FusionInsight Manager, choose **Cluster** > **Services** > **ClickHouse**, click the **Instance** tab, and add *n* ClickHouseServer instances to the cluster.

----End

Alarm Clearance

This alarm needs to be manually cleared after the fault is rectified.

Related Information

None.

1.3.401 ALM-45432 ClickHouse User Synchronization Process Fails

Alarm Description

The system checks the status of the ClickHouse user role synchronization process every 5 minutes. This alarm is generated when the system detects that the ClickHouse user role synchronization process is faulty or the user role synchronization fails.

This alarm is automatically cleared when the ClickHouse user role synchronization process or function becomes normal.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45432	Major	Error handling	Tenant plane	ClickHouse	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

Some ClickHouseServer instances are unavailable.

Possible Causes

- The ClickHouse user role synchronization process is not started properly or exits abnormally.
- The ClickHouse user role synchronization process fails to synchronize user role information because the LdapServer service is faulty.

Handling Procedure

Check whether the ClickHouse user role synchronization process is normal.

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Alarms**. On the page that is displayed, search for **ALM-45432 ClickHouse User Synchronization Process Fails**.

Step 2 Check the host name and additional information in the alarm details.

- If the additional information is "Process clickhouse-ugsync is not exit.", go to **Step 3**.
- If the additional information is "Process clickhouse-ugsync sync user failed.", go to **Step 6**.

Step 3 Log in to the faulty host as user **omm** and run the following command to check whether the ClickHouse user role synchronization process is normal:

ps -ef | grep 'clickhouse-ugsync'

Abnormal result of the synchronization process:

```
[omm@server-2110081635-0001 ~]$ ps -ef | grep 'clickhouse-ugsync'
omm      20104 13146  0 15:57 pts/7    00:00:00 grep --color=auto clickhouse-ugsync
```

- If yes, the alarm is automatically cleared. If the alarm is cleared, no further action is required. If the alarm persists, go to **Step 8**.
- If no, go to **Step 4**.

Step 4 Log in to the faulty host as user **omm** and run the following command to check whether the crontab daemon task is correctly configured:

crontab -l

Normal setting of the crontab daemon task:

```
*/5 * * * * bash /xxxxx/clickhouse_ugsync_check.sh >/dev/null 2>&1
```

- If yes, check whether the alarm is cleared 5 minutes later. If the alarm is cleared, no further action is required. If the alarm persists, go to **Step 8**.
- If no, go to **Step 5**.

Step 5 Log in to FusionInsight Manager, choose **Cluster** > **Services** > **ClickHouse**. On the page that is displayed, click the **Instance** tab. On this tab page, find the abnormal ClickHouseServer instance based on the fault information, and restart it. Wait for 5 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Check whether the LdapServer service is normal.

Step 6 Log in to FusionInsight Manager, choose **Cluster** > **Services**, and check whether **Running Status** of LdapServer is **Normal**.

- If yes, go to **Step 8**.
- If no, go to **Step 7**.

Step 7 Handle the LdapServer service unavailable alarm according to ALM-25000 LdapServer Service Unavailable.

After **Running Status** of LdapServer becomes **Normal**, check whether this alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Collect fault information.

Step 8 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 9 Expand the **Service** drop-down list, and select **ClickHouse** for the target cluster.

Step 10 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the abnormal host, and click **OK**.

Step 11 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.402 ALM-45433 ClickHouse AZ Topology Exception

Alarm Description

If the cross-AZ HA function is enabled for a cluster where ClickHouse has been deployed, the ClickHouse topology remains unchanged. This alarm is generated when the cross-AZ HA does not take effect if backup nodes of the same shard are in the same AZ.

This alarm is automatically cleared when the system detects that all shards meet the cross-AZ HA deployment requirements.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45433	Critical	Quality of service	Tenant plane	ClickHouse	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

The current deployment of the ClickHouse service does not support cross-AZ HA.

Possible Causes

After cross-AZ HA is enabled, all backup nodes of a shard are in the same AZ.

Handling Procedure

Modify the AZ of backup nodes.

Step 1 Log in to the node where the client is installed as the client installation user. Run the following command to switch to the client installation directory:

cd *{Client installation path}*

Step 2 Run the following command to configure environment variables:

source bigdata_env

Step 3 Run the following command to authenticate the user (skip this step in normal mode):

kinit *Component service user*

Step 4 Run the following command to log in to the client tool:

zkCli.sh -server *Service IP address of the node where the ZooKeeper instance resides*: *Client port*

Step 5 Run the following command to view the current topology:

get /clickhouse/topo

NOTE

If the ClickHouse is installed with multiple services, run the **get /clickhouse{-n}/topo** command. For example, if the ClickHouse-1 is installed, run the **get /clickhouse-1/topo** command.

```
[zk: 192.168.20.36:24002(CONNECTED) 0] get /clickhouse/topo

<topo>
  <mcluster>
    <shard id="14" index="1">
      <server id="15">
        <replica>1</replica>
        <az>AZ1</az>
        <host>192-168-20-205</host>
        <port>21427</port>
      </server>
      <server id="16">
        <replica>2</replica>
        <az>AZ1</az>
        <host>192-168-20-2205</host>
        <port>21427</port>
      </server>
    </shard>
  </mcluster>
</topo>
```

Step 6 Select a host from the hosts in the same AZ in the shard obtained in **Step 5** and deploy the host into another AZ.

Step 7 Log in to FusionInsight Manager, click **Host**, select the host you have deployed in **Step 6** and choose **More** > **Reinstall** to reinstall the host.

Step 8 Choose **Cluster** > **Cross-AZ HA**, click **Configure AZ and Policy** and change the AZ information of the reinstalled host to the AZ planned in the **Step 6**.

Step 9 Wait 5 minutes and check whether the alarm is automatically cleared.

- If yes, no further action is required.
- If no, go to **Step 10**.

Collect fault information.

Step 10 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 11 Expand the **Service** drop-down list, and select **ClickHouse** for the target cluster.

Step 12 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the abnormal host, and click **OK**.

Step 13 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 14 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.403 ALM-45434 A Single Replica Exists in the ClickHouse Data Table

Alarm Description

This alarm is generated when a single replica is detected in a custom logical cluster after the custom logical cluster is enabled for ClickHouse.

This alarm is automatically cleared when the system detects that the custom logical cluster uses multiple replicas.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45434	Major	Quality of service	Tenant plane	ClickHouse	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

If a hardware fault occurs, data cannot be restored.

Possible Causes

The **metrika.xml** file in the ClickHouse configuration directory contains single-replica configuration.

Handling Procedure

Check whether the configuration in metrika.xml of the ClickHouse instance is correct.

Step 1 In the alarm list on FusionInsight Manager, locate the row that contains the alarm, and click ⌄ to view the name of the host for which the alarm is generated. On the **Hosts** page, view the host IP address based on the host name.

Step 2 Log in to the host where the ClickHouse instance is abnormal, go to the configuration directory of the ClickHouse instance, and run the following commands:

cd ${BIGDATA_HOME}**/FusionInsight_ClickHouse_***Version***/**x_x_**ClickHouseServer/etc**

cat metrika.xml

Step 3 View the number of shards in each custom logical cluster and check that a single replica exists. Then, go to **Step 4**.

NOTE

If a shard contains only one node, a single replica exists in a logical cluster, as shown in the following:

```
<shard>
  <internal_replication>true</internal_replication>
  <replica>
    <host>host-name1</host>
    <port>port</port>
    <user>clickhouse</user>
    <password/>
  </replica>
</shard>
```

Collect fault information.

Step 4 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 5 Expand the **Service** drop-down list, and select **ClickHouse** for the target cluster.

Step 6 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the abnormal host, and click **OK**.

Step 7 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 8 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.404 ALM-45435 Inconsistent Metadata of ClickHouse Tables

Alarm Description

This alarm is generated when the metadata in a distributed table or in the local table of the distributed table has been inconsistent for 180 min.

This alarm is automatically cleared when the metadata in the distributed table or in the local table of the distributed table becomes consistent.

Metadata consistency includes:

- Consistent quantity, name, sequence, and type of each column in the table
- Consistent partition keys
- Consistent sorting keys
- Consistent primary keys
- Consistent sampling keys

NOTE

If this alarm exists, table metadata is inconsistent in the ClickHouse cluster to which the current node belongs. The inconsistency may be caused by multiple reasons, not limited to those mentioned in additional information.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45435	Minor	Quality of service	Tenant plane	ClickHouse	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

Subsequent operations such as INSERT and ALTER on the table may fail.

Possible Causes

Table metadata modification fails or is not executed on one or more ClickHouseServer nodes.

Handling Procedure

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**, and view the role name and the IP address for the hostname in **Location**.

Step 2 Log in to the node where the client is installed as the client installation user and run the following commands:

cd *{Client installation path}*

source bigdata_env

- For a cluster with Kerberos authentication enabled (security mode):

  kinit *Component service user*

  clickhouse client --host *IP address of the ClickHouseServer instance for which the alarm is reported* **--port** 21427 **--secure**

- For a cluster with Kerberos authentication disabled (normal mode):

  clickhouse client --host *IP address of the ClickHouseServer instance for which the alarm is reported* **--user** *Username* **--password --port** 21423

Step 3 Check whether any task is being executed for the table to which the alarm is generated.

Run the following command to check whether any SQL task is being executed:

select * from system.processes where current_database='*Database name***' and query like '%***Table name***%'**

Run the following command to check whether a mutation task is being executed:

select * from system.mutations where database=*'Database name'* **and table=***'Table name'***;**

- If the query result is empty, go to **Step 4**.
- If the query result contains error information, rectify the fault accordingly. If the fault cannot be rectified based on the error information, go to **Step 6**.
- If the query result contains information about an on-going task with no error, the SQL/mutation task is being executed.

  Wait for 5 minutes. If the alarm is cleared, no further action is required. If the alarm persists, go to **Step 4**.

Step 4 Modify the table structure, delete a table, or add a table based on service requirements until the table metadata of all nodes in the cluster is consistent. After 5 minutes, check whether this alarm is cleared.

- If yes, no further action is required.

- If no, go to **Step 5**.

Step 5 If the table has been deleted, manually clear the alarm and check whether the alarm is reported again.

- If yes, go to **Step 6**.
- If no, no further action is required.

Collect fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **ClickHouse** for the target cluster.

Step 8 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the abnormal host, and click **OK**.

Step 9 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.405 ALM-45436 Skew ClickHouse Table Data

Alarm Description

This alarm is generated when data skew occurs in the local table of a distributed table between ClickHouse nodes. This alarm is automatically cleared when data becomes balanced.

Data skew check method:

- If **min_table_check_data_bytes** is set to **0**, data skew check is disabled.
- If **min_table_check_data_bytes** is greater than **0**, data skew check is enabled.

After data skew check is enabled, if the data volume in a table is less than the **min_table_check_data_bytes** value, no alarm will be reported due to data skew. When the data volume is greater than the **min_table_check_data_bytes** value and the data volume difference between the same table on different nodes is greater than the percentage specified in **min_table_data_varies_rate**, data skew occurs and this alarm is reported.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45436	Minor	Quality of service	Tenant plane	ClickHouse	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	Table	Specifies the name of the table or database in the cluster for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

SQL execution efficiency may be lowered.

Possible Causes

The data write policy is improper, causing unbalanced data among nodes.

Handling Procedure

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**, and view the role name and the IP address for the hostname in **Location**.

Step 2 Log in to the node where the client is installed as the client installation user and run the following commands:

cd *{Client installation path}*

source bigdata_env

- Security mode (with Kerberos enabled):

  kinit *Component service user*

  clickhouse client --host *IP address of the ClickHouseServer instance for which the alarm is reported* **--port** 21427 **--secure**

- Normal mode (with Kerberos disabled):

  clickhouse client --host *IP address of the ClickHouseServer instance for which the alarm is reported* **--user** *Username* **--password --port** 21423

Step 3 View data distribution.

select FQDN(), database, table, sum(data_compressed_bytes) from clusterAllReplicas(*Name of the logical cluster***, system.parts) where database='***Database name***' and table='***Table name***' and active=1 group by (FQDN(), database, table);**

Step 4 Balance data with a few clicks or migrate data based on service requirements. For details, see **Component Operation Guide** > **Using ClickHouse** > **Migrating ClickHouse Data** in MapReduce Service (MRS) 3.3.1-LTS User Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Usage Guide (for Huawei Cloud Stack 8.3.1).

Step 5 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **ClickHouse** for the target cluster.

Step 8 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the abnormal host, and click **OK**.

Step 9 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.406 ALM-45437 Excessive Parts in the ClickHouse Table

Alarm Description

This alarm is generated when the number of parts exceeds the threshold specified by **part_num_threshold**.

This alarm is automatically cleared when the number of parts is less than the **part_num_threshold** value.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45437	Minor	Quality of service	Tenant plane	ClickHouse	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	Table	Specifies the name of the table or database in the cluster for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

Service errors may occur.

Possible Causes

The data distribution in the ClickHouse table is improper, or the background merge task is executed slowly.

Handling Procedure

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**, and view the role name and the IP address for the hostname in **Location**.

Step 2 Log in to the node where the client is installed as the client installation user and run the following commands:

cd *{Client installation path}*

source bigdata_env

- Security mode (with Kerberos enabled):

  kinit *Component service user*

clickhouse client --host *IP address of the ClickHouseServer instance for which the alarm is reported* **--port** 21427 **--secure**

- Normal mode (with Kerberos disabled):

  clickhouse client --host *IP address of the ClickHouseServer instance for which the alarm is reported* **--user** *Username* **--password --port** 21423

Step 3 Run the following command to manually merge parts:

optimize table *Database name*.*Table name* **final;**

Step 4 Check whether the number of parts has decreased.

select FQDN(), database, table, count(1) from clusterAllReplicas(default_cluster, system.parts) where database='*Database name***' and table='***Table name***' and active=1 group by (FQDN(), database, table);**

1. If the number of parts is less than the threshold, wait for 5 minutes and check whether the alarm is cleared.
   - If yes, no further action is required.
   - If no, go to **Step 5**.
2. If the number of parts does not decrease, check whether the partition key of the table is set properly. If the number of partitions is too large, rectify the service logic.
3. If the command output is empty, the table does not exist. This alarm is a historical alarm and can be ignored. Manually clear it.

Collect fault information.

Step 5 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 6 Expand the **Service** drop-down list, and select **ClickHouse** for the target cluster.

Step 7 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the abnormal host, and click **OK**.

Step 8 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.407 ALM-45438 ClickHouse Disk Usage Exceeds 80%

Alarm Description

The system checks the disk capacity of the ClickHouseServer node every 1 minute. This alarm is generated when the usage of the disk where the ClickHouse data directory or metadata directory resides exceeds 80%.

This alarm is automatically cleared when the usage of the disk where the ClickHouse data directory or metadata directory is located is lower than 80%.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45438	Major	Quality of service	Tenant plane	ClickHouse	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	DiskPath	Specifies the path of the disk in the cluster for which the alarm is generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

The ClickHouse write operation may fail.

Possible Causes

The disk capacity of the ClickHouseServer node is too small.

Handling Procedure

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**, and view the role name and the IP address for the hostname in **Location**.

Step 2 Expand the disk capacity of the node for which the alarm is generated. For details, see ClickHouse-related chapters in MapReduce Service (MRS) 3.3.1-LTS Physical Machine Cluster Capacity Expansion Guide (for Huawei Cloud Stack 8.3.1).

Step 3 Go to **Step 4** if the expansion fails or the alarm persists after the expansion.

Collect fault information.

Step 4 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 5 Expand the **Service** drop-down list, and select **ClickHouse** for the target cluster.

Step 6 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the abnormal host, and click **OK**.

Step 7 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 8 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Related Information

None.

1.3.408 ALM-45439 ClickHouse Node Enters the Read-Only Mode

Alarm Description

The system checks the disk capacity of the ClickHouseServer node every 1 minute. This alarm is generated when the system detects that the disk capacity exceeds 90% and the ClickHouseServer node enters the read-only mode.

This alarm is automatically cleared when the system detects that the disk capacity is lower than 90% and the ClickHouseServer node exits the read-only mode.

NOTE

If the ClickHouseServer node is in read-only mode and you need to log in to the client to clear data, you can manually exit the read-only mode using the following method:

Log in to FusionInsight Manager, choose **Cluster** > **Services** > **ClickHouse** > **Configurations** > **All Configurations**, search for **profiles.default.readonly**, and change its value to **0**.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45439	Major	Quality of service	Tenant plane	ClickHouse	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	DiskPath	Specifies the path of the disk in the cluster for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

After the ClickHouseServer node enters the read-only mode, all write, modification, and deletion operations fail.

Possible Causes

The disk usage of the ClickHouse node exceeds 90%.

Handling Procedure

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**, and view the role name and the IP address for the hostname in **Location**.

Step 2 Expand the disk capacity of the node for which the alarm is generated. For details, see ClickHouse-related chapters in MapReduce Service (MRS) 3.3.1-LTS Physical Machine Cluster Capacity Expansion Guide (for Huawei Cloud Stack 8.3.1).

Step 3 Go to **Step 4** if the expansion fails or the alarm persists after the expansion.

NOTE

After the capacity expansion, this alarm can be automatically cleared only when **profiles.default.readonly** is **auto**. If its value has been manually changed, change it back to **auto**. If **profiles.default.readonly** needs to be set to **0** or **1** based on service requirements, manually clear this alarm.

Collect fault information.

Step 4 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 5 Expand the **Service** drop-down list, and select **ClickHouse** for the target cluster.

Step 6 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the abnormal host, and click **OK**.

Step 7 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 8 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.409 ALM-45440 Inconsistency Between ClickHouse Replicas

Alarm Description

When the number of ClickHouse replicas is greater than 1, the system periodically checks the replicated table. This alarm is generated if replicated table data is not synchronized. This alarm is cleared when data in all replicated tables between replicas becomes synchronized.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45440	Minor	Quality of service	Tenant plane	ClickHouse	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.

Type	Parameter	Description
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	Table	Indicates the name of the table in the cluster for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

The data reliability of the ClickHouse replicated table is affected, causing data differences and affecting the query result of the distributed table.

Possible Causes

- The ClickHouse service is overloaded.
- The connection between the ClickHouse and ZooKeeper is abnormal.

Handling Procedure

Check whether the ClickHouse service load is heavy.

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**, and view the database name, table name, role name and IP address for the hostname in **Location**.

Step 2 Log in to the node where the client is installed as the client installation user and run the following commands:

cd *{Client installation path}*

source bigdata_env

- For a cluster with Kerberos authentication enabled (security mode):

  kinit *Component service user*

  clickhouse client --host *IP address of the ClickHouseServer instance for which the alarm is reported* **--port** 21427 **--secure**

- For a cluster with Kerberos authentication disabled (normal mode):

  clickhouse client --host *IP address of the ClickHouseServer instance for which the alarm is reported* **--user** *Username* **--password --port** 21423

Step 3 Run the following statement to check whether data is frequently written to the system table. If yes, wait until the service execution is complete and check whether the alarm is cleared.

NOTE

You are advised not to write data frequently. It is best practice to optimize the service logic to avoid frequent data write. For details, see the ClickHouse development specifications.

SELECT query_id, user, FQDN(), elapsed, query FROM system.processes ORDER BY query_id;

- If yes, no further action is required.
- If no, go to **Step 4**.

Step 4 Check whether a large amount of data is written. If yes, wait until the task is complete and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Step 5 Run the following statement to check whether replicas are synchronized:

select table,absolute_delay, queue_size, inserts_in_queue, merges_in_queue from system.replicas where absolute_delay > 0 order by absolute_delay desc limit 10;

- If yes, go to **Step 6**.
- If no, go to **Step 9**.

Step 6 If **inserts_in_queue** contains a large amount of content to be inserted, run the following SQL statement to query the replica synchronization queue and locate the error cause:

SELECT database,table,type,any(last_exception),any(postpone_reason),min(create_time),max(last_attempt_time),max(last_postpone_time),max(num_postponed) AS max_postponed,max(num_tries) AS max_tries,min(num_tries) AS

min_tries,countIf(last_exception != '') AS count_err,countIf(num_postponed > 0) AS count_postponed,countIf(is_currently_executing) AS count_executing,count() AS count_all FROM system.replication_queue GROUP BY database,table,type ORDER BY count_all DESC

Check whether an error message similar to the following is displayed:

```
Not executing fetch of part xxx because n fetches already executing, max n
```

- If yes, go to **Step 7**.
- If no, go to **Step 9**.

Step 7 On FusionInsight Manager, choose **Cluster** > **Services** > **ClickHouse** > **Configurations** > **All Configurations**, and check whether the value of **background_pool_size** is twice the number of cores on the node.

- If yes, go to **Step 9**.
- If no, go to **Step 8**.

Step 8 Set this parameter to twice the number of cores on the node and synchronize the configuration. Wait for a while and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Check the connectivity between ClickHouse and ZooKeeper.

Step 9 Log in to the node where the ClickHouseServer instance is located, go to **$ {BIGDATA_HOME}/FusionInsight_ClickHouse_*/*_*_ClickHouseServer/etc**, and check whether the port numbers of the ClickHouseServer and ZooKeeper in the **config.xml** file are the same, as shown in the following information in bold:

NOTE

To view the ZooKeeper port number, choose **Cluster** > **Services** > **ZooKeeper** > **Configurations** > **All Configurations** on FusionInsight Manager, and check the value of **clientPort**.

```
<zookeeper>
  <session_timeout_ms>10000</session_timeout_ms>
  <node index="1">
    <host>server-2110082001-0019</host>
    <port>24002</port>
  </node>
  <node index="2">
    <host>server-2110082001-0018</host>
    <port>24002</port>
  </node>
  <node index="3">
    <host>server-2110082001-0017</host>
    <port>24002</port>
  </node>
</zookeeper>
```

- If yes, go to **Step 11**.
- If no, go to **Step 10**.

Step 10 Change the port number to the ZooKeeper port number, restart the ClickHouseServer instance, and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 11**.

Collect fault information.

Step 11 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 12 Expand the **Service** drop-down list, and select **ClickHouse** for the target cluster.

Step 13 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the abnormal host, and click **OK**.

Step 14 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 15 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.410 ALM-45441 Zookeeper Disconnected

Alarm Description

The system checks the connection between ClickHouse and ZooKeeper every minute. This alarm is generated when the connection fails. The alarm is reported because the ZooKeeper connection is abnormal. If the connection fails for three consecutive times, the system generates an alarm.

This alarm is automatically cleared when the system detects that the connection is normal.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45441	Critical	Quality of service	Tenant plane	ClickHouse	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.

Type	Parameter	Description
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

If ClickHouse is disconnected from ZooKeeper, the ClickHouse service cannot be used.

Possible Causes

- The ZooKeeper service is abnormal.
- The ClickHouse service is overloaded.

Handling Procedure

Check whether ZooKeeper is normal.

Step 1 On FusionInsight Manager, choose **Cluster** > **Services** > **ZooKeeper** > **quorumpeer**.

Step 2 Check whether ZooKeeper instances are normal.

- If yes, go to **Step 6**.
- If no, go to **Step 3**.

Step 3 Select instances whose status is not good and choose **More** > **Restart Instance**.

Step 4 Check whether the instance status is good after restart.

- If yes, go to **Step 5**.
- If no, go to **Step 10**.

Step 5 Choose **O&M** > **Alarm** > **Alarms** and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Check whether the ClickHouse service load is heavy.

Step 6 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**, and view the role name and the IP address for the hostname in **Location**.

Step 7 Log in to the node where the client is installed as the client installation user and run the following commands:

cd *{Client installation path}*

source bigdata_env

- For a cluster with Kerberos authentication enabled (security mode):

  kinit *Component service user*

  clickhouse client --host *IP address of the ClickHouseServer instance for which the alarm is reported* **--port** 21427 **--secure**
- For a cluster with Kerberos authentication disabled (normal mode):

  clickhouse client --host IP address of the ClickHouseServer instance for which the alarm is reported **--user** *User name* **--password --port** 21423

Step 8 Run the following statement to check whether data is frequently written to the system table. If yes, wait until the service execution is complete and check whether the alarm is cleared.

NOTE

You are advised not to write data frequently. It is best practice to optimize the service logic to avoid frequent data write. For details, see the ClickHouse development specifications.

SELECT query_id, user, FQDN(), elapsed, query FROM system.processes ORDER BY query_id;

- If yes, no further action is required.
- If no, go to **Step 9**.

Step 9 Check whether a large amount of data is written. If yes, wait until the task is complete and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 10**.

Collect fault information.

Step 10 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 11 Expand the **Service** drop-down list, and select **ClickHouse** for the target cluster.

Step 12 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the abnormal host, and click **OK**.

Step 13 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 14 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.411 ALM-45442 Too Many Concurrent SQL Statements

Alarm Description

The alarm module checks the number of concurrent ClickHouse requests every 30 seconds. This alarm is generated when the number of concurrent ClickHouse requests exceeds the concurrency threshold configured on the UI.

This alarm is cleared when the system detects that the actual number of concurrent requests is less than concurrency threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45442	Major	Quality of service	Tenant plane	ClickHouse	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.

Type	Parameter	Description
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

If there are too many concurrent SQL statements, a large number of system resources are consumed. As a result, system response becomes slow.

Possible Causes

The ClickHouse service is overloaded.

Handling Procedure

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**, and view the role name and the IP address for the hostname in **Location**.

Step 2 Choose **Cluster** > **ClickHouse** > **Instance**, select an instance based on the alarm information. Choose **Chart** > **Concurrency** to check whether the actual number of concurrent SQL statements is greater than SQL concurrency threshold.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 Confirm with the user whether a large number of tasks were being executed during the alarming period.

- If yes, go to **Step 4**.
- If no, go to **Step 5**.

Step 4 On FusionInsight Manager, choose **O&M** and click **Alarm** > **Thresholds** in the navigation pane on the left. On the displayed page, click **ClickHouse** > **Concurrency** and adjust the threshold, or wait until the task is complete. Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Collect fault information.

Step 5 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 6 Expand the **Service** drop-down list, and select **ClickHouse** for the target cluster.

Step 7 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the abnormal host, and click **OK**.

Step 8 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.412 ALM-45443 Slow SQL Queries in the Cluster

Alarm Description

The system checks slow SQL queries for ClickHouse every 1 minute. This alarm is generated when the execution time of a SQL statement is longer than or equal to the slow SQL threshold.

This alarm is automatically cleared when the system detects that the execution time of the SQL statement is shorter than the slow SQL threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45443	Major	Quality of service	Tenant plane	ClickHouse	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

The performance of the ClickHouse service deteriorates, which slows the response of other services. If there are too many slow SQL statements, the service may be unavailable.

Possible Causes

- The ClickHouse service is overloaded.
- The execution of SQL statements takes a long time.

Handling Procedure

Check whether the ClickHouse service load is heavy.

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**, and view the role name and the IP address for the hostname in **Location**.

Step 2 Log in to the node where the client is installed as the client installation user and run the following commands:

cd *{Client installation path}*

source bigdata_env

- For a cluster with Kerberos authentication enabled (security mode):

  kinit *Component service user*

  clickhouse client --host *IP address of the ClickHouseServer instance for which the alarm is reported* **--port** 21427 **--secure**
- For a cluster with Kerberos authentication disabled (normal mode):

  clickhouse client --host *IP address of the ClickHouseServer instance for which the alarm is reported* **--user** *Username* **--password --port** 21423

Step 3 Run the following statement to check whether data is frequently written to the system table. If yes, wait until the service execution is complete and check whether the alarm is cleared.

NOTE

You are advised not to write data frequently. It is best practice to optimize the service logic to avoid frequent data write. For details, see the ClickHouse development specifications.

SELECT query_id, user, FQDN(), elapsed, query FROM system.processes ORDER BY query_id;

- If yes, no further action is required.
- If no, go to **Step 4**.

Checking whether the SQL statements take a long time.

Step 4 Check the logical cluster to which the alarm object belongs. Log in to FusionInsight Manager, click **Cluster**, choose **Services** > **ClickHouse**, and click **Logic Cluster**. On the displayed page, choose **Query Management** > **Ongoing Slow Queries**. Check which SQL statements take a long time on the displayed page, confirm with the user to adjust services, optimize slow SQL statements, and check whether the optimization is successful.

- If yes, go to **Step 5**.
- If no, go to **Step 6**.

Step 5 After the SQL statements are complete, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **ClickHouse** for the target cluster.

Step 8 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the abnormal host, and click **OK**.

Step 9 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.413 ALM-45444 Abnormal ClickHouse Process

Alarm Description

The health check module checks ClickHouse instances every 30 seconds. If the number of consecutive failures exceeds 20, an alarm is reported and the ClickHouse process may stop responding. As a result, service tasks will fail.

The alarm is cleared when the system detects that the ClickHouse process is running properly.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45444	Critical	Quality of service	Tenant plane	ClickHouse	Yes

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

If the ClickHouse process is abnormal, services cannot run properly.

Possible Causes

The ClickHouse process runs improperly.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Handling Procedure

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**, and view the role name and the IP address for the hostname in **Location**.

Step 2 Log in to the node where the client is installed as the client installation user and run the following commands:

cd *{Client installation path}*

source bigdata_env

- For a cluster with Kerberos authentication enabled (security mode):

  kinit *Component service user*

  clickhouse client --host *IP address of the ClickHouseServer instance for which the alarm is reported* **--port** 21427 **--secure**

- For a cluster with Kerberos authentication disabled (normal mode):

  clickhouse client --host *IP address of the ClickHouseServer instance for which the alarm is reported* **--user** *Username* **--password --port** 21423

Step 3 Run the following statement to check whether the result can be properly returned:

SELECT 1;

- If yes, go to **Step 4**.
- If no, go to **Step 5**.

Step 4 Wait for several minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Collect fault information.

Step 5 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 6 Expand the **Service** drop-down list, and select **ClickHouse** for the target cluster.

Step 7 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the abnormal host, and click **OK**.

Step 8 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

1.3.414 ALM-45445 Failed to Send Data Files to Remote Shards When ClickHouse Writes Data to a Distributed Table

Alarm Description

The ClickHouse instance checks the distributed table every 300 seconds. If the number of consecutive failures exceeds the threshold, an alarm is generated. In this case, the node where the ClickHouse instance writes data to the distributed table cannot send data files to remote shard nodes.

This alarm is cleared when the number of consecutive failures falls below the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45445	Major	Quality of service	Tenant plane	ClickHouse	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
New	3.3.1	New alarm	New alarm

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.

Impact on the System

The results of operations such as distributed table queries are abnormal.

Possible Causes

The status of some ClickHouse shard nodes is abnormal.

Handling Procedure

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**, and view the role name and the IP address of the hostname in **Location**.

Step 2 Log in to the node where the client is installed as the client installation user and run the following commands:

cd *{Client installation path}*

source bigdata_env

- For a cluster with Kerberos authentication enabled (security mode):

  kinit *Component service user*

  clickhouse client --host *IP address of the ClickHouseServer instance for which the alarm is reported* **--port** 21427 **--secure**

- For a cluster with Kerberos authentication disabled (normal mode):

  clickhouse client --host *IP address of the ClickHouseServer instance for which the alarm is reported* **--user** *Username* **--password --port** 21423

Step 3 Run the following SQL statement to obtain the shard based on the value of **data_path**. For example, if the value of **data_path** is **/srv/Bigdata/clickhouse/data1.../shard2_all_replicas**, the desired shard is **shard2**.

select database, table, data_path, data_files, error_count from system.distribution_queue where data_files != 0 and error_count != 0;

Step 4 Run the following SQL statement to obtain the node IP address (value of the **host** field in the system table **system.clusters**) of the shard where data fails to be sent to (**shard_num** obtained in **Step 3**):

select * from system.clusters;

Step 5 Log in to the ClickHouse node (IP address obtained in **Step 2**) by referring to **Step 4**, run the following statement, and check whether the result can be returned:

SELECT 1;

If yes, go to **Step 6**.

If no, go to **Step 10**.

Step 6 Log in to the ClickHouse node (IP address obtained in **Step 2**) by referring to **Step 4**, run the following statement (**database_name** and **table_name** indicate the database name and table name of the local table corresponding to the distributed table):

select name,type from system.columns where database='*database_name***' and table='***table_name***'**

Step 7 Log in to the ClickHouse node for which the alarm is generated by referring to **Step 2** and run the following statement (**database_name** and **table_name** indicate the database name and table name of the distributed table to which data is written):

select name,type from system.columns where database='*database_name***' and table='***table_name***'**

Step 8 Check whether the results obtained in **Step 6** and **Step 7** are the same.

If yes, go to **Step 10**.

If no, ensure that the column information of the distributed table is consistent with that of the corresponding local table, and then try to write data to the distributed table.

Step 9 Wait for several minutes and check whether the alarm is cleared.

If yes, no further action is required.

If no, go to **Step 10**.

Collect fault information.

Step 10 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 11 Expand the **Service** drop-down list, and select **ClickHouse** for the target cluster.

Step 12 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the abnormal host, and click **OK**.

Step 13 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 14 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.415 ALM-45446 Mutation Task of ClickHouse Is Not Complete for a Long Time

Alarm Description

The system checks mutation tasks every 5 minutes. This alarm is generated when the system detects that a mutation task has been running for at least **slow_mutation_cost_time** minutes. This alarm is automatically cleared when the system does not detect any running mutation task or the running time of a mutation task is less than **slow_mutation_cost_time** minutes.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45446	Minor	Quality of service	Tenant plane	ClickHouse	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
New	3.3.1	New alarm	New alarm

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

- Server resources are occupied, and the performance of the ClickHouse service deteriorates.
- Data is inconsistent.

Possible Causes

The data volume is too large. As a result, the mutation task runs slowly or is suspended.

Handling Procedure

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**, and view the role name and the IP address for the hostname in **Location**.

Step 2 Log in to the node where the client is installed and run the following commands:

cd *{Client installation path}*

source bigdata_env

- Security mode (with Kerberos enabled):

  kinit *Component service user*

clickhouse client --host *IP address of the ClickHouseServer instance for which the alarm is reported* **--port** 21427 **--secure**

- Normal mode (with Kerberos disabled):

  clickhouse client --host *IP address of the ClickHouseServer instance for which the alarm is reported* **--user** *Username* **--password --port** 21423

Step 3 Log in to FusionInsight Manager, choose **Cluster** > **Services** > **ClickHouse**, click **Configurations** and then **All Configurations**. Search for the value of the **slow_mutation_cost_time** parameter, enter the parameter value in the following SQL statement, and run the following statement to check whether any result is returned:

SELECT * FROM system.mutations WHERE is_done = 0 AND create_time < now() - INTERVAL *The value* **SECOND**

NOTE

Add the actual value of **slow_mutation_cost_time** to the preceding statement.

- If yes, go to **Step 4**.
- If no, go to **Step 7**.

Step 4 Wait for a while and run the statement in **Step 3** again. Check whether the value of **parts_to_do** in the returned result decreases.

- If yes, wait until the mutation task is complete.
- If no, go to **Step 5**.

Step 5 If the value of **parts_to_do** remains unchanged, stop the mutation task. Run the following statement and run the statement in **Step 3** again to check whether the current mutation task is in the returned result list:

KILL MUTATION WHERE database = '*Database name***' AND table = '***Table name***' AND mutation_id ='mutation ID'**

- If yes, go to **Step 7**.
- If no, go to **Step 6**.

Step 6 Wait for several minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect fault information.

Step 7 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 8 Expand the **Service** drop-down list, and select **ClickHouse** for the target cluster.

Step 9 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the abnormal host, and click **OK**.

Step 10 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 11 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.416 ALM-45447 ClickHouse Table Read-Only

Alarm Description

The system checks the table status every minute. This alarm is generated when the system detects that a table is read-only. This alarm is automatically cleared when no table is read-only.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45447	Minor	Quality of service	Tenant plane	ClickHouse	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
New	3.3.1	New alarm	New alarm

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.

Type	Parameter	Description
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

- Data cannot be written to or modified.
- Data synchronization in the replication table is interrupted, causing data inconsistency.

Possible Causes

The ZooKeeper is overloaded and metadata is lost.

Handling Procedure

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**, and view the role name and the IP address of the hostname in **Location**.

Step 2 Log in to the node where the client is installed and run the following commands:

cd *{Client installation path}*

source bigdata_env

- Security mode (with Kerberos enabled):

  kinit *Component service user*

  clickhouse client --host *IP address of the ClickHouseServer instance that reports the alarm* **--port** 21427 **--secure**

- Normal mode (with Kerberos disabled):

  clickhouse client --host *IP address of the ClickHouseServer instance for which the alarm is reported* **--user** *Username* **--password --port** 21423

Step 3 Run the following SQL statement to check whether any table is in the read-only state:

select database,table from system.replicas where is_readonly = 1

- If yes, go to **Step 4**.
- If no, go to **Step 8**.

Step 4 Specify the database and table queried in **Step 3** in the following statements and run them in sequence. Then, run the SQL statement in **Step 3** and check whether the result contains any read-only table.

system restore replica *database.table*;

system restart replica *database.table*;

- If yes, go to **Step 5**.
- If no, go to **Step 8**.

Step 5 Specify the database and table queried in **Step 3** in the following statements and run them in sequence. Then, run the SQL statement in **Step 3** and check whether the result contains the read-only table.

detach table *database.table*;

attach table *database.table*;

- If yes, go to **Step 6**.
- If no, go to **Step 8**.

Step 6 Run the following SQL statement to view the structure information of the read-only table. In the statement, database and table are those queried in **Step 3**.

show create table *database.table*;

Step 7 Run the following SQL statement to delete the read-only table and create a read-only table based on the table structure information in **Step 6**. Wait for several minutes, run the SQL statement in **Step 3**, and check whether the result contains the read-only table.

drop database.table no delay;

- If yes, go to **Step 9**.
- If no, go to **Step 8**.

database	table	mutation_id	command	parts_to_do_names	parts_to_do
default	test123_local	0000000012	UPDATE address = 'wuhan' WHERE 1 = 1	['202312_0_622_4_1400','202312_623_747_3_1400','202312_748_912_3_1400','202312_913_1051_3_1400']	4

Step 8 Wait several minutes and check whether the alarm is automatically cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Collect fault information.

Step 9 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 10 Expand the **Service** drop-down list, and select **ClickHouse** for the target cluster.

Step 11 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the abnormal host, and click **OK**.

Step 12 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 13 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.417 ALM-45448 Rapid Increase of Znodes Used by ClickHouse

Alarm Description

Metadata in ClickHouse is stored on ZooKeeper Znodes. The number of occupied Znodes may increase sharply even if service requirements do not change greatly. This alarm is generated when the number of occupied Znodes in two hours exceeds the threshold. If a large amount of data is imported or services are migrated, ignore this alarm.

This alarm is cleared when the system detects that the increase in two hours is lower than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45448	Major	Quality of service	Tenant plane	ClickHouse	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
New	3.3.1	New alarm	New alarm

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

ZooKeeper server resources are occupied. The number of Znodes will reach the upper limit in a short period of time, affecting the ClickHouse service.

Possible Causes

- If the ClickHouse service volume retains at large scale, increase the value of **ZNODE_GROWTH_LIMIT** on the ClickHouse configuration page.
- Major service changes, migration, and data import have been performed in ClickHouse.

Handling Procedure

Step 1 Choose **Cluster** > **ClickHouse** > **Instances** > **All Configurations**, and search for **ZNODE_GROWTH_LIMIT**, increase the value of **ZNODE_GROWTH_LIMIT**. The default value is **100000**, the maximum value is **200000**, and the value is configured based a step of 50000. Wait for 2 hours and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 2**.

Step 2 Confirm with the service party whether there are new service requests or a large amount of data is imported or migrated during the period when the alarm is reported.

- If yes, go to **Step 3**.
- If no, go to **Step 4**.

Step 3 Wait for 2 hours and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 4**.

Collect fault information.

Step 4 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 5 Expand the **Service** drop-down list, and select **ClickHouse** for the target cluster.

Step 6 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the abnormal host, and click **OK**.

Step 7 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 8 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Related Information

None.

1.3.418 ALM-45449 The Counter Number of zxid Used by ClickHouse Exceeds the Threshold

Alarm Description

ClickHouse uses ZooKeeper Transaction ID (**zxid**) to manage transactions. The **zxid** is a 64-bit number used to keep consistency of the distributed system. The **zxid** has two parts: the high order 32-bits for the epoch and the low order 32-bits for the counter. The epoch number represents the lifecycle of the leader, and the counter number indicates the location of a transaction in the request. Each time a new transaction is generated, the counter number is automatically increased by 1. When the value of **zxid** reaches the maximum value, that is, the counter number reaches **0xffffffff**, the cluster forcibly elects the leader and ZooKeeper is unavailable in a short period. The system checks the counter number every two hours. This alarm is generated when the the counter number of **zxid** exceeds the threshold.

This alarm is cleared when the counter number is smaller than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45449	Major	Quality of service	Tenant plane	ClickHouse	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
New	3.3.1	New alarm	New alarm

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.

Type	Parameter	Description
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

ZooKeeper leader election is forcibly triggered at an uncertain time, which may interrupt the ClickHouse service.

Possible Causes

The counter number of ZooKeeper zxid exceeds the threshold.

Handling Procedure

Step 1 Log in to FusionInsight Manager and choose **Cluster** > **Services** > **ZooKeeper**. On the **Dashboard** page of the ZooKeeper service, click **More** and select **Service Rolling Restart** in the upper right corner. In the displayed dialog box, enter the password and click **OK**. On the **Service Rolling Restart** page, click **OK** and wait until the rolling restart of the ZooKeeper service is complete.

NOTE

Restart the ZooKeeper service during off-peak hours of ClickHouse.

Step 2 Wait for 2 hours and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 3**.

Collect fault information.

Step 3 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 4 Expand the **Service** drop-down list, and select **ClickHouse** for the target cluster.

Step 5 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the abnormal host, and click **OK**.

Step 6 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 7 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.419 ALM-45450 ClickHouse Failed to Obtain a Temporary Agency Credential

Alarm Description

After the cold-hot separation function and an agency are configured, the system checks the status of the temporary agency credential every minute. This alarm is generated when the the temporary agency credential fails to be obtained for three consecutive times.

This alarm is automatically cleared when the system successfully obtains the temporary agency credential.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45450	Critical	Quality of service	Tenant plane	ClickHouse	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
New	3.3.1	New alarm	New alarm

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	Alarm Severity	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

The system cannot access OBS after the temporary agency credential expires. Operations such as reading and writing cold data in OBS cannot be performed on tables configured with cold and hot separation policies.

Possible Causes

- The OBS parameters configured for ClickHouse are incorrect.
- The IAM service is abnormal.

Handling Procedure

Step 1 Check whether the cold and hot separation configuration is correct by referring to "Configuring ClickHouse Cold and Hot Data Separation" in MapReduce Service (MRS) 3.3.1-LTS User Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Usage Guide (for Huawei Cloud Stack 8.3.1). If the configuration is incorrect, modify the configuration and restart the ClickHouse instance. Wait for 3 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 2**.

Collect fault information.

Step 2 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 3 Expand the **Service** drop-down list, and select **ClickHouse** for the target cluster.

Step 4 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the abnormal host, and click **OK**.

Step 5 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 6 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.420 ALM-45451 ClickHouse Failed to Access OBS

Alarm Description

When cold-hot separation is enabled, the system checks the OBS access every minute. This alarm is generated when the system detects that OBS cannot be accessed for three consecutive times.

This alarm is automatically cleared when the system successfully accesses OBS.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45451	Critical	Quality of service	Tenant plane	ClickHouse	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
New	3.3.1	New alarm	New alarm

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	HostName	Specifies the host for which the alarm was generated.
	Alarm Severity	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

For tables configured with the cold-hot separation policy, cold data on OBS cannot be read or written. Hot data on local disks cannot be moved to OBS.

Possible Causes

- Parameters such as the endpoint used by ClickHouse to access OBS are incorrect.
- OBS is abnormal.

Handling Procedure

Step 1 Check whether the cold and hot separation configuration is correct by referring to "Configuring ClickHouse Cold and Hot Data Separation" in MapReduce Service (MRS) 3.3.1-LTS User Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Usage Guide (for Huawei Cloud Stack 8.3.1). If the configuration is incorrect, modify the configuration and restart the ClickHouse instance. Wait for 3 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 2**.

Collect fault information.

Step 2 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 3 Expand the **Service** drop-down list, and select **ClickHouse** for the target cluster.

Step 4 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the abnormal host, and click **OK**.

Step 5 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 6 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Related Information

None.

1.3.421 ALM-45452 ClickHouse's Local Disk Space Is Below the Cold-Hot Separation Threshold

Alarm Description

When cold-hot separation is enabled, the system checks the remaining space of the local disk specified in the cold-hot separation policy every 5 minutes. This alarm is generated if the remaining space is lower than the **move_factor** threshold.

This alarm is automatically cleared when the remaining space of the local disk is greater than the **move_factor** threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45452	Major	Quality of service	Tenant plane	ClickHouse	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
New	3.3.1	New alarm	New alarm

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	Alarm Severity	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

Some hot data on the local disk is moved to OBS, affecting the read and write performance of the system.

Possible Causes

The local disk capacity configured for cold-hot separation on the ClickHouseServer node is too small.

Handling Procedure

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**, and view the role name and the IP address of the hostname in **Location**.

Step 2 Expand the disk capacity of the node for which the alarm is generated. For details, see ClickHouse-related chapters in MapReduce Service (MRS) 3.3.1-LTS Physical Machine Cluster Capacity Expansion Guide (for Huawei Cloud Stack 8.3.1).

Step 3 Check whether the alarm is cleared after disk expansion.

- If yes, no further action is required.
- If no, go to **Step 4**.

Collect fault information.

Step 4 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 5 Expand the **Service** drop-down list, and select **ClickHouse** for the target cluster.

Step 6 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the abnormal host, and click **OK**.

Step 7 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 8 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.422 ALM-45585 IoTDB Service Unavailable

Alarm Description

The system checks the IoTDB service status every 300 seconds. This alarm is generated when the IoTDB service is unavailable. This alarm is cleared when the IoTDB service recovers.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45585	Critical	Error handling	Tenant plane	IoTDB	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.

Type	Parameter	Description
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	Alarm Severity	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Details	Specifies additional alarm information.

Impact on the System

The IoTDB service is unavailable for read and write operations.

Possible Causes

- The KrbServer service is abnormal.
- More than 50% of IoTDBServer instances are faulty.
- Failed to connect to the IoTDBServer JMX. As a result, the node status cannot be obtained.
- A disk is aged or damaged.

Handling Procedure

Check whether the KrbServer service on which the IoTDB depends is abnormal.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. In the alarm list, view the host name and IP address in **Location** of the alarm whose ID is **45585**.

Step 2 In the alarm list, check whether ALM-25500 KrbServer Service Unavailable exists.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 Handle the alarm by referring to **ALM-25500 KrbServer Service Unavailable**.

Step 4 After **ALM-25500** is cleared, wait several minutes and check whether this alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check whether IoTDBServer instances are faulty.

Step 5 On FusionInsight Manager, choose **Cluster** > **Services** > **IoTDB** > **Instance**.

Step 6 Check whether the percentage of faulty IoTDBServer instances exceeds 50%. If yes, restart the faulty IoTDBServer instances and check whether the status is restored.

- If yes, no further action is required.
- If no, go to **Step 7**.

Check whether the IoTDBServer instance is started properly.

Step 7 Log in to the host obtained in **Step 1**, switch to user **omm**, and run the **jps** command to check whether the IoTDBServer process exists in the command output.

- If yes, no further action is required.
- If no, go to **Step 8**.

Step 8 On FusionInsight Manager, choose **Cluster** > **Services** > **IoTDB** > **Instance**, select the IoTDBServer instance for which this alarm is generated, click **More**, and select **Restart Instance**.

Step 9 After the instance is restarted, wait several minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 10**.

Check disks.

Step 10 Check whether the disks of the host for which the alarm is generated exist, or check whether the disks can be used properly after being moved to another host.

- If yes, no further action is required.
- If no, go to **Step 11**.

Collect fault information.

Step 11 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 12 Expand the **Service** drop-down list, select **IoTDB** for the target cluster, and click **OK**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 13 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 14 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.423 ALM-45586 IoTDBServer Heap Memory Usage Exceeds the Threshold

Alarm Description

The system checks the IoTDBServer process status every 60 seconds. The alarm is generated when the heap memory usage of the IoTDBServer process exceeds the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45586	Critical (default threshold: 100%) Major (default threshold: 90%)	Quality of service	Tenant plane	IoTDB	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.

Type	Parameter	Description
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	Alarm Severity	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

The read and write performance of the IoTDBServer process deteriorates, memory overflow occurs, and the IoTDBServer process breaks down.

Possible Causes

The heap memory of the IoTDBServer process is overused or the heap memory is inappropriately allocated.

Handling Procedure

Check the heap memory usage.

Step 1 Log in to FusionInsight Manager and choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**. On the page that is displayed, locate the row

containing the alarm whose **Alarm ID** is **45586**, view the role name in **Location**, and check the instance IP address.

Step 2 Choose **Cluster** > *Name of the desired cluster* > **Service** > **IoTDB** > **Instance**. Click the IoTDBServer for which the alarm is generated to go to **Dashboard**. Click the drop-down list in the upper right corner of the chart area and choose **Customize** > **Memory**. In the dialog box that is displayed, select **IoTDBServer Heap Memory Resource Percentage**, and click **OK**. Check whether the used non-heap memory of the IoTDBServer process reaches 90% (by default) of the maximum non-heap memory specified for IoTDBServer.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 Choose **Cluster** > *Name of the desired cluster* > **Service** > **IoTDB** > **Configuration**, click **All Configurations**, choose **IoTDBServer** > **System**, and increase the value of **-Xmx** in the **GC_OPTS** parameter.

NOTE

- The default value of **-Xmx** is **2G**.
- If this alarm is occasionally generated, increase the value by 0.5 times. If this alarm is frequently generated, double the value.
- In the case of large service volume and high service concurrency, you are advised to add instances.

Step 4 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Collect the fault information.

Step 5 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 6 Expand the **Service** drop-down list, select **IoTDB** for the target cluster, and click **OK**.

Step 7 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 8 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.424 ALM-45587 IoTDBServer GC Duration Exceeds the Threshold

Alarm Description

The system checks the GC duration of the IoTDBServer process every 60 seconds. This alarm is generated when the GC duration exceeds the threshold for three consecutive times. You can choose **O&M** > **Alarm** > **Threshold Configuration** > *Name of the desired cluster* > **IoTDB** > **GC** > **Total GC duration of IoTDBServer process (IoTDBServer)** to change the threshold. This alarm is cleared when the GC duration is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45587	Critical (default threshold: 30000ms) Major (default threshold: 12000ms)	Quality of service	Tenant plane	IoTDB	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	Alarm Severity	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

The IoTDBServer process may be unavailable for read and write operations.

Possible Causes

The heap memory of the IoTDBServer process is overused or inappropriately allocated, causing frequent occurrence of the GC process.

Handling Procedure

Check the GC duration.

Step 1 Log in to FusionInsight Manager and choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**. On the page that is displayed, locate the row containing the alarm whose **Alarm ID** is **45587**, view the role name in **Location**, and check the instance IP address.

Step 2 Choose **Cluster** > *Name of the desired cluster* > **Service** > **IoTDB** > **Instance**. Click the IoTDBServer for which the alarm is generated to go to **Dashboard**. Click the drop-down list in the upper right corner of the chart area and choose **Customize** > **GC**. In the dialog box that is displayed, select **Garbage Collection (GC) Time of IoTDBServer**, and click **OK**. Check whether the GC time of the IoTDBServer process is greater than 12 seconds.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 Choose **Cluster** > *Name of the desired cluster* > **Service** > **IoTDB** > **Configuration**, click **All Configurations**, choose **IoTDBServer** > **System**, and increase the value of **-Xmx** in the **GC_OPTS** parameter.

NOTE

- The default value of **-Xmx** is **2G**.
- If this alarm is occasionally generated, increase the value by 0.5 times. If this alarm is frequently generated, double the value.
- In the case of large service volume and high service concurrency, you are advised to add instances.

Step 4 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Collect the fault information.

Step 5 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 6 Expand the **Service** drop-down list, select **IoTDB** for the target cluster, and click **OK**.

Step 7 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 8 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.425 ALM-45588 IoTDBServer Direct Memory Usage Exceeds the Threshold

Alarm Description

The system checks the direct memory usage of the IoTDBServer service every 60 seconds. This alarm is generated when the direct memory usage of the IoTDBServer instance exceeds the threshold for five consecutive times. This alarm is cleared when the IoTDBServer direct memory usage is less than or equal to the threshold.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45588	Critical (default threshold: 100%) Major (default threshold: 90%)	Quality of service	Tenant plane	IoTDB	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	Alarm Severity	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

Direct memory overflow may cause service unavailability, and the IoTDBServer process may be unavailable for read and write operations.

Possible Causes

The direct memory of the IoTDBServer process is overused or the direct memory is inappropriately allocated.

Handling Procedure

Check the direct memory usage.

Step 1 Log in to FusionInsight Manager and choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**. On the page that is displayed, locate the row containing the alarm whose **Alarm ID** is **45588**, view the role name in **Location**, and check the instance IP address.

Step 2 Choose **Cluster** > *Name of the desired cluster* > **Service** > **IoTDB** > **Instance**. Click the IoTDBServer for which the alarm is generated to go to **Dashboard**. Click the drop-down list in the upper right corner of the chart area and choose **Customize** > **Memory**. In the dialog box that is displayed, select **IoTDBServer Direct Buffer Resource Percentage**, and click **OK**.

Step 3 Check whether the direct memory used by the IoTDBServer reaches the threshold (90% of the maximum direct memory by default).

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Service** > **IoTDB** > **Configuration**, click **All Configurations**, choose **IoTDBServer** > **System**, increase the value of **-XX:MaxDirectMemorySize** in the **GC_OPTS** parameter as required, and save the configuration.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

NOTE

- If this alarm is generated, the direct memory configured for the IoTDBServer process cannot meet the requirements of the IoTDBServer process.
- You are advised to set **-XX:MaxDirectMemorySize** in **GC_OPTS** to twice the direct memory used by the IoTDBServer process. (You can change the value based on the actual service scenario.)
- To obtain the size of the direct memory used by the IoTDBServer process, choose **Customize** > **Memory** > **IoTDBServer Direct Memory Resource Status**. If **GC_OPTS** does not contain the **-XX:MaxDirectMemorySize** parameter, add it manually.

Step 5 Restart the affected services or instances and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect the fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **IoTDBServer** for the target cluster.

Step 8 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.426 ALM-45589 ConfigNode Heap Memory Usage Exceeds the Threshold

Alarm Description

The system checks the ConfigNode process status every 60 seconds. The alarm is generated when the heap memory usage of the ConfigNode process exceeds the threshold. This alarm is cleared when the heap memory usage of the ConfigNode process is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45589	Critical (default threshold: 100%) Major (default threshold: 90%)	Quality of service	Tenant plane	IoTDB	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	Alarm Severity	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

The read and write performance of the ConfigNode process deteriorates, memory overflow occurs, and the ConfigNode process breaks down.

Possible Causes

The heap memory configured for the node is improper. As a result, the usage exceeds the threshold.

Handling Procedure

Check the heap memory configuration.

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. In the real-time alarm list, click ⌄ in front of this alarm and view the role name and instance IP address in **Location**.

Step 2 Choose **Cluster** > **Services** > **IoTDB**. Click **Instance**, click the ConfigNode corresponding to the IP address obtained in **Step 1**, and check whether **ConfigNode Heap Memory Usage** on the **Dashboard** tab page reaches the threshold specified for the ConfigNode process.

If the chart is not displayed, click the drop-down list in the upper right corner of the chart area and choose **Customize** > **Memory**. In the dialog box that is displayed, select **ConfigNode Heap Memory Usage** and click **OK**.

NOTE

You can choose **O&M** > **Alarm** > **Threshold Configuration** > *Name of the desired cluster* > **IoTDB** > **Memory** > **ConfigNode Heap Memory Usage (ConfigNode)** to view the threshold.

- If yes, go to **Step 3**.
- If no, go to **Step 6**.

Step 3 Choose **Cluster** > **Services** > **IoTDB**. Click **Configurations** then **All Configurations**, click **ConfigNode**, and choose **System**. Set **-Xmx** in **GC_OPTS** to a larger value and save the configuration.

NOTE

- The default value of -**Xmx** is **2G**.
- If this alarm is occasionally generated, increase the value of **-Xmx** by 0.5 times. If this alarm is frequently generated, double the value of **-Xmx**.
- In the case of large service volume and high service concurrency, you are advised to add instances.

Step 4 Click **Dashboard**. Click **Restart Service** to restart the IoTDB service for the configuration to take effect.

Step 5 Wait for about 120 seconds and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, select **IoTDB** for the target cluster, and click **OK**.

Step 8 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the hosts to which the role belongs, and click **OK**.

Step 9 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.427 ALM-45590 ConfigNode GC Duration Exceeds the Threshold

Alarm Description

The system checks the GC duration of the ConfigNode process every 60 seconds. This alarm is generated when the GC duration exceeds the threshold for three consecutive times. This alarm is cleared when the GC duration is less than the threshold.

NOTE

You can choose **O&M** > **Alarm** > **Threshold Configuration** > *Name of the desired cluster* > **IoTDB** > **GC** > **Total GC duration of ConfigNode process (ConfigNode)** to increase the threshold by 20% each time.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45590	Critical (default threshold: 30000ms) Major (default threshold: 12000ms)	Quality of service	Tenant plane	IoTDB	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	Alarm Severity	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

The read and write performance of the ConfigNode process may deteriorate.

Possible Causes

The heap memory configured on the node is improper. As a result, GC occurs frequently.

Handling Procedure

Check the heap memory configuration.

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. In the real-time alarm list, click ⌄ in the row containing this alarm and view the role name and instance IP address in **Location**.

Step 2 Choose **Cluster** > **Services** > **IoTDB**. Click **Instance**, click the ConfigNode corresponding to the IP address obtained by **Step 1**. Switch to the **Dashboard** tab page, locate the **Total GC Duration of ConfigNode** chart, and check whether the GC duration of the ConfigNode process exceeds the threshold.

If the GC duration of ConfigNode is not displayed, click the drop-down list in the upper right corner of the chart area and choose **Customize** > **GC**. In the displayed dialog box, select **Total GC Duration of ConfigNode** and click **OK**.

NOTE

You can choose **O&M** > **Alarm** > **Threshold Configuration** > *Name of the desired cluster* > **IoTDB** > **GC** > **Total GC duration of ConfigNode process (ConfigNode)** to view the threshold.

- If yes, go to **Step 3**.
- If no, go to **Step 6**.

Step 3 Choose **Cluster** > **Services** > **IoTDB**. Click **Configurations** then **All Configurations**, click **ConfigNode**, and choose **System**. Set **-Xmx** in **GC_OPTS** to a larger value and save the configuration.

NOTE

- The default value of **-Xmx** is **2G**.
- If this alarm is occasionally generated, increase the value by 0.5 times. If this alarm is frequently generated, double the value.
- In the case of large service volume and high service concurrency, you are advised to add instances.

Step 4 Click **Dashboard**. Click **Restart Service** to restart the IoTDB service for the configuration to take effect.

Step 5 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, select **IoTDB** for the target cluster, and click **OK**.

Step 8 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the hosts to which the role belongs, and click **OK**.

Step 9 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.428 ALM-45591 ConfigNode Direct Memory Usage Exceeds the Threshold

Alarm Description

The system checks the direct memory usage of the ConfigNode process every 60 seconds. This alarm is generated when the direct memory usage of the ConfigNode exceeds the threshold for five consecutive times. That is, the direct memory configured for ConfigNode cannot meet service requirements. This alarm is cleared when the direct memory usage of ConfigNode is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45591	Critical (default threshold: 100%) Major (default threshold: 90%)	Quality of service	Tenant plane	IoTDB	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	Alarm Severity	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

Direct memory overflow may cause instance unavailability, and the ConfigNode process may be unavailable for read and write operations.

Possible Causes

The direct memory configured for the node is improper. As a result, the usage exceeds the threshold.

Handling Procedure

Check the direct memory configuration.

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. In the real-time alarm list, click in front of this alarm and view the role name and instance IP address in **Location**.

Step 2 Choose **Cluster** > **Services** > **IoTDB**. Click **Instance**, click the ConfigNode corresponding to the IP address obtained in **Step 1**, and check whether **ConfigNode Direct Memory Usage** on the **Dashboard** tab page reaches the threshold specified for the ConfigNode process (90% of the maximum direct memory by default).

If the chart is not displayed, click the drop-down list in the upper right corner of the chart area and choose **Customize** > **Memory**. In the dialog box that is displayed, select **ConfigNode Direct Memory Usage** and click **OK**.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **IoTDB**. Click **Configurations** then **All Configurations**. Click **ConfigNode** and select **System**. Set **-XX:MaxDirectMemorySize** in **GC_OPTS** to a larger value as required and save the configuration.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

NOTE

- You are advised to set **-XX:MaxDirectMemorySize** in **GC_OPTS** to twice the direct memory used by the ConfigNode process. (You can change the value based on the actual service scenario.)
- To obtain the size of the direct memory used by the ConfigNode process, choose **Customize** > **Memory** > **ConfigNode Direct Memory Resource Status**.
- If **GC_OPTS** does not contain the **-XX:MaxDirectMemorySize** parameter, add it.

Step 4 Restart the affected IoTDB service or instances and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Collect fault information.

Step 5 On FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 6 Expand the **Service** drop-down list, and select **ConfigNode** for the destination cluster.

Step 7 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the hosts to which the role belongs, and click **OK**.

Step 8 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.429 ALM-45592 IoTDBServer RPC Execution Duration Exceeds the Threshold

Alarm Description

The system checks the RPC execution duration of the IoTDBServer process every 60 seconds. This alarm is generated when the execution duration exceeds the threshold. This alarm is cleared when the RPC execution time of the IoTDBServer process is less than the threshold.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45592	Critical (default threshold: 60,000 ms) Major (default threshold: 50,000ms)	Quality of service	Tenant plane	IoTDB	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	Alarm Severity	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

The read and write performance of the IoTDBServer process deteriorates.

Possible Causes

The processing duration of an IoTDBServer RPC request exceeds the threshold. Logs need to be further analyzed to locate the cause.

Handling Procedure

Collect fault information.

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. In the real-time alarm list, click in front of this alarm and view the role name and instance IP address in **Location**.

Step 2 Choose **O&M** > **Log** > **Download**.

Step 3 Expand the **Service** drop-down list, select **IoTDB** for the target cluster, and click **OK**.

Step 4 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the host queried in **Step 1**, and click **OK**.

Step 5 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 6 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

1.3.430 ALM-45593 IoTDBServer Flush Execution Duration Exceeds the Threshold

Alarm Description

This alarm is generated when the data flush duration exceeds the threshold. This alarm is cleared when the flush duration is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45593	Critical (default threshold: 300,000 ms) Major (default threshold: 200,000ms)	Quality of service	Tenant plane	IoTDB	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	Alarm Severity	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

The data writes are blocked, which causes write performance deterioration.

Possible Causes

The IoTDB flushing on the node is slow. You need to further analyze logs.

Handling Procedure

Collect fault information.

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. In the real-time alarm list, click in front of this alarm and view the role name and instance IP address in **Location**.

Step 2 Choose **O&M** > **Log** > **Download**.

Step 3 Expand the **Service** drop-down list, select **IoTDB** for the target cluster, and click **OK**.

Step 4 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the host queried in **Step 1**, and click **OK**.

Step 5 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 6 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.431 ALM-45594 IoTDBServer Intra-Space Merge Duration Exceeds the Threshold

Alarm Description

This alarm is generated when the merge duration in the space exceeds the threshold. This alarm is cleared when the merge duration in the space is less than the threshold.

Alarm Attributes

Alarm Attributes	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45594	Major	Quality of service	Tenant plane	IoTDB	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

Data write is blocked and the write operation performance is affected.

Possible Causes

The merge task in the IoTDB space of the node is slow. You need to further analyze logs.

Handling Procedure

Collect fault information.

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. In the real-time alarm list, click in front of this alarm and view the role name and instance IP address in **Location**.

Step 2 Choose **O&M** > **Log** > **Download**.

Step 3 Expand the **Service** drop-down list, select **IoTDB** for the target cluster, and click **OK**.

Step 4 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the host queried in **Step 1**, and click **OK**.

Step 5 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 6 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.432 ALM-45595 IoTDBServer Cross-Space Merge Duration Exceeds the Threshold

Alarm Description

This alarm is generated when the cross-space merge duration exceeds the threshold. This alarm is cleared when the cross-space merge duration is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45595	Critical (default threshold: 1,800,000 ms) Major (default threshold: 1,000,000 ms)	Quality of service	Tenant plane	IoTDB	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	Alarm Severity	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

Data writes are blocked, which causes write performance deterioration.

Possible Causes

The IoTDB cross-space merge task on the node is slow. You need to further analyze logs.

Handling Procedure

Collect fault information.

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. In the real-time alarm list, click ⌄ in front of this alarm and view the role name and instance IP address in **Location**.

Step 2 Choose **O&M** > **Log** > **Download**.

Step 3 Expand the **Service** drop-down list, select **IoTDB** for the target cluster, and click **OK**.

Step 4 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the host queried in **Step 1**, and click **OK**.

Step 5 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 6 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.433 ALM-45596 Procedure Execution Failed

Alarm Description

Procedures are the tasks managed and executed by the ConfigNode leader. This alarm is generated when a procedure fails to be executed. This alarm is cleared when the procedure is successfully executed.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45596	Major	Error handling	Tenant plane	IoTDB	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	Alarm Severity	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	ProcedureInformation	Specifies the procedure-related information.

Impact on the System

Operation consistency is affected.

Possible Causes

- The task for adding IoTDB replicas fails to be executed.
- The task for deleting the storage group fails to be executed.

Handling Procedure

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**, locate this alarm, and click ⌄.

Step 2 Check the value of **ProcedureInformation** in **Location**. The value starts with the procedure type and contains main information about the procedure.

Check whether the task for adding replicas fails.

Step 3 Check whether the value of **ProcedureInformation** starts with **AddRegionProcedure** or **ReJoinDataNodeProcedure**.

- If yes, the task fails. Go to **Step 4**.

- If no, go to **Step 5**.

Step 4 Wait for half an hour. If the region is successfully added, the alarm is automatically cleared. Otherwise, go to **Step 5**.

Check whether the task for deleting the storage group fails.

Step 5 Check whether the value of **ProcedureInformation** starts with **DeleteStorageGroupProcedure**.

- If yes, the storage group fails to be deleted. Go to **Step 6**.
- If no, go to **Step 7**.

Step 6 Delete the storage group displayed in **ProcedureInformation** again on the IoTDB client. If the deletion is successful, the alarm is automatically cleared. Otherwise, go to **Step 7**.

Collect fault information.

Step 7 Choose **Cluster** > **Services** > **IoTDB** > **Instance** to view the hosts where all IoTDBServer and ConfigNode instances are located.

Step 8 Choose **O&M** > **Log** > **Download**.

Step 9 Expand the **Service** drop-down list, select **IoTDB** for the target cluster, and click **OK**.

Step 10 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the host queried in **Step 7**, and click **OK**.

Step 11 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.434 ALM-45615 CDL Service Unavailable

Alarm Description

The system checks the CDL health status every 60 seconds. This alarm is generated when the CDL health status is **DOWN**. This alarm is cleared when the system detects that the CDL health status is **UP**.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45615	Critical	Quality of service	Tenant plane	CDL	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

The CDL service is abnormal. You cannot use FusionInsight Manager to perform cluster operations on the CDL service. The CDL service function is unavailable.

Possible Causes

All CDLService or CDLConnector instances of the CDL service are abnormal, and the Kafka service is unavailable.

Handling Procedure

Check whether the Kafka service on which the CDL service depends is abnormal.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**.

Step 2 In the alarm list, check whether ALM-38000 Kafka Service Unavailable exists.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 Handle the alarm by referring to "ALM-38000 Kafka Service Unavailable".

Step 4 After the alarm is cleared, wait a few minutes and check whether the alarm HetuServer Service Unavailable is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check whether CDL instances are faulty.

Step 5 On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Service** > **CDL** > **Instance**.

Step 6 Check whether all CDLService and CDLConnector instances are faulty.

- If yes, restart the CDL service and choose **Cluster** > *Name of the desired cluster* > **Services** > **CDL** > **More** > **Restart Service**. If the fault persists after the restart, go to **Step 7** and contact O&M personnel to check CDL logs.
- If no, go to **Step 7**.

Collect the fault information.

Step 7 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 8 Expand the **Service** drop-down list, and select **CDL** for the target cluster.

Step 9 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

After the service is restored, the system automatically clears the alarm.

Related Information

None.

1.3.435 ALM-45616 CDL Job Execution Exception

Alarm Description

The system checks whether a CDL job is normal every 60 seconds. This alarm is reported when the CDL job is abnormal. This alarm is cleared when the job is restored or stopped.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45616	Major	Quality of service	Tenant plane	CDL	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	JobName	Specifies the job for which the alarm was generated.
	Username	Specifies the username of the job for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

CDL tasks fail, and real-time data integration is interrupted.

Possible Causes

The CDL task fails to be executed due to incorrect parameter settings or other reasons. On the **Job Management** page of the CDL web UI, locate the row where the job is located and click **Failed**/**Abnormal running** in the **Status** column to view the failure cause, or view the failure cause in the logs.

Handling Procedure

Step 1 Log in to FusionInsight Manager as a user who has the CDL job creation or administrator permission.

Step 2 Choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**, click ⌄ in the row where **Alarm ID** is **45616**, and view the name of the job for which this alarm is generated in **Location**.

Step 3 Choose **Cluster** > **Services** > **CDL** and click the link next to **CDLService UI** to go to the CDL web UI.

Step 4 Locate the failed job based on the task name in **Step 2** and check whether **Source** is **Hudi**.

- If yes, go to **Step 5**.
- If no, go to **Step 6**.

Step 5 On Manager, choose **Cluster** > **Services** > **Yarn** and click the link next to **ResourceManager Web UI** to go to the Yarn web UI. Search for the ID of the latest failed task in **Step 2**, select the task ID, click **Logs**, search for **stdout**, and go to **Step 8**.

Step 6 Click **Abnormal running** or **Failed** in the **Status** column.

Step 7 On the page that is displayed, view the error information and rectify the fault. For example, **Figure 1-17** shows that the task running on Yarn is manually killed. For details, see trace error information, as shown in **Figure 1-18**.

Figure 1-17 CDL job exception

Figure 1-18 Trace error information

Step 8 Rectify the fault based on the error information, execute the task again, and check whether the task can be executed successfully.

- If yes, no further action is required.
- If no, go to **Step 9**.

Collect the fault information.

Step 9 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 10 Select **CDL** in the required cluster for **Service**.

Step 11 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact technical support and provide the collected logs.

----End

Alarm Clearance

After the job is successfully restored or stopped, the alarm is cleared if it has been reported.

Related Information

None.

1.3.436 ALM-45617 Data Queued in the CDL Replication Slot Exceeds the Threshold

Alarm Description

If a large number of write-ahead logs (WALs) are stacked in the PostgreSQL/Opengauss database, the PostgreSQL/Opengauss disk space may be used up. The system checks whether the amount of data queued in the replication slot configured for a CDL job exceeds the threshold (5120 MB by default) every 5 minutes. This alarm is generated when the amount of data queued in the replication slot exceeds the threshold. This alarm is cleared when the number of data queued in the replication slot falls below the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45617	Major	Environment	Tenant plane	CDL	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.

Type	Parameter	Description
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	JobName	Specifies the job for which the alarm was generated.
	DBName	Specifies the database for which the alarm was generated.
	SlotName	Specifies the database replication slot for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Lag	Specifies the volume of stacked data in the replication slot configured for a CDL task.

Impact on the System

Disk space of the source PostgreSQL or openGauss database may be used up and the database cannot provide services.

Possible Causes

The CDL job is abnormal, and data processing stops; the source database is updated quickly, and CDL data processing is slow.

Handling Procedure

Step 1 Log in to FusionInsight Manager as a user who has the CDL job creation or administrator permission.

Step 2 Choose **O&M**. In the navigation pane on the left, choose **Alarm** > **Alarms**, click ⌄ in the row where **Alarm ID** is **45617**, and view the name of the job for which this alarm is generated in **Location**.

Step 3 Check whether **ALM-45616 CDL Job Execution Exception** is displayed in the alarm list.

- If yes, handle the alarm by performing operations provided for **ALM-45616 CDL Job Execution Exception**.
- If no, go to **Step 4**.

Step 4 Choose **Cluster** > **Services** > **CDL**. Click the link next to **CDLService UI** to go to the CDL web UI and check whether the job is displayed in the job list based on its name obtained in **Step 2**.

- If yes, check whether the job is abnormal.
  - If it is abnormal, go to **Step 5**.
  - If it is not, data processing is slow. Contact technical support.
- If no, go to **Step 7**.

Step 5 Click **Abnormal** or **Failed** in the row where the job is located and rectify the fault based on the error information displayed on the page.

Step 6 After rectifying the fault, run the job again and check whether the job can be executed successfully.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect the fault information.

Step 7 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 8 Select **CDL** in the required cluster for **Service**.

Step 9 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is cleared when the amount of data queued in the replication slot is less than the threshold. You do not need to manually clear the alarm.

Related Information

None.

1.3.437 ALM-45635 FlinkServer Job Execution Failure

Alarm Description

The system checks whether FlinkServer jobs fail to be executed every 10 seconds. This alarm is generated when a FlinkServer job fails. This alarm is cleared when the job is successfully restarted.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45635	Major	Quality of service	Tenant plane	Flink	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	ApplicationName	Specifies the name of the application for which the alarm was generated.
	JobName	Specifies the job for which the alarm was generated.
	UserName	Specifies the username for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

This alarm is a job-level alarm and does not affect FlinkServer. You need to view Flink job logs to find out the failure cause.

Possible Causes

You can view failure causes in specific logs.

Handling Procedure

Step 1 Log in to Manager as a user who has the FlinkServer management permission.

Step 2 Choose **Cluster** > **Services** > **Yarn** and click the link next to **ResourceManager WebUI** to go to the native Yarn page.

Step 3 Locate the failed task based on its name displayed in **Location**, search for and record the application ID of the job, and check whether the job logs are available on the native Yarn page.

Figure 1-19 Application ID of a job

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 Click the application ID of the failed job to go to the job page.

1. Click **Logs** in the **Logs** column to view JobManager logs.

Figure 1-20 Clicking Logs

2. Click the ID in the **Attempt ID** column and click **Logs** in the **Logs** column to view TaskManager logs.

Figure 1-21 Clicking the ID in the Attempt ID column

Figure 1-22 Clicking Logs

NOTE

You can also log in to Manager as a user who has the FlinkServer management permission. Choose **Cluster** > **Services** > **Flink**, and click the link next to **Flink WebUI**. On the displayed Flink web UI, click **Job Management**, click **More** in the **Operation** column, and select **Job Monitoring** to view TaskManager logs.

Step 5 View the logs of the failed job to rectify the fault, or contact the technical support and send the collected fault logs. No further action is required.

If logs are unavailable on the Yarn page, download logs from HDFS.

Step 6 On Manager, choose **Cluster** > **Services** > **HDFS**, click the link next to **NameNode WebUI** to go to the HDFS page, choose **Utilities** > **Browse the file system**, and download logs in the **/tmp/logs/***Username***/logs/***Application ID of the failed job* directory.

Step 7 View the logs of the failed job to rectify the fault, or contact the technical support and send the collected fault logs.

----End

Alarm Clearance

After the job is successfully restarted, the alarm is cleared if it has been reported.

Related Information

None.

1.3.438 ALM-45636 Number of Consecutive Checkpoint Failures of a Flink Job Exceeds the Threshold

Alarm Description

The system checks the number of consecutive checkpoint failures based on the configured alarm checking interval. This alarm is generated when the number of consecutive checkpoint failures of a FlinkServer job reaches the configured threshold. This alarm is cleared when checkpoints are recovered or the job is successfully restarted.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45636	Major	Quality of service	Tenant plane	Flink	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	ApplicationName	Specifies the name of the application for which the alarm was generated.
	JobName	Specifies the job for which the alarm was generated.
	UserName	Specifies the username for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	ThreshHoldValue	Specifies the threshold value for triggering the alarm.
	CurrentValue	Specifies the value that triggered the alarm.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

The Flink job may fail. You need to check the status and logs of the Flink job to locate the fault. This is a job-level alarm and has no impact on FlinkServer.

Possible Causes

You can view failure causes in specific logs.

Handling Procedure

Step 1 Log in to Manager as a user who has the FlinkServer management permission.

Step 2 Choose **Cluster** > **Services** > **Yarn** and click the link next to **ResourceManager WebUI** to go to the native Yarn page.

Step 3 Locate the failed task based on its name displayed in **Location**, search for and record the application ID of the job, and check whether the job logs are available on the native Yarn page.

Figure 1-23 Application ID of a job

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 Click the application ID of the failed job to go to the job page.

1. Click **Logs** in the **Logs** column to view JobManager logs.

Figure 1-24 Clicking Logs

2. Click the ID in the **Attempt ID** column and click **Logs** in the **Logs** column to view TaskManager logs.

Figure 1-25 Clicking the ID in the Attempt ID column

Figure 1-26 Clicking Logs

NOTE

You can also log in to Manager as a user who has the FlinkServer management permission. Choose **Cluster** > **Services** > **Flink**, and click the link next to **Flink WebUI**. On the displayed Flink web UI, click **Job Management**, click **More** in the **Operation** column, and select **Job Monitoring** to view TaskManager logs.

Step 5 View the logs of the failed job to rectify the fault, or contact the technical support and send the collected fault logs. No further action is required.

If logs are unavailable on the Yarn page, download logs from HDFS.

Step 6 On Manager, choose **Cluster** > **Services** > **HDFS**, click the link next to **NameNode WebUI** to go to the HDFS page, choose **Utilities** > **Browse the file system**, and download logs in the **/tmp/logs/***Username***/logs/***Application ID of the failed job* directory.

Step 7 View the logs of the failed job to rectify the fault, or contact the technical support and send the collected fault logs.

----End

Alarm Clearance

This alarm is cleared when FlinkServer job checkpoints are recovered or the job is successfully restarted.

Related Information

None.

1.3.439 ALM-45637 Continuous Back Pressure Time of a Flink Job Exceeds the Threshold

Alarm Description

The system checks the back pressure duration of FlinkServer tasks based on the configured alarm checking interval. This alarm is generated when the back pressure duration of a FlinkServer task reaches the configured threshold. This alarm is cleared when the task back pressure is recovered or the job is successfully restarted.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45637	Minor	Quality of service	Tenant plane	Flink	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	ApplicationName	Specifies the name of the application for which the alarm was generated.
	JobName	Specifies the job for which the alarm was generated.
	UserName	Specifies the username for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ThreshHoldValue	Specifies the threshold value for triggering the alarm.
	CurrentValue	Specifies the value that triggered the alarm.

Impact on the System

Continuous back pressure of Flink jobs may cause performance problems or checkpoint failures. Flink jobs fail. You need to check the status and logs of the Flink jobs to locate the cause. This is a job-level alarm and has no impact on FlinkServer.

Possible Causes

You can view the causes in the specific logs.

Handling Procedure

Step 1 Log in to Manager as a user who has the FlinkServer management permission.

Step 2 Choose **Cluster** > **Services** > **Yarn** and click the link next to **ResourceManager WebUI** to go to the native Yarn page.

Step 3 Locate the failed task based on its name displayed in **Location**, search for and record the application ID of the job, and check whether the job logs are available on the native Yarn page.

Figure 1-27 Application ID of a job

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 Click the application ID of the failed job to go to the job page.

1. Click **Logs** in the **Logs** column to view JobManager logs.

Figure 1-28 Clicking Logs

2. Click the ID in the **Attempt ID** column and click **Logs** in the **Logs** column to view TaskManager logs.

Figure 1-29 Clicking the ID in the Attempt ID column

Figure 1-30 Clicking Logs

NOTE

You can also log in to Manager as a user who has the FlinkServer management permission. Choose **Cluster** > **Services** > **Flink**, and click the link next to **Flink WebUI**. On the displayed Flink web UI, click **Job Management**, click **More** in the **Operation** column, and select **Job Monitoring** to view TaskManager logs.

Step 5 View the logs of the failed job to rectify the fault, or contact the technical support and send the collected fault logs. No further action is required.

If logs are unavailable on the Yarn page, download logs from HDFS.

Step 6 On Manager, choose **Cluster** > **Services** > **HDFS**, click the link next to **NameNode WebUI** to go to the HDFS page, choose **Utilities** > **Browse the file system**, and download logs in the **/tmp/logs/***Username***/logs/***Application ID of the failed job* directory.

Step 7 View the logs of the failed job to rectify the fault, or contact the technical support and send the collected fault logs.

----End

Alarm Clearance

This alarm is cleared when FlinkServer task back pressure is recovered or the job is successfully restarted.

Related Information

None.

1.3.440 ALM-45638 Number of Restarts After Flink Job Failures Exceeds the Threshold

Alarm Description

The system checks the times a FlinkServer job restarts based on the alarm checking interval. This alarm is generated when the number exceeds the configured threshold. This alarm is cleared when the job is restarted.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45638	Major	Quality of service	Tenant plane	Flink	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	ApplicationName	Specifies the name of the application for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	JobName	Specifies the job for which the alarm was generated.
	UserName	Specifies the username for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	ThreshHoldValue	Specifies the threshold value for triggering the alarm.
	CurrentValue	Specifies the value that triggered the alarm.

Impact on the System

Flink jobs are frequently restarted due to the failures. You need to locate the cause. This is a job-level alarm and has no impact on FlinkServer.

Possible Causes

You can view the causes in the specific logs.

Handling Procedure

Step 1 Log in to Manager as a user who has the FlinkServer management permission.

Step 2 Choose **Cluster** > **Services** > **Yarn** and click the link next to **ResourceManager WebUI** to go to the native Yarn page.

Step 3 Locate the failed task based on its name displayed in **Location**, search for and record the application ID of the job, and check whether the job logs are available on the native Yarn page.

Figure 1-31 Application ID of a job

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 Click the application ID of the failed job to go to the job page.

1. Click **Logs** in the **Logs** column to view JobManager logs.

Figure 1-32 Clicking Logs

2. Click the ID in the **Attempt ID** column and click **Logs** in the **Logs** column to view TaskManager logs.

Figure 1-33 Clicking the ID in the Attempt ID column

Figure 1-34 Clicking Logs

NOTE

You can also log in to Manager as a user who has the FlinkServer management permission. Choose **Cluster** > **Services** > **Flink**, and click the link next to **Flink WebUI**. On the displayed Flink web UI, click **Job Management**, click **More** in the **Operation** column, and select **Job Monitoring** to view TaskManager logs.

Step 5 View the logs of the failed job to rectify the fault, or contact the technical support and send the collected fault logs. No further action is required.

If logs are unavailable on the Yarn page, download logs from HDFS.

Step 6 On Manager, choose **Cluster** > **Services** > **HDFS**, click the link next to **NameNode WebUI** to go to the HDFS page, choose **Utilities** > **Browse the file system**, and download logs in the **/tmp/logs/***Username***/logs/***Application ID of the failed job* directory.

Step 7 View the logs of the failed job to rectify the fault, or contact the technical support and send the collected fault logs.

----End

Alarm Clearance

This alarm is cleared when the FlinkServer job is successfully restarted.

Related Information

None.

1.3.441 ALM-45639 Checkpointing of a Flink Job Times Out

Alarm Description

The system checks the checkpointing timeout of Flink jobs every 30 seconds. This alarm is generated if the checkpointing timeout of a Flink job is longer than the threshold (600 seconds by default). This alarm is cleared when the checkpointing timeout of a job is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45639	Minor	Quality of service	Tenant plane	Flink	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ServiceName	Specifies the cluster service for which the alarm was generated.
	ApplicationName	Specifies the name of the application for which the alarm was generated.
	JobName	Specifies the job for which the alarm was generated.
	UserName	Specifies the username for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	ThreshHoldValue	Specifies the threshold value for triggering the alarm.
	CurrentValue	Specifies the value that triggered the alarm.

Impact on the System

The checkpointing fails. You need to locate the cause. This is a job-level alarm and has no impact on FlinkServer.

Possible Causes

The job may be in the sub-healthy state. The possible causes are as follows:

- The memory for the TaskManager of the job is insufficient.
- The state memory is too large, making checkpointing time-consuming.

Handling Procedure

Step 1 Log in to Manager as a user who has the FlinkServer management permission.

Step 2 Choose **O&M** > **Alarm** > **Alarms** > **ALM-45639 Checkpointing of a Flink Job Times Out**, view **Location**, and obtain the name of the task for which the alarm is generated.

Step 3 Choose **Cluster** > **Services** > **Yarn** and click the link next to **ResourceManager WebUI** to go to the native Yarn page.

Step 4 Locate the failed task based on its name displayed in **Location**, search for and record the application ID of the job, and check whether the job logs are available on the Yarn page.

Figure 1-35 Application ID of a job

- If yes, go to **Step 5**.
- If no, go to **Step 7**.

Step 5 Click the application ID of the failed job to go to the job page.

1. Click **Logs** in the **Logs** column to view JobManager logs.

Figure 1-36 Clicking Logs

2. Click the ID in the **Attempt ID** column and click **Logs** in the **Logs** column to view TaskManager logs.

Figure 1-37 Clicking the ID in the Attempt ID column

Figure 1-38 Clicking Logs

NOTE

You can also log in to Manager as a user who has the FlinkServer management permission. Choose **Cluster** > **Services** > **Flink**, and click the link next to **Flink WebUI**. On the displayed Flink web UI, click **Job Management**, click **More** in the **Operation** column, and select **Job Monitoring** to view TaskManager logs.

Step 6 View the logs of the failed job to rectify the fault, or contact the technical support and send the collected fault logs. No further action is required.

If logs are unavailable on the Yarn page, download logs from HDFS.

Step 7 On Manager, choose **Cluster** > **Services** > **HDFS**, click the link next to **NameNode WebUI** to go to the HDFS page, choose **Utilities** > **Browse the file system**, and download logs in the **/tmp/logs/***Username***/logs/***Application ID of the failed job* directory.

Step 8 View the logs of the failed job to rectify the fault, or contact the technical support and send the collected fault logs.

----End

Alarm Clearance

This alarm is cleared when the checkpointing timeout a Flink job is less than or equal to the threshold.

Related Information

None.

1.3.442 ALM-45640 FlinkServer Heartbeat Interruption Between the Active and Standby Nodes

Alarm Description

This alarm is generated when the FlinkServer active node or standby node does not receive heartbeat messages from the peer for 30 seconds (heartbeat interruption duration configured in keepalive).

This alarm is cleared when the heartbeat recovers.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45640	Minor	Heartbeat	Tenant plane	Flink	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.

Type	Parameter	Description
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	Alarm Severity	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

The impact varies depending on the cause. If the heartbeat is interrupted due to other reasons, for example, network problems, two active nodes may exist because the standby node became the active node. Data synchronization between the active and standby nodes is abnormal, but FlinkServer can still provide services.

Possible Causes

- The active or standby FlinkServer instance is in the stopped state.
- The NIC of the floating IP address of the HA system used by the FlinkServer node is incorrectly configured. FlinkServer fails to be started.
- The link between the active and standby FlinkServer nodes is abnormal.

Handling Procedure

Check the status of the active and standby FlinkServer instances.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 1 Log in to FusionInsight Manager, choose **Cluster** > **Services** > **Flink** > **Instance**, and check the state of FlinkServer is normal.

- If yes, go to **Step 3**.
- If no, go to **Step 2**.

Step 2 Select the abnormal FlinkServer instance and start the instance. After the instance is started, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 3**.

NOTICE

During restart, the FlinkServer instance cannot provide services, but submitted jobs are not affected.

Check whether the link between the standby FlinkServer nodes is normal.

Step 3 Choose **Cluster** > **Services** > **Flink** > **Instance**, and check the two service IP addresses of FlinkServer.

Step 4 Log in to the server where the abnormal FlinkServer instance locates as user **root**.

Step 5 Run the following command to check whether the server of the other FlinkServer instance is reachable:

ping *IP address of the other FlinkServer instance*

- If yes, go to **Step 8**.
- If no, go to **Step 6**.

Step 6 Ask the network administrator to handle the network exception.

Step 7 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Check whether the logs of the node where the abnormal FlinkServer instance locates contains error information.

Step 8 Log in to the server where the abnormal FlinkServer instance locates as user **root**.

Step 9 Open the log file in the default directory **/var/log/Bigdata/flink/flinkserver/prestart.log** and check whether there is error message **Float ip** *x.x.x.x* **is invalid**.

- If yes, go to **Step 10**.
- If no, go to **Step 12**.

Step 10 On FusionInsight Manager, choose **Cluster** > **Services** > **Flink** > **Configurations** > **All Configurations** and search for **flink.ha.floatip**. Change the parameter value to the correct floating IP address, save the configuration, and restart the Flink service.

NOTE

- Contact the network engineer to obtain the new floating IP address.
- During service restart, FlinkServer cannot provide services, but submitted jobs are not affected.
- During restart, the FlinkServer instance cannot provide services, but submitted jobs are not affected.

Step 11 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 12**.

Collect fault information.

Step 12 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 13 Select the Flink service in the required cluster for **Service**.

Step 14 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the hosts to which the role belongs, and click **OK**.

Step 15 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 16 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.443 ALM-45641 Data Synchronization Exception Between the Active and Standby FlinkServer Nodes

Alarm Description

The system checks data synchronization between the active and standby FlinkServer nodes every 60 seconds. This alarm is generated when the standby FlinkServer node fails to synchronize files with the active FlinkServer node.

This alarm is cleared when the standby FlinkServer synchronizes files with the active FlinkServer.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45641	Major	Quality of service	Tenant plane	Flink	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

After an active/standby switchover, some configurations may be lost. Some jobs and connections of the FlinkServer are interrupted, but the FlinkServer can still provide services properly.

Possible Causes

- The link between the active and standby FlinkServer nodes is interrupted.
- The synchronization file does not exist or the file permission is required.

Handling Procedure

Check whether the network between the active and standby FlinkServer is in normal state.

Step 1 On FusionInsight Manager, choose **Cluster** > **Services** > **ClickHouse** > **Instance**. View and record the IP addresses of active and standby FlinkServer.

Step 2 Log in to the active FlinkServer node as user **root**.

Step 3 Run the following command to check whether the standby FlinkServer is reachable:

ping *IP address of the standby FlinkServer*

- If yes, go to **Step 6**.
- If no, go to **Step 4**.

Step 4 Contact the network administrator to check whether the network is faulty.

- If yes, go to **Step 5**.
- If no, go to **Step 6**.

Step 5 Rectify the network fault and check whether the alarm is cleared from the alarm list.

- If yes, no further action is required.
- If no, go to **Step 6**.

Check whether the storage space of the /srv/BigData/LocalBackup directory is full.

Step 6 Run the following command to check whether the storage space of the **/srv/BigData/LocalBackup** directory is full:

df -hl /srv/BigData/LocalBackup

- If yes, go to **Step 7**.
- If no, go to **Step 10**.

Step 7 Run the following command to clear unnecessary backup files:

rm -rf *Directory to be cleared*

The following are two examples:

rm -rf /srv/BigData/LocalBackup/0/default-oms_20191211143443

Step 8 On FusionInsight Manager, choose **O&M** > **Backup and Restoration** > **Backup Management**.

In the **Operation** column of the backup task, click **Configure** and change the value of **Maximum Number of Backup Copies** to reduce the number of backup file sets.

Step 9 Wait for 1 minute and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 10**.

Check whether the synchronization file exists and whether the file permission is valid.

Step 10 Run the following command to check whether the synchronization file exists:

find /srv/BigData/ -name "sed*"

find /opt -name "sed*"

- If yes, go to **Step 11**.
- If no, go to **Step 12**.

Step 11 Run the following command to check the synchronization file information and permission queried in **Step 10**:

ll *Path of the file you want to search for*

- If the file size is 0 and all values in the permission column are -, the file is a junk file. Run the following command to delete it:

  rm -rf *Files to be deleted*

  Wait for several minutes and check whether the alarm is cleared. If the alarm persists, go to **Step 12**.
- If the file size is not 0, go to **Step 12**.

Step 12 View the log file generated when the alarm is reported.

1. Run the following command to go to the HA run log file path of the current cluster:

   cd /var/log/Bigdata/flink/flinkserver/ha/runlog
2. Decompress log file and view the logs generated when the alarm is reported.

   For example, if the name of the file is **ha.log.2021-03-22_12-00-07.gz**, run the following command:

   gunzip *ha.log.2021-03-22_12-00-07.gz*

   vi *ha.log.2021-03-22_12-00-07*

   Check whether error information is displayed before and after the alarm generation time in the logs.

   – If it is displayed, rectify the fault based on the error information. Go to **Step 13**.

     For example, if the following error information is displayed, the directory permission is required. In this case, obtain the directory permission that is the same as the permission on a normal node.

```
[2021-03-22 14:03:35,339][10195489349][0][  INFO][add task((null)) to list successful.][HA][sync_module.c:__SYNC_ActiveTask,1151][ha.bin,26572,35]
[2021-03-22 14:03:35,339][10195489349][0][  INFO][Start Task All_Sync][HA][sync_core_inf.c:SYNC_StartTask,183][ha.bin,26572,35]
[2021-03-22 14:03:35,339][10195489349][0][NOTICE][send sync task(alltask) to component successful][HA][sync_module.c:__SYNC_SendSyncTask,832][ha.bin,26572,35
[2021-03-22 14:03:35,344][10195489353][0][  INFO][open lstat failed:(/opt/Bigdata/apache-tomcat-7.0.78/conf/security/tomcat_om.crt ). Permission denied.][HA]
gt.c:__Create_TravelFname_Open,482][ha.bin,26572,41]
[2021-03-22 14:03:35,344][10195489353][0][ ERROR][Travel stack failed.][HA][sync_filemgt.c:__Create_TravelFname,613][ha.bin,26572,41]
[2021-03-22 14:03:35,344][10195489353][0][ ERROR][mgtcreatelistfail][HA][sync_filemgt.c:__SYNC_CreateFileList,855][ha.bin,26572,41]
[2021-03-22 14:03:35,344][10195489353][0][ ERROR][CreateFileList failed][HA][sync_core.c:__SYNC_Task_SendEnd,1866][ha.bin,26572,41]
[2021-03-22 14:03:35,344][10195489353][0][ ERROR][[41][SendEnd][Task]Failed][HA][sync_core.c:__SYNC_DbgMsgErr,202][ha.bin,26572,41]
[2021-03-22 14:03:35,344][10195489353][0][ ERROR][TaskEnd Failed][HA][sync_core.c:__SYNC_Err_TaskEnd,2728][ha.bin,26572,41]
[2021-03-22 14:03:35,344][10195489353][0][NOTICE][hasendalarm_info: id=1,category=0,cause=0,locainfo=(),addinfo=(),lochost=(node-master1qnFC),locha=(192-168-
```

– If no, go to **Step 14**.

Step 13 Wait for about 10 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 14**.

Collect fault information.

Step 14 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 15 Select FlinkServer information from **Services** and click **OK**.

Step 16 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the hosts to which the role belongs, and click **OK**.

Step 17 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 18 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.444 ALM-45642 RocksDB Continuously Triggers Write Traffic Limiting

Alarm Description

The system checks the RocksDB monitoring data of jobs at the user-specified alarm reporting interval (**metrics.reporter.alarm.job.alarm.rocksdb.metrics.duration**, 180s by default). This alarm is generated when RocksDB for a job continuously triggers write traffic limiting, that is, the RocksDB write rate is not 0. This alarm is cleared when the RocksDB write rate of the job becomes 0.

The **rocksdb.actual-delayed-write-rate** parameter specifies the RocksDB write rate of a job. Value **0** indicates that the rate is not limited, and other values indicate traffic limiting.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45642	Minor	Quality of service	Tenant plane	Flink	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	ApplicationName	Specifies the name of the application for which the alarm was generated.
	JobName	Specifies the job for which the alarm was generated.
	UserName	Specifies the username for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

The checkpoint performance of Flink jobs is affected. There is no impact on the FlinkServer.

Possible Causes

When the rate at which Flink jobs write data to RocksDB is not 0, write traffic limiting is triggered. The possible causes are as follows:

- There are too many MemTables. As a result, write traffic is limited or write stops, and **ALM-45643 MemTable Size of RocksDB Continuously Exceeds the Threshold** is generated.
- The size of SST files at level 0 is too large, and **ALM-45644 Number of SST Files at Level 0 of RocksDB Continuously Exceeds the Threshold** is generated.
- The estimated compaction size exceeds the threshold, and **ALM-45647 Estimated Pending Compaction Size of RocksDB Continuously Exceeds the Threshold** is generated.

Handling Procedure

Check whether write traffic limiting or write stop is caused due to too many MemTables.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**.

Step 2 In the alarm list, check whether **ALM-45643 MemTable Size of RocksDB Continuously Exceeds the Threshold** exists.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 Handle the alarm by following the instructions provided in section **ALM-45643 MemTable Size of RocksDB Continuously Exceeds the Threshold**.

Step 4 After ALM-45643 is cleared, wait a few minutes and check whether this alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check whether write traffic limiting or write stop is caused due to too many SST files at level 0.

Step 5 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**.

Step 6 In the alarm list, check whether **ALM-45644 Number of SST Files at Level 0 of RocksDB Continuously Exceeds the Threshold** exists.

- If yes, go to **Step 7**.
- If no, go to **Step 9**.

Step 7 Handle the alarm by following the instructions provided in section **ALM-45644 Number of SST Files at Level 0 of RocksDB Continuously Exceeds the Threshold**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 8 After ALM-45644 is cleared, wait a few minutes and check whether this alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Check whether write traffic limiting or write stop is caused because the estimated compaction size exceeds the threshold.

Step 9 In the alarm list, check whether **ALM-45647 Estimated Pending Compaction Size of RocksDB Continuously Exceeds the Threshold** exists.

- If yes, go to **Step 10**.
- If no, go to **Step 12**.

Step 10 Handle the alarm by following the instructions provided in section **ALM-45647 Estimated Pending Compaction Size of RocksDB Continuously Exceeds the Threshold**.

Step 11 After ALM-45647 is cleared, wait a few minutes and check whether this alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 12**.

Collect fault information.

Step 12 Log in to FusionInsight Manager as a user who has the FlinkServer management permission.

Step 13 Choose **O&M** > **Alarm** > **Alarms** > **ALM-45642 RocksDB Continuously Triggers Write Traffic Limiting**, view **Location**, and obtain the name of the task for which the alarm is generated.

Step 14 Choose **Cluster** > **Services** > **Yarn** and click the link next to **ResourceManager WebUI** to go to the native Yarn page.

Step 15 Locate the abnormal task based on its name displayed in **Location**, search for and record the application ID of the job, and check whether the job logs are available on the native Yarn page.

Figure 1-39 Application ID of a job

- If yes, go to **Step 16**.
- If no, go to **Step 18**.

Step 16 Click the application ID of the failed job to go to the job page.

1. Click **Logs** in the **Logs** column to view JobManager logs.

Figure 1-40 Clicking Logs

2. Click the ID in the **Attempt ID** column and click **Logs** in the **Logs** column to view and save TaskManager logs.

Figure 1-41 Clicking the ID in the Attempt ID column

Figure 1-42 Clicking Logs

NOTE

You can also log in to Manager as a user who has the FlinkServer management permission. Choose **Cluster** > **Services** > **Flink**, and click the link next to **Flink WebUI**. On the displayed Flink web UI, click **Job Management**, click **More** in the **Operation** column, and select **Job Monitoring** to view TaskManager logs.

Step 17 View the job logs to rectify the fault, or contact the technical support and send the collected fault logs. No further action is required.

If logs are unavailable on the Yarn page, download logs from HDFS.

Step 18 On Manager, choose **Cluster** > **Services** > **HDFS**, click the link next to **NameNode WebUI** to go to the HDFS page, choose **Utilities** > **Browse the file system**, and download logs in the **/tmp/logs/***Username***/bucket-logs-tfile/***Last four digits of the task application ID/Application ID of the task* directory.

Step 19 View the logs of the failed job to rectify the fault, or contact the technical support and send the collected fault logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.445 ALM-45643 MemTable Size of RocksDB Continuously Exceeds the Threshold

Alarm Description

The system checks the RocksDB monitoring data of jobs at the user-specified alarm reporting interval (**metrics.reporter.alarm.job.alarm.rocksdb.metrics.duration**, 180s by default). This alarm is generated when the MemTable size of RocksDB for a job continuously exceeds the threshold (**metrics.reporter.alarm.job.alarm.rocksdb.get.micros.threshold**, 50000 microseconds by default). This alarm is cleared when the MemTable size of RocksDB for the job is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45643	Minor	Quality of service	Tenant plane	Flink	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ServiceName	Specifies the cluster service for which the alarm was generated.
	ApplicationName	Specifies the name of the application for which the alarm was generated.
	JobName	Specifies the job for which the alarm was generated.
	UserName	Specifies the username for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	ThreshHoldValue	Specifies the threshold value for triggering the alarm.
	CurrentValue	Specifies the value that triggered the alarm.

Impact on the System

The checkpoint performance of Flink jobs is affected. There is no impact on the FlinkServer.

Possible Causes

The write pressure of RocksDB is high.

Handling Procedure

Check TaskManager logs for the write pressure of RocksDB and collect logs.

Step 1 Log in to FusionInsight Manager as a user who has the FlinkServer management permission.

Step 2 Choose **O&M** > **Alarm** > **Alarms** > **ALM-45643 MemTable Size of RocksDB Continuously Exceeds the Threshold**, view **Location**, and obtain the name of the task for which the alarm is generated.

Step 3 Choose **Cluster** > **Services** > **Yarn** and click the link next to **ResourceManager WebUI** to go to the native Yarn page.

Step 4 Locate the abnormal task based on its name displayed in **Location**, search for and record the application ID of the job, and check whether the job logs are available on the Yarn page.

Figure 1-43 Application ID of a job

- If yes, go to **Step 5**.
- If no, go to **Step 6**.

Step 5 Click the application ID of the failed job to go to the job page.

1. Click **Logs** in the **Logs** column to view JobManager logs.

Figure 1-44 Clicking Logs

2. Click the ID in the **Attempt ID** column and click **Logs** in the **Logs** column to view and save TaskManager logs. Then go to **Step 7**.

Figure 1-45 Clicking the ID in the Attempt ID column

Figure 1-46 Clicking Logs

NOTE

You can also log in to Manager as a user who has the management permission for the current Flink job. Choose **Cluster** > **Services** > **Flink**, and click the link next to **Flink WebUI**. On the displayed Flink web UI, click **Job Management**, click **More** in the **Operation** column, and select **Job Monitoring** to view TaskManager logs.

If logs are unavailable on the Yarn page, download logs from HDFS.

Step 6 On Manager, choose **Cluster** > **Services** > **HDFS**, click the link next to **NameNode WebUI** to go to the HDFS page, choose **Utilities** > **Browse the file system**, and

download logs in the **/tmp/logs/***Username***/bucket-logs-tfile/***Last four digits of the task application ID/Application ID of the task* directory.

Check whether the write pressure of RocksDB is high.

Step 7 Check whether the value of **rocksdb.size-all-mem-tables** (unit: byte) in the TaskManager monitoring logs (keyword **RocksDBMetricPrint**) is greater than or equal to the total write buffer size (Total write buffer = **write_buffer_size** x **max_write_buffer_number**).

- If yes, adjust the values of the following custom parameters on the job development page of the Flink web UI, save the settings, and go to **Step 8**.

  Table 1-7 Custom parameters

Parameter	Default Value	Description
state.backend.rocksdb.writebuffer.count	– **2** – **4**: enables **SPINNING_DISK_OPTIMIZED_HIGH_MEM**.	– Number of buffers – **2** to **10** are recommended. Adjust the value based on service requirements.
state.backend.rocksdb.writebuffer.size	**64MB**	– Buffer size – **64MB** to **256MB** are recommended.
state.backend.rocksdb.thread.num	– **2** – **4**: enables **SPINNING_DISK_OPTIMIZED_HIGH_MEM**.	– Number of flush threads. Increase the number of threads to quickly flush memory data to disks. – When the number of threads is increased, the number of vCores also needs to be increased. – **2** to **10** are recommended.

- If no, go to **Step 9**.

Step 8 Restart the job and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Step 9 Contact technical support and send the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.446 ALM-45644 Number of SST Files at Level 0 of RocksDB Continuously Exceeds the Threshold

Alarm Description

The system checks the RocksDB monitoring data of jobs at the user-specified alarm reporting interval (**metrics.reporter.alarm.job.alarm.rocksdb.metrics.duration**, 180s by default). This alarm is generated when the number of SST files at level 0 of RocksDB for a job continuously exceeds the threshold (**state.backend.rocksdb.level0_slowdown_writes_trigger**, 20 by default). This alarm is cleared when the number of SST files at level 0 of RocksDB for the job is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45644	Minor	Quality of service	Tenant plane	Flink	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	ApplicationName	Specifies the name of the application for which the alarm was generated.
	JobName	Specifies the job for which the alarm was generated.
	UserName	Specifies the username for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	ThreshHoldValue	Specifies the threshold value for triggering the alarm.
	CurrentValue	Specifies the value that triggered the alarm.

Impact on the System

The checkpoint performance of Flink jobs is affected. There is no impact on the FlinkServer.

Possible Causes

Possible causes are as follows:

- The compaction pressure of RocksDB is too high, and **ALM-45646 Pending Compaction Size of RocksDB Continuously Exceeds the Threshold** and **ALM-45647 Estimated Pending Compaction Size of RocksDB Continuously Exceeds the Threshold** are generated.
- There are too many SST files at level 0.

Handling Procedure

Check whether the compaction pressure of RocksDB is too high and ALM-45646 is generated.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**.

Step 2 In the alarm list, check whether **ALM-45646 Pending Compaction Size of RocksDB Continuously Exceeds the Threshold** exists.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 Handle the alarm by following the instructions provided in section **ALM-45646 Pending Compaction Size of RocksDB Continuously Exceeds the Threshold**.

Step 4 After ALM-45646 is cleared, wait a few minutes and check whether this alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check whether the compaction pressure of RocksDB is too high and ALM-45647 is generated.

Step 5 In the alarm list, check whether **ALM-45647 Estimated Pending Compaction Size of RocksDB Continuously Exceeds the Threshold** exists.

- If yes, go to **Step 6**.
- If no, go to **Step 8**.

Step 6 Handle the alarm by following the instructions provided in section **ALM-45647 Estimated Pending Compaction Size of RocksDB Continuously Exceeds the Threshold**.

Step 7 After ALM-45647 is cleared, wait a few minutes and check whether this alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Check TaskManager logs for the number of SST files at level 0 and collect logs.

Step 8 Log in to FusionInsight Manager as a user who has the FlinkServer management permission.

Step 9 Choose **O&M** > **Alarm** > **Alarms** > **ALM-45644 Number of SST Files at Level 0 of RocksDB Continuously Exceeds the Threshold**, view **Location**, and obtain the name of the task for which the alarm is generated.

Step 10 Choose **Cluster** > **Services** > **Yarn** and click the link next to **ResourceManager WebUI** to go to the native Yarn page.

Step 11 Locate the abnormal task based on its name displayed in **Location**, search for and record the application ID of the job, and check whether the job logs are available on the Yarn page.

Figure 1-47 Application ID of a job

- If yes, go to **Step 12**.
- If no, go to **Step 13**.

Step 12 Click the application ID of the failed job to go to the job page.

1. Click **Logs** in the **Logs** column to view JobManager logs.

Figure 1-48 Clicking Logs

2. Click the ID in the **Attempt ID** column and click **Logs** in the **Logs** column to view and save TaskManager logs. Then go to **Step 14**.

Figure 1-49 Clicking the ID in the Attempt ID column

Figure 1-50 Clicking Logs

NOTE

You can also log in to Manager as a user who has the management permission for the current Flink job. Choose **Cluster** > **Services** > **Flink**, and click the link next to **Flink WebUI**. On the displayed Flink web UI, click **Job Management**, click **More** in the **Operation** column, and select **Job Monitoring** to view TaskManager logs.

If logs are unavailable on the Yarn page, download logs from HDFS.

Step 13 On Manager, choose **Cluster** > **Services** > **HDFS**, click the link next to **NameNode WebUI** to go to the HDFS page, choose **Utilities** > **Browse the file system**, and download logs in the **/tmp/logs/***Username***/bucket-logs-tfile/***Last four digits of the task application ID/Application ID of the task* directory.

Check whether the number of SST files at level 0 is too large.

Step 14 Check whether the value of **rocksdb.num-files-at-level0** in TaskManager monitoring logs (keyword **RocksDBMetricPrint**) is greater than or equal to the value of **state.backend.rocksdb.level0_slowdown_writes_trigger** or **state.backend.rocksdb.level0_stop_writes_trigger**.

- If yes, adjust the values of the following custom parameters on the job development page of the Flink web UI, save the settings, and go to **Step 15**.

Table 1-8 Custom parameters

Parameter	Default Value	Description
state.backend.rocksdb.level0_slowdown_writes_trigger	20	– Number of files that trigger slowdown at level 0 – **20** to **30** are recommended.
state.backend.rocksdb.level0_stop_writes_trigger	36	– Maximum number of files that trigger stop at level 0 – **36** to **46** are recommended.

- If no, go to **Step 16**.

Step 15 Restart the job and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 16**.

Step 16 Contact technical support and send the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.447 ALM-45645 Pending Flush Size of RocksDB Continuously Exceeds the Threshold

Alarm Description

The system checks the RocksDB monitoring data of jobs at the user-specified alarm reporting interval (**metrics.reporter.alarm.job.alarm.rocksdb.metrics.duration**, 180s by default). This alarm is generated when the number of pending flush requests of RocksDB for a job continuously reaches *n* times the number of flush/compaction threads. This alarm is cleared when the number of pending flush requests of RocksDB for the job is less than or equal to the threshold.

- The number of flush/compaction threads is the value of **state.backend.rocksdb.thread.num**. The default value is **2**. If **SPINNING_DISK_OPTIMIZED_HIGH_MEM** is enabled, the default value is **4**.
- The **metrics.reporter.alarm.job.alarm.rocksdb.background.jobs.multiplier** parameter specifies *n* times the number of flush/compaction threads. The default value is **2**.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45645	Minor	Quality of service	Tenant plane	Flink	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	ApplicationName	Specifies the name of the application for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	JobName	Specifies the job for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ThreshHoldValue	Specifies the threshold value for triggering the alarm.
	CurrentValue	Specifies the value that triggered the alarm.

Impact on the System

The checkpoint performance of Flink jobs is affected. There is no impact on the FlinkServer.

Possible Causes

The number of pending flush requests of RocksDB for the Flink job is too large.

Handling Procedure

Check TaskManager logs for the number of pending flush requests and collect logs.

Step 1 Log in to FusionInsight Manager as a user who has the FlinkServer management permission.

Step 2 Choose **O&M** > **Alarm** > **Alarms** > **ALM-45645 Pending Flush Size of RocksDB Continuously Exceeds the Threshold**, view **Location**, and obtain the name of the task for which the alarm is generated.

Step 3 Choose **Cluster** > **Services** > **Yarn** and click the link next to **ResourceManager WebUI** to go to the native Yarn page.

Step 4 Locate the abnormal task based on its name displayed in **Location**, search for and record the application ID of the job, and check whether the job logs are available on the Yarn page.

Figure 1-51 Application ID of a job

- If yes, go to **Step 5**.
- If no, go to **Step 6**.

Step 5 Click the application ID of the failed job to go to the job page.

1. Click **Logs** in the **Logs** column to view JobManager logs.

Figure 1-52 Clicking Logs

2. Click the ID in the **Attempt ID** column and click **Logs** in the **Logs** column to view and save TaskManager logs. Then go to **Step 7**.

Figure 1-53 Clicking the ID in the Attempt ID column

Figure 1-54 Clicking Logs

NOTE

You can also log in to Manager as a user who has the management permission for the current Flink job. Choose **Cluster** > **Services** > **Flink**, and click the link next to **Flink WebUI**. On the displayed Flink web UI, click **Job Management**, click **More** in the **Operation** column, and select **Job Monitoring** to view TaskManager logs.

If logs are unavailable on the Yarn page, download logs from HDFS.

Step 6 On Manager, choose **Cluster** > **Services** > **HDFS**, click the link next to **NameNode WebUI** to go to the HDFS page, choose **Utilities** > **Browse the file system**, and download logs in the **/tmp/logs/***Username***/bucket-logs-tfile/***Last four digits of the task application ID/Application ID of the task* directory.

Check whether there are too many pending flush requests.

Step 7 Check whether the sum of the values of **rocksdb.mem-table-flush-pending** and **rocksdb.compaction-pending** in TaskManager monitoring logs (keyword **RocksDBMetricPrint**) is greater than *n* times the number of RocksDB threads (**metrics.reporter.alarm.job.alarm.rocksdb.background.jobs.multiplier**, 2 by default). If it is, you can increase the number of RocksDB threads.

- If yes, adjust the values of the following custom parameters on the job development page of the Flink web UI, save the settings, and go to **Step 8**.

Table 1-9 Custom parameters

Parameter	Default Value	Description
state.backend.rocksdb.thread.num	– **2** – **4**: enables **SPINNING_DISK_OPTIMIZED_HIGH_MEM**.	– Number of flush threads. Increase the number of threads to quickly flush memory data to disks. – When the number of threads is increased, the number of vCores also needs to be increased. – **2** to **10** are recommended.

- If no, go to **Step 9**.

Step 8 Restart the job and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Step 9 Contact technical support and send the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.448 ALM-45646 Pending Compaction Size of RocksDB Continuously Exceeds the Threshold

Alarm Description

The system checks the RocksDB monitoring data of jobs at the user-specified alarm reporting interval (**metrics.reporter.alarm.job.alarm.rocksdb.metrics.duration**, 180s by default). This alarm is generated when the number of pending compaction requests of RocksDB for a job continuously reaches *n* times the number of flush/compaction threads. This alarm is cleared when the number of pending compaction requests of RocksDB for the job is less than or equal to the threshold.

- The number of flush/compaction threads is the value of **state.backend.rocksdb.thread.num**. The default value is **2**. If **SPINNING_DISK_OPTIMIZED_HIGH_MEM** is enabled, the default value is **4**.
- The **metrics.reporter.alarm.job.alarm.rocksdb.background.jobs.multiplier** parameter specifies *n* times the number of flush/compaction threads. The default value is **2**.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45646	Minor	Quality of service	Tenant plane	Flink	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	ApplicationName	Specifies the name of the application for which the alarm was generated.
	JobName	Specifies the job for which the alarm was generated.
	UserName	Specifies the username for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ThreshHoldValue	Specifies the threshold value for triggering the alarm.
	CurrentValue	Specifies the value that triggered the alarm.

Impact on the System

The checkpoint performance of Flink jobs is affected. There is no impact on the FlinkServer.

Possible Causes

The number of pending compaction requests of RocksDB for the Flink job is too large.

Handling Procedure

Check TaskManager logs for the number of pending compaction requests and collect logs.

Step 1 Log in to FusionInsight Manager as a user who has the FlinkServer management permission.

Step 2 Choose **O&M** > **Alarm** > **Alarms** > **ALM-45646 Pending Compaction Size of RocksDB Continuously Exceeds the Threshold**, view **Location**, and obtain the name of the task for which the alarm is generated.

Step 3 Choose **Cluster** > **Services** > **Yarn** and click the link next to **ResourceManager WebUI** to go to the native Yarn page.

Step 4 Locate the abnormal task based on its name displayed in **Location**, search for and record the application ID of the job, and check whether the job logs are available on the Yarn page.

Figure 1-55 Application ID of a job

- If yes, go to **Step 5**.
- If no, go to **Step 6**.

Step 5 Click the application ID of the failed job to go to the job page.

1. Click **Logs** in the **Logs** column to view JobManager logs.

Figure 1-56 Clicking Logs

2. Click the ID in the **Attempt ID** column and click **Logs** in the **Logs** column to view and save TaskManager logs. Then go to **Step 7**.

Figure 1-57 Clicking the ID in the Attempt ID column

Figure 1-58 Clicking Logs

NOTE

You can also log in to Manager as a user who has the management permission for the current Flink job. Choose **Cluster** > **Services** > **Flink**, and click the link next to **Flink WebUI**. On the displayed Flink web UI, click **Job Management**, click **More** in the **Operation** column, and select **Job Monitoring** to view TaskManager logs.

If logs are unavailable on the Yarn page, download logs from HDFS.

Step 6 On Manager, choose **Cluster** > **Services** > **HDFS**, click the link next to **NameNode WebUI** to go to the HDFS page, choose **Utilities** > **Browse the file system**, and download logs in the **/tmp/logs/***Username***/bucket-logs-tfile/***Last four digits of the task application ID/Application ID of the task* directory.

Check whether there are too many pending compaction requests.

Step 7 Check whether the sum of the values of **rocksdb.mem-table-flush-pending** and **rocksdb.compaction-pending** in TaskManager monitoring logs (keyword **RocksDBMetricPrint**) is greater than **n** times the number of RocksDB threads (**metrics.reporter.alarm.job.alarm.rocksdb.background.jobs.multiplier**, 2 by default). If it is, you can increase the number of RocksDB threads.

- If yes, adjust the values of the following custom parameters on the job development page of the Flink web UI, save the settings, and go to **Step 8**.

Table 1-10 Custom parameters

Parameter	Default Value	Description
state.backend.rocksdb.thread.num	– **2** – **4**: enables **SPINNING_DISK_OPTIMIZED_HIGH_MEM**.	– Number of flush threads. Increase the number of threads to quickly flush memory data to disks. – When the number of threads is increased, the number of vCores also needs to be increased. – **2** to **10** are recommended.

- If no, go to **Step 9**.

Step 8 Restart the job and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.449 ALM-45647 Estimated Pending Compaction Size of RocksDB Continuously Exceeds the Threshold

Alarm Description

The system checks the RocksDB monitoring data of jobs at the user-specified alarm reporting interval (**metrics.reporter.alarm.job.alarm.rocksdb.metrics.duration**, 180s by default). This alarm is generated when the estimated pending compaction size of RocksDB for a job continuously exceeds the threshold. This alarm is cleared when the estimated pending compaction size of RocksDB for the job is less than or equal to the threshold.

The threshold of the estimated pending compaction size is the smaller value of the following two parameters:

- **state.backend.rocksdb.soft-pending-compaction-bytes-limit**. The default value is **64GB**.
- **state.backend.rocksdb.hard-pending-compaction-bytes-limit**. The default value is **256GB**.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45647	Minor	Quality of service	Tenant plane	Flink	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	ApplicationName	Specifies the name of the application for which the alarm was generated.
	JobName	Specifies the job for which the alarm was generated.
	UserName	Specifies the username for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ThreshHoldValue	Specifies the threshold value for triggering the alarm.
	CurrentValue	Specifies the value that triggered the alarm.

Impact on the System

The checkpoint performance of Flink jobs is affected. There is no impact on the FlinkServer.

Possible Causes

The estimated compaction data size of RocksDB is too large.

Handling Procedure

Check TaskManager logs for the estimated compaction data size and collect logs.

Step 1 Log in to FusionInsight Manager as a user who has the FlinkServer management permission.

Step 2 Choose **O&M** > **Alarm** > **Alarms** > **ALM-45647 Estimated Pending Compaction Size of RocksDB Continuously Exceeds the Threshold**, view **Location**, and obtain the name of the task for which the alarm is generated.

Step 3 Choose **Cluster** > **Services** > **Yarn** and click the link next to **ResourceManager WebUI** to go to the native Yarn page.

Step 4 Locate the abnormal task based on its name displayed in **Location**, search for and record the application ID of the job, and check whether the job logs are available on the Yarn page.

Figure 1-59 Application ID of a job

- If yes, go to **Step 5**.
- If no, go to **Step 6**.

Step 5 Click the application ID of the failed job to go to the job page.

1. Click **Logs** in the **Logs** column to view JobManager logs.

Figure 1-60 Clicking Logs

2. Click the ID in the **Attempt ID** column and click **Logs** in the **Logs** column to view and save TaskManager logs. Then go to **Step 7**.

Figure 1-61 Clicking the ID in the Attempt ID column

Figure 1-62 Clicking Logs

NOTE

You can also log in to Manager as a user who has the management permission for the current Flink job. Choose **Cluster** > **Services** > **Flink**, and click the link next to **Flink WebUI**. On the displayed Flink web UI, click **Job Management**, click **More** in the **Operation** column, and select **Job Monitoring** to view TaskManager logs.

If logs are unavailable on the Yarn page, download logs from HDFS.

Step 6 On Manager, choose **Cluster** > **Services** > **HDFS**, click the link next to **NameNode WebUI** to go to the HDFS page, choose **Utilities** > **Browse the file system**, and download logs in the **/tmp/logs/***Username***/bucket-logs-tfile/***Last four digits of the task application ID/Application ID of the task* directory.

Check whether the estimated compaction data size of RocksDB is too large.

Step 7 Check whether the value of **rocksdb.estimate-pending-compaction-bytes** (unit: byte) in TaskManager monitoring logs (keyword **RocksDBMetricPrint**) is greater than or equal to the **soft/hard-pending-compaction** size (values of **state.backend.rocksdb.soft-pending-compaction-bytes-limit** and **state.backend.rocksdb.hard-pending-compaction-bytes-limit**).

- If yes, adjust the values of the following custom parameters on the job development page of the Flink web UI, save the settings, and go to **Step 8**.

Table 1-11 Custom parameters

Parameter	Default Value	Description
state.backend.rocksdb.soft-pending-compaction-bytes-limit	64GB	– When the pending compaction size exceeds the threshold, the write traffic is limited. – **64GB** to **512GB** are recommended.
state.backend.rocksdb.hard-pending-compaction-bytes-limit	256GB	– When the pending compaction size exceeds the threshold, write operations are stopped. – **64GB** to **512GB** are recommended.

- If no, go to **Step 9**.

Step 8 Restart the job and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Step 9 Contact technical support and send the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.450 ALM-45648 RocksDB Frequently Encounters Write-Stopped

Alarm Description

The system checks the RocksDB monitoring data of jobs at the user-specified alarm reporting interval (**metrics.reporter.alarm.job.alarm.rocksdb.metrics.duration**, 180s by default). This alarm is generated when RocksDB for a job continuously encounters the **is-write-stopped** state. This alarm is cleared when RocksDB for the job no longer or does not continuously encounter the **is-write-stopped** state within an alarm reporting interval.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45648	Minor	Quality of service	Tenant plane	Flink	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	ApplicationName	Specifies the name of the application for which the alarm was generated.
	JobName	Specifies the job for which the alarm was generated.
	UserName	Specifies the username for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

The checkpoint performance of Flink jobs is affected. There is no impact on the FlinkServer.

Possible Causes

The possible causes are as follows:

- There are too many MemTables and **ALM-45643 MemTable Size of RocksDB Continuously Exceeds the Threshold** is generated.
- There are too many SST files at level 0, and **ALM-45644 Number of SST Files at Level 0 of RocksDB Continuously Exceeds the Threshold** is generated.
- The estimated compaction size exceeds the threshold, and **ALM-45647 Estimated Pending Compaction Size of RocksDB Continuously Exceeds the Threshold** is generated.

Handling Procedure

Check whether there are too many MemTables.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**.

Step 2 In the alarm list, check whether **ALM-45643 MemTable Size of RocksDB Continuously Exceeds the Threshold** exists.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 Handle the alarm by following the instructions provided in section **ALM-45643 MemTable Size of RocksDB Continuously Exceeds the Threshold**.

Step 4 After ALM-45643 is cleared, wait a few minutes and check whether this alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check whether the number of SST files at level 0 is too large.

Step 5 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**.

Step 6 In the alarm list, check whether **ALM-45644 Number of SST Files at Level 0 of RocksDB Continuously Exceeds the Threshold** exists.

- If yes, go to **Step 7**.
- If no, go to **Step 9**.

Step 7 Handle the alarm by following the instructions provided in section **ALM-45644 Number of SST Files at Level 0 of RocksDB Continuously Exceeds the Threshold**.

Step 8 After ALM-45644 is cleared, wait a few minutes and check whether this alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Check whether the estimated compaction size exceeds the threshold.

Step 9 In the alarm list, check whether **ALM-45647 Estimated Pending Compaction Size of RocksDB Continuously Exceeds the Threshold** exists.

- If yes, go to **Step 10**.
- If no, go to **Step 12**.

Step 10 Handle the alarm by following the instructions provided in section **ALM-45647 Estimated Pending Compaction Size of RocksDB Continuously Exceeds the Threshold**.

Step 11 After ALM-45647 is cleared, wait a few minutes and check whether this alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 12**.

Collect fault information.

Step 12 Log in to Manager as a user who has the management permission for the current Flink job.

Step 13 Choose **O&M** > **Alarm** > **Alarms** > **ALM-45648 RocksDB Frequently Encounters Write-Stopped**, view **Location**, and obtain the name of the task for which the alarm is generated.

Step 14 Choose **Cluster** > **Services** > **Yarn** and click the link next to **ResourceManager WebUI** to go to the native Yarn page.

Step 15 Locate the abnormal task based on its name displayed in **Location**, search for and record the application ID of the job, and check whether the job logs are available on the Yarn page.

Figure 1-63 Application ID of a job

- If yes, go to **Step 16**.
- If no, go to **Step 18**.

Step 16 Click the application ID of the failed job to go to the job page.

1. Click **Logs** in the **Logs** column to view JobManager logs.

Figure 1-64 Clicking Logs

2. Click the ID in the **Attempt ID** column and click **Logs** in the **Logs** column to view and save TaskManager logs.

Figure 1-65 Clicking the ID in the Attempt ID column

Figure 1-66 Clicking Logs

NOTE

You can also log in to Manager as a user who has the management permission for the current Flink job. Choose **Cluster** > **Services** > **Flink**, and click the link next to **Flink WebUI**. On the displayed Flink web UI, click **Job Management**, click **More** in the **Operation** column, and select **Job Monitoring** to view TaskManager logs.

Step 17 View the job logs to rectify the fault, or contact the technical support and send the collected fault logs. No further action is required.

If logs are unavailable on the Yarn page, download logs from HDFS.

Step 18 On Manager, choose **Cluster** > **Services** > **HDFS**, click the link next to **NameNode WebUI** to go to the HDFS page, choose **Utilities** > **Browse the file system**, and download logs in the **/tmp/logs/***Username***/bucket-logs-tfile/***Last four digits of the task application ID/Application ID of the task* directory.

Step 19 View the logs of the failed job to rectify the fault, or contact the technical support and send the collected fault logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.451 ALM-45649 P95 Latency of RocksDB Get Requests Continuously Exceeds the Threshold

Alarm Description

The system checks the RocksDB monitoring data of jobs at the user-specified alarm reporting interval

(**metrics.reporter.alarm.job.alarm.rocksdb.metrics.duration**, 180s by default). This alarm is generated when the P95 latency of RocksDB Get requests exceeds the threshold (**metrics.reporter.alarm.job.alarm.rocksdb.get.micros.threshold**, 50000 microseconds by default). This alarm is cleared when the P95 latency of RocksDB Get requests is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45649	Minor	Quality of service	Tenant plane	Flink	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	ApplicationName	Specifies the name of the application for which the alarm was generated.
	JobName	Specifies the job for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	UserName	Specifies the username for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	ThreshHoldValue	Specifies the threshold value for triggering the alarm.
	CurrentValue	Specifies the value that triggered the alarm.

Impact on the System

The checkpoint performance of Flink jobs is affected. There is no impact on the FlinkServer.

Possible Causes

The possible causes are as follows:

- There are too many SST files at level 0, causing slow queries. In addition, **ALM-45644 Number of SST Files at Level 0 of RocksDB Continuously Exceeds the Threshold** is generated.
- The cache hit ratio is lower than 60%, causing frequent swap-ins and swap-outs of the block cache.

Handling Procedure

Check whether the number of SST files at level 0 is too large.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**.

Step 2 In the alarm list, check whether **ALM-45644 Number of SST Files at Level 0 of RocksDB Continuously Exceeds the Threshold** exists.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 Handle the alarm by following the instructions provided in section **ALM-45644 Number of SST Files at Level 0 of RocksDB Continuously Exceeds the Threshold**.

Step 4 After ALM-45644 is cleared, wait a few minutes and check whether this alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check the cache hit ratio in TaskManager logs and collect logs.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 5 Log in to FusionInsight Manager as a user who has the FlinkServer management permission.

Step 6 Choose **O&M** > **Alarm** > **Alarms** > **ALM-45649 P95 Latency of RocksDB Get Requests Continuously Exceeds the Threshold**, view **Location**, and obtain the name of the task for which the alarm is generated.

Step 7 Choose **Cluster** > **Services** > **Yarn** and click the link next to **ResourceManager WebUI** to go to the native Yarn page.

Step 8 Locate the abnormal task based on its name displayed in **Location**, search for and record the application ID of the job, and check whether the job logs are available on the Yarn page.

Figure 1-67 Application ID of a job

- If yes, go to **Step 9**.
- If no, go to **Step 10**.

Step 9 Click the application ID of the failed job to go to the job page.

1. Click **Logs** in the **Logs** column to view JobManager logs.

Figure 1-68 Clicking Logs

2. Click the ID in the **Attempt ID** column and click **Logs** in the **Logs** column to view and save TaskManager logs. Then go to **Step 11**.

Figure 1-69 Clicking the ID in the Attempt ID column

Figure 1-70 Clicking Logs

NOTE

You can also log in to Manager as a user who has the management permission for the current Flink job. Choose **Cluster** > **Services** > **Flink**, and click the link next to **Flink WebUI**. On the displayed Flink web UI, click **Job Management**, click **More** in the **Operation** column, and select **Job Monitoring** to view TaskManager logs.

If logs are unavailable on the Yarn page, download logs from HDFS.

Step 10 On Manager, choose **Cluster** > **Services** > **HDFS**, click the link next to **NameNode WebUI** to go to the HDFS page, choose **Utilities** > **Browse the file system**, and download logs in the **/tmp/logs/***Username***/bucket-logs-tfile/***Last four digits of the task application ID/Application ID of the task* directory.

Check whether the cache hit ratio is too low.

Step 11 Check the values of **rocksdb.block.cache.hit** (cache hit) and **rocksdb.block.cache.miss** (cache miss) in TaskManager monitoring logs (keyword **RocksDBMetricPrint**). Calculate the hit ratio using the following formula and check whether it is less than 60%:

rocksdb.block.cache.hit/(rocksdb.block.cache.hit+rocksdb.block.cache.miss)

- If yes, adjust the values of the following custom parameters on the job development page of the Flink web UI, save the settings, and go to **Step 12**.

Table 1-12 Custom parameters

Parameter	Default Value	Description
state.backend.rocksdb.block.cache-size	– **8MB** – **256MB**: enables **SPINNING_DISK_OPTIMIZED_HIGH_MEM**.	– Cache size – **8MB** to **1GB** are recommended.
state.backend.rocksdb.block.blocksize	– **4KB** – **128KB**: enables **SPINNING_DISK_OPTIMIZED_HIGH_MEM**.	– Block size – **4KB** to **256KB** are recommended.
state.backend.rocksdb.use-bloom-filter	**false**	– Whether to speed up indexing. If it is **true**, each new SST file will contain a Bloom filter. – **true** is recommended.

- If no, go to **Step 13**.

Step 12 Restart the job and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 13**.

Step 13 Contact technical support and send the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.452 ALM-45650 P95 Latency of RocksDB Write Requests Continuously Exceeds the Threshold

Alarm Description

The system checks the RocksDB monitoring data of jobs at the user-specified alarm reporting interval (**metrics.reporter.alarm.job.alarm.rocksdb.metrics.duration**, 180s by default). This alarm is generated when the P95 latency of RocksDB write requests exceeds the threshold (**metrics.reporter.alarm.job.alarm.rocksdb.write.micros.threshold**, 50000 microseconds by default). This alarm is cleared when the P95 latency of RocksDB write requests is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45650	Minor	Quality of service	Tenant plane	Flink	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	ApplicationName	Specifies the name of the application for which the alarm was generated.
	JobName	Specifies the job for which the alarm was generated.
	UserName	Specifies the username for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	ThreshHoldValue	Specifies the threshold value for triggering the alarm.
	CurrentValue	Specifies the value that triggered the alarm.

Impact on the System

The checkpoint performance of Flink jobs is affected. There is no impact on the FlinkServer.

Possible Causes

The possible causes are as follows:

- There are too many MemTables. As a result, write traffic is limited or write stops, and **ALM-45643 MemTable Size of RocksDB Continuously Exceeds the Threshold** is generated.
- There are too many SST files at level 0, and **ALM-45644 Number of SST Files at Level 0 of RocksDB Continuously Exceeds the Threshold** is generated.
- The estimated compaction size exceeds the threshold, and **ALM-45647 Estimated Pending Compaction Size of RocksDB Continuously Exceeds the Threshold** is generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Handling Procedure

Check whether write traffic limiting or write stop is caused due to too many MemTables.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**.

Step 2 In the alarm list, check whether **ALM-45643 MemTable Size of RocksDB Continuously Exceeds the Threshold** exists.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 Handle the alarm by following the instructions provided in section **ALM-45643 MemTable Size of RocksDB Continuously Exceeds the Threshold**.

Step 4 After ALM-45643 is cleared, wait a few minutes and check whether this alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check whether the number of SST files at level 0 is too large.

Step 5 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**.

Step 6 In the alarm list, check whether **ALM-45644 Number of SST Files at Level 0 of RocksDB Continuously Exceeds the Threshold** exists.

- If yes, go to **Step 7**.
- If no, go to **Step 9**.

Step 7 Handle the alarm by following the instructions provided in section **ALM-45644 Number of SST Files at Level 0 of RocksDB Continuously Exceeds the Threshold**.

Step 8 After ALM-45644 is cleared, wait a few minutes and check whether this alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Check whether the estimated compaction size exceeds the threshold.

Step 9 In the alarm list, check whether **ALM-45647 Estimated Pending Compaction Size of RocksDB Continuously Exceeds the Threshold** exists.

- If yes, go to **Step 10**.
- If no, go to **Step 12**.

Step 10 Handle the alarm by following the instructions provided in section **ALM-45647 Estimated Pending Compaction Size of RocksDB Continuously Exceeds the Threshold**.

Step 11 After ALM-45647 is cleared, wait a few minutes and check whether this alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 12**.

Collect fault information.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 12 Log in to FusionInsight Manager as a user who has the FlinkServer management permission.

Step 13 Choose **O&M** > **Alarm** > **Alarms** > **ALM-45650 P95 Latency of RocksDB Write Requests Continuously Exceeds the Threshold**, view **Location**, and obtain the name of the task for which the alarm is generated.

Step 14 Choose **Cluster** > **Services** > **Yarn** and click the link next to **ResourceManager WebUI** to go to the native Yarn page.

Step 15 Locate the abnormal task based on its name displayed in **Location**, search for and record the application ID of the job, and check whether the job logs are available on the Yarn page.

Figure 1-71 Application ID of a job

- If yes, go to **Step 16**.
- If no, go to **Step 18**.

Step 16 Click the application ID of the failed job to go to the job page.

1. Click **Logs** in the **Logs** column to view JobManager logs.

Figure 1-72 Clicking Logs

2. Click the ID in the **Attempt ID** column and click **Logs** in the **Logs** column to view and save TaskManager logs.

Figure 1-73 Clicking the ID in the Attempt ID column

Figure 1-74 Clicking Logs

NOTE

You can also log in to Manager as a user who has the FlinkServer management permission. Choose **Cluster** > **Services** > **Flink**, and click the link next to **Flink WebUI**. On the displayed Flink web UI, click **Job Management**, click **More** in the **Operation** column, and select **Job Monitoring** to view TaskManager logs.

Step 17 View the job logs to rectify the fault, or contact the technical support and send the collected fault logs. No further action is required.

If logs are unavailable on the Yarn page, download logs from HDFS.

Step 18 On Manager, choose **Cluster** > **Services** > **HDFS**, click the link next to **NameNode WebUI** to go to the HDFS page, choose **Utilities** > **Browse the file system**, and download logs in the **/tmp/logs/***Username***/bucket-logs-tfile/***Last four digits of the task application ID/Application ID of the task* directory.

Step 19 View the logs of the failed job to rectify the fault, or contact the technical support and send the collected fault logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.453 ALM-45652 Flink Service Unavailable

Alarm Description

The alarm module checks the Flink status every 60 seconds. This alarm is generated when the Flink service is unavailable. This alarm is cleared when the Flink service recovers.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45652	Critical	Environment	Tenant plane	Flink	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.

Type	Parameter	Description
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

Flink jobs cannot be submitted with FlinkServer and the Flink client.

Possible Causes

The ZooKeeper, HDFS, Yarn, KrbServer, or DBService service on which Flink depends is unavailable.

Handling Procedure

Check whether the ZooKeeper service on which Flink depends is abnormal.

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Alarms**.

Step 2 In the alarm list, check whether "ALM-13000 ZooKeeper Service Unavailable" exists.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 Handle the alarm by referring to "ALM-13000 ZooKeeper Service Unavailable."

Step 4 After the alarm is cleared, wait a few minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check whether the HDFS service on which Flink depends is abnormal.

Step 5 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**.

Step 6 In the alarm list, check whether "ALM-14000 HDFS Service Unavailable" exists.

- If yes, go to **Step 7**.
- If no, go to **Step 9**.

Step 7 Handle the alarm by referring to "ALM-14000 HDFS Service Unavailable."

Step 8 After the alarm is cleared, wait a few minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Check whether the Yarn service on which Flink depends is abnormal.

Step 9 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**.

Step 10 In the alarm list, check whether "ALM-18000 Yarn Service Unavailable" exists.

- If yes, go to **Step 11**.
- If no, go to **Step 13**.

Step 11 Handle the alarm by referring to "ALM-18000 Yarn Service Unavailable."

Step 12 After the alarm is cleared, wait a few minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 13**.

Check whether the KrbServer service on which Flink depends is abnormal.

Step 13 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**.

Step 14 In the alarm list, check whether "ALM-25500 KrbServer Service Unavailable" exists.

- If yes, go to **Step 15**.
- If no, go to **Step 17**.

Step 15 Handle the alarm by referring to "ALM-25500 KrbServer Service Unavailable."

Step 16 After the alarm is cleared, wait a few minutes and check whether the alarm is cleared.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If yes, no further action is required.
- If no, go to **Step 17**.

Check whether the DBService service on which Flink depends is abnormal.

Step 17 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**.

Step 18 In the alarm list, check whether "ALM-27001 DBService Service Unavailable" exists.

- If yes, go to **Step 19**.
- If no, go to **Step 21**.

Step 19 Handle the alarm by referring to "ALM-27001 DBService Service Unavailable."

Step 20 After the alarm is cleared, wait a few minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 21**.

Collect fault information.

Step 21 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 22 Expand the **Service** drop-down list, and select **Flink** for the target cluster.

Step 23 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time respectively. Then, click **Download**.

Step 24 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.454 ALM-45653 Invalid Flink HA Certificate File

Alarm Description

Flink checks whether the HA certificate file is valid (whether the certificate exists and whether its format is correct) in the first health check or at 01:00:00 every day. This alarm is generated when the certificate file is invalid. This alarm is automatically cleared when the certificate file becomes valid again.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45653	Major	Environment	Tenant plane	Flink	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

FlinkServer in active/standby mode cannot provide services for external systems, and Flink jobs cannot be submitted on the FlinkServer.

Possible Causes

The HA certificate file is invalid.

Handling Procedure

View alarm information.

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** > **ALM-45653 Invalid Flink HA Certificate File**, view **Location**, obtain the name of the host for which the alarm is generated, and click the host name to view its IP address.

Check whether the HA certificate file in the system is valid.

Step 2 Log in to the host for which the alarm is generated as user **omm**.

Step 3 Run the **cd ${BIGDATA_HOME}/FusionInsight_Flink_*/install/FusionInsight-Flink-*/ha/local/cert** command to go to the directory where the HA certificate is stored.

Step 4 Run the **ls -l** command to check whether the **server.crt** file exists.

- If yes, go to **Step 5**.
- If no, go to **Step 6**.

Step 5 Run the **openssl x509 -in server.crt -text -noout** command and check whether the command output is normal.

- If yes, go to **Step 9**.
- If no, go to **Step 6**.

Step 6 Run the **cd ${BIGDATA_HOME}/FusionInsight_Flink_*/install/FusionInsight-Flink-*/flink/sbin** command to go to the Flink script directory.

Step 7 Run the **sh proceed_ha_ssl_cert.sh** command to generate a new HA certificate. Then, check whether the alarm is cleared 1 minute later.

- If yes, go to **Step 8**.
- If no, go to **Step 9**.

Step 8 Check whether this alarm is generated again during periodic system check.

- If yes, go to **Step 9**.
- If no, no further action is required.

Collect fault information.

Step 9 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 10 Expand the **Service** drop-down list, and select **Flink** for the target cluster.

Step 11 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.455 ALM-45654 Flink HA Certificate Is About to Expire

Alarm Description

Flink checks whether the HA certificate file is about to expire in the first health check or at 01:00:00 every day. This alarm is generated when the remaining validity period is less than or equal to 30 days. This alarm is automatically cleared when the remaining validity period is greater than 30 days.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45654	Major	Environment	Tenant plane	Flink	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

If the certificate expires, the HA function of the FlinkServer in active/standby mode is affected. Flink jobs cannot be submitted on the FlinkServer. For FlinkServers in dual-active mode, the HA function is not affected.

Possible Causes

The HA certificate is about to expire.

Handling Procedure

View alarm information.

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** > **ALM-45654 Flink HA Certificate Is About to Expire**, view **Location**, obtain the name of the host for which the alarm is generated, and click the host name to view its IP address.

Check whether the HA certificate file in the system is valid. If it is not, generate a new one.

Step 2 Log in to the host for which the alarm is generated as user **omm**.

Step 3 Run the **cd ${BIGDATA_HOME}/FusionInsight_Flink_*/install/FusionInsight-Flink-*/ha/local/cert** command to go to the directory where the HA certificate is stored.

Step 4 Run the **openssl x509 -noout -text -in server.crt** command to query the effective time and due time of the HA certificate.

Step 5 Perform **Step 6** to **Step 7** during off-peak hours to update the certificate file as needed.

Step 6 Run the **cd ${BIGDATA_HOME}/FusionInsight_Flink_*/install/FusionInsight-Flink-*/flink/sbin** command to go to the Flink script directory.

Step 7 Run the **sh proceed_ha_ssl_cert.sh** command to generate a new HA certificate. Then, check whether the alarm is cleared 1 minute later.

- If yes, go to **Step 9**.
- If no, go to **Step 8**.

Step 8 On the node where the standby FlinkServer instance is located, repeat **Step 6** to **Step 7**. Then, check whether the alarm is cleared 1 minute later.

- If yes, go to **Step 9**.
- If no, go to **Step 10**.

Step 9 Check whether this alarm is generated again during periodic system check.

- If yes, go to **Step 10**.
- If no, no further action is required.

Collect fault information.

Step 10 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 11 Expand the **Service** drop-down list, and select **Flink** for the target cluster.

Step 12 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 13 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.456 ALM-45655 Flink HA Certificate File Has Expired

Alarm Description

Flink checks whether the HA certificate file has expired in the first health check or at 01:00:00 every day. This alarm is generated when the HA certificate has expired. This alarm is automatically cleared when the certificate file becomes valid again.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45655	Major	Overlimit	Tenant plane	Flink	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

FlinkServer in active/standby mode cannot provide services for external systems, and Flink jobs cannot be submitted on the FlinkServer.

Possible Causes

The HA certificate file has expired.

Handling Procedure

View alarm information.

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** > **ALM-45655 Flink HA Certificate File Has Expired**, view **Location**, obtain the name of the host for which the alarm is generated, and click the host name to view its IP address.

Check whether the HA certificate file in the system is valid. If it is not, generate a new one.

Step 2 Log in to the host for which the alarm is generated as user **omm**.

Step 3 Run the **cd ${BIGDATA_HOME}/FusionInsight_Flink_*/install/FusionInsight-Flink-*/ha/local/cert** command to go to the directory where the HA certificate is stored.

Step 4 Run the **openssl x509 -noout -text -in server.crt** command to query the effective time and due time of the HA certificate and check whether the HA certificate file is valid.

- If yes, go to **Step 9**.
- If no, go to **Step 5**.

Step 5 Run the **cd ${BIGDATA_HOME}/FusionInsight_Flink_*/install/FusionInsight-Flink-*/flink/sbin** command to go to the Flink script directory.

Step 6 Run the **sh proceed_ha_ssl_cert.sh** command to generate a new HA certificate. Then, check whether the alarm is cleared 1 minute later.

- If yes, go to **Step 8**.
- If no, go to **Step 7**.

Step 7 On the node where the standby FlinkServer instance is located, repeat **Step 5** to **Step 6**. Then, check whether the alarm is cleared 1 minute later.

- If yes, go to **Step 8**.
- If no, go to **Step 9**.

Step 8 Check whether this alarm is generated again during periodic system check.

- If yes, go to **Step 9**.
- If no, no further action is required.

Collect fault information.

Step 9 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 10 Expand the **Service** drop-down list, and select **Flink** for the target cluster.

Step 11 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.457 ALM-45736 Guardian Service Unavailable

Alarm Description

The alarm module checks the Guardian service status every 60 seconds. This alarm is generated if Guardian is unavailable.

This alarm is cleared after Guardian recovers.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45736	Critical	Error handling	Tenant plane	Guardian	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

Guardian cannot work properly, and OBS cannot be accessed.

Possible Causes

- The HDFS or Zookeeper service on which the Guardian service depends is abnormal.
- The TokenServer role instance is abnormal.

Handling Procedure

Check the HDFS service status.

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Alarms**. On the page that is displayed, check whether "ALM-14000 HDFS Service Unavailable" is reported.

- If yes, go to **Step 2**.
- If no, go to **Step 3**.

Step 2 Clear "ALM-14000 HDFS Service Unavailable" according to the alarm help.

After the alarm is cleared, wait a few minutes and check whether the alarm GuardianService Unavailable is cleared.

- If yes, no further action is required.

- If no, go to **Step 3**.

Check the Zookeeper status.

Step 3 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Alarms**. On the page that is displayed, check whether "ALM-13000 ZooKeeper Service Unavailable" is reported.

- If yes, go to **Step 4**.
- If no, go to **Step 5**.

Step 4 Clear "ALM-13000 ZooKeeper Service Unavailable" according to the alarm help.

After those alarms are cleared, wait a few minutes and check whether this alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check all TokenServer instances.

Step 5 Log in to the node where the TokenServer instance resides as user **omm** and run the **ps -ef|grep "guardian.token.server.Server"** command to check whether the TokenServer process exists on the node.

- If yes, go to **Step 7**.
- If no, restart the faulty TokenServer instance and go to **Step 6**.

Step 6 In the alarm list, check whether the alarm "Guardian Service Unavailable" is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect fault information.

Step 7 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 8 Expand the **Service** drop-down list, and select **Guardian** for the destination cluster.

Step 9 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.458 ALM-45737 Guardian TokenServer Heap Memory Usage Exceeds the Threshold

Alarm Description

The system checks the heap memory usage of the TokenServer service every 60 seconds. This alarm is generated when the heap memory usage of the TokenServer instance exceeds the threshold for 10 consecutive times.

This alarm is automatically cleared when the system detects that the heap memory usage is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45737	Critical (default threshold: 95%) Major (default threshold: 85%)	Quality of service	Tenant plane	Guardian	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

If the heap memory of the Guardian TokenServer instance overflows, OBS cannot be accessed.

Possible Causes

The heap memory of the TokenServer instance is overused or the heap memory is inappropriately allocated.

Handling Procedure

Check heap memory usage.

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Alarms** > **ALM-45737 TokenServer Heap Memory Usage Exceeds the Threshold**. Check the location information of the alarm and view the host name of the instance for which the alarm is generated.

Step 2 On FusionInsight Manager, choose **Cluster** > **Services** > **Guardian**. On the page that is displayed, click the **Instance** tab. On this tab page, select the role corresponding to the host name of the instance for which the alarm is generated. Click the drop-down list in the upper right corner of the chart area and choose **Customize** > **CPU and Memory** > **TokenServer Heap Memory Usage**. Then click **OK**.

Step 3 Check whether the heap memory used by TokenServer reaches the threshold (95% of the maximum heap memory by default).

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On FusionInsight Manager, choose **Cluster** > **Services** > **Guardian**. On the page that is displayed, click the **Instance** tab. On this tab page, choose **TokenServer** > **Instance Configuration**. Click **All Configurations**, and choose **TokenServer** > **System**. Set **-Xmx** in the **GC_OPTS** parameter to a larger value based on site requirements and save the configuration.

NOTE

If this alarm is generated, the heap memory configured for TokenServer cannot meet the heap memory required by the TokenServer process. You are advised to change the value of **-Xmx** in **GC_OPTS** to twice that of the heap memory used by TokenServer. You can change the value based on the actual service scenario. Refer to **Step 2** to view the TokenServer heap memory usage.

Step 5 Restart the affected services or instances and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **Guardian** for the destination cluster.

Step 8 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.459 ALM-45738 Guardian TokenServer Direct Memory Usage Exceeds the Threshold

Alarm Description

The system checks the direct memory usage of the TokenServer service every 60 seconds. This alarm is generated when the direct memory usage of the TokenServer instance exceeds the threshold for five consecutive times.

This alarm is automatically cleared when the system detects that the TokenServer direct memory usage is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45738	Critical (default threshold: 95%) Major (default threshold: 85%)	Quality of service	Tenant plane	Guardian	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

If the direct memory of the Guardian TokenServer instance overflows, OBS cannot be accessed.

Possible Causes

The direct memory of the TokenServer process is overused or the direct memory is inappropriately allocated.

Handling Procedure

Check the direct memory usage.

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Alarms** > **ALM-45738 TokenServer Direct Memory Usage Exceeds the Threshold**. Check the location information of the alarm and view the host name of the instance for which the alarm is generated.

Step 2 On FusionInsight Manager, choose **Cluster** > **Services** > **Guardian**. On the page that is displayed, click the **Instance** tab. On this tab page, select the role corresponding to the host name of the instance for which the alarm is generated. Click the drop-down list in the upper right corner of the chart area and choose **Customize** > **CPU and Memory** > **TokenServer Direct Memory Usage**. Then click **OK**.

Step 3 Check whether the direct memory used by TokenServer reaches the threshold (80% of the maximum direct memory by default).

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On FusionInsight Manager, choose **Cluster** > **Services** > **Guardian**. On the page that is displayed, click the **Instance** tab. On this tab page, choose **TokenServer** > **Instance Configuration**. Click **All Configurations**, and choose **TokenServer** > **System**. Set **-XX:MaxDirectMemorySize** in the **GC_OPTS** parameter to a larger value based on site requirements and save the configuration.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

NOTE

If this alarm is generated, the direct memory configured for TokenServer cannot meet the direct memory required by the TokenServer process. You are advised to check the direct memory usage of TokenServer and change the value of **-XX:MaxDirectMemorySize** in **GC_OPTS** to the twice of the direct memory used by TokenServer. You can change the value based on the actual service scenario. Refer to **Step 2** to view the TokenServer direct memory usage.

Step 5 Restart the affected services or instances and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **Guardian** for the destination cluster.

Step 8 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.460 ALM-45739 Guardian TokenServer Non-Heap Memory Usage Exceeds the Threshold

Alarm Description

The system checks the non-heap memory usage of the TokenServer service every 60 seconds. This alarm is generated when the non-heap memory usage of the TokenServer instance exceeds the threshold for 5 consecutive times.

This alarm is automatically cleared when the system detects that the non-heap memory usage is less than the threshold.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45739	Critical (default threshold: 95%) Major (default threshold: 85%)	Quality of service	Tenant plane	Guardian	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

If the non-heap memory of the Guardian TokenServer instance overflows, OBS cannot be accessed.

Possible Causes

The non-heap memory of the TokenServer instance is overused or the non-heap memory is inappropriately allocated.

Handling Procedure

Check non-heap memory usage.

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Alarms** > **ALM-45739 TokenServer Non-Heap Memory Usage Exceeds the Threshold**. Check the location information of the alarm and view the host name of the instance for which the alarm is generated.

Step 2 On FusionInsight Manager, choose **Cluster** > **Services** > **Guardian**. On the page that is displayed, click the **Instance** tab. On this tab page, select the role corresponding to the host name of the instance for which the alarm is generated. Click the drop-down list in the upper right corner of the chart area and choose **Customize** > **CPU and Memory** > **TokenServer Non-Heap Memory Usage**. Then click **OK**.

Step 3 Check whether the non-heap memory used by TokenServer reaches the threshold (80% of the maximum non-heap memory by default).

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On FusionInsight Manager, choose **Cluster** > **Services** > **Guardian**. On the page that is displayed, click the **Instance** tab. On this tab page, choose **TokenServer** > **Instance Configuration**. Click **All Configurations**, and choose **TokenServer** > **System**. Set **-XX: MaxPermSize** in the **GC_OPTS** parameter to a larger value based on site requirements and save the configuration.

NOTE

If this alarm is generated, the non-heap memory size configured for the TokenServer instance cannot meet the non-heap memory required by the TokenServer process. You are advised to change the value of **-XX:MaxPermSize** in **GC_OPTS** to twice that of the current non-heap memory size or change the value based on site requirements.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 5 Restart the affected services or instances and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **Guardian** for the destination cluster.

Step 8 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.461 ALM-45740 Guardian TokenServer GC Duration Exceeds the Threshold

Alarm Description

The system checks the GC duration of the TokenServer process every 60 seconds. This alarm is generated when the GC duration of the TokenServer process exceeds the threshold for five consecutive times.

This alarm is automatically cleared when the system detects that the GC duration is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45740	Critical (default threshold: 15000 ms) Major (default threshold: 12000 ms)	Quality of service	Tenant plane	Guardian	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the alarm triggering condition.

Impact on the System

TokenServer responds slowly, and OBS cannot be accessed.

Possible Causes

The heap memory of the TokenServer process is overused or inappropriately allocated, causing frequent occurrence of the GC process.

Handling Procedure

Check the GC duration.

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Alarms** > **ALM-45740 TokenServer GC Duration Exceeds the Threshold**. Check the location information of the alarm and view the host name of the instance for which the alarm is generated.

Step 2 On FusionInsight Manager, choose **Cluster** > **Services** > **Guardian**. On the page that is displayed, click the **Instance** tab. On this tab page, select the role corresponding to the host name of the instance for which the alarm is generated and click the drop-down list in the upper right corner of the chart area. Choose **Customize** > **GC** > **TokenServer GC Duration**. Then click **OK**.

Step 3 Check whether the GC duration of the TokenServer process collected every minute exceeds the threshold (12 seconds by default).

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 On FusionInsight Manager, choose **Cluster** > **Services** > **Guardian**. On the page that is displayed, click the **Instance** tab. On this tab page, choose **TokenServer** > **Instance Configuration**. Click **All Configurations**, and choose **TokenServer** > **System**. Set **-Xmx** in the **GC_OPTS** parameter to a larger value based on site requirements and save the configuration.

NOTE

If this alarm is generated, the heap memory configured for TokenServer cannot meet the heap memory required by the TokenServer process. You are advised to change the value of **-Xmx** in **GC_OPTS** to twice that of the heap memory used by TokenServer. You can change the value based on the actual service scenario. Refer to **Step 2** to view the TokenServer heap memory usage.

Step 5 Restart the affected services or instances and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On FusionInsight Manager, choose **O&M** > **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **Guardian** for the destination cluster.

Step 8 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Related Information

None.

1.3.462 ALM-45741 Guardian Failed to Call the ECS securitykey API

Alarm Description

Guardian caches the temporary AK/SK of the ECS agency. When the cache does not exist or is about to expire, Guardian calls the securitykey API of ECS to update the AK/SK. This alarm is generated when calling to the API fails.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45741	Major	Quality of service	Tenant plane	Guardian	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

The task may fail to obtain the temporary AK/SK for accessing OBS. As a result, OBS cannot be accessed.

Possible Causes

- No ECS agency is bound to the cluster.
- An underlying interface of ECS is abnormal.

Handling Procedure

Check whether an agency is bound to the cluster.

Step 1 Log in to the MRS management console.

Step 2 In the navigation pane on the left, choose **Clusters** > **Active Clusters**. On the page that is displayed, click the cluster name to go to its overview page. Then, check whether the cluster is bound to an agency in the O&M management area.

- If yes, go to **4**.
- If no, go to **3**.

Step 3 Click **Manage Agency**. On the page that is displayed, rebind the cluster to an agency. Then check whether the alarm is cleared a few minutes later.

- If yes, no further action is required.
- If no, go to **4**.

Collect fault information.

Step 4 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 5 Expand the **Service** drop-down list, and select **Guardian** for the destination cluster.

Step 6 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 7 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.463 ALM-45742 Guardian Failed to Call the ECS Metadata API

Alarm Description

When Guardian calls an IAM API to obtain the temporary AK/SK, it needs to first obtain related metadata via the ECS Metadata API. This alarm is generated when Guardian fails to call the Metadata API.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45742	Major	Quality of service	Tenant plane	Guardian	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

The task may fail to obtain the temporary AK/SK for accessing OBS. As a result, OBS cannot be accessed.

Possible Causes

An underlying interface of ECS is abnormal.

Handling Procedure

Collect fault information.

Step 1 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 2 Expand the **Service** drop-down list, and select **Guardian** for the destination cluster.

Step 3 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 4 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.464 ALM-45743 Guardian Failed to Call the IAM API

Alarm Description

This alarm is generated when Guardian fails to call the IAM API to obtain a temporary AK/SK.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
45743	Major	Quality of service	Tenant plane	Guardian	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

The task may fail to obtain the temporary AK/SK for accessing OBS. As a result, OBS cannot be accessed.

Possible Causes

The IAM service is abnormal.

Handling Procedure

Collect fault information.

Step 1 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 2 Expand the **Service** drop-down list, and select **Guardian** for the destination cluster.

Step 3 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 4 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.465 ALM-46001 MOTService Unavailable

Alarm Description

The system checks the MOTService status every 30 seconds. This alarm is generated when the MOTService service is unavailable.

This alarm is automatically cleared when the MOTService service recovers.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
46001	Critical	Quality of service	Tenant plane	MOTServic e	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceI nstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

The MOTService database service is unavailable and cannot provide functions such as data import and query for upper-layer services.

Possible Causes

- There is no active MOTServer instance.
- The floating IP address of MOTService does not exist.
- The active and standby MOTServer processes are abnormal.

Handling Procedure

Check whether the active MOTServer instance exists in the cluster.

Step 1 On FusionInsight Manager, choose **Cluster** > **Services** > **MOTService**, and click the **Instance** tab.

Step 2 Check whether the **MOTServer(Active)** instance exists.

- If yes, go to **Step 4**.
- If no, go to **Step 3**.

Step 3 Return to the **Dashboard** tab, click **More**, and select **Restart Service**. Then enter the user password to restart the MOTService service. After the service is restarted, check whether the **MOTServer(Active)** instance exists.

- If yes, check whether the alarm is cleared. If it is, no further action is required. If it is not, go to **Step 4**.
- If no, go to **Step 15**.

Check whether the floating IP address of MOTService exists in the cluster.

Step 4 On FusionInsight Manager, choose **Cluster** > **Services** > **MOTService**, and click the **Instance** tab.

Step 5 Locate the **MOTServer(Active)** instance and record the service IP address.

Step 6 Log in to the host obtained in **Step 5** as user **omm** and run the **ifconfig** command to check whether the floating IP address of MOTService exists.

- If yes, record the network port name (for example, **eth0:MOT**) and go to **Step 7**.
- If no, go to **Step 15**.

Step 7 Run the **ping** *Floating IP address* command to check whether the floating IP address of MOTService can be pinged.

- If yes, go to **Step 8**.
- If no, go to **Step 15**.

Step 8 Log in to the host where the MOTService floating IP address is located as user **root** and run the following command:

ifconfig *Network port name* **down**

Example: **ifconfig eth0:MOT down**

Step 9 On FusionInsight Manager, choose **Cluster** > **Services** > **MOTService**, click **More**, and select **Restart Service**. In the dialog box that is displayed, enter the password to restart the MOTService service.

Step 10 After the service is restarted, check whether this alarm is cleared in the alarm list.

- If yes, no further action is required.
- If no, go to **Step 11**.

Check the status of the active and standby MOTServer database processes.

Step 11 Log in to the host where the floating IP address of MOTService is located as user **omm** and run the following command to go to the installation directory of MOTService:

cd ${MOTSERVER_HOME}

Step 12 Run the following command to check whether the active and standby HA processes of MOTService are in the abnormal state:

sh sbin/status-motserver.sh

- If yes, go to **Step 13**.
- If no, go to **Step 15**.

Step 13 On FusionInsight Manager, choose **Cluster** > **Services** > **MOTService**, click **More**, and select **Restart Service**. In the dialog box that is displayed, enter the password to restart the MOTService service.

Step 14 Wait about 2 minutes and check whether the alarm is cleared in the alarm list.

- If yes, no further action is required.
- If no, go to **Step 15**.

Collect fault information.

Step 15 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 16 Expand the **Service** drop-down list, select **MOTService** for the target cluster, and click **OK**.

Step 17 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the hosts to which the role belongs.

Step 18 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 19 Contact O&M personnel/Technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Related Information

None

1.3.466 ALM-46003 MOTService Heartbeat Interruption Between the Active and Standby Nodes

Alarm Description

This alarm is generated when the active or standby MOTService node has not received heartbeat messages from the peer node for 7 seconds.

This alarm is cleared when the heartbeat recovers.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
46003	Major	Heartbeat	Tenant plane	MOTServic e	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceI nstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Local MOTService HA Name	Specifies a local MOTService HA.
	Peer MOTService HA Name	Specifies a peer MOTService HA.
	SYNC_PERCENT	Specifies the synchronization percentage of the active and standby MOTService nodes.

Impact on the System

During the MOTService heartbeat interruption, only one node provides the service. Once this node becomes faulty, the MOTService service cannot be switched to a standby node and will become unavailable.

Possible Causes

The network between the active and standby MOTService nodes is abnormal.

Handling Procedure

Check whether the network between the active and standby MOTService servers is normal.

Step 1 On FusionInsight Manager, choose **Cluster** > **Services** > **MOTService** > **Instance**. View and record the service IP addresses of **MOTServer(Active)** and **MOTServer(Standby)** instances.

Step 2 Log in to the **MOTServer(Active)** node as user **omm**.

Step 3 Run the following command to check whether the network connection between the active and standby MOTService nodes is normal:

ping *Service IP address of the* ***MOTServer(Standby)*** *node*

- If yes, go to **Step 6**.

- If no, go to **Step 4**.

Step 4 Contact the network administrator to check whether the network is faulty.

- If yes, go to **Step 5**.
- If no, go to **Step 6**.

Step 5 Rectify the network fault and check whether the alarm is cleared in the alarm list.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list and select **MOTService**.

Step 8 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the hosts to which the role belongs.

Step 9 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact O&M personnel/Technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.3.467 ALM-46004 Data Inconsistency Between Active and Standby MOTService Nodes

Alarm Description

The system checks the data synchronization status between the active and standby MOTService nodes every 10 seconds. This alarm is generated when the synchronization status cannot be queried for six consecutive times or the synchronization status is abnormal.

This alarm is cleared when the synchronization status becomes normal.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
46004	Critical	Quality of service	Tenant plane	MOTServic e	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceI nstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	Local MOTService HA Name	Specifies a local MOTService HA.
	Peer MOTService HA Name	Specifies a peer MOTService HA.

Impact on the System

If the active instance is abnormal, data will be lost or abnormal.

Possible Causes

- The network between the active and standby nodes is unstable.
- The standby MOTService is abnormal.
- The disk space of the standby node is full.
- The CPU usage of the GaussDB process on the active MOTService node is high. (You need to locate the fault based on logs.)

Handling Procedure

Check whether the network between the active and standby nodes is normal.

Step 1 On FusionInsight Manager, choose **Cluster** > **Services** > **MOTService** > **Instance**. View and record the service IP addresses of **MOTServer(Active)** and **MOTServer(Standby)** instances.

Step 2 Log in to the **MOTServer(Active)** node as user **omm**.

Step 3 Run the following command to check whether the active and standby MOTService nodes are connected:

ping *Service IP address of the **MOTServer(Standby)** node*

- If yes, go to **Step 6**.
- If no, go to **Step 4**.

Step 4 Contact the network administrator to check whether the network is faulty.

- If yes, go to **Step 5**.
- If no, go to **Step 6**.

Step 5 Rectify the network fault and check whether the alarm is cleared in the alarm list.

- If yes, no further action is required.
- If no, go to **Step 6**.

Check whether the standby MOTService is normal.

Step 6 Log in to the **MOTServer(Standby)** node as user **omm**.

Step 7 Run the following commands to check whether the GaussDB resource status of the standby MOTService is normal:

cd ${MOTSERVER_HOME}/sbin

./status-motserver.sh

For example, if the following information is displayed in the line where **ResName** is **gaussDB**, the service is normal:

```
10_10_10_231 gaussDB Standby_normal Normal Active_standby
```

- If yes, go to **Step 8**.
- If no, go to **Step 14**.

Check whether the disk space of the standby node is full.

Step 8 Log in to the **MOTServer(Standby)** node as user **omm**.

Step 9 Go to the **${MOTSERVER_HOME}** directory and run the following commands to obtain the MOTService data directory:

cd ${MOTSERVER_HOME}

source .motservice_profile

echo ${MOTSERVICE_DATA_DIR}

Step 10 Run the **df -h** command to check the system disk partition usage.

Step 11 Check whether the space of the MOTService data directory is full.

- If yes, go to **Step 12**.
- If no, go to **Step 14**.

Step 12 Expand the disk capacity of the node.

Step 13 After the disk capacity is expanded, wait 2 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 14**.

Collect fault information.

Step 14 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 15 Expand the **Service** drop-down list, select **MOTService** for the target cluster, and click **OK**.

Step 16 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the hosts to which the role belongs.

Step 17 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 18 Contact O&M personnel/Technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.3.468 ALM-46005 MOTService Database Connection Usage Exceeds the Threshold

Alarm Description

The system checks the database connection usage of the MOTServer node every 30 seconds and compares the actual database connection usage with the threshold. This alarm is generated when the database connection usage exceeds the threshold (90% by default) for five consecutive times (5 by default).

- If **Trigger Count** is **1**, this alarm is cleared when the database connection usage is less than or equal to the threshold.
- If **Trigger Count** is greater than **1**, this alarm is cleared when the database connection usage is less than or equal to 90% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
46005	Major	Communications	Tenant plane	MOTService	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold for triggering the alarm.

Impact on the System

If there are too many MOTService database connections, upper-layer services may fail to connect to the MOTService database.

Possible Causes

- There are too many database connections.
- The maximum number of database connections is set improperly.
- The alarm threshold or alarm trigger count is improperly configured.

Handling Procedure

Check whether there are too many database connections.

Step 1 On FusionInsight Manager, choose **Cluster** > **Services** > **MOTService**. The **Dashboard** page is displayed.

Step 2 In the **Chart** area, view the **Connections Used by MOT User** chart to check whether there are too many database connections.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 Reduce the number of database connections based on the service scenario, that is, close some connections.

Step 4 Wait 2 minutes and check whether the alarm is automatically cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check whether the maximum number of database connections is set properly.

Step 5 On FusionInsight Manager, choose **Cluster** > **Services** > **MOTService** > **Configuration** > **All Configurations** and check whether the maximum number of database connections **motservice.database.max.connections** meets service requirements.

- If yes, go to **Step 9**.
- If no, go to **Step 6**.

Step 6 Increase the maximum number of database connections based on site requirements. The maximum number of database connections must be greater than the number of service data connections.

Step 7 On the **Dashboard** page, click **More** and select **Restart Service**. Enter the user password and click **OK** to restart the MOTService service.

Step 8 Wait 2 minutes and check whether the alarm is automatically cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Check whether the alarm threshold or alarm trigger count is properly configured.

Step 9 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Thresholds**, click the name of the desired cluster, choose **MOTService** > **Database** > **MOT Connections Usage (MOTServer)**, and check whether the alarm trigger count and alarm threshold are set properly.

- If yes, go to **Step 12**.
- If no, go to **Step 10**.

Step 10 Change the trigger count and alarm threshold based on the actual number of of database connections, and apply the changes.

Step 11 Wait 2 minutes and check whether the alarm is automatically cleared.

- If yes, no further action is required.
- If no, go to **Step 12**.

Collect fault information.

Step 12 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 13 Expand the **Service** drop-down list and select **MOTService**.

Step 14 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the hosts to which the role belongs.

Step 15 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 16 Contact O&M personnel/Technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.3.469 ALM-46006 Disk Space Usage of the MOTService Data Directory Exceeds the Threshold

Alarm Description

The system checks the disk space usage of the data directory on the active MOTServer node every 30 seconds and compares the actual disk space usage with the threshold. This alarm is generated when the disk space usage of the data directory exceeds the threshold (80% by default) for five consecutive times (5 by default).

- If **Trigger Count** is **1**, this alarm is cleared when the disk space usage of the data directory is less than or equal to the threshold.
- If **Trigger Count** is greater than **1**, this alarm is cleared when the disk space usage of the data directory is less than 90% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
46006	Major	Physical resource	Tenant plane	MOTServic e	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceI nstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.

Type	Parameter	Description
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	PartitionName	Specifies the disk partition for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold for triggering the alarm.

Impact on the System

- If the disk space of the MOTService data directory is insufficient, service processes may be unavailable.
- When the disk space usage of the data directory exceeds 90%, the database enters the read-only mode and **ALM-46007 MOTService Database Enters the Read-Only Mode** is generated. As a result, service data is lost.

Possible Causes

- The alarm threshold is improperly configured.
- The database data volume is too large or the disk configuration cannot meet service requirements. As a result, the disk usage reaches the upper limit.

Handling Procedure

Check whether the threshold is set properly.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Thresholds**, click the name of the desired cluster, choose **MOTService** > **Database** > **MOT Disk Space Usage of the Data Directory (MOTServer)**, and check whether the alarm threshold is **80%**.

If yes, go to **Step 4**.

If no, go to **Step 2**.

Step 2 Change the alarm threshold based on the actual usage, and apply the change.

Step 3 Wait 2 minutes and check whether the alarm is automatically cleared.

If yes, no further action is required.

If no, go to **Step 4**.

Check whether large files are incorrectly written to the disk.

Step 4 Log in to the active MOTService node as user **omm**.

Step 5 Run the following commands to check whether files with more than 500 MB are incorrectly written into the disk space of the data directory:

```
source $MOTSERVER_HOME/.motservice_profile
find "$MOTSERVICE_DATA_DIR"/../ -type f -size +500M
```

If yes, go to **Step 6**.

If no, go to **Step 7**.

Step 6 Handle the incorrectly written files and check whether the alarm is cleared 2 minutes later.

If yes, no further action is required.

If no, go to **Step 7**.

Collect fault information.

Step 7 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 8 Expand the **Service** drop-down list and select **MOTService**.

Step 9 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the hosts to which the role belongs.

Step 10 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 11 Contact O&M personnel/Technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.3.470 ALM-46007 MOTService Database Enters the Read-Only Mode

Alarm Description

The system checks the disk space usage of the data directory on the active MOTServer node every 30 seconds. This alarm is generated when the disk space usage of the data directory exceeds 70%.

This alarm is cleared when the disk space usage of the data directory falls below 70%.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
46007	Critical	Quality of service	Tenant plane	MOTServic e	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceI nstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold for triggering the alarm.

Impact on the System

The MOTService database in read-only mode cannot provide the data import function for upper-layer services.

Possible Causes

The disk configuration cannot meet service requirements. The disk usage reaches the upper limit.

Handling Procedure

Check whether the disk space usage reaches the upper limit.

Step 1 On FusionInsight Manager, choose **Cluster** > **Services** > **MOTService**.

Step 2 On the **Dashboard** page, view the **MOT Disk Space Usage of the Data Directory** chart to check whether the disk space usage of the data directory exceeds 70%. If the chart is not displayed, click on the right and click **Customize** to select the chart.

If yes, go to **Step 3**.

If no, go to **Step 9**.

Step 3 Click the **Instance** tab and obtain the service IP address of the active MOTService instance.

Step 4 Run the following commands to check whether the database enters the read-only mode:

source $MOTSERVER_HOME/.motservice_profile

gsql -d postgres -p 20105

*Enter the password of user **omm** for the MOTService database.*

show default_transaction_read_only;

NOTE

- Contact the cluster administrator to obtain the **omm** password of the MOTService database.
- You can run the **\q** command to exit the database.

Check whether the value of **default_transaction_read_only** is **on**.

```
openGauss=# show default_transaction_read_only;
 default_transaction_read_only
-------------------------------
 on
(1 row)
```

- If yes, go to **Step 5**.
- If no, go to **Step 9**.

Step 5 Log in to the active MOTServer node as user **omm**. Run the following commands to check whether files with more than 500 MB are incorrectly written into the disk space of the data directory:

source $MOTSERVER_HOME/.motservice_profile

find "$MOTSERVICE_DATA_DIR"/../ -type f -size +500M

- If yes, go to **Step 6**.
- If no, go to **Step 9**.

Step 6 Delete the incorrectly written files based on site requirements.

Step 7 Run the following command to disable the read-only mode of the database:

gs_guc reload -Z datanode -N all -I all -c "default_transaction_read_only=off"

Step 8 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Collect fault information.

Step 9 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 10 Expand the **Service** drop-down list and choose **Containers** > **CenterServer**.

Step 11 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the hosts to which the role belongs.

Step 12 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 13 Contact O&M personnel/Technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.3.471 ALM-46008 MOTService Memory Usage Exceeds the Threshold

Alarm Description

The system checks the memory usage every 30 seconds and compares the actual memory usage with the threshold. This alarm is generated when the memory usage exceeds the threshold.

- If **Trigger Count** is **1**, this alarm is cleared when the MOTService memory usage is less than or equal to the threshold.
- If **Trigger Count** is greater than **1**, this alarm is cleared when the MOTService memory usage is less than or equal to 70% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
46008	Critical (default threshold: 80%) Major (default threshold: 75%)	Physical resource	Tenant plane	MOTServic e	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceI nstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold for triggering the alarm.

Impact on the System

Service processes respond slowly or become unavailable. As a result, the MOTService database cannot provide functions such as data import and query for upper-layer services.

Possible Causes

- The alarm threshold or alarm trigger count is improperly configured.
- The memory size cannot meet service requirements, and the memory usage reaches the upper limit.

Handling Procedure

Check whether the alarm threshold or alarm trigger count is properly configured.

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Thresholds**, click the name of the desired cluster, choose **MOTService** > **Database** > **MOT Used Memory Percentage (MOTServer)**, and check whether the alarm trigger count and alarm threshold are set properly.

- If yes, go to **Step 4**.
- If no, go to **Step 2**.

Step 2 Change the trigger count and alarm threshold based on the actual memory usage, and apply the changes.

Step 3 Wait 2 minutes and check whether the alarm is automatically cleared.

- If yes, no further action is required.
- If no, go to **Step 4**.

Check the memory usage.

Step 4 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. In the right pane, click this alarm and obtain the host name in **Location**.

Step 5 Choose **Hosts** and click the host for which the alarm is generated.

Step 6 Observe the real-time data of the MOTService memory usage for about 5 minutes. If the memory usage exceeds the threshold for multiple times, contact the MRS cluster administrator to increase the memory.

Step 7 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Collect fault information.

Step 8 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 9 Expand the **Service** drop-down list and select **MOTService**.

Step 10 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the hosts to which the role belongs.

Step 11 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact O&M personnel/Technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.3.472 ALM-46009 MOTService CPU Usage Exceeds the Threshold

Alarm Description

The system checks the CPU usage of the MOTService every 30 seconds and compares the actual CPU usage with the threshold. This alarm is generated when the CPU usage exceeds the threshold (80% by default) for multiple consecutive times (10 by default).

- If **Trigger Count** is **1**, this alarm is cleared when the CPU usage is less than or equal to the threshold.
- If **Trigger Count** is greater than **1**, this alarm is cleared when the CPU usage is less than or equal to 90% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
46009	Major	Physical resource	Tenant plane	MOTServic e	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceI nstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold for triggering the alarm.

Impact on the System

Service processes respond slowly or become unavailable. As a result, the MOTService database cannot provide functions such as data import and query for upper-layer services.

Possible Causes

- The alarm threshold or alarm trigger count is improperly configured.
- The CPU configuration cannot meet service requirements, and the CPU usage reaches the upper limit.

Handling Procedure

Check whether the alarm threshold or alarm trigger count is properly configured.

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Thresholds**, click the name of the desired cluster, choose **MOTService** > **Database** > **MOT Used CPU Percentage (MOTServer)**, and check whether the alarm trigger count and alarm threshold are set properly.

- If yes, go to **Step 4**.
- If no, go to **Step 2**.

Step 2 Change the trigger count and alarm threshold based on the actual CPU usage, and apply the changes.

Step 3 Wait 2 minutes and check whether the alarm is automatically cleared.

- If yes, no further action is required.
- If no, go to **Step 4**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Check whether the CPU usage reaches the upper limit.

Step 4 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. In the right pane, click this alarm and obtain the host name in **Location**.

Step 5 Choose **Hosts** and click the host for which the alarm is generated.

Step 6 Observe the real-time data of the host CPU usage for about 5 minutes. If the CPU usage exceeds the threshold for multiple times, contact the MRS cluster administrator to increase the CPU.

Step 7 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Collect fault information.

Step 8 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 9 Expand the **Service** drop-down list and select **MOTService**.

Step 10 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the hosts to which the role belongs.

Step 11 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact O&M personnel/Technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.3.473 ALM-46010 MOTService Certificate File Is About to Expire

Alarm Description

The system checks the certificate file in the system on the hour. This alarm is generated when the certificate file is about to expire in less than 30 days.

This alarm is cleared when a certificate that is not about to expire is imported and the alarm detection mechanism is triggered on the next hour.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
46010	Minor	Security	Tenant plane	MOTServic e	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceI nstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold for triggering the alarm.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

If the MOTService certificate is about to expire, the system is not affected. If the certificate has expired, functions such as data import and query cannot be provided for upper-layer services.

Possible Causes

The remaining validity period of the MOTService certificate file (MOTService root certificate or MOTService user certificate) is less than 30 days.

Handling Procedure

Locate the alarm cause.

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Alarms**. In the right pane, locate this alarm and click ⌄.

View **Additional Information** to obtain the additional information about the alarm.

- If **MOTService HA root Certificate** is displayed in the additional information, view **Location** to obtain the name of the host for which the alarm is generated. Then, log in to the host as user **omm** and go to **Step 2**.
- If **MOTService HA server Certificate** is displayed in the additional information, view **Location** to obtain the name of the host for which the alarm is generated. Then, log in to the host as user **omm** and go to **Step 3**.
- If **MOTService root Certificate** is displayed in the additional information, view **Location** to obtain the name of the host for which the alarm is generated. Then, log in to the host as user **omm** and go to **Step 4**.
- If **MOTService server Certificate** is displayed in the additional information, view **Location** to obtain the name of the host for which the alarm is generated. Then, log in to the host as user **omm** and go to **Step 5**.

Check the validity period of the certificate files in the system.

Step 2 Check whether the remaining validity period of the MOTService HA root certificate is smaller than the alarm threshold.

Run the **openssl x509 -noout -text -in ${MOTSERVER_HOME}/ha/local/cert/root-ca.crt** command to check the effective time and due time of the MOTService HA root certificate.

- If yes, go to **Step 6**.
- If no, go to **Step 8**.

Step 3 Check whether the remaining validity period of the MOTService HA user certificate is smaller than the alarm threshold.

Run the **openssl x509 -noout -text -in ${MOTSERVER_HOME}/ha/local/cert/server.crt** command to check the effective time and due time of the MOTService HA user certificate.

- If yes, go to **Step 6**.
- If no, go to **Step 8**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 4 Check whether the remaining validity period of the MOTService root certificate is smaller than the alarm threshold.

Run the **openssl x509 -noout -text -in ${MOTSERVER_HOME}/security/root-ca.crt** command to check the effective time and due time of the MOTService root certificate.

- If yes, go to **Step 7**.
- If no, go to **Step 8**.

Step 5 Check whether the remaining validity period of the MOTService user certificate is smaller than the alarm threshold.

Run the **openssl x509 -noout -text -in ${MOTSERVER_HOME}/security/server.crt** command to check the effective time and due time of the MOTService user certificate.

- If yes, go to **Step 7**.
- If no, go to **Step 8**.

The following is an example of the effective time and due time of a certificate:

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      97:d5:0e:84:af:ec:34:d8
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=CN, ST=xxx, L=yyy, O=zzz, OU=IT, CN=HADOOP.COM
    Validity
      Not Before: Dec 13 06:38:26 2016 GMT          // Effective time
      Not After : Dec 11 06:38:26 2026 GMT          // Due time
```

Import certificate files.

Step 6 Import a new MOTService HA certificate file.

Apply for or generate a new HA certificate file and import it to the system. For details, see "Replacing the MOTService HA Certificate" in MapReduce Service (MRS) 3.3.1-LTS User Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Usage Guide (for Huawei Cloud Stack 8.3.1). Manually clear the alarm and check whether this alarm is generated again during periodic check.

- If yes, go to **Step 8**.
- If no, no further action is required.

Step 7 Import a new MOTService certificate file.

Apply for or generate a new MOTService certificate file and import it to the system. For details, see "Replacing the MOTService Certificate" in MapReduce Service (MRS) 3.3.1-LTS User Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Usage Guide (for Huawei Cloud Stack 8.3.1). Manually clear the alarm and check whether this alarm is generated again during periodic check.

- If yes, go to **Step 8**.
- If no, no further action is required.

Collect fault information.

Step 8 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 9 Expand the **Service** drop-down list, select **Controller**, **OmmServer**, **OmmCore**, and **Tomcat**, and click **OK**.

Step 10 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 11 Contact O&M personnel/Technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.3.474 ALM-46011 MOTService Certificate File Has Expired

Alarm Description

The system checks whether the certificate file in the system has expired on the hour. This alarm is generated when the certificate file has expired.

This alarm is cleared when a valid certificate is imported and the alarm detection mechanism is triggered on the next hour.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
46011	Major	Security	Tenant plane	MOTServic e	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceI nstance	Specifies the microservice for which the alarm was generated.

Type	Parameter	Description
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold for triggering the alarm.

Impact on the System

If the MOTService certificate has expired, some MOTService functions such as data import and query cannot be provided for upper-layer services.

Possible Causes

The MOTService certificate file (MOTService root certificate or MOTService user certificate) has expired.

Handling Procedure

Locate the alarm cause.

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Alarms**. In the right pane, locate this alarm and click ⌄.

View **Additional Information** to obtain the additional information about the alarm.

- If **MOTService HA root Certificate** is displayed in the additional information, view **Location** to obtain the name of the host for which the alarm is generated. Then, log in to the host as user **omm** and go to **Step 2**.
- If **MOTService HA server Certificate** is displayed in the additional information, view **Location** to obtain the name of the host for which the alarm is generated. Then, log in to the host as user **omm** and go to **Step 3**.
- If **MOTService root Certificate** is displayed in the additional information, view **Location** to obtain the name of the host for which the alarm is generated. Then, log in to the host as user **omm** and go to **Step 4**.
- If **MOTService server Certificate** is displayed in the additional information, view **Location** to obtain the name of the host for which the alarm is generated. Then, log in to the host as user **omm** and go to **Step 5**.

Check the validity period of the certificate files in the system.

Step 2 Check whether the current system time is within the validity period of the MOTService HA root certificate.

Run the **openssl x509 -noout -text -in ${MOTSERVER_HOME}/ha/local/cert/root-ca.crt** command to check the effective time and due time of the MOTService HA root certificate.

- If yes, go to **Step 8**.
- If no, go to **Step 6**.

Step 3 Check whether the current system time is within the validity period of the MOTService HA user certificate.

Run the **openssl x509 -noout -text -in ${MOTSERVER_HOME}/ha/local/cert/server.crt** command to check the effective time and due time of the MOTService HA user certificate.

- If yes, go to **Step 8**.
- If no, go to **Step 6**.

Step 4 Check whether the current system time is within the validity period of the MOTService root certificate.

Run the **openssl x509 -noout -text -in ${MOTSERVER_HOME}/security/root-ca.crt** command to check the effective time and due time of the MOTService root certificate.

- If yes, go to **Step 8**.
- If no, go to **Step 7**.

Step 5 Check whether the current system time is within the validity period of the MOTService user certificate.

Run the **openssl x509 -noout -text -in ${MOTSERVER_HOME}/security/server.crt** command to check the effective time and due time of the MOTService user certificate.

- If yes, go to **Step 8**.
- If no, go to **Step 7**.

The following is an example of the effective time and due time of a certificate:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            97:d5:0e:84:af:ec:34:d8
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=CN, ST=xxx, L=yyy, O=zzz, OU=IT, CN=HADOOP.COM
        Validity
            Not Before: Dec 13 06:38:26 2016 GMT            // Effective time
            Not After : Dec 11 06:38:26 2026 GMT            // Due time
```

Import certificate files.

Step 6 Import a new MOTService HA certificate file.

Apply for or generate a new MOTService HA certificate file and import it to the system. For details, see "Replacing the MOTService HA Certificate" in MapReduce Service (MRS) 3.3.1-LTS User Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Usage Guide (for Huawei Cloud Stack 8.3.1). The alarm is automatically cleared after the MOTService HA certificate is imported. Check whether this alarm is reported again during periodic check.

- If yes, go to **Step 8**.
- If no, no further action is required.

Step 7 Import a new MOTService certificate file.

Apply for or generate a new MOTService certificate file and import it to the system. For details, see "Replacing the MOTService Certificate" in MapReduce Service (MRS) 3.3.1-LTS User Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Usage Guide (for Huawei Cloud Stack 8.3.1). The alarm is automatically cleared after the MOTService certificate is imported. Check whether this alarm is reported again during periodic check.

- If yes, go to **Step 8**.
- If no, no further action is required.

Collect fault information.

Step 8 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 9 Expand the **Service** drop-down list, select **Controller**, **OmmServer**, **OmmCore**, and **Tomcat**, and click **OK**.

Step 10 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 11 Contact O&M personnel/Technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.3.475 ALM-46012 Abnormal Nginx of MOTService

Alarm Description

The system checks the Nginx status of MOTService every 10 seconds. This alarm is generated when the Nginx service has been detected to be abnormal for 10 consecutive times during the HA health check.

This alarm is cleared when the Nginx service becomes normal during the HA health check.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
46012	Major	Quality of service	Tenant plane	MOTServic e	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceI nstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

If Nginx is abnormal, services may fail to access MOTService using the floating IP address. As a result, MOTService is unavailable and cannot provide functions such as data import and query for upper-layer services.

Possible Causes

The Ngnix service is not running properly.

Handling Procedure

Check whether the Ngnix service on the node where MOTService resides is normal.

Step 1 Log in to FusionInsight Manager.

Step 2 Choose **O&M** > **Alarm** > **Alarms**. On the page that is displayed, locate the row containing this alarm, and obtain the name of the host for which the alarm is generated in **Location**.

Step 3 Choose **Cluster** > **Services** > **MOTService**. On the page that is displayed, click the **Instance** tab and obtain the service IP address of the host for which this alarm is generated.

Step 4 Log in to the node in **Step 3** as user **omm**.

Step 5 Run the following command to check the Nginx status:

lsof -i "TCP@$*MOTService floating IP address:***20105" | grep -q "nginx"**

If the following information is displayed, the status is normal:

```
ngnix  Normal  Normal   Single_active
```

NOTE

You can also log in to FusionInsight Manager, choose **Cluster** > **Services** > **MOTService** > **Configurations** > **All Configurations**, search for the **motservice.floatip** parameter, and obtain its value, which is the floating IP address of MOTService.

- If yes, go to **Step 8**.
- If no, go to **Step 6**.

Step 6 Contact the network administrator to check whether the network is faulty and whether the floating IP address is incorrect.

- If yes, repair the network, configure a correct floating IP address, and go to **Step 7**.
- If no, go to **Step 8**.

Step 7 Wait 5 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Collect fault information.

Step 8 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 9 Expand the **Service** drop-down list and select **MOTService**.

Step 10 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 11 Contact O&M personnel/Technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.3.476 ALM-47001 MemArtsCC Service Unavailable

Alarm Description

The system checks the status of the ZooKeeper service on which the MemArtsCC depends every 60 seconds. This alarm is generated when the ZooKeeper service is unavailable.

This alarm is automatically cleared when the ZooKeeper service is normal.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
47001	Critical	Error handling	Tenant plane	MemArtsCC	Yes

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Changes

Change Type	Version	Description	Reason for Change
New	3.3.1	New alarm	New alarm

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

The service will be unavailable.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Possible Causes

The ZooKeeper service on which the MemArtCC service depends is unavailable.

Handling Procedure

Handling ZooKeeper exceptions

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Alarms**. On the ZooKeeper dashboard page, check whether the ZooKeeper service is faulty.

- If yes, go to **Step 2**.
- If no, go to **Step 4**.

Step 2 Rectify the ZooKeeper fault based on the error information and alarm information and the ZooKeeper help document.

Step 3 After the ZooKeeper service becomes normal, wait for 60 seconds and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 4**.

Collect fault information.

Step 4 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 5 Expand the **Service** drop-down list, and select **MemArtsCC** for the target cluster.

Step 6 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 7 Contact technical support and send the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.3.477 ALM-47002 MemArtsCC Disk Fault

Alarm Description

The alarm module checks the status of the local disk used by MemArtsCC every 60 seconds. This alarm is generated when the alarm module detects that the disk status is abnormal. This alarm is cleared when the disk becomes normal.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
47002	Major	Error handling	Tenant plane	MemArtsCC	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

MemArtsCC becomes abnormal or its performance deteriorates.

Possible Causes

The disk used by MemArtsCC is damaged or the permission is read-only.

Handling Procedure

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**, search for "ALM-47002 MemArtsCC Disk Fault", and locate the abnormal disk directory based on the alarm information.

Step 2 Contact technical support to check whether the disk is faulty.

- If yes, replace the disk, restart the CCSideCar and CCWorker roles of the faulty node, and go to **Step 3**.
- If no, go to **Step 4**.

Step 3 Choose **O&M** > **Alarm** > **Alarms** and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 4**.

Collect fault information.

Step 4 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 5 Expand the **Service** drop-down list, and select **MemArtsCC** for the target cluster.

Step 6 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 7 Contact technical support and send the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.3.478 ALM-50201 Doris Service Unavailable

Alarm Description

The alarm module checks the Doris service status every 60 seconds. This alarm is generated when the alarm module detects that all FE and BE instances are abnormal.

This alarm is cleared when any FE or BE instance recovers.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
50201	Critical	Error handling	Tenant plane	Doris	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

FusionInsight Manager cannot be used to perform cluster operations on the Doris service, and Doris service functions are unavailable.

Possible Causes

The FE and BE instances are abnormal.

Handling Procedure

Restart the Doris service.

Step 1 Log in to FusionInsight Manager and choose **Cluster** > **Services** > **Doris**.

Step 2 On the page that is displayed, click **More** and select **Restart Service**. In the displayed dialog box, verify the password and click **OK** to restart the Doris service. After the service is started, go to **Step 3**.

Step 3 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. In the alarm list, check whether this alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 4**.

Collect fault information.

Step 4 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 5 Expand the **Service** drop-down list, select **Doris** for the target cluster, and click **OK**.

Step 6 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 7 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.479 ALM-50202 Doris FE CPU Usage Exceeds the Threshold

Alarm Description

The system checks the CPU usage of the FE instance every 30 seconds. The CPU usage has a default threshold. This alarm is generated when the CPU usage exceeds the threshold for multiple consecutive times (**3** by default).

This alarm is cleared when **Trigger Count** is **1** and the CPU usage is less than or equal to the threshold. This alarm is cleared when **Trigger Count** is greater than 1 and the CPU usage is less than or equal to 80% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
50202	Critical (default threshold: 95%) Major (default threshold: 90%)	Quality of service	Tenant plane	Doris	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the alarm triggering condition.

Impact on the System

Processes respond slowly or do not work.

Possible Causes

The alarm threshold or alarm trigger count is improperly configured.

Handling Procedure

Check whether the alarm threshold or alarm trigger count is properly configured.

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Thresholds**, select the name of the desired cluster, and choose **Doris** > **CPU and Memory** > **CPU Usage of FE (FE)**.

Step 2 Click the edit button next to **Trigger Count**, change the number based on site requirements, and click **OK**.

NOTE

Trigger Count specifies how many times the threshold can be hit before an alarm is generated.

Step 3 Click **Modify** in the **Operation** column, change the alarm threshold based on site requirements, and click **OK**.

Step 4 Wait 2 minutes and check whether the alarm is automatically cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Collect fault information.

Step 5 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 6 Expand the **Service** drop-down list, select **Doris** for the target cluster, and click **OK**.

Step 7 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 8 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.480 ALM-50203 Doris FE Memory Usage Exceeds the Threshold

Alarm Description

The system checks the memory usage of the FE instance every 30 seconds. This alarm is generated when the memory usage exceeds the threshold for multiple consecutive times (**3** by default).

This alarm is cleared when **Trigger Count** is **1** and the memory usage is less than or equal to the threshold. This alarm is cleared when **Trigger Count** is greater than 1 and the memory usage is less than or equal to 80% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
50203	Critical (default threshold: 90%) Major (default threshold: 85%)	Quality of service	Tenant plane	Doris	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.

Type	Parameter	Description
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the alarm triggering condition.

Impact on the System

Processes respond slowly or do not work.

Possible Causes

- The alarm threshold or alarm trigger count is improperly configured.

Handling Procedure

Check whether the alarm threshold or alarm trigger count is properly configured.

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Thresholds**, select the name of the desired cluster, and choose **Doris** > **CPU and Memory** > **Memory Usage of FE (FE)**.

Step 2 Click the edit button next to **Trigger Count**, change the number based on site requirements, and click **OK**.

NOTE

Trigger Count specifies how many times the threshold can be hit before an alarm is generated.

Step 3 Click **Modify** in the **Operation** column, change the alarm threshold based on site requirements, and click **OK**.

Step 4 Wait 2 minutes and check whether the alarm is automatically cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Collect fault information.

Step 5 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 6 Expand the **Service** drop-down list, select **Doris** for the target cluster, and click **OK**.

Step 7 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 8 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.481 ALM-50205 Doris BE CPU Usage Exceeds the Threshold

Alarm Description

The system checks the CPU usage of the BE instance every 30 seconds. This alarm is generated when the CPU usage exceeds the threshold for multiple consecutive times (**3** by default).

This alarm is cleared when **Trigger Count** is **1** and the CPU usage is less than or equal to the threshold. This alarm is cleared when **Trigger Count** is greater than 1 and the CPU usage is less than or equal to 80% of the threshold.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
50205	Critical (default threshold: 95%) Major (default threshold: 90%)	Quality of service	Tenant plane	Doris	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the alarm triggering condition.

Impact on the System

Processes respond slowly or do not work.

Possible Causes

The alarm threshold or alarm trigger count is improperly configured.

Handling Procedure

Check whether the alarm threshold or alarm trigger count is properly configured.

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Thresholds**, click the name of the desired cluster, and choose **Doris** > **CPU and Memory** > **CPU Usage of BE (BE)**.

Step 2 Click the edit button next to **Trigger Count**, change the number based on site requirements, and click **OK**.

NOTE

Trigger Count specifies how many times the threshold can be hit before an alarm is generated.

Step 3 Click **Modify** in the **Operation** column, change the alarm threshold based on site requirements, and click **OK**.

Step 4 Wait 2 minutes and check whether the alarm is automatically cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Collect fault information.

Step 5 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 6 Expand the **Service** drop-down list, select **Doris** for the target cluster, and click **OK**.

Step 7 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 8 Contact technical support and provide the collected logs.

----End

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.482 ALM-50206 Doris BE Memory Usage Exceeds the Threshold

Alarm Description

The system checks the memory usage of the BE instance every 30 seconds. This alarm is generated when the memory usage exceeds the threshold for multiple consecutive times (**3** by default).

This alarm is cleared when **Trigger Count** is **1** and the memory usage is less than or equal to the threshold. This alarm is cleared when **Trigger Count** is greater than 1 and the memory usage is less than or equal to 80% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
50206	Critical (default threshold: 90%) Major (default threshold: 85%)	Quality of service	Tenant plane	Doris	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the alarm triggering condition.

Impact on the System

Processes respond slowly or do not work.

Possible Causes

The alarm threshold or alarm trigger count is improperly configured.

Handling Procedure

Check whether the alarm threshold or alarm trigger count is properly configured.

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Thresholds**, click the name of the desired cluster, and choose **Doris** > **CPU and Memory** > **Memory Usage of BE (BE)**.

Step 2 Click the edit button next to **Trigger Count**, change the number based on site requirements, and click **OK**.

NOTE

Trigger Count specifies how many times the threshold can be hit before an alarm is generated.

Step 3 Click **Modify** in the **Operation** column, change the alarm threshold based on site requirements, and click **OK**.

Step 4 Wait 2 minutes and check whether the alarm is automatically cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Collect fault information.

Step 5 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 6 Expand the **Service** drop-down list, select **Doris** for the target cluster, and click **OK**.

Step 7 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 8 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.483 ALM-50207 Ratio of Connections to the Doris FE MySQL Port to the Maximum Connections Allowed Exceeds the Threshold

Alarm Description

The system checks the number of MySQL port connections every 30 seconds. This alarm is generated when the ratio of the number of current connections to the maximum number of FE port connections exceeds the threshold (95% by default). The maximum number of FE port connections in the current cluster is specified by the **qe_max_connection** parameter. The default value is **1024**.

This alarm is cleared when the number of MySQL port connections on the FE node is less than or equal to the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
50207	Minor	Quality of service	Tenant plane	Doris	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the alarm triggering condition.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

The FE is overloaded. The FE processes client requests slowly.

Possible Causes

- After the MySQL client is connected to Doris, the connection is not closed.
- A large number of services are concurrently connected to Doris.

Handling Procedure

Check whether the alarm threshold or alarm trigger count is properly configured.

Step 1 Log in to FusionInsight Manager, choose **O&M**, and click **Alarm** > **Thresholds** in the navigation pane on the left. Click the name of the desired cluster > **Doris** > **Connection** > **FE MySQL Port Connections (FE)**.

Step 2 Click the edit button next to **Trigger Count**, change the number based on site requirements, and click **OK**.

Step 3 Click **Modify** in the **Operation** column, change the alarm threshold based on site requirements, and click **OK**.

NOTE

If there are a large number of connections, ensure there are only necessary connections. Otherwise, the service performance may be degraded or even the service may be unavailable.

Step 4 Wait for 2 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Collect fault information.

Step 5 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 6 Expand the **Service** drop-down list, select **Doris** for the target cluster, and click **OK**.

Step 7 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 8 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

1.3.484 ALM-50208 Failures to Clear Doris Historical Metadata Images Exceed the Threshold

Alarm Description

The system checks the number of failures to clear historical metadata image files on the FE node every 30 seconds. This alarm is generated when the number of failures exceeds the threshold (**1** by default).

This alarm is cleared when the system detects that the number of failures is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
50208	Critical	Error handling	Tenant plane	Doris	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the alarm triggering condition.

Impact on the System

Doris metadata occupies more and more disk space, which may cause service exceptions.

Possible Causes

The Doris service is abnormal.

Handling Procedure

Check whether the Doris service is normal.

Step 1 Log in to FusionInsight Manager and choose **Cluster** > **Services** > **Doris**.

Step 2 Check whether **Running Status** of the Doris service is **Normal**.

- If yes, go to **Step 4**.
- If no, go to **Step 3**.

Step 3 If the service process is not started, start it first and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 4**.

Step 4 Check whether other Doris-related alarms are generated in the cluster. If yes, clear them by referring to the alarm help. Then, check whether this alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Collect fault information.

Step 5 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 6 Expand the **Service** drop-down list, select **Doris** for the target cluster, and click **OK**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 7 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 8 Contact technical support and provide the collected logs.

----End

Alarm Clearance

You need to manually clear the alarm after the fault is rectified.

Related Information

None.

1.3.485 ALM-50209 Failures to Generate Doris Metadata Image Files Exceed the Threshold

Alarm Description

The system checks the number of failures to generate metadata image files on the FE node every 30 seconds. This alarm is generated when the number of failures exceeds the threshold (**1** by default).

This alarm is cleared when the system detects that the number of failures is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
50209	Critical	Error handling	Tenant plane	Doris	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the alarm triggering condition.

Impact on the System

The non-master FE node cannot receive the latest metadata image file. As a result, the system reliability deteriorates.

Possible Causes

When the checkpoint thread of the Doris FE detects that the FE memory usage exceeds 75%, the thread determines that the write operation to the image file fails.

Handling Procedure

Check the Doris service status.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. In the alarm list, view the role name and obtain the IP address of the instance in **Location** of the alarm whose ID is **50209**.

Step 2 Choose **Cluster** > **Services** > **Doris** > **Instances**, click the FE instance for which the alarm is generated, and click the **Chart** tab of the instance.

Select **CPU and Memory** from the chart categories on the left, and check whether the value of **Memory Usage of FE** exceeds 75%.

- If yes, go to **Step 3**.
- If no, go to **Step 6**.

Step 3 Choose **Cluster** > **Service** > **Doris**, and click the **Configurations** tab. Search for the **FE_GC_OPTS** parameter, and increase the value of **-Xmx**. The default value is 8 GB.

- If this alarm is occasionally generated, increase the value by 0.5 times. If this alarm is frequently generated, double the value.
- In the case of large service volume and high service concurrency, you are advised to add instances.

Step 4 Click **Save**. Click **Instances**, select an FE instance whose configuration has expired, and choose **More** > **Restart Instance**.

Step 5 After restart, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, select **Doris** for the target cluster, and click **OK**.

Step 8 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

You need to manually clear the alarm after the fault is rectified.

Related Information

None.

1.3.486 ALM-50210 Maximum Compaction Score of All Doris BE Nodes Exceeds the Threshold

Alarm Description

The system checks the maximum compaction score of all BE nodes every 30 seconds. This alarm is generated when the maximum compaction score exceeds the threshold (50 by default).

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
50210	Major	Quality of service	Tenant plane	Doris	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	Alarm Severity	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the alarm triggering condition.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

Query or write may be delayed.

Possible Causes

The number of concurrent service requests is large in the cluster, or the compaction queue is small.

Handling Procedure

Check whether the alarm threshold or alarm trigger count is properly configured.

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Thresholds**, click the name of the desired cluster, and choose **Doris** > **Performance** > **Maximum compaction score of all BE nodes (BE)**.

Step 2 Click the edit button next to **Trigger Count**, change the number based on site requirements, and click **OK**.

Step 3 Click **Modify** in the **Operation** column, change the alarm threshold based on site requirements, and click **OK**.

Step 4 Wait 2 minutes and check whether the alarm is cleared in the alarm list.

- If yes, no further action is required.
- If no, go to **Step 5**.

Step 5 Choose **Cluster** > **Services** > **Doris** > **Configurations** > **All Configurations** > **BE(Role)** > **Customization**, add the **max_base_compaction_threads** parameter to **be.conf** with a value of **10**, and add the **max_cumu_compaction_threads** parameter with a value **20**.

Step 6 Click **Save**. Click **Instances**, select the BE instances whose configuration has expired, click **More**, and select **Restart Instance** to restart the Doris BE instances.

Step 7 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Collect fault information.

Step 8 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 9 Expand the **Service** drop-down list, select **Doris** for the target cluster, and click **OK**.

Step 10 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 11 Contact technical support and provide the collected logs.

----End

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.487 ALM-50211 Doris FE Queue Length of BE Periodic Report Tasks Exceeds the Threshold

Alarm Description

The system checks the queue length of each BE periodic report task on FE every 30 seconds. This alarm is generated when the queue length exceeds the threshold (10 by default). This value indicates the number of report tasks waiting on the master FE node. A large value indicates a poor FE processing capability.

This alarm is cleared when the system detects that the queue length of BE periodic report tasks on FE is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
50211	Minor	Quality of service	Tenant plane	Doris	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the alarm triggering condition.

Impact on the System

The processing capability of FE is insufficient, affecting the service query speed.

Possible Causes

The processing capability of the master FE node is insufficient due to a large number of concurrent service requests in the Doris cluster or insufficient memory for FE processes.

Handling Procedure

Check the GC duration.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. In the alarm list, view the role name and obtain the IP address of the instance in **Location** of the alarm whose ID is **50211**.

Step 2 Choose **Cluster** > **Services** > **Doris** > **Instances**, click the FE instance for which the alarm is generated, and click the **Chart** tab of the instance.

Select **JVM** from **Chart Category** on the left, and check whether **Accumulated GC duration of the old generation** of the FE process is greater than 3 seconds.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 Choose **Cluster** > **Services** > **Doris** > **Configurations** > **All Configurations** > **FE(Role)** > **JVM**, and increase the value of **-Xmx** in **FE_GC_OPTS**. The default value is **8GB**.

- If this alarm is generated occasionally, increase the value by 0.5 times. If this alarm is generated frequently, double the parameter value.
- In the case of large service volume and high service concurrency, you are advised to add instances.

Step 4 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check whether the alarm threshold or alarm trigger count is properly configured.

Step 5 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Thresholds**, click the name of the desired cluster, and choose **Doris** > **Queue** > **Queue Length of BE Periodic Report Tasks on the FE (FE)**.

Step 6 Click the edit button next to **Trigger Count**, change the number based on site requirements, and click **OK**.

Step 7 Click **Modify** in the **Operation** column, change the alarm threshold based on site requirements, and click **OK**.

Step 8 Wait 2 minutes and check whether the alarm is automatically cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Collect fault information.

Step 9 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 10 Expand the **Service** drop-down list, and select **Doris** for the target cluster.

Step 11 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.488 ALM-50212 Accumulated Old-Generation GC Duration of the Doris FE Process Exceeds the Threshold

Alarm Description

The system checks the accumulated old-generation GC duration of the FE process every 30 seconds. This alarm is generated when the accumulated GC duration exceeds the threshold (3000 ms by default).

This alarm is cleared when the system detects that the accumulated old-generation GC duration of the FE process is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
50212	Major	Quality of service	Tenant plane	Doris	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the alarm triggering condition.

Impact on the System

A long GC duration of the FE process may interrupt the services.

Possible Causes

The heap memory of the FE process is overused or inappropriately allocated, causing frequent occurrence of the GC process.

Handling Procedure

Check the GC duration.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**. In the alarm list, view the role name and obtain the IP address of the instance in **Location** of the alarm whose ID is **50212**.

Step 2 Choose **Cluster** > **Services** > **Doris** > **Instances**, click the FE instance for which the alarm is generated, and click the **Chart** tab of the instance.

Select **JVM** from **Chart Category** on the left, and check whether **Accumulated GC duration of the old generation** of the FE process is greater than 3 seconds.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 Choose **Cluster** > **Services** > **Doris** > **Configurations** > **All Configurations** > **FE(Role)** > **JVM**, and increase the value of **-Xmx** in **FE_GC_OPTS**. The default value is **8G**.

- If this alarm is occasionally generated, increase the value by 0.5 times. If this alarm is frequently generated, double the value.
- In the case of large service volume and high service concurrency, you are advised to add instances.

Step 4 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Collect fault information.

Step 5 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 6 Expand the **Service** drop-down list, and select **Doris** for the target cluster.

Step 7 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 30 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 8 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.489 ALM-50213 Number of Tasks Queuing in the Doris FE Thread Pool for Interacting with BE Exceeds the Threshold

Alarm Description

The system checks the number of queuing tasks in the FE thread pool for interacting with BE every 30 seconds. This alarm is generated when the number of queuing tasks exceeds the threshold (10 by default). This FE thread pool is the working thread pool of ThriftServer. It is specified by **rpc_port** in the **fe.conf** file and is used to interact with BE.

This alarm is cleared when the system detects that the number of tasks queuing in the FE thread pool for interacting with BE is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
50213	Minor	Quality of service	Tenant plane	Doris	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.

Type	Parameter	Description
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the alarm triggering condition.

Impact on the System

The read and write of the Doris service slows down.

Possible Causes

There are a large number of concurrent service requests, causing too many queuing tasks.

Handling Procedure

Check whether the alarm threshold or alarm trigger count is properly configured.

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Thresholds**, click the name of the desired cluster, and choose **Doris** > **Queue** > **Number of tasks that**

are queuing in the thread pool for interaction between the FE and the BE (FE).

Step 2 Click the edit button next to **Trigger Count**, change the number based on site requirements, and click **OK**.

Step 3 Click **Modify** in the **Operation** column, change the alarm threshold based on site requirements, and click **OK**.

Step 4 Wait 2 minutes and check whether the alarm is automatically cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Collect fault information.

Step 5 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 6 Expand the **Service** drop-down list, and select **Doris** for the target cluster.

Step 7 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 8 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.490 ALM-50214 Number of Tasks Queuing in the Doris FE Thread Pool for Task Processing Exceeds the Threshold

Alarm Description

The system checks the number of queuing tasks in the FE thread pool for processing tasks every 30 seconds. This alarm is generated when the number of queuing tasks exceeds the threshold (10 by default). This thread pool is used by the NIO MySQL Server to process tasks.

This alarm is cleared when the system detects that the number of tasks queuing in the FE thread pool for processing tasks is less than the threshold.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
50214	Minor	Quality of service	Tenant plane	Doris	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the alarm triggering condition.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

The task execution of the entire system becomes slow and blocked.

Possible Causes

Large tasks may block the task execution of the queue.

Handling Procedure

Check the execution status of FE tasks.

Step 1 On FusionInsight Manager, choose **Cluster** > **Services** > **Doris**. Click the **Chart** tab, select **Connection** from **Chart Category** in the left pane, and view the **FE MySQL Port Connections** chart. If the number of connections is large, click **Instances**, select the FE instance, and click the **Chart** tab. Select **CPU and Memory** from **Chart Category** and view the **CPU Usage of FE** chart. If the CPU usage is high, check the **Time** field in FE audit **log /var/log/Bigdata/audit/doris/fe/fe.audit.log** to collect statistics on the average task duration. If the value is also high, the alarm is caused by large concurrent tasks.

Step 2 After connecting to Doris, run the following command to check whether the default value of **queryTimeout** is too large. The default value is **300** seconds.

show variables like 'query_timeout';

- If yes, go to **Step 3**.
- If no, go to **Step 4**.

Step 3 Run the following command to shorten the timeout period based on site requirements to block the tasks that take a long time:

set global query_timeout=*xxx*;

Step 4 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Thresholds**, click the name of the desired cluster, and choose **Doris** > **Queue** > **Queue Length of Query Execution Thread Pool (BE)**.

Step 5 Click the edit button next to **Trigger Count**, change the number based on site requirements, and click **OK**.

Step 6 Click **Modify** in the **Operation** column, change the alarm threshold based on site requirements, and click **OK**.

Step 7 Wait 10 minutes and check whether the alarm is automatically cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Collect fault information.

Step 8 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 9 Expand the **Service** drop-down list, and select **Doris** for the target cluster.

Step 10 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 11 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.491 ALM-50215 Longest Duration of RPC Requests Received by Each Doris FE Thrift Method Exceeds the Threshold

Alarm Description

The system checks the longest duration of RPC requests received by each FE Thrift method every 30 seconds. This alarm is generated when the longest duration exceeds the threshold (5000 ms by default).

This alarm is cleared when the longest duration of RPC requests received by each FE Thrift method is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
50215	Major	Quality of service	Tenant plane	Doris	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the alarm triggering condition.

Impact on the System

A longer RPC duration indicates a higher performance load and slower network request processing, which may cause service congestion.

Possible Causes

- The network has a latency.
- There are too many concurrent large SQL tasks.

Handling Procedure

Step 1 Log in to the host where the faulty node is deployed as user **root** and run **ping** *IP addresses of all Doris nodes* to check whether the peer host can be pinged.

- If yes, go to **Step 3**.
- If no, go to **Step 2**.

Step 2 Contact the network administrator to restore the network.

Step 3 On FusionInsight Manager, choose **Cluster** > **Services** > **Doris**. Click the **Chart** tab, select **Connection** from **Chart Category** in the left pane, and view the **FE MySQL Port Connections** chart. If the number of connections is large, click **Instances**, select the FE instance, and click the **Chart** tab. Select **CPU and Memory** from **Chart Category** and view the **CPU Usage of FE** chart. If the CPU usage is high,

check the **Time** field in FE audit **log /var/log/Bigdata/audit/doris/fe/fe.audit.log** to collect statistics on the average task duration. If the value is also high, the alarm is caused by large concurrent tasks.

Step 4 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Thresholds**, click the name of the desired cluster, and choose **Doris** > **Performance** > **Longest duration of RPC requests received by each method of the FE thrift interface (FE)**.

Step 5 Click the edit button next to **Trigger Count**, change the number based on site requirements, and click **OK**.

Step 6 Click **Modify** in the **Operation** column, change the alarm threshold based on site requirements, and click **OK**.

Step 7 Wait 10 minutes and check whether the alarm is automatically cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Collect fault information.

Step 8 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 9 Expand the **Service** drop-down list, and select **Doris** for the target cluster.

Step 10 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 11 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.492 ALM-50216 Memory Usage of the Doris FE Node Exceeds the Threshold

Alarm Description

The system checks the memory usage of the FE node every 30 seconds. This alarm is generated when the memory usage exceeds the threshold (95% by default).

This alarm is cleared when the memory usage of the FE node falls below the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
50216	Major	Quality of service	Tenant plane	Doris	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
Modify	3.3.1	Alarm Severity: changed from Critical to Major.	Alarm Severity: Accuracy optimized

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the alarm triggering condition.

Impact on the System

Task execution and client connection to the FE are affected.

Possible Causes

The FE heap memory is too small.

Handling Procedure

Check the FE heap memory usage.

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Thresholds**, select the name of the desired cluster, and choose **Doris** > **CPU and Memory** > **Memory usage of the FE node (FE)**.

1. Click the edit button next to **Trigger Count**, change the number based on site requirements, and click **OK**.
2. Click **Modify** in the **Operation** column, change the alarm threshold based on site requirements, and click **OK**.

Step 2 Log in to the FE node for which the alarm is generated as user **omm**, run the **top** command to check the memory usage of processes, locate the process with high memory usage, and check whether the process belongs to the current service and is running properly.

- If yes, go to **Step 3**.
- If no, isolate or stop the process, or adjust the memory size, and check whether the memory is released.

Step 3 Restart the affected services or instances and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 4**.

Collect fault information.

Step 4 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 5 Expand the **Service** drop-down list, and select **Doris** for the target cluster.

Step 6 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 7 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.493 ALM-50217 Heap Memory Usage of the Doris FE Node Exceeds the Threshold

Alarm Description

The system checks the heap memory usage of the FE node every 30 seconds. This alarm is generated when the heap memory usage exceeds the threshold (95% by default).

This alarm is cleared when the heap memory usage of the FE node falls below the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
50217	Major	Quality of service	Tenant plane	Doris	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
Modify	3.3.1	Alarm Severity: changed from Critical to Major.	Alarm Severity: Accuracy optimized

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the alarm triggering condition.

Impact on the System

Task execution and client connection to the FE are affected.

Possible Causes

The FE heap memory is too small.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Handling Procedure

Check heap memory usage.

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Thresholds**, select the name of the desired cluster, and choose **Doris** > **CPU and Memory** > **Heap memory usage of the FE node (FE)**.

1. Click the edit button next to **Trigger Count**, change the number based on site requirements, and click **OK**.
2. Click **Modify** in the **Operation** column, change the alarm threshold based on site requirements, and click **OK**.

Step 2 On FusionInsight Manager, choose **Cluster** > **Services** > **Doris** > **FE** > **Configurations** > **All Configurations**, search for the **FE_GC_OPTS** parameter, increase the value of **-Xmx** as required, click **Save**, and click **OK**.

NOTE

- If this alarm is generated, the heap memory configured for the current Doris instance is not enough for data transmission. You are advised to open the instance monitoring page, display the Doris heap memory resource status monitoring chart, and observe the change trend of the heap memory used by Doris in the monitoring chart. Then change the value of **-Xmx** to twice the current heap memory usage or to another value to meet site requirements.
- When setting the heap memory, you can set **-Xms** and **-Xmx** to approximately the same value to prevent performance deterioration caused by heap size adjustment after each GC.
- The sum of **-Xmx** and **XX:MaxPermSize** cannot be greater than the actual physical memory of the node server.

Step 3 Restart the affected services or instances and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 4**.

Collect fault information.

Step 4 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 5 Expand the **Service** drop-down list, and select **Doris** for the target cluster.

Step 6 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 7 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

1.3.494 ALM-50219 Length of the Queue in the Thread Pool for Doris Query Execution Exceeds the Threshold

Alarm Description

The system checks the length of the waiting queue in the query execution thread pool every 30 seconds. This alarm is generated when the length exceeds the threshold (20 by default).

This alarm is cleared when the length of the waiting queue in the current query execution thread pool is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
50219	Major	Quality of service	Tenant plane	Doris	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the alarm triggering condition.

Impact on the System

The task execution of the entire system becomes slow and blocked.

Possible Causes

Large tasks may block the task execution of the queue.

Handling Procedure

Check the execution status of tasks.

Step 1 On FusionInsight Manager, choose **Cluster** > **Services** > **Doris**. Click the **Chart** tab, select **Connection** from **Chart Category** in the left pane, and view the **FE MySQL Port Connections** chart. If the number of connections is large, click **Instances**, select the FE instance, and click the **Chart** tab. Select **CPU and Memory** from **Chart Category** and view the **CPU Usage of FE** chart. If the CPU usage is high, check the **Time** field in FE audit **log /var/log/Bigdata/audit/doris/fe/fe.audit.log** to collect statistics on the average task duration. If the value is also high, the alarm is caused by large concurrent tasks.

Step 2 After connecting to Doris, run the following command to check the **queryTimeout** value of the system:

show variables like 'query_timeout';

If the value is too large, run the **set global query_timeout=*xxx*;** command to shorten the timeout interval and block tasks that last for a long time.

Step 3 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Thresholds**, click the name of the desired cluster, and choose **Doris** > **Queue** > **Queue Length of Query Execution Thread Pool (BE)**.

Step 4 Click the edit button next to **Trigger Count**, change the number based on site requirements, and click **OK**.

Step 5 Click **Modify** in the **Operation** column, change the alarm threshold based on site requirements, and click **OK**.

Step 6 Wait 10 minutes and check whether the alarm is automatically cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Collect fault information.

Step 7 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 8 Expand the **Service** drop-down list, and select **Doris** for the target cluster.

Step 9 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.495 ALM-50220 Error Rate of Doris TCP Packet Receiving Exceeds the Threshold

Alarm Description

The system checks the rate of TCP packet receiving errors every 30 seconds. This alarm is generated when the error rate exceeds the threshold (5% by default).

This alarm is cleared when the error rate is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
50220	Critical	Quality of service	Tenant plane	Doris	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the alarm triggering condition.

Impact on the System

The task fails or data is lost.

Possible Causes

The network is faulty, so data cannot be sent.

Handling Procedure

Step 1 Log in to the host where the faulty node is deployed as user **root** and run **ping** *IP addresses of all Doris nodes* to check whether the peer host can be pinged.

- If yes, go to **Step 4**.
- If no, go to **Step 2**.

Step 2 Contact the network administrator to restore the network.

Step 3 Wait for a while and check whether the alarm is cleared in the alarm list.

- If yes, no further action is required.
- If no, go to **Step 4**.

Collect fault information.

Step 4 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 5 Expand the **Service** drop-down list, and select **Doris** for the target cluster.

Step 6 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 7 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.496 ALM-50221 Doris BE Data Disk Usage Exceeds the Threshold

Alarm Description

The system checks the usage of BE data disks every 30 seconds. This alarm is generated when the disk usage exceeds the threshold (95% by default).

This alarm is cleared when the system detects that the disk usage is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
50221	Major	Quality of service	Tenant plane	Doris	Yes

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Changes

Change Type	Version	Description	Reason for Change
Modify	3.3.1	Alarm Severity: changed from Critical to Major.	Alarm Severity: Accuracy optimized

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the alarm triggering condition.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

New data fails to be written, and the task is interrupted.

Possible Causes

- The disk space of the cluster is full.
- Data skew occurs among BE nodes.

Handling Procedure

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**, and view the role name and the IP address for the hostname in **Location**.

Step 2 Expand the disk capacity of the node for which the alarm is generated. For details, see Doris-related chapters in MapReduce Service (MRS) 3.3.1-LTS Physical Machine Cluster Capacity Expansion Guide (for Huawei Cloud Stack 8.3.1).

Step 3 Go to **Step 4** if the expansion fails or the alarm persists after the expansion.

Collect fault information.

Step 4 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 5 Expand the **Service** drop-down list, and select **Doris** for the target cluster.

Step 6 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the abnormal host, and click **OK**.

Step 7 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 8 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.497 ALM-50222 Disk Status of a Specified Data Directory on Doris BE Is Abnormal

Alarm Description

The system checks the disk status of a specified data directory on BE every 30 seconds. This alarm is generated when the disk status is not **1** (**1** indicates the normal state and **0** indicates the abnormal state). This alarm is cleared when the disk status of the specified data directory on BE becomes normal.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
50222	Critical	Quality of service	Tenant plane	Doris	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the alarm triggering condition.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Impact on the System

Service data may be unavailable, and data queries on the Doris client may fail.

Possible Causes

- The hard disk is faulty.
- The disk permissions are set incorrectly.

Handling Procedure

Check whether a disk alarm is generated.

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** and check whether **ALM-12014 Partition Lost** or **ALM-12033 Slow Disk Fault** exists.

- If yes, go to **Step 2**.
- If no, go to **Step 4**.

Step 2 Rectify the fault by referring to the handling procedure of **ALM-12014 Partition Lost** or **ALM-12033 Slow Disk Fault**. Then, check whether the alarm is cleared.

- If yes, go to **Step 3**.
- If no, go to **Step 4**.

Step 3 Wait 5 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 4**.

Modify disk permissions.

Step 4 Choose **O&M** > **Alarm** > **Alarms** and view **Location** and **Additional Information** of the alarm to obtain the location of the faulty disk.

Step 5 Log in to the node for which the alarm is generated as user **root**. Go to the directory where the faulty disk is located, and run the **ll** command to check whether the permission for the faulty disk is **711** and whether the user is **omm**.

- If yes, go to **Step 7**.
- If no, go to **Step 6**.

Step 6 Modify the permission of the faulty disk. For example, if the faulty disk is **data1**, run the following commands:

chown omm:wheel data1

chmod 711 data1

Step 7 Choose **Cluster** > **Services** > **Doris** > **Instances**, select this BE instance, click **More**, and select **Restart Instance**. Wait 5 minutes and check whether an alarm is generated.

- If no, no further action is required.
- If yes, go to **Step 8**.

Collect fault information.

Step 8 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 9 Expand the **Service** drop-down list, and select **Doris** and **OMS** for the target cluster.

Step 10 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 20 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 11 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.498 ALM-50223 Maximum Memory Required by Doris BE Is Greater Than the Remaining Memory of the Machine

Alarm Description

The system checks whether the maximum memory required by BE is greater than the available memory every 30 seconds. This alarm is generated when the value is not **1** (**1** indicates that the maximum required memory is less than or equal to the available memory, and **0** indicates that the maximum required memory is greater than the available memory).

This alarm is cleared when the maximum required memory is less than or equal to the available memory.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
50223	Major	Error handling	Tenant plane	Doris	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.

Type	Parameter	Description
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the alarm triggering condition.

Impact on the System

A task may fail to apply for memory when running.

Possible Causes

Too much BE node memory has been occupied by other processes, or the maximum memory set for the BE service is too large.

Handling Procedure

Check whether the maximum memory set for the BE node is proper.

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Thresholds**, click the name of the desired cluster, and choose **Doris** > **CPU and Memory** > **Relationship**

between the maximum memory size of the BE and the remaining memory size of the machine (BE).

Step 2 Click the edit button next to **Trigger Count**, change the number based on site requirements, and click **OK**.

Step 3 Click **Modify** in the **Operation** column, change the alarm threshold based on site requirements, and click **OK**.

Step 4 Wait 2 minutes and check whether the alarm is automatically cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Step 5 Log in to the BE node for which the alarm is generated as user **omm**, run the **top** command to check the memory usage of processes, locate the process with high memory usage, and check whether the process belongs to the current service and is running properly.

- If yes, go to **Step 6**.
- If no, isolate or stop the process, or adjust the memory size, and check whether the memory is released.

Step 6 Log in to the BE node for which the alarm is generated as user **omm** and run the **free -g** command to check the total memory and remaining memory in the system and estimate the memory usage.

Step 7 On FusionInsight Manager, choose **Cluster** > **Services** > **Doris** > **Configurations** > **All Configurations** > **BE(Role)** > **Memory** and decrease the value of **mem_limit**. This parameter specifies the maximum memory allowed for BE. Then save the modification and restart the BE instance.

Step 8 After the BE instance is restarted, wait 5 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 9**.

Collect fault information.

Step 9 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 10 Expand the **Service** drop-down list, and select **Doris** for the target cluster.

Step 11 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.499 ALM-50224 Failures a Certain Task Type on Doris BE Are Increasing

Alarm Description

The system checks whether the number of failed tasks of a certain type on BE is increasing every 30 seconds. This alarm is generated when the system detects that the value is not **1** (**1** indicates that the number of failed tasks of a certain type does not increase, and **0** indicates that the failed tasks of a certain type are increasing).

This alarm is cleared when the system detects that the number of failed tasks of a certain type on BE does not increase.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
50224	Major	Error handling	Tenant plane	Doris	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the alarm triggering condition.

Impact on the System

A task fails to be executed repeatedly in a certain scenario.

Possible Causes

A BE exception may occur. As a result, the number of failed tasks increases in a certain scenario.

Handling Procedure

Check whether the alarm threshold or alarm trigger count is properly configured.

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Thresholds**, click the name of the desired cluster, and choose **Doris** > **Exception** > **Check whether the number of failed tasks of a certain type increases (BE)**.

Step 2 Click the edit button next to **Trigger Count**, change the number based on site requirements, and click **OK**.

Step 3 Click **Modify** in the **Operation** column, change the alarm threshold based on site requirements, and click **OK**.

Step 4 Wait 2 minutes and check whether the alarm is automatically cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Collect fault information.

Step 5 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 6 Expand the **Service** drop-down list, select **Doris** for the target cluster, and click **OK**.

Step 7 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 8 Contact technical support and provide the collected logs.

----End

Alarm Clearance

You need to manually clear the alarm after the fault is rectified.

Related Information

None.

1.3.500 ALM-50225 Unavailable Doris FE Instances

Alarm Description

The system checks the FE process status every 30 seconds. This alarm is generated when the value is greater than **0** (**0** indicates that the FE process is normal and **1** indicates that the FE process is abnormal).

This alarm is cleared when the system detects that the FE process becomes normal.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
50225	Critical	Error handling	Tenant plane	Doris	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.

Type	Parameter	Description
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the alarm triggering condition.

Impact on the System

The FE instance is unavailable and cannot respond to client requests.

Possible Causes

- The FE instance is faulty or restarted.
- The local disk space of FE nodes is insufficient.
- FE node memory is insufficient.

Handling Procedure

View the FE instance status.

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Alarms**. In the alarm list, view the role name and obtain the IP address of the instance in **Location** of the alarm whose ID is **50225**.

Step 2 Choose **Cluster** > **Services** > **Doris** > **Instances**, click the FE instance for which the alarm is generated, and check whether **Running Status** of the instance is **Unknown** or **Restoring**.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 Return to the **Instances** page, select the FE instance, and choose **More** > **Restart Instance**.

Step 4 After the FE instance is restarted, choose **O&M** > **Alarm** > **Alarms**. In the alarm list, check whether alarm "Unavailable Doris FE Instances" is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

View the local disk space of FE.

Step 5 Log in to the node where the FE instance queried in **Step 1** is deployed and check the value of **meta_dir** in the **${BIGDATA_HOME}/FusionInsight_Doris_*/*_*_FE/etc/fe.conf** file.

For example, the value of **meta_dir** is as follows:

```
meta_dir = /srv/BigData/doris_fe/doris-meta
```

Step 6 Run the following command to check whether the disk usage of **meta_dir** reaches 100%:

df -h */srv/BigData/doris_fe/doris-meta*

For example, the following command output indicates that the disk usage of **meta_dir** is 40%:

```
Filesystem      Size  Used Avail Use% Mounted on
/dev/vda2        98G   37G   57G  40% /
```

- If yes, go to **Step 7**.
- If no, go to **Step 8**.

Step 7 Delete unnecessary information from the directory to ensure that the over 80% of disk space is available. Wait for several minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

View the FE node memory.

Step 8 Log in to FusionInsight Manager, choose **Cluster** > **Services** > **Doris** > **Instances**. Click the FE instance for which the alarm is generated, click **Chart**, select **CPU and Memory** from the chart category, and check whether the FE memory usage reaches 100%.

- If yes, go to **Step 9**.
- If no, go to **Step 10**.

Step 9 If the FE memory usage is too high, the processes connected to the FE service will be stopped and the occupied resources will be released. Wait for several minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 10**.

Collect fault information.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 10 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 11 Expand the **Service** drop-down list, select **Doris** for the target cluster, and click **OK**.

Step 12 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 13 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.501 ALM-50226 Unavailable Doris BE Instances

Alarm Description

The system checks the BE process status every 30 seconds. This alarm is generated when the value is greater than **0** (**0** indicates that the BE process is normal and **1** indicates that the BE process is abnormal).

This alarm is cleared when the system detects that the BE process becomes normal.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
50226	Critical	Error handling	Tenant plane	Doris	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.

Type	Parameter	Description
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the alarm triggering condition.

Impact on the System

The BE instance is unavailable and cannot provide the data read and write functions.

Possible Causes

- The BE instance is faulty or restarted.
- The BE node disks are abnormal.
- The local disk space of BE nodes is insufficient.

Handling Procedure

View the BE instance status.

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Alarms**. In the alarm list, view the role name and obtain the IP address of the instance in **Location** of the alarm whose ID is **50226**.

Step 2 Choose **Cluster** > **Services** > **Doris** > **Instances**, click the BE instance for which the alarm is generated, and check whether **Running Status** of the instance is **Unknown** or **Restoring**.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 Return to the **Instances** page, select the BE instance, and choose **More** > **Restart Instance**.

Step 4 After the BE instance is restarted, choose **O&M** > **Alarm** > **Alarms**. In the alarm list, check whether alarm "Unavailable Doris BE Instances" is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Check BE node disks.

Step 5 In the alarm list, check whether the BE instances listed in **Step 1** report the "Disk Status of a Specified Data Directory on Doris BE Is Abnormal" alarm.

- If yes, go to **Step 6**.
- If no, go to **Step 8**.

Step 6 Contact technical support to repair the disk.

Step 7 In the alarm list, check whether the "Unavailable Doris BE Instances" alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 8**.

Check the local disk space of BE nodes.

Step 8 In the alarm list, check whether the BE instance in **Step 1** reports the "Doris BE Data Disk Usage Exceeds the Threshold" alarm.

- If yes, go to **Step 9**.
- If no, go to **Step 11**.

Step 9 Perform the following operations to increase the BE disk space:

- Check the value of **storage_root_path** in the **${BIGDATA_HOME}/FusionInsight_Doris_*/*_*_BE/etc/be.conf** file and mount more disks to the directory as you need.
- Delete data from partitions that are no longer used in the table based on service demand.
- On FusionInsight Manager, choose **Cluster** > **Service** > **Doris** > **Instances** > **Add Instance**, and add BE nodes as you need.
- After the MySQL client is connected to Doris, run the following command to reduce the number of table replicas based on service demand:

  alter table *tblName* **set ("replication_allocation" = "tag.location.default:** *xxx***");**

Step 10 In the alarm list, check whether the "Unavailable Doris BE Instances" alarm is cleared.

- If yes, no further action is required.

- If no, go to **Step 11**.

Collect fault information.

Step 11 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 12 Expand the **Service** drop-down list, select **Doris** for the target cluster, and click **OK**.

Step 13 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 14 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.502 ALM-50227 Concurrent Doris Tenant Queries Exceeds the Threshold

Alarm Description

The system checks concurrent tenant queries on FE nodes every 30 seconds. This alarm is generated when the number exceeds the threshold (90% by default).

This alarm is cleared when the number of concurrent queries from the FE nodes falls below the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
50227	Major	Quality of service	Tenant plane	Doris	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
New	3.3.1	New alarm	New alarm

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the alarm triggering condition.

Impact on the System

Too many concurrent queries consume a large number of system resources. This leads to slow response and even request rejection.

Possible Causes

There is a large amount of service requests.

Handling Procedure

Check the actual number of concurrent tenant queries on FE nodes.

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Alarms**. In the alarm list, view the role name and obtain the IP address of the instance in **Location** of the alarm whose ID is **50227**.

Step 2 Choose **Cluster** > **Services** > **Doris** > **Instances**, select the FE instance for which the alarm is generated, and click **Chart**. Click **Tenant Resource** in the **Chart Category** pane, and check whether the actual number of concurrent queries in the **Number of Concurrent Tenant Queries** chart is greater than the threshold. The default value is 90%.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 Check whether a large number of tasks were being executed during the alarm period.

- If yes, go to **Step 4**.
- If no, go to **Step 5**.

Step 4 On FusionInsight Manager, choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Doris** > **Tenant Resources**. Increase the threshold value and trigger counts based on service requirements. Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Collect fault information.

Step 5 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 6 Expand the **Service** drop-down list, and select **Doris** for the target cluster.

Step 7 Expand the **Hosts** drop-down list. In the **Select Host** dialog box that is displayed, select the abnormal host, and click **OK**.

Step 8 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

1.3.503 ALM-50228 Memory Usage of a Doris Tenant Exceeds the Threshold

Alarm Description

The system checks the memory usage of BE nodes every 30 seconds. This alarm is generated when the memory usage of a tenant exceeds the threshold.

This alarm is cleared when the system detects that the memory usage of tenant's BE nodes is lower than the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
50228	Critical (default threshold: 90%) Major (default threshold: 85%)	Quality of service	Tenant plane	Doris	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
New	3.3.1	New alarm	New alarm

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the alarm triggering condition.

Impact on the System

Processes respond slowly or do not work.

Possible Causes

The data queried by the tenant is too large, and memory soft limit is not enabled.

Handling Procedure

Check the memory used by the BE nodes of the tenant.

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Alarms**. In the alarm list, view the role name and obtain the IP address of the instance in **Location** of the alarm whose ID is **50228**.

Step 2 Click **Thresholds** and choose *Name of the desired cluster* > **Doris** > **Tenant Resources** > **Memory Usage Exceeds Threshold** to view and record the threshold.

Step 3 Choose **Cluster** > **Services** > **Doris** > **Instances**, select the BE instance for which the alarm is generated, click **Chart**. Click **Tenant Resource** from the **Chart Category** pane, and check whether the actual memory usage in the **Memory Used by Tenants** chart is greater than the threshold obtained in **Step 2**, record the name of the tenant whose memory usage exceeds the threshold.

- If yes, go to **Step 3**.
- If no, go to **Step 8**.

Step 4 Check whether a large amount of table data were being queried during the alarm period.

- If yes, go to **Step 5**.
- If no, go to **Step 8**.

Step 5 Choose **Tenant Resources** > **Tenant Resources Management**. In the tenant list, click the tenant name in **Step 2**, and then the **Resource** tab. Click the edit button on the right of **Resource Details**, and check whether **Memory Soft Limit** is enabled.

- If yes, go to **Step 7**.
- If no, go to **Step 6**.

Step 6 Enable **Soft Memory Limit** and click **OK**. Check whether the alarm is cleared in the alarm list.

- If yes, no further action is required.
- If no, go to **Step 7**.

Step 7 Choose **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Doris** > **Tenant Resources**. Increase the threshold value and trigger counts based on service requirements. Check whether the alarm is cleared in the alarm list.

- If yes, no further action is required.
- If no, go to **Step 8**.

Collect fault information.

Step 8 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 9 Expand the **Service** drop-down list, and select **Doris** for the target cluster.

Step 10 In the Host area, select the host to which the role belongs and click OK.

Step 11 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.504 ALM-50229 Doris FE Failed to Connect to OBS

Alarm Description

The system checks whether the connection between the Doris FE nodes and OBS is available every 30 seconds. This alarm is generated when the connection status code is not 0.

This alarm is cleared when the connection status code is 0.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
50229	Critical	Environment	Tenant plane	Doris	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
New	3.3.1	New alarm	New alarm

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the alarm triggering condition.

Impact on the System

Some functions of Doris are unavailable, for example, cold-hot separation and Hive OBS Catalog.

Possible Causes

- The obtained AK/SK is invalid.
- This alarm is generated when OBS connection fails.

Handling Procedure

Determine the cause.

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Alarms**. In the alarm list, view the role name and obtain the IP address of the instance in **Location** of the alarm whose ID is **50229**, and check the **CurrentValue** in **Additional Information**.

- If **CurrentValue** is **2**, the obtained AK/SK is invalid. Go to **Step 2**.
- If **CurrentValue** is **3**, OBS fails to be connected. Go to **Step 7**.

The obtained AK/SK is invalid.

Step 2 Log in to ManageOne Operation Portal, click the username in the upper right corner, and select **My Settings** from the drop-down list.

Step 3 On the displayed page, click **Access Keys**. In the list, check whether the ID in the **Access Key ID** column contains the AK value.

- If yes, go to **Step 7**.
- If no, go to **Step 4**.

Step 4 Click **Create Access Key** and click **OK**. Download the new access key and obtain the AK and SK.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 5 Set the **obs.access_key** and **obs.secret_key** parameters to the obtained AK/SK.

Step 6 Wait for about 1 minute, log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**, and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Failed to connect to OBS.

Step 7 Check whether the network connection between the cluster and OBS is normal. For details, see "Initializing the Configuration" in the obsutil tool guide.

- If yes, go to **Step 8**.
- If no, go to **Step 12**.

Step 8 Log in to ManageOne Operation Portal, choose **Organization** > **VDCs**, and click the VDC name of cluster in the list.

Step 9 Choose **User Groups**, click each user group, and check whether the IAM user synchronized from the cluster exists in a user group.

- If yes, go to **Step 12**.
- If no, go to **Step 10**.

Step 10 Add IAM users and grant permissions by following the instructions provided in the user guide.

Step 11 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**, and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 12**.

Step 12 Contact technical support for fault diagnosis and rectification.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.505 ALM-50230 Doris BE Cannot Connect to OBS

Alarm Description

The system checks whether the connection between the Doris BE nodes and OBS is available every 30 seconds. This alarm is generated when the connection status code is not 0.

This alarm is cleared when the connection status code is 0.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
50230	Critical	Environment	Tenant plane	Doris	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
New	3.3.1	New alarm	New alarm

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Detail	Specifies the alarm triggering condition.

Impact on the System

Some functions of Doris are unavailable, for example, cold-hot separation and Hive OBS Catalog.

Possible Causes

- The obtained AK/SK is invalid.
- This alarm is generated when OBS connection fails.

Handling Procedure

Determine the cause.

Step 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Alarms**. In the alarm list, view the role name and obtain the IP address of the instance in **Location** of the alarm whose ID is **50229**, and check the **CurrentValue** in **Additional Information**.

- If **CurrentValue** is **2**, the obtained AK/SK is invalid. Go to **Step 2**.
- If **CurrentValue** is **3**, OBS fails to be connected. Go to **Step 7**.

The obtained AK/SK is invalid.

Step 2 Log in to ManageOne Operation Portal, click the username in the upper right corner, and select **My Settings** from the drop-down list.

Step 3 On the displayed page, click **Access Keys**. In the list, check whether the ID in the **Access Key ID** column contains the AK value.

- If yes, go to **Step 7**.
- If no, go to **Step 4**.

Step 4 Click **Create Access Key** and click **OK**. Download the new access key and obtain the AK and SK.

Step 5 Set the **obs.access_key** and **obs.secret_key** parameters to the obtained AK/SK.

Step 6 Wait for about 1 minute, log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**, and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 7**.

Failed to connect to OBS.

Step 7 Check whether the network connection between the cluster and OBS is normal. For details, see "Initializing the Configuration" in the obsutil tool guide.

- If yes, go to **Step 8**.
- If no, go to **Step 12**.

Step 8 Log in to ManageOne Operation Portal, choose **Organization** > **VDCs**, and click the VDC name of cluster in the list.

Step 9 Choose **User Groups**, click each user group, and check whether the IAM user synchronized from the cluster exists in a user group.

- If yes, go to **Step 12**.
- If no, go to **Step 10**.

Step 10 Add IAM users and grant permissions by following the instructions provided in the user guide.

Step 11 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**, and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 12**.

Step 12 Contact technical support for fault diagnosis and rectification.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.506 ALM-50401 Number of JobServer Waiting Tasks Exceeds the Threshold

Alarm Description

The system checks the number of jobs submitted to JobServer every 30 seconds. This alarm is generated when the number of jobs to be executed exceeds 800.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
50401	Critical (default threshold: 900) Major (default threshold: 800)	Quality of service	Tenant plane	JobGateway	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

Too many JobServer tasks are detected in the queue. For details about the task queue usage, see the additional information field of this alarm. The impacts are as follows:

1. When the number of JobServer tasks in the queue reaches the maximum (1000 by default), new tasks cannot be added.
2. Before the number of JobServer tasks in the queue reaches the maximum, new JobServer tasks cannot be submitted quickly. For example, it takes more time (even hours) to submit tasks in the queue or new tasks to YARN. The time for submitting a new task to the Yarn component is prolonged, which may reach the hour level.

Possible Causes

Too many jobs are submitted instantaneously.

Handling Procedure

Step 1 Log in to FusionInsight Manager and choose **Cluster** > **Services** > **JobGateway**.

Step 2 Click the **Instance** tab, click **Add Instance**, and add JobServer instances based on the number of submitted jobs.

Step 3 After the instances are added, restart the JobGateway service.

Step 4 Wait 5 minutes and check whether the alarm is automatically cleared.

If yes, no further action is required.

If no, go to **Step 5**.

Collect fault information.

Step 5 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 6 Expand the **Service** drop-down list, and select **JobGateway** for the target cluster.

Step 7 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 8 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.507 ALM-50402 JobGateway Service Unavailable

Alarm Description

The system checks the JobGateway service status every 60 seconds. This alarm is generated when the JobGateway service is abnormal.

This alarm is cleared when the JobGateway service recovers.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
50402	Critical	Error handling	Tenant plane	JobGateway	Yes

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

Users cannot use the job functions related to the JobGateway component. For example, jobs cannot be submitted, terminated, or viewed on the MRS management plane, and MRS job management APIs (V2) cannot be called.

Possible Causes

The node where the JobGateway service locates is faulty.

Handling Procedure

Step 1 Log in to FusionInsight Manager, choose **Cluster** > **Services** > **JobGateway**, and click the **Instance** tab. Check for JobServer or JobBalancer instances that are faulty or not started and view the host names of these instances.

Step 2 On the **Alarm** page of FusionInsight Manager, check whether the **NodeAgent Process Is Abnormal** alarm is generated.

- If yes, go to **Step 3**.
- If no, go to **Step 6**.

Step 3 Check whether the host name in the alarm information is the same as the host name in **Step 1**.

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 4 Clear the alarm by following the instructions provided in **ALM-12006 NodeAgent Process Is Abnormal**.

Step 5 In the alarm list, check whether alarm **JobGateway Service Unavailable** is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Expand the **Service** drop-down list, and select **JobGateway** for the target cluster.

Step 8 Click in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 9 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None.

1.3.508 ALM-51201 LakeSearch Unavailable

Alarm Description

The system checks the LakeSearch service availability every 60 seconds. This alarm is generated when the system detects that the LakeSearch service is unavailable. The alarm is cleared when the LakeSearch service recovers.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
51201	Critical	Error handling	Tenant plane	LakeSearch	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
New	3.3.1	New alarm	New alarm

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.

Impact on the System

LakeSearch cannot provide services for external systems.

Possible Causes

The component on which LakeSearch depends is unavailable.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Handling Procedure

Check the running status of DBService, KrbServer, HBase, and Elasticsearch on which LakeSearch depends.

Step 1 Log in to FusionInsight Manager and choose **Cluster** > **Services**.

Step 2 Check whether **Running Status** of DBService, KrbServer, HBase, and Elasticsearch is **Normal**.

- If yes, go to **Step 6**.
- If no, go to **Step 3**.

Step 3 Click the name of a component whose **Running Status** is not **Normal**.

Step 4 In the **Instances** tab, select the faulty instance, choose **More** > **Restart Instance**, and check whether the instance can be started successfully.

- If yes, go to **Step 5**.
- If no, go to **Step 6**.

Step 5 Wait for one minute and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 6**.

Collect fault information.

Step 6 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 7 Select **LakeSearch** for **Service** and click **OK**.

Step 8 In the **Hosts** area, select the host where the role is located.

Step 9 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 1 hour ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 10 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

1.3.509 ALM-51202 LakeSearch Heap Memory Usage Exceeds the Threshold

Alarm Description

The system checks the heap memory usage of LakeSearch every 60 seconds. This alarm is generated when the number of times that the heap memory usage exceeds the threshold reaches the alarm trigger count.

If **Trigger Count** is **1**, this alarm is cleared when LakeSearch heap memory usage is less than or equal to the threshold. If **Trigger Count** is greater than **1**, this alarm is cleared when LakeSearch heap memory usage is less than or equal to 90% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
51202	Critical (default threshold: 95%) Major (default threshold: 90%)	Quality of service	Tenant plane	LakeSearch	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
New	3.3.1	New alarm	New alarm

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold for triggering the alarm.

Impact on the System

If the available LakeSearch heap memory is insufficient, the LakeSearch semantic search performance is affected, and even memory overflow occurs. As a result, the LakeSearch instance process becomes unavailable.

Possible Causes

LakeSearch heap memory is insufficient.

Handling Procedure

Check the LakeSearch JVM memory configuration and adjust it.

Step 1 Log in to FusionInsight Manager and choose **Cluster** > **Services** > **LakeSearch**. Click **Configurations** and click **All Configurations**.

Step 2 In the upper right corner of the configuration page, enter **GC_OPTS** in the search box. The **GC_OPTS** parameters of all instances are displayed.

Step 3 Select the instance whose parameter **GC_OPTS** needs to be modified, and check whether the differentiated configuration icon is displayed next to the instance value configuration box.

- If the icon is displayed, go to **Step 4**.
- If the icon is not displayed, go to **Step 5**.

Step 4 Click . In the displayed dialog box, click on the right and click **OK**.

Step 5 Change the values of **-Xms** and **-Xmx** of the **GC_OPTS** parameter by referring to the following note.

NOTE

Suggestions on GC parameter settings for LakeSearch instances:

- Change the values of **-Xms** and **-Xmx** of the **GC_OPTS** parameter to **8G**.
- Set **-Xms** and **-Xmx** to the same value to prevent dynamic adjustment of the heap memory size, which may affect performance.

Step 6 After the modification, click **Save** in the upper left corner. In the displayed dialog box, click **OK**.

Step 7 Click **Instances**, select the instances whose configuration status is **Expired**, and choose **More** > **Restart Instance** to restart them as prompted.

Step 8 Wait for one minute and check whether the alarm is cleared.

- If the alarm is cleared, no further action is required.
- If the alarm is not cleared, go to **Step 9**.

Collect fault information.

Step 9 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 10 Expand the **Service** drop-down list, and select **LakeSearch** for the target cluster.

Step 11 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 12 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.3.510 ALM-51203 GC Duration of the LakeSearch Instance Exceeds the Threshold

Alarm Description

The system checks the garbage collection (GC) duration of the LakeSearch instance process every 60 seconds. This alarm is generated when the GC duration exceeds the threshold (30 seconds by default).

If **Trigger Count** is **1**, this alarm is cleared when the GC duration of the LakeSearch instance process is less than or equal to the threshold. If **Trigger Count** is greater than **1**, this alarm is cleared when the GC duration of the LakeSearch instance process is less than or equal to 90% of the threshold.

Alarm Attributes

Alarm ID	Alarm Severity	Alarm Type	Alarm Category	Service Type	Auto Cleared
51203	Major	Quality of service	Tenant plane	LakeSearch	Yes

Alarm Changes

Change Type	Version	Description	Reason for Change
New	3.3.1	New alarm	New alarm

Alarm Parameters

Type	Parameter	Description
Location Information	Region	Specifies the region where the alarm was generated.
	CloudService	Specifies the cloud service for which the alarm was generated.
	MicroServiceInstance	Specifies the microservice for which the alarm was generated.
	RegionId	Specifies the ID of the region where the alarm was generated.
	DomainId	Specifies the ID of the domain where the alarm was generated.
	ClusterId	Specifies the ID of the cluster where the alarm was generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Parameter	Description
	TenantId	Specifies the ID of the tenant for which the alarm was generated.
	UserName	Specifies the user for which the alarm was generated.
	Source	Specifies the source in the cluster for which the alarm was generated.
	ServiceName	Specifies the cluster service for which the alarm was generated.
	RoleName	Specifies the role for which the alarm was generated.
	HostName	Specifies the host for which the alarm was generated.
	AlarmLevel	Specifies the alarm severity.
Additional Information	CloudService	Specifies the cloud service for which the alarm was generated.
	Trigger Condition	Specifies the threshold for triggering the alarm.

Impact on the System

A long GC duration of the LakeSearch instance process may interrupt the services.

Possible Causes

Service load of the LakeSearch instance on the node is high or the heap memory is not properly configured. As a result, GC frequently occurs.

Handling Procedure

Check the heap memory of the instance.

Step 1 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**, expand alarm "GC Duration of the LakeSearch Instance Exceeds the Threshold", and check the **HostName** in **Location**.

Step 2 Choose **Cluster** > **Services** > **LakeSearch**, click **Instances**, and click the SearchServer and SearchFactory instance names corresponding to the host for which the alarm is generated. On the displayed page, check whether the GC duration is continuously greater than the threshold by checking **SearchServer GC Duration Statistics** and **SearchFactory GC Duration Statistics** displayed in charts. If related charts do not exist, click the triangle icon next to the time editing button in the chart area, click **Customize**. On the displayed page, click **Garbage Collection**, select the charts, and click **OK**.

- If the GC duration is continuously greater than the threshold, go to **Step 3**.
- If the GC duration threshold is properly set, go to **Step 11**.

Step 3 Choose **Cluster** > **Services** > **LakeSearch**. Click **Configurations** and click **All Configurations**.

Step 4 In the upper right corner of the configuration page, enter **GC_OPTS** in the search box. The **GC_OPTS** parameters of all instances are displayed.

Step 5 Select the instance whose parameter **GC_OPTS** needs to be modified, and check whether the differentiated configuration icon is displayed next to the instance value configuration box.

- If the icon is displayed, go to **Step 6**.
- If the icon is not displayed, go to **Step 7**.

Step 6 Click . In the displayed dialog box, click on the right and click **OK**.

Step 7 Change the values of **-Xms** and **-Xmx** of the **GC_OPTS** parameter by referring to the following note.

NOTE

Suggestions on GC parameter settings for LakeSearch instances:

- Change the values of **-Xms** and **-Xmx** of the **GC_OPTS** parameter to **8G**.
- Set **-Xms** and **-Xmx** to the same value to prevent dynamic adjustment of the heap memory size, which may affect performance.

Step 8 After the modification, click **Save** in the upper left corner. In the displayed dialog box, click **OK**.

Step 9 Click **Instances**, select the instances whose configuration status is **Expired**, and choose **More** > **Restart Instance** to restart them as prompted.

Step 10 Wait for one minute and check whether the alarm is cleared.

- If it is cleared, no further action is required.
- If it persists, go to **Step 11**.

Collect fault information.

Step 11 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log** > **Download**.

Step 12 Expand the **Service** drop-down list, and select **LakeSearch** for the target cluster.

Step 13 Click the edit icon in the upper right corner, and set **Start Date** and **End Date** for log collection to 10 minutes ahead of and after the alarm generation time, respectively. Then, click **Download**.

Step 14 Contact technical support and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

1.4 Appendix

1.4.1 Logging In to and Out of Service OM

This section describes how to log in to Service OM to perform management operations.

Prerequisites

- You have set the resolution of the local PC as required. Recommended resolutions are 1366 x 768 and 1440 x 900. To ensure optimal user experience, use a horizontal resolution that is greater than or equal to 1280p.
- You have obtained the IP address of ManageOne Maintenance Portal.
- You have obtained the username and password for logging in to ManageOne Maintenance Portal.

Logging In to Service OM

Step 1 Log in to ManageOne Maintenance Portal using a browser.

- Login with the URL: **https://***Domain name of ManageOne Maintenance Portal***:31943**. Alternatively, access **https://***Address for accessing the ManageOne unified portal* to log in to the ManageOne unified portal and choose OperationCenter to access ManageOne Maintenance Portal.

  Obtain the domain name of ManageOne Maintenance Portal on the "2.3 Portal" sheet of the deployment parameter table exported from HCC Turnkey during the installation of Huawei Cloud Stack basic services.

- Login using a password: Enter the username and password.

  Default account: bss_admin. To obtain the default password, contact the system administrator or refer to the default password of the ManageOne Maintenance Portal account on the "Type A (Portal)" sheet in ***Huawei Cloud Stack 8.3.1 Account List*** .

  NOTE

  For ManageOne upgraded from 8.2.0 or an earlier version, the default account name is **admin**.

- Login using a USB key: Insert a USB key with preset user certificates, select the required device and certificate, and enter a PIN.

Step 2 On the maintenance portal homepage, click Service_OM in **Common Links**. Select a region to switch to the **Service OM** page.

----End

Logging Out of Service OM

In the upper right corner of the web client, click the username and choose **Log Out**. Then, you are switched to the login page.

1.4.2 Determining the Active/Standby Status of MRS-DB Nodes

Symptom

MRS-DB nodes MRS_DB-01 and MRS_DB-02 are active and standby nodes. If an active DB node is faulty, the standby DB node automatically becomes the active one, ensuring system reliability.

Procedure

Step 1 Log in to the MRS_DB-01 VM as user **opsadmin** by referring to **Logging In to an MRS Management Node**. Then, run the following command to switch to user **root**:

su - root

See ***Huawei Cloud Stack 8.3.1 Account List*** or contact the system administrator to obtain the default password.

Step 2 Run the following commands to query the primary/standby status of the database and the floating IP address (vip) of the database:

su - mysql

dbstatus

hastatus

```
[mysql@MRS-DB-01 ~]$ dbstatus
+----------------+-----------+-----------+----------------+-----------+---------+-----------------+-----------+------+-------+---------------------+---------------------+
| node_ip        | ha_status | db_status |      vip       | rep_state | db_role |  master_host    | read_only | sync | delay |    heartbeat_time   |      check_time     |
+----------------+-----------+-----------+----------------+-----------+---------+-----------------+-----------+------+-------+---------------------+---------------------+
|                |   online  |   online  |                |   Normal  | Primary |                 |    OFF    |  -   |   -   | 2022-03-23 10:04:05 | 2022-03-23 10:04:05 |
|                |   online  |   online  |       -        |   Normal  | Standby |                 |    ON     | 100  |   0   | 2022-03-23 10:04:05 | 2022-03-23 10:04:07 |
+----------------+-----------+-----------+----------------+-----------+---------+-----------------+-----------+------+-------+---------------------+---------------------+
[mysql@MRS-DB-01 ~]$ hastatus
+----------------+-----------+-----------+---------+----------+-----------+---------+---------------------+
|    node_ip     | ha_status | Collector | Monitor | Failover | Switchover |  Sync  |      Check Time     |
+----------------+-----------+-----------+---------+----------+-----------+---------+---------------------+
|                |   online  |   online  | online  |  online  |   online  | online | 2022-03-23 10:04:32 |
|                |   online  |   online  | online  |  online  |   online  | online | 2022-03-23 10:04:33 |
+----------------+-----------+-----------+---------+----------+-----------+---------+---------------------+
```

----End

1.4.3 Logging In to an MRS Management Node

Huawei Cloud Stack provides a security O&M channel through the CLI terminal (an optional module). When you install the security O&M channel, the way of logging in to backend nodes changes. This section describes how to log in to a backend node in different scenarios.

The module provides security O&M capabilities for ManageOne Maintenance Portal, including SSH login without password, command execution or interception, file upload and download, and O&M command audit. The module provides a unified O&M portal. This enhances O&M management, control, and audit, simplifies the remote O&M access process, improves O&M efficiency, and enhances account and password security.

The module is selected by default and can be deselected. It is not upgraded by default and can be added after the upgrade.

NOTE

The CLI supports the following accounts in different scenarios:

- Accounts of cloud services where the security O&M channel is not installed can only be used to log in to nodes over SSH.
- Accounts of cloud services where the security O&M channel is installed but that are not reclaimed can only be used to log in to nodes over SSH.
- Accounts of cloud services where the secure O&M channel is installed and that are reclaimed can be used to log in to nodes over SSH by applying for a password because its password has been changed to a random one after reclamation.
- Accounts of cloud services where the secure O&M channel is installed, that are reclaimed, and that have obtained the one-click login permission can be used to log in to nodes through the CLI terminal or over SSH by applying for a password.

Prerequisites

- You have logged in to ManageOne Maintenance Portal as a system administrator.
- You have obtained the permission to perform operations on the CLI.
- If the command whitelist is enabled, only whitelisted commands can be executed on the CLI. If the function is disabled, any commands can be executed on the CLI.

Logging In to an MRS Management Node Through the CLI Terminal

Step 1 Check whether secure O&M channel has been installed.

Choose **O&M** from the main menu and check whether the CLI terminal is displayed in the navigation pane.

- If yes, the secure O&M channel has been installed. Go to **Step 2**.
- If no, the secure O&M channel is not installed. In this case, log in to a management node over SSH. For details, see **Logging In to an MRS Management Node Over SSH**.

Step 2 Check whether the account has been managed by an external system.

1. Choose **O&M** > **Accounts** from the main menu.
2. Check whether the account for logging in to the backend node has been remotely managed based on information displayed in the **Application/Cloud Service**, **Resource Name**, and **Account Management Party** columns.
   - If yes, use an SSH client, such as PuTTY, to log in to a node.
   - If no, go to **Step 3**.

Step 3 Use either of the following methods to log in to a backend node:

- Login using SSH

  Apply for permission to use an account password to log in to the node over SSH. For details, see section "Account Request" > "Creating a Request for Obtaining Passwords" in the **Huawei Cloud Stack 8.3.1 O&M Guide**.
- One-click login on the CLI

a. Choose **O&M** > **CLI** from the main menu.

b. In the navigation pane on the left, expand the corresponding nodes one by one and check whether the account for logging in to the backend node is displayed.

- If yes, the account has obtained the permission for one-click login. Go to **Step 4**.
- If no, apply for the one-click login permission to log in to the node. For details, see section "Account Request" > "Creating a Request for Obtaining Passwords" in the **Huawei Cloud Stack 8.3.1 O&M Guide**. Then, go to **Step 4**.

Step 4 Click **Execute Command** to log in to the backend node. Then, proceed with other operations.

NOTE

Only commands in the trustlist can be executed. If the following error message is displayed during the execution, contact the administrator to add the commands to the trustlist. For details, see the **Huawei Cloud Stack 8.3.1 O&M Guide**.
Your command is highly risky. Please check the whitelisted commands.

----End

Logging In to an MRS Management Node Over SSH

Step 1 Log in to ManageOne Maintenance Portal as the system administrator. In the **Common Links** navigation tree, click Service_OM and select a region to go to the Service OM page.

Step 2 Choose **Services** > **Resource** > **Compute Resource**.

Step 3 Click the **VMs** tab, enter a keyword in the search box to search for the VM name, for example, **EICommon-Region-Master**, **MRS_DB**, **Console-DB**, or **Console-Static**, and record the IP address of the VM.

Step 4 Use PuTTY to log in to any VM whose **Status** is **Running** as user **opsadmin**. For example, log in to the **EICommon-Region-Master-01**, **MRS_DB-01**, **Console-DB-01**, or **Console-Static-01** VM.

Obtain the default password by referring to ***Huawei Cloud Stack 8.3.1 Account List*** or contacting the system administrator.

NOTE

If **Status** of all VMs is not **Running**, contact the cluster administrator.

----End

2 Troubleshooting

2.1 Troubleshooting Process

The troubleshooting process consists of the following operations: collecting fault information, diagnosing the fault, locating the fault, and rectifying the fault. **Figure 2-1** shows the troubleshooting process.

NOTE

Before handling a critical fault, contact technical support.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 2-1 Troubleshooting process

Collecting Fault Information

Collect as much fault information as possible, because fault information helps maintenance engineers correctly diagnose faults.

Diagnosing the Fault

Before rectifying the fault, determine the fault type and the impact scope based on the collected information.

Fault Location

Fault locating refers to the process of finding the root cause of the fault from multiple possible causes. By using certain methods or measures to analyze and compare the possible causes of the fault, the system maintenance personnel finally find the real cause of the fault after excluding impossible causes.

The common fault locating methods are as follows:

- Checking alarm information on the management page
- Querying monitoring results on the management page to discover possible exceptions
- Querying operation logs to discover possible misoperations
- Checking configuration data on the management page
- Checking device indicator status

Troubleshooting

Fault rectification refers to the process of rectifying a fault according to different causes of the fault. This process involves checking and repairing lines, modifying configurations, restarting processes, and restarting servers.

NOTE

If you cannot rectify the fault, contact the technical support.

Verifying Fault Rectification

Check the device status, indicators, and alarms to ensure that the system is running properly, and perform service commissioning as necessary to ensure that services are running properly.

Recording the Troubleshooting Process

After rectifying the fault, record the key points about troubleshooting and the measures taken to prevent the faults of the same type from recurring.

2.2 Collecting Information

2.2.1 Statements

Observe the following principles during information collection:

- Before using the information collection tool, notify the customer of when and why you use the tool.
- Perform maintenance operations only after being approved by the customer.
- Transfer fault locating data out of the customer's network only after being approved by the customer.

2.2.2 Collecting Site Information

When a fault occurs, collect site information to inform technical support and R&D engineers of the site situation, and provide them with the field engineers' contact information to ensure smooth contact. **Table 2-1** lists the site information to be collected.

Table 2-1 Site information to be collected

Carrier or Enterprise	Site	Networking Diagram	Onsite Engineer Name and Phone Number	Name and Phone Number of Customer
-	-	-	-	-
Version information	-			
Remote maintenance information	-			

2.2.3 Collecting Fault Information

Collect basic fault information to learn the site situation, device status before the fault occurs, and possible causes of the fault. **Table 2-2** lists the specific information to be collected.

Table 2-2 Basic fault information to be collected

Information	Description
Fault symptom	-
Fault occurrence time	-
Fault occurrence frequency	-
Impact on services	-
Whether the fault is rectified	-
Whether any adjustment or operation is performed after the fault occurs	-
Whether the fault occurs during site deployment	-
Procedure where the fault occurred (scale-out, cutover, or upgrade)	-
Operations performed for rectifying the fault that occurred during maintenance	-
Measures taken to handle the fault	-
Result of the measures	-
Whether alarms are generated	-

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Information	Description
Whether alarm information is collected	-

2.2.4 Collecting Log and System Information

Scenario

If an exception occurs, maintenance engineers can log in to ManageOne Maintenance Portal and the service host background to collect system logs of the management plane and locate the fault.

Prerequisites

- You have obtained the administrator account.
- You have logged in to ManageOne Maintenance Portal.

Downloading Management Plane Logs on the Web UI

Step 1 Log in to ManageOne Maintenance Portal using a browser.

- Login with the URL: **https://***Domain name of ManageOne Maintenance Portal***:31943**. Alternatively, access **https://***Address for accessing the ManageOne unified portal* to log in to the ManageOne unified portal and choose OperationCenter to access ManageOne Maintenance Portal.

  Obtain the domain name of ManageOne Maintenance Portal on the "2.3 Portal" sheet of the deployment parameter table exported from HCC Turnkey during the installation of Huawei Cloud Stack basic services.

- Login using a password: Enter the username and password.

  Default account: bss_admin. To obtain the default password, contact the system administrator or refer to the default password of the ManageOne Maintenance Portal account on the "Type A (Portal)" sheet in ***Huawei Cloud Stack 8.3.1 Account List*** .

  NOTE

  For ManageOne upgraded from 8.2.0 or an earlier version, the default account name is **admin**.

- Login using a USB key: Insert a USB key with preset user certificates, select the required device and certificate, and enter a PIN.

Step 2 Choose **O&M** > **Logs** > **Run Logs** > **Management Run Log Download**.

Step 3 On the displayed page, click **Add Download Log Task**. On the **Add Download Log Task** page, click the **Custom** tab, enter a task name, and set **Period**.

Step 4 In the **Log File** area, select the target MRS logs and click **OK** to add the download task.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 5 After the download task is successfully added, click **Download** in the **Download File** column to download logs.

Step 6 Analyze the log error cause and locate the fault.

----End

Viewing Logs by Logging to the Management Host

Step 1 Log in to the **EICommon-Region-Master-01** VM as user **opsadmin**. For details, see **Logging In to an MRS Management Node**.

Run the **su - root** command to switch to user **root**.

Obtain the default password by referring to ***Huawei Cloud Stack 8.3.1 Account List*** or contacting the system administrator.

Step 2 Switch to the target log directory and view the logs. The log directories are as follows:

- MRS-Performance logs:
  - /var/log/paas/cam-tiller/
  - /var/log/paas/canal/
  - /var/log/paas/cce-agent/
  - /var/log/paas/haproxy-keepalived/
  - /var/log/paas/kubernetes/

Step 3 Run the following command to query the names of all MRS containers in the cluster and obtain the IP addresses in the **NODE** column:

kubectl get pods -n mrs -owide

```
NAME                        READY   STATUS    RESTARTS   AGE     IP          NODE          NOMINATED
NODE   READINESS GATES
mrsapigw-6f56bc476d-c5cs9      1/1     Running   0          19h     10.16.0.69    10.69.26.187   <none>
<none>
mrsapigw-6f56bc476d-smqn8      1/1     Running   0          5d13h   10.16.0.20    10.69.26.197
<none>           <none>
mrsdeployer-5988d78867-2prk6   1/1     Running   0          43h     10.16.0.55    10.69.26.194   <none>
<none>
mrsdeployer-5988d78867-8lb5p   1/1     Running   0          43h     10.16.0.25    10.69.26.197   <none>
```

```
<none>
mrsdeployer-5988d78867-gwqb7   1/1     Running   0          43h     10.16.0.86    10.69.26.189
<none>           <none>
```

Step 4 Log in to the **MRS-Api** or **MRS-Deploy** node using the IP address obtained in **Step 3** as user **opsadmin**. (The node name is the container name starting with **mrsapigw** or **mrsdeployer** in **Step 3**.)

Run the **su - root** command to switch to user **root**.

Obtain the default password by referring to ***Huawei Cloud Stack 8.3.1 Account List*** or contacting the system administrator.

Step 5 Switch to the target log directory and view the logs. The log directories are as follows:

- MRS-Api logs:
  - /var/log/mrs/apigw/hwctrace/
  - /var/log/mrs/apigw/apigateway/
- MRS-Deploy logs:
  - /var/log/mrs/deployer/hwctrace/
  - /var/log/mrs/deployer/service-deployer/

Step 6 Click the **VMs** tab, enter the keyword **MRS_Region_Node** in the search box to search for the VM, and record the IP address of the VM.

NOTE

In the non-DR deployment scenario of the MRS management plane, the ZooKeeper process is deployed on the **MRS_Region_Node** VM. In the cross-AZ DR deployment scenario of the MRS management plane, the ZooKeeper process is deployed on the **MRS-Zookeeper** and **MRS-Zookeeper-DC** VMs.

Step 7 Log in to the VM as user **opsadmin**.

Run the **su - root** command to switch to user **root**.

Obtain the default password by referring to ***Huawei Cloud Stack 8.3.1 Account List*** or contacting the system administrator.

Step 8 Switch to the target log directory and download the logs. The log directories are as follows:

MRS-ZooKeeper logs:

- /opt/cloud/logs/zookeeper/

Step 9 Click the **VMs** tab, enter the keyword **MRS_DB** in the search box to search for the VM, and record the IP address of the VM.

Step 10 Log in to the VM as user **opsadmin**.

Run the **su - root** command to switch to user **root**.

Obtain the default password by referring to ***Huawei Cloud Stack 8.3.1 Account List*** or contacting the system administrator.

Step 11 Switch to the target log directory and download the logs. The log directories are as follows:

MRS-HCS-MySQL logs:

- /data/mysql/logs/

Step 12 Analyze the log error cause and locate the fault.

----End

2.3 MRS Management and Control Plane Troubleshooting

2.3.1 ServiceDeployer Fault

Symptom

The Deployer process crashes or starting the process fails.

Possible Causes

- The user who starts the Deployer process is not user **service**.
- Failed to connect to ZooKeeper.

Troubleshooting

1. Check whether the current user of the process is **service**.
2. View the **/opt/cloud/logs/service-deployer/service-deployer-service-deployer.log** file to locate the fault.

Procedure

Step 1 Log in to the EICommon-Region-Master-01 node as the **opsadmin** user. For details, see **Logging In to an MRS Management Node**. Run the following command to query and access the corresponding service container:

su - root

Obtain the default password by referring to ***Huawei Cloud Stack 8.3.1 Account List*** or contacting the system administrator.

kubectl get pods -n mrs -o wide

kubectl exec -it -n mrs *Container name* **bash**

Example:

```
NAME                          READY   STATUS    RESTARTS   AGE     IP           NODE           NOMINATED
NODE   READINESS GATES
mrsapigw-6f56bc476d-c5cs9      1/1     Running   0          19h     10.16.0.69    10.69.26.187   <none>
<none>
mrsapigw-6f56bc476d-smqn8      1/1     Running   0          5d13h   10.16.0.20    10.69.26.197
<none>           <none>
mrsdeployer-5988d78867-2prk6   1/1     Running   0          43h     10.16.0.55    10.69.26.194   <none>
<none>
mrsdeployer-5988d78867-8lb5p   1/1     Running   0          43h     10.16.0.25    10.69.26.197   <none>
<none>
mrsdeployer-5988d78867-gwqb7   1/1     Running   0          43h     10.16.0.86    10.69.26.189
<none>           <none>
```

kubectl exec -it -n mrs *mrsdeployer-5988d78867-2prk6* **bash**

Step 2 If the error occurs because the user who starts the process is not the **service** user, perform the following steps:

1. Run the **ps -ef |grep service-deployer** command to obtain the process ID of Deployer.
2. Run the **kill -9 [deployer-process-id]** command to stop the Deployer process.
3. Run the **su - service** command on the node where Deployer is deployed to switch the user.
4. Run the following commands to stop and restart the service:

   cd /opt/cloud/MRS-Deployer/bin/

   sh stop.sh

   sh start.sh

----End

2.3.2 APIGateway Fault

Symptom

The APIGateway process crashes or starting the process fails.

Possible Causes

The user who starts the APIGateway process is not user **service**.

Troubleshooting

1. Check whether the current user of the process is **service**.
2. View the **/opt/cloud/logs/apigateway/api-gateway.log** file to locate the fault.

Procedure

Step 1 Log in to the EICommon-Region-Master-01 node as the **opsadmin** user. For details, see **Logging In to an MRS Management Node**. Run the following command to query and access the corresponding service container:

su - root

Obtain the default password by referring to ***Huawei Cloud Stack 8.3.1 Account List*** or contacting the system administrator.

kubectl get pods -n mrs -o wide

kubectl exec -it -n mrs *Container name* **bash**

Example:

```
NAME                        READY   STATUS    RESTARTS   AGE     IP          NODE          NOMINATED
NODE   READINESS GATES
mrsapigw-6f56bc476d-c5cs9      1/1     Running   0          19h     10.16.0.69    10.69.26.187   <none>
<none>
mrsapigw-6f56bc476d-smqn8      1/1     Running   0          5d13h   10.16.0.20    10.69.26.197
```

```
<none>          <none>
mrsdeployer-5988d78867-2prk6   1/1     Running   0          43h     10.16.0.55    10.69.26.194   <none>
<none>
mrsdeployer-5988d78867-8lb5p   1/1     Running   0          43h     10.16.0.25    10.69.26.197   <none>
<none>
mrsdeployer-5988d78867-gwqb7   1/1     Running   0          43h     10.16.0.86    10.69.26.189
<none>          <none>
```

kubectl exec -it -n mrs *mrsapigw-6f56bc476d-c5cs9* **bash**

Step 2 If the error occurs because the user who starts the process is not the **service** user, perform the following steps:

1. Run the **ps -ef |grep apigateway** command to obtain the ID of the current Tomcat process.
2. Run the **kill -9** *[apigateway-process-id]* command.
3. Run the **su - service** command on the node where APIGateway is deployed to switch the user.
4. Run the following commands to stop and restart the service:

   cd /opt/cloud/MRS-APISvc/bin/

   sh stop.sh

   sh start.sh

----End

2.3.3 ManageOne Maintenance Portal Component Alarm Is Not Cleared After a Component Is Deleted from an MRS Cluster

Symptom

After a component is deleted from an MRS cluster, no alarm about the component is displayed on the console, but the alarm of the component is not cleared on ManageOne Maintenance Portal.

Troubleshooting

The alarm on ManageOne Maintenance Portal is not synchronized with that in the MRS cluster. You need to manually clear the alarm on ManageOne Maintenance Portal.

Procedure

Step 1 Log in to ManageOne Maintenance Portal using a browser.

- Login with the URL: **https://***Domain name of ManageOne Maintenance Portal***:31943**. Alternatively, access **https://***Address for accessing the ManageOne unified portal* to log in to the ManageOne unified portal and choose OperationCenter to access ManageOne Maintenance Portal.

  Obtain the domain name of ManageOne Maintenance Portal on the "2.3 Portal" sheet of the deployment parameter table exported from HCC Turnkey during the installation of Huawei Cloud Stack basic services.
- Login using a password: Enter the username and password.

Default account: bss_admin. To obtain the default password, contact the system administrator or refer to the default password of the ManageOne Maintenance Portal account on the "Type A (Portal)" sheet in ***Huawei Cloud Stack 8.3.1 Account List*** .

NOTE

For ManageOne upgraded from 8.2.0 or an earlier version, the default account name is **admin**.

- Login using a USB key: Insert a USB key with preset user certificates, select the required device and certificate, and enter a PIN.

Step 2 Choose **Alarm Management** > **Alarms** > **Current Alarms**. On the displayed page, click **Filter** in the upper left corner. In **Advanced Settings**, set the following parameters and click **OK**.

- **Alarm Source**: Enter the name of the cluster whose component alarm is to be cleared. (If the cluster name has been changed, use both the old and new names as the search criteria. The keywords can be separated using line delimiters.)
- **Object Type**: Enter the name of the deleted component.

Step 3 In the search result, check whether the alarm of the component is cleared in the MRS cluster.

- If yes, select the check box of the component in the alarm list and click **Clear**. In the displayed dialog box, deselect **Also clear the alarm in peer system or devices** and click **Yes**. Wait until the alarm is cleared.
- If no, you do not need to manually clear the alarm. No further action is required.

----End

2.3.4 Failed to Create an MRS Cluster

Symptom

After MRS is installed, a tenant fails to create an MRS cluster on the MRS console.

Possible Causes

- Network exceptions
- Flavor exceptions

Fault Locating

- Check the network connection.
  - Check that the POD zone on the tenant plane can access the OBS or Swift domain name.
  - Check that the POD zone on the tenant plane can access the DNS server.
  - Check the network between the DMZ_Service network plane and the External_Relay_Network network plane.
  - If OBS is used, check the network between External_Relay_Network and the OBS 3.0 service address.

  - If SwiftAdapter is used, check the network between External_Relay_Network and **podlb_lvs_adv_float_01_ip**.
- Check the VM flavor configurations.
  - Check the ECS flavors.
  - Check that the host resources meet the flavor requirements.
  - For BMS clusters, check that the BMS flavors match the BMS information.

Checking the Network

Step 1 Check that the POD zone on the tenant plane can access the OBS or Swift domain name.

1. Log in to any created ECS node as user **root**. If no ECS node is available in the current environment, you can create one.
2. Run the **ping** *Domain name of OBS or SWIFT* command to check whether the network connection is normal.

   For details about the OBS or Swift domain name, contact the system administrator. If the current node is an OMS node in the MRS cluster, you can obtain the domain name from the **/var/log/mrs_init.log** file.

```
10.64.248.175
set timezone as /usr/share/zoneinfo/Asia/Shanghai
Redirecting to /bin/systemctl stop ntpd.service
object-store.cn-hnlcj-1.hnlcjcloud.com is not connected and retry 0.
object-store.cn-hnlcj-1.hnlcjcloud.com is not connected and retry 1.
object-store.cn-hnlcj-1.hnlcjcloud.com is not connected and retry 2.
object-store.cn-hnlcj-1.hnlcjcloud.com is not connected and retry 3.
object-store.cn-hnlcj-1.hnlcjcloud.com is not connected and retry 4.
object-store.cn-hnlcj-1.hnlcjcloud.com is not connected and retry 5.
object-store.cn-hnlcj-1.hnlcjcloud.com is not connected and retry 6.
object-store.cn-hnlcj-1.hnlcjcloud.com is not connected and retry 7.
object-store.cn-hnlcj-1.hnlcjcloud.com is not connected and retry 8.
object-store.cn-hnlcj-1.hnlcjcloud.com is not connected and retry 9.
object-store.cn-hnlcj-1.hnlcjcloud.com is not connected and retry 10.
object-store.cn-hnlcj-1.hnlcjcloud.com is not connected and retry 11.
object-store.cn-hnlcj-1.hnlcjcloud.com is not connected and retry 12.
object-store.cn-hnlcj-1.hnlcjcloud.com is not connected and retry 13.
object-store.cn-hnlcj-1.hnlcjcloud.com is not connected and retry 14.
object-store.cn-hnlcj-1.hnlcjcloud.com is not connected and retry 15.
object-store.cn-hnlcj-1.hnlcjcloud.com is not connected and retry 16.
object-store.cn-hnlcj-1.hnlcjcloud.com is not connected and retry 17.
object-store.cn-hnlcj-1.hnlcjcloud.com is not connected and retry 18.
object-store.cn-hnlcj-1.hnlcjcloud.com is not connected and retry 19.
```

   - If yes, go to **Step 2**.
   - If no, contact network engineers.

Step 2 Check the network between the POD zone on the tenant plane and DNS server.

1. Log in to any ECS server provisioned on the tenant plane as user **root**.
2. Run the **ping** *IP address of the DNS service node* command to check whether the network connection is normal.

   You can obtain the IP address of the DNS service node by referring to **dns_ntp_tenant_ip_01** and **dns_ntp_tenant_ip_02** in the **Basic_Parameters** sheet of the parameter summary table exported in the environment installation project.

   If the current node is an OMS node in an MRS cluster, you can also run the following command to obtain the IP address:

   cat /etc/resolv.conf

```
[root@node-master1bTob ~]# cat /etc/resolv.conf

nameserver 10.35.152.7
nameserver 10.35.152.8
```

- If yes, go to **Step 3**.
- If no, contact network engineers.

Step 3 Check the network between the DMZ_Service network plane and the External_Relay_Network network plane.

1. Log in to Service OM and choose **Services** > **Resource** > **Compute Resource**. In the VMs list, search for any ECS node in the cluster using the cluster ID and obtain the IP addresses of the VMs in the External_Relay_Network network segment.

You can obtain the cluster ID from the cluster list on the MRS console.

2. Search for and log in to any MRS_Region_Node-*xx* and run the **ping** *IP address in the External_Relay_Network network segment* command to check whether the network is connected.
   - If yes, go to **Step 4**.
   - If no, contact network engineers.

Step 4 If OBS is used, check the network between External_Relay_Network and the OBS 3.0 service address.

Log in to an ECS provisioned on the tenant plane as user **root** and run the following command:

ping *obsv3_address*

NOTE

You can search for **obsv3_address** on the **Basic_Parameters** sheet of the parameter summary table exported in the environment installation project.

Step 5 If SwiftAdapter is used, check the network between External_Relay_Network and **podlb_lvs_adv_float_01_ip**.

Log in to an ECS provisioned on the tenant plane as user **root** and run the following command:

ping *podlb_lvs_adv_float_01_ip*

NOTE

You can check the value of **podlb_lvs_adv_float_01_ip** in the template exported during the first installation of gPaaS & AI DaaS services. This parameter is not used in subsequent installations.

----End

Checking the Flavors

Check ECS flavors (for provisioning ECS clusters).

Step 1 Log in to Service OM. For details, see **Logging In to Service OM**.

Step 2 Choose **Services** > **Resource** > **Compute Resource** > **Flavors** from the main menu.

Step 3 Search for the flavor used for creating the MRS cluster and click its name to go to the flavor details page.

Step 4 Click **Configure** to check whether the flavor is a non-typical one (which is manually created after the cloud service is installed).

Step 5 Check that the manually created flavor meets the following requirements:

- The flavor ID and its name are the same.
- The AZ information of the flavor contains the AZ to which the cluster to be created belongs.
- In the custom tags of the flavor, check that **cond:operation:az** is configured with the correct AZ information and **quota:local_disk** is configured with the number and size of disks as required, and then record the number and size of disks.
- Check and record the huge page memory and NUMA settings in the **Feature Configuration** area.

  In the **Associate Host Group** area, click the name of the host group associated with the flavor to go to the host group details page.

  On the **Summary** page, check which memory is the largest among huge page memory (2 MB), huge page memory (1 GB), and small page memory. If huge page memory (2 MB) is the largest, the huge page memory of the flavor must be set to **2**. If the huge page memory (1 GB) is the largest, it must be set to **1,024**. If the small page memory is the largest, it can be left empty.

  Check that the current flavor configuration is the same as the huge page configuration of the host group flavor.
- Click each host name to go to the **Summary** page. In the **Total Resources** area, check that the number of disks (data disks of disk-intensive VMs) on each host is the same as that specified in the flavor.
- Check the disk size of each host in the disk information on the FusionSphere OpenStack page based on the host ID. The disk size specified in the flavor cannot be greater than the disk size on the host. (The disk sizes on the same host must be the same.)

----End

Check host resources.

Step 1 On the homepage of **Service OM**, choose **Services** > **Resource** > **Compute Resource** > **Flavors** to view the flavor list.

Step 2 Click the flavor name. In the **Associate Host Group** area on the **Configuration** page, click the name of the host group associated with the flavor to go to the host group details page.

Step 3 Based on the scale of the cluster to be created and the number of VMs that have been created using the flavor, check that the number of host groups meets the requirements for creating a cluster. The number of VMs created using this flavor must be no bigger than the number of hosts using the current flavor.

Step 4 Click **Configuration**. In the **Custom Tag** area, check **cpu_allocation_ratio tag**, whose value must be **1**.

Step 5 Click **Hosts** to view the CPU and memory of the host. The CPU and memory specified in the flavor must be no bigger than those of each host.

----End

Check BMS flavors (for provisioning BMS clusters).

Step 1 Log in to Service OM. For details, see **Logging In to Service OM**.

Step 2 Choose **Services** > **Bare Metal Resource** from the main menu.

Step 3 On the **Flavors** page, view the flavor list and check the name of the flavor used for creating the cluster.

The BMS flavor used for creating an MRS cluster must start with **physical.ks1ne** in the ARM architecture, and must start with **physical.d4/d3/d2/d1** in x86 architecture.

Step 4 Click the flavor name to go to the flavor details page and check the flavor configuration.

- For a non-typical configuration, check that **Distributed Gateway** is set to **Yes** in the **Basic Information** area.
- In the **Custom Tag** area, ensure that **baremetal:__support_evs** is set to **false** and **cond:operation:az** is set to the AZ to be associated with the flavor.

Step 5 On the **Bare Metal Servers** page, check whether the flavor used for creating the cluster matches the planned BMS information. Ensure that the number of CPUs, memory, and disks of the BMS is the same as that in the flavor.

Step 6 Check that the BMS used for creating the cluster is in the deployable state.

----End

2.4 MRS Tenant Plane Troubleshooting

2.4.1 ClickHouse

2.4.1.1 Error Message "Not enough privileges" Is Displayed When the Client Performs Operations on the ClickHouse Database and Tables

Symptom

During the operation of creating a database or table, querying data, or inserting data into a table on the ClickHouse client, the error message "Not enough privileges" is displayed.

Possible Causes

In a cluster in security mode, the user role authenticated during client login does not have the operation permission on the corresponding database and table.

Fault Locating

Log in to FusionInsight Manager and check whether the user role for client login authentication has the operation permission on the corresponding database and table.

Procedure

Step 1 Log in to FusionInsight Manager, choose **System** > **Permission** > **User**, and click the button of the user to view and save the role of the user.

Step 2 Choose **System** > **Permission** > **Role**, locate the row that contains the role name obtained in **Step 1**, and choose **Modify** > ***Cluster name*** > **ClickHouse** in the **Operation** column.

Step 3 Determine whether to create a role with administrator permission based on service requirements.

NOTE

- The ClickHouse administrator has all the database operation permissions except the permissions to create, delete, and modify users and roles.
- Only the built-in user **clickhouse** of ClickHouse has the permission to manage users and roles.

- If yes, go to **Step 4**.
- If no, go to **Step 5**.

Step 4 Select **SUPER_USER_GROUP** and click **OK**.

Step 5 Click **ClickHouse Scope**. The ClickHouse database resource list is displayed. If you select **create**, the role has the create permission on the database.

Determine whether to grant the permission based on the service requirements.

- If yes, click **OK**.
- If no, go to **Step 6**.

Step 6 Click the resource name and select the *Database resource name to be operated*. On the displayed page, select **read** (SELECT permission) or **write** (INSERT permission) based on service requirements, and click **OK**.

----End

Reference Information

None.

2.4.1.2 Error Message "connect timed out" Is Displayed When the ClickHouse Client Is Being Connected

Symptom

When the **clickhouse client** command is used to connect to the node where the ClickHouse client is installed, the error message "connect timed out" is displayed.

Possible Causes

- The network between the host where the client is located and the node where the ClickHouse cluster instance is located is disconnected.
- The IP address of the ClickHouse instance node specified in the **clickhouse client** command is incorrect.

Fault Locating

1. Log in to the host where the client is located and run the **ping** *ClickHouse instance node* command to check whether the network connection of the current node is normal.
2. Check whether the host IP address specified in the **--host** parameter of the **clickhouse client** command is correct.

Procedure

Step 1 Log in to the host where the client is located and run the **ping** *ClickHouse instance node* command to check whether the network between the current node and the instance is normal.

Step 2 On FusionInsight Manager, choose **Cluster** > **Services** > **ClickHouse** > **Instance**. On the displayed page, view the service IP column of the **ClickHouseServer** role instance to obtain the IP address of the ClickHouse instance to be connected.

Step 3 Check whether the IP address specified by the **--host** parameter in the **clickhouse client** command is the same as the service IP address of the **ClickHouseServer** instance queried in **Step 2**. If they are different, change the IP address and try to log in again.

----End

Reference Information

None.

2.4.1.3 Failed to Start the ClickHouse Service After Changing the Storage Path

Symptom

After a user modifies the **_clickhouse.storage_configuration.disks** parameter, the service fails to be started and the following error message is displayed: The local set of parts of table... in zookeeper:xxx in filesystem are suspicious. There are xx unexpected parts with xxx rows.

Possible Causes

The part information stored locally is inconsistent with that stored in ZooKeeper.

Fault Locating

Check the part information stored locally and in ZooKeeper.

Procedure

Step 1 Run the following command to view the local part information:

ls /srv/Bigdata/clickhouse/data1/clickhouse/store/*Table UUID***/part/all_0_9_1**

Step 2 Log in to the ZooKeeper client.

1. Use PuTTY to log in to the server where the ZooKeeper client is installed as user **root**. For example, the installation directory is **/opt/hadoopclient**.
2. For example, if the directory is **/opt/Bigdata/client**, run the following command to go to the directory:

   cd /opt/hadoopclient
3. Run the following command to set environment variables:

   source bigdata_env
4. (Optional) Run the following command and enter the user password to authenticate the user identity (this step is required only for the cluster with the security mode enabled, and user **admin** is used only as an example):

   kinit admin
5. Run the following command to log in to the ZooKeeper client:

   sh zkCli.sh -server *Service plane IP address of any ZooKeeper instance*:*Client port number*

   The default client port number is **24002**.

   For example, run **sh zkCli.sh -server 192.168.0.151:24002**.

Step 3 Run the following command to view the part information:

ls /clickhouse/default_cluster/*Database name***/***Table name***/***Shard number 1***/***Replica number 1***/part**

Step 4 Check whether the part information stored locally exceeds 50% of that in ZooKeeper.

- If yes, go to **Step 5**.

- If no, contact technical support.

Step 5 Log in to the ClickHouse client by referring to "Using ClickHouse from Scratch" in *MapReduce Service (MRS) 3.3.1-LTS User Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Usage Guide (for Huawei Cloud Stack 8.3.1)*. Run the following command to obtain the values of **shard** and **replica**:

select * from system.macros

```
10-244-225-12 :) select * from system.macros;

SELECT *
FROM system.macros

Query id: 33db0ab7-218b-41fc-ad2f-861ad0c01294

┌─macro───┬─substitution─┐
│ id      │ 65           │
│ replica │ 2            │
│ shard   │ 0            │
└─────────┴──────────────┘

3 rows in set. Elapsed: 0.002 sec.
```

Step 6 Run the following command to search for the metadata of the table on the ClickHouseServer node:

cat /srv/BigData/clickhouse/data1/metadata/metadata/*Database name***/***Table.sql*

```
ATTACH TABLE _ UUID 'dbcfec6a-361a-4aad-b0b5-3e71fda93558'
(
    `EventDate` DateTime,
    `CounterID` UInt32,
    `UserID` UInt32,
    `ver` UInt16
)
ENGINE = ReplicatedMergeTree('/clickhouse/tables/{shard}/test001_1631490479.test001_1631490479', '{replica}')
PARTITION BY CounterID
ORDER BY (CounterID, EventDate, intHash32(UserID))
SETTINGS index_granularity = 8192
~
~
```

Obtain the content highlighted with a red box behind **ReplicatedMergeTree** in the preceding figure. Replace the content in braces ({}) with the values of **shard** and **replica** obtained in **Step 5** to get a directory, for example, **/clickhouse/tables/64/test3/replicas/1**.

Step 7 Log in to the ZooKeeper client by referring to **Step 2**, create an empty file, and upload it to the **/clickhouse/tables/64/test3/replicas/1/flags/** directory obtained in **Step 6**.

Step 8 Restart the ClickHouse service.

----End

2.4.1.4 Failed to Perform Operations as a User That Was Created When the Metadata Disk Was Faulty

Symptom

A user is successfully created on FusionInsight Manager, but this user does not have the permission to perform operations on some nodes.

Possible Causes

This user is created when the metadata disk becomes read-only.

Fault Locating

On FusionInsight Manager, check whether an alarm is generated indicating that the ClickHouse metadata disk is abnormal.

Procedure

Step 1 Log in to FusionInsight Manager and choose **Cluster** > **Services** > **ClickHouse**. On the displayed page, Click **Configurations** and click **All Configurations** in the left pane. Enter **path** in the search box to obtain the path where the ClickHouse metadata is stored.

Step 2 Use PuTTY to log in to the faulty node as user **root** and run the following command to check the mount point:

df -h

```
[omm@10-244-225-12 ~]$ df -h
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs         32G     0   32G   0% /dev
tmpfs            32G  4.0K   32G   1% /dev/shm
tmpfs            32G  3.1G   29G  10% /run
tmpfs            32G     0   32G   0% /sys/fs/cgroup
/dev/vda4        35G   18G   16G  54% /
tmpfs            32G  3.3G   28G  11% /tmp
/dev/vda2       976M  104M  806M  12% /boot
/dev/vda1       200M  6.3M  194M   4% /boot/efi
/dev/vdb1        96G   56G   36G  61% /opt
/dev/vdb2       141G   14G  121G  10% /srv
tmpfs           6.3G     0  6.3G   0% /run/user/2000
tmpfs           6.3G     0  6.3G   0% /run/user/0
```

Step 3 Log in to FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms**, and check whether an alarm is generated indicating that the metadata disk is unavailable or the I/O is abnormal.

- If yes, go to **Step 4**.

- If no, contact technical support.

Step 4 Contact the hardware administrator to rectify the disk fault, delete the user, and create a user again.

----End

2.4.2 Containers

2.4.2.1 BLUs Are Successfully Added but Cannot Be Deployed

Symptom

After a BLU is correctly added on the **Business Manager** page of the Containers service on FusionInsight Manager, the **Deployment Status** of the BLU is always **Concerning**, indicating that the BLU is not deployed and cannot provide services.

Possible Causes

- Container is abnormal.
- An internal logic error occurs in the BLU.

Fault Locating

1. Check whether the Containers service is normal.
2. Collect logs and check whether the internal logic of the BLU is incorrect.
3. Fault recovery takes about 10 minutes.

Troubleshooting

Step 1 Log in to FusionInsight Manager, choose **Cluster** > **Services**, and check whether the Containers service is running properly.

- If yes, go to **Step 2**.
- If no, reinstall the Containers service.

Step 2 Choose **O&M** > **Log** > **Download**.

On the displayed page, set **Service** to **Containers** > **WebContainer** and set the host to the node IP address of the container where the BLU is deployed. Set the start time and end time to the period from the time when the BLU is added to the current time.

Step 3 Click **Download** to download logs, and contact BLU developers to analyze the logs.

The log file path is **/var/log/Bigdata/containers/container/{container-name}/blus/{war-name}**.

Step 4 BLU developers analyze the internal logic error of the BLU, rectify the error, repack the BLU, delete the original BLU on FusionInsight Manager, and add the modified BLU again.

Step 5 If the fault persists, contact Huawei technical support.

----End

Related Information

None

2.4.2.2 A Message Is Displayed on the SGP Management Page Indicating that the Consumer Contained in a Newly Added BLU Does Not Exist

Symptom

The BLU of the service consumer has been successfully added.

A message is displayed on the SGP management page, indicating that the consumer contained in the BLU does not exist.

Possible Causes

- The service consumer has not initiated an invoking request.
- The service and version number required by the service consumer are incorrectly configured.

Fault Locating

1. Invoke a service.
2. Check configuration files.
3. Fault recovery takes about 10 minutes.

Troubleshooting

Step 1 Invoke a service to trigger the service consumer to access the service provider. After the service invoking is complete, check the service list. If the status is **OK**, the fault is rectified. Otherwise, go to **Step 2**.

Step 2 Check the **service.xml** file of the service consumer BLU to see whether the consumer's reference to the service is correct. The following is a segment of the **service.xml** file. Check whether the value of **interface** is the same as that of the service provider and whether the value of **version** is ***** or the same as that of the service provider. If no problem is found, go to **Step 3**.

```
<dubbo:reference id="demoService"
 interface="demo.provider.itf.CustomerServiceItf" version="1.1.6"
 timeout="1000"/>
```

Step 3 Log in to FusionInsight Manager, choose **O&M** > **Log** > **Download**.

On the displayed page, set **Service** to **Containers** and set the host to the node IP address of the container where the BLU is deployed. Set the start time and end time to the period from the time when the consumer BLU is created to the time when the fault occurs.

Contact service consumer R&D engineers to analyze logs.

Step 4 BLU developers analyze the internal logic error of the BLU, rectify the error, repack the BLU, delete the original BLU on FusionInsight Manager, and add the modified BLU again.

Step 5 If the fault persists, contact Huawei technical support.

----End

Related Information

None

2.4.2.3 A Message Is Displayed on the SGP Management Page Indicating that the Service Contained in a Newly Added BLU Does Not Exist

Symptom

The service BLU is added successfully.

A message is displayed on the SGP management page, indicating that the service contained in the BLU does not exist.

Possible Causes

- ZooKeeper is abnormal.
- The **service.xml** configuration file is incorrect.

Fault Locating

1. Check the status of ZooKeeper.
2. Check configuration files.
3. Fault recovery takes about 10 minutes.

Troubleshooting

Step 1 Log in to FusionInsight Manager and check whether ZooKeeper is normal.

- If yes, go to **Step 2**.
- If no, reinstall the ZooKeeper service.

Step 2 Choose **O&M** > **Log** > **Download**.

On the displayed page, set **Service** to **Containers** > **WebContainer** and set the host to the node IP address of the container where the BLU is deployed. Set the start time and end time to the period from the time when the BLU is added to the current time.

Step 3 Contact R&D engineers to analyze logs.

The log file path is **/var/log/Bigdata/containers/container/{container-name}/blus/{war-name}/sgp.log**.

If the log file contains **java.lang.ClassNotFoundException**, check whether the Java class corresponding to the class configuration item exists in the **service.xml** configuration file.

Step 4 If the fault persists, contact Huawei technical support.

----End

Related Information

None

2.4.2.4 ZooKeeper Connection Loss Alarm Cannot Be Automatically Cleared After the ZooKeeper SSL Is Modified and the Service Is Restarted

Symptom

After the ZooKeeper SSL is modified and the service is restarted, the ZooKeeper connection loss alarm cannot be automatically cleared.

Possible Causes

The OMS Tomcat is not restarted after the ZooKeeper SSL configuration is modified.

Fault Locating

Check whether the ZooKeeper connection loss alarm is triggered in the alarm column and whether the alarm source is the service IP address of the OMS node. Fault recovery takes about 10 minutes.

Troubleshooting

Step 1 Log in to FusionInsight Manager and check whether ZooKeeper is normal.

- If yes, go to **Step 2**.
- If no, reinstall the ZooKeeper service and check whether the alarm is cleared. No further action is required.

Step 2 Restart the OMS Tomcat.

sh ${OM_TOMCAT_HOME}/bin/shutdown.sh && sh ${OM_TOMCAT_HOME}/bin/startup.sh

----End

2.4.2.5 RTD Service Is Abnormal After the Cluster Is Powered Off and Restarted

Symptom

The RTD service deployment is abnormal after the cluster is restarted due to unexpected power-off.

Possible Causes

After the cluster is restarted due to unexpected power-off, the RTD service deployment may be abnormal because the service initialization sequence of each component is different.

Fault Locating

After the cluster is restarted due to an unexpected power failure, check whether services are properly deployed on the Containers service management page.

Troubleshooting

Step 1 Log in to FusionInsight Manager and check whether Containers is normal.

- If yes, go to **Step 2**.
- If no, restart the Containers service and check whether the service is properly deployed.

Step 2 Choose **O&M** > **Log** > **Download**.

On the displayed page, set **Service** to **Containers** > **WebContainer** and set the host to the node IP address of the container where the BLU is deployed. Set the start time and end time to the period from time when the cluster is powered off to the current time.

----End

2.4.3 DBService

2.4.3.1 Failed to Configure HA Parameters During the DBService Installation

Symptom

The service or cluster installation fails because an HA configuration failure occurs during the installation of DBService.

Possible Causes

- The DBService parameter **dbservice.floatip** is incorrectly configured.
- The DBService parameter **dbservice.mediator.ip** is incorrectly configured.

Fault Locating

1. When the DBService parameter is incorrectly configured, "Failed to config HA" may be displayed in the fault log displayed on the FusionInsight Manager page. Check whether the preceding parameters are correctly configured.
2. It takes about 15 minutes to rectify the fault.

Procedure

Step 1 Log in to any node where DBService is located as user root.

Step 2 Log in to the FusionInsight Manager portal, and choose **Cluster >** *Name of the desired cluster* **> Service** > **DBService** > **Configuration** to check the DBService parameter configuration. Perform the following steps to verify the parameter configuration.

Step 3 Check whether the **dbservice.floatip** parameter configuration is correct.

1. The value of **dbservice.floatip** must be the unique IP address that is not used in the network.
2. Run **ping** *dbservice.floatip* in the Linux environment. If the floating IP address can be pinged, it is enabled.
3. Log in to the node that the floating IP address is located, run **ifconfig** *dbservice.floatip.interface* **down** in the Linux environment to disable the floating IP address, and ping the floating IP address again to check whether it exists.
4. If the floating IP address cannot be pinged, it is working properly. Otherwise, the floating IP address exists but it is used on multiple nodes. In this case, change the value of this parameter to the unique IP address on the FusionInsight Manager portal.

Step 4 Run **route** in the Linux environment, and check whether the value of **dbservice.mediator.ip** is consistent with the gateway address. If not, change the value of this parameter to the gateway address on the FusionInsight Manager portal.

Step 5 Log in to the FusionInsight Manager portal, click **Cluster >** *Name of the desired cluster* **> Service > DBService > More > Restart Service**, and restart DBService.

----End

Reference Information

None.

2.4.3.2 Default Port 20051 Is Occupied

Symptom

DBService startup fails during the cluster installation or DBService restart operation, and information indicating that port 20051 is occupied is displayed in the printed fault log.

Possible Causes

- The default port 20051 that DBService uses is occupied by other processes.
- The DBService process is not stopped, and the port used by DBService is not released.

Fault Locating

1. Check whether "already exists for port:20051" exists in the fault log displayed on the FusionInsight Manager portal.
2. It takes about 10 minutes to rectify the fault.

Procedure

Step 1 Log in to the node host where a DBService installation error is reported as user root, and run **ps -ef | grep "20051"**.

Step 2 Run the **kill** command to forcibly stop the processes using port 20051.

Step 3 About 2 minutes later, run the ***netstat -nap | grep 20051*** command again to check whether any process uses the port.

- If yes, go to **Step 4**.
- If no, go to **Step 5**.

Step 4 Check the service to which the process belongs and change the port for the service.

NOTE

Port 20051 is dedicated for DBservice, and cannot be used by other processes.

Step 5 Run the **find . -name '*20051*'** command in the **/tmp** and **/var/run/FusionInsight-DBService** directories, and delete all files found.

Step 6 Log in to the FusionInsight Manager portal, click **Cluster** > *Name of the desired cluster* > **Service** > **DBService** > **More** > **Restart Service**, and restart DBService.

----End

Reference Information

None.

2.4.3.3 Component Depending on DBService Fails to Be Started when the Active and Standby DBService Instances Are Reinstalled

Symptom

If the active and standby DBService instances or the two hosts where the DBService is located are reinstalled, and data is cleared, the component may fail to be started.

Possible Causes

After the active and standby DBService instances are reinstalled, the password of the component database that depends on the DBService is restored to the default value. If the component connects to the DBService database when being started, the startup fails.

Procedure

Step 1 Log in to FusionInsight Manager.

Enter the address in the address box of your browser. The address format is **https://FusionInsight Manager** *WebService floating IPaddress*:**28443/web**.

Step 2 Choose **Cluster** > *Name of the desired cluster* > **Service** > **Component that fails to be started** > **More** > **Changed Database Password**. On the displayed **Verify Identity** dialog box, enter the password and click **OK**.

Step 3 Set **Old Password** to the default password, specify **New Password** and **Confirm Password**, and select **I have read the information and understand the impact**. Then, click **OK**.

NOTE

- If the component does not have a default database password before the host is reinstalled, the startup will not fail.
- If the message "The account has been locked" is displayed, unlock the database user of the component that fails to be started by following the instructions in **Abnormality Caused by Component Database User Password Change**. Then, perform this step again.

Step 4 Restart the component.

----End

Related Information

None

2.4.4 Elasticsearch

2.4.4.1 The group and permission information is normal, but the access to the Elasticsearch service is rejected and permission denied is returned.

Symptom

In the MRS cluster, when a customized user (For example, the user which is added into elasticsearch group or supergroup group) created is used to access the Elasticsearch service, permission denied is returned.

Possible Causes

The cache information of the sssd process is not updated.

Fault Locating

When the **id *username*** command is executed, no normal group(For example, the elasticsearch group) information is displayed in the command output, for example.

Procedure

Log in to each node of the cluster as the **root** user and perform the following operations:

Step 1 Delete the cache file of the sssd process.

rm -rf /var/lib/sss/db/cache_default.ldb

Step 2 Query the sssd process ID.

ps -ef | grep sssd

Step 3 Stop all processes displayed in **Step 2**.

kill -9 *pid1 pid2 pid3*

----End

2.4.4.2 Error Message "max file descriptors [4096] for elasticsearch process is too low, increase to at least [65536]" Is Displayed When an Elasticsearch Instance Fails to Be Started

Symptom

An Elasticsearch instance fails to be started and the error message "max file descriptors [4096] for elasticsearch process is too low, increase to at least [65536]" is displayed.

Possible Causes

The system file descriptor is modified. As a result, the file descriptor does not meet the requirements for starting an Elasticsearch instance.

Fault Locating

Log in to the node where the fault instance resides as the **omm** user and run the **ulimit -n** command. It is found that the command output is less than 65536.

NOTE

If you have logged in to the node where the fault instance resides as the **omm** user before, you must log out and log in as the **omm** user again.

Procedure

Step 1 Log in to the node where the fault instance resides as the **root** user .

Step 2 Run the **cat /etc/security/limits.d/90-nofile.conf** command and check whether the values of *** hard nofile** and *** soft nofile** are greater than 65535.

- If yes, go to **Step 4**.
- If no, go to **Step 3**.

Step 3 Run the **vi /etc/security/limits.d/90-nofile.conf** command to change the values of *** hard nofile** and *** soft nofile** to a value (for example, **640000**) greater than **65535**.

```
*          hard    nofile    640000
*          soft    nofile    640000
```

Step 4 Run the following commands to restart the nodeagent node where the fault instance resides.

su - omm

sh $NODE_AGENT_HOME/bin/stop-agent.sh

sh $NODE_AGENT_HOME/bin/start-agent.sh

Step 5 Restart the fault Elasticsearch instance.

----End

2.4.4.3 Reindex Operation Fails on Elasticsearch of the Source Version After the MRS Cluster Is Upgraded from 6.5.x to 8.x

Symptom

After the cluster is upgraded from 6.5.*x* to 8.*x*, performing a reindex operation on an earlier version of Elasticsearch results in an error if the date format is **yyyy-M-dd** (for example, **2023-1-15**).

```
{
  "error" : {
    "root_cause" : [
      {
        "type" : "mapper_parsing_exception",
        "reason" : "failed to parse field [date] of type [date] in document with id '1'. Preview of field's value:
'2023-1-15'"
      }
    ],
    "type" : "mapper_parsing_exception",
    "reason" : "failed to parse field [date] of type [date] in document with id '1'. Preview of field's value:
'2023-1-15'",
    "caused_by" : {
      "type" : "illegal_argument_exception",
      "reason" : "failed to parse date field [2023-1-15] with format [yyyy-MM-dd HH:mm:ss||yyyy-MM-dd||
epoch_millis]",
      "caused_by" : {
        "type" : "date_time_parse_exception",
        "reason" : "Failed to parse with all enclosed parsers"
      }
    }
  },
  "status" : 400
}
```

Possible Causes

While clusters on version 6.5.*x* recognize the **yyyy-M-dd** format, MRS 8.*x* does not, leading to errors.

Procedure

Specify the **yyyy-M-dd** format when creating an index in MRS 8.*x*. Here is an example: The following is an example.

PUT test_date

{

"mappings": {

"properties": {

"date": {

```
"type": "date",
"format": "yyyy-MM-dd HH:mm:ss||yyyy-MM-dd||epoch_millis||yyyy-M-dd"
}
}
}
}
```

2.4.5 Flume

2.4.5.1 Flume Client WCC Encryption Failed and FileNotFound Is Reported

Symptom

When the Flume client is used to obtain the plaintext ciphertext, the following error is reported.

```
[root@node-master1MBBC bin]# ./genPwFile.sh
Please input key password:
Please Confirm password:
Result:-1
ERROR: Exception in main.Exception.
org.wcc.framework.AppRuntimeException: org.wcc.framework.AppRuntimeException: org.wcc.framework.AppRuntimeException: FileNotFound
        at org.wcc.framework.util.encrypt.Crypter.encrypt(Crypter.java:125)
        at com.omm.encrypt.EncryptCommandWithoutParam.encryptCommandLine(EncryptCommandWithoutParam.java:115)
        at com.omm.encrypt.EncryptCommandWithoutParam.main(EncryptCommandWithoutParam.java:165)
Caused by: org.wcc.framework.AppRuntimeException: org.wcc.framework.AppRuntimeException: FileNotFound
        at org.wcc.framework.util.encrypt.CrypterProxy.encryptWithDomain(CrypterProxy.java:256)
        at org.wcc.framework.util.encrypt.Crypter.encrypt(Crypter.java:115)
        ... 2 more
```

Possible Causes

In Euler 2.9 and Kylin Linux Advanced Server release V10 (Tercel), the **t** permission cannot be granted to the **/tmp** directory. Otherwise, users outside the **omm/ficommon** group will fail to encrypt or decrypt data through WCC.

Security hardening has been performed on the Euler system. Users outside the owner group are not allowed to use it, and files in the directories with the **t** permission cannot be opened in read and write mode.

Fault Locating

Check the permissions of the **/tmp** directory.

```
[root@          tmp]# ll -d /tmp
drwxrwxrwt 35 root root 1200 Dec 16 15:46 /tmp
[root@          tmp]# ll
total 2432
-rw-rw---- 1 omm    ficommon       0 Dec 12 18:26 2431D845C6781B1A5674FD45A0DE13D1BBD54615700E0177C00771C378159F57.plock
-rw-rw-rw- 1 omm    wheel          0 Dec 13 21:07 248D9E715A1437E225F805917779FEE93503A78ABC53A9A564F3DBCE230A67B5.plock
-rw-rw---- 1 omm    ficommon       0 Dec 12 18:26 D55E11D4CE9921E3AF1110943F8AF3CCE7431BC9FBEF5B2B5D8354DDF193823C
-rw-rw-rw- 1 omm    wheel          0 Dec 15 15:30 D9A91B013191E13CE0D1D33DDCECA0F50BAF480383949C73E2323946B943472E.plock
-rw------- 1 root   root       75205 Dec 16 14:58 debug.log
drwx------ 2 root   root          60 Dec 15 15:34 diskmgt
-rw------- 1 omm    wheel          0 Dec 16 15:46 dntrash_lockfile
drwx------ 2 omm    wheel         40 Dec 15 21:30 elasticsearch-116356950099966644
drwx------ 3 omm    wheel         60 Dec 15 21:10 embedded-jetty-jsp
-rw------- 1 omm    wheel        424 Dec 14 10:18 executor-reconfig.log
-rw------- 1 root   root       28820 Dec 15 15:34 fi-preinstall.log
drwxr-x--- 4 omm    wheel         80 Dec 16 12:51 flink-web-f13058ae-0fb1-448a-9c24-f6ac716cfc5e
drwx------ 4 omm    wheel         80 Dec 16 14:19 FusionInsight-Client
-rw-r----- 1 omm    wheel     198568 Dec 16 14:32 hadoop1328285560882397 91.tmp
drwx------ 3 omm    wheel         60 Dec 12 19:33 hadoop-omm
drwx------ 4 omm    wheel         80 Dec 16 14:45 hadoop-unjar3583691701179822109
drwx------ 5 omm    wheel        100 Dec 16 14:46 hadoop-unjar3733375382858240593
drwx------ 3 root   root          60 Dec 16 14:29 HBase
drwxr-x--- 2 omm    wheel        920 Dec 16 15:46 hsperfdata_omm
drwxr-x--- 2 ommdba wheel         60 Dec 16 15:46 hsperfdata_ommdba
drwx------ 2 root   root          60 Dec 16 15:45 hsperfdata_root
drwx------ 2 omm    wheel         40 Dec 15 20:06 jetty-8-99-8-7-25013-journal-_-any-9132888559714302336
drwx------ 2 omm    wheel         40 Dec 15 20:05 jetty-8-99-8-7-25021-router-_-any-3926309382281159720
drwx------ 3 omm    wheel         60 Dec 15 20:58 jetty-8-99-8-7-26006-hadoop-yarn-common-3_1_1-hw-ei-302053_jar-_-any-23734509077
drwx------ 2 omm    wheel         40 Dec 15 20:41 jetty-localhost-25016-datanode-_-any-1281595840763214320
-rw------- 1 omm    wheel        146 Dec 12 19:03 KerberosClient
-rw------- 1 omm    wheel        424 Dec 14 10:18 knox-reconfig.log
-rw------- 1 root   root         875 Dec 16 15:41 krb5cc_0
-rw------- 1 omm    wheel      77859 Dec 15 20:12 liblz4-java-6105954007771057054.so
-rw------- 1 omm    wheel          0 Dec 15 20:12 liblz4-java-6105954007771057054.so.lck
-rw------- 1 root   root           0 Dec 14 10:17 mountdisk_success
drwxr-x--- 2 omm    wheel         40 Dec 16 15:45 omm
-rw------- 1 root   root          90 Dec 15 15:28 preset_temp.tar.gz.sha256.temp
-rw------- 1 omm    wheel         74 Dec 15 21:43 PRESTART_LOG
-rw------- 1 omm    wheel       9658 Dec 16 15:45 report.json
drwx------ 3 root   root          60 Dec 16 14:29 root
-rw-r----- 1 omm    wheel     133104 Dec 16 14:32 snappy918899074705917354.tmp
drwx------ 3 root   root          60 Dec 15 17:19 systemd-private-dfd7cca37c3e44508f3b78e05c24befa-ntpd.service-W2kNMS
drwx------ 3 root   root          60 Dec 12 18:18 systemd-private-dfd7cca37c3e44508f3b78e05c24befa-systemd-logind.service-IJEpas
-rw------- 1 omm    wheel          0 Dec 16 15:46 tmp_error
drwx------ 3 omm    wheel         60 Dec 15 21:44 tomcat.4114272991010493119.29861
drwx------ 3 omm    wheel         60 Dec 15 21:43 tomcat.4496489467618032617.29880
drwx------ 3 omm    wheel         60 Dec 12 19:33 tomcat.6667174223875379994.29861
drwx------ 3 omm    wheel         60 Dec 12 19:33 tomcat.7552101220935832663.29880
drwx------ 2 omm    wheel         40 Dec 12 19:33 tomcat-docbase.1422917257033642362.29880
drwx------ 2 omm    wheel         40 Dec 15 21:44 tomcat-docbase.2854779939139656220.29861
drwx------ 2 omm    wheel         40 Dec 15 21:43 tomcat-docbase.6947113845883371222.29880
drwx------ 2 omm    wheel         40 Dec 12 19:33 tomcat-docbase.7761033508875374815.29861
-rw-rw---- 1 omm    ficommon       0 Dec 12 18:25 _wcc_file_locker_
-rw-r----- 1 omm    wheel     1181776 Dec 16 14:32 zstd2846212490650482034.tmp
```

Procedure

Run the following command to delete the permission on the **/tmp** directory:

chmod o-t /tmp

2.4.6 FTP-Server

2.4.6.1 FTP Client Cannot Be Logged In to and Error Message "530 Authentication failed" Is Displayed

Symptom

In the cluster in security model, a login failure occurs when you log in to the FTP server using the correct username and password. The FTP server returns the error message "530 Authentication failed".

Possible Causes

- HDFS fault

  The FTP server will be suspended for a short period if the HDFS is faulty. If this occurs, no thread in the thread pool can respond to the login request from the client and no result will be returned.

- Ldap fault

  The authentication of the FTP server depends on the Ldap service. The authentication fails if the Ldap service is faulty.

- sssd service exception

  The authentication of the FTP server requires a check on the group to which the user belongs and this check depends on the sssd service.

Fault Locating

1. Check the HDFS service status.
2. Check the Ldap service status.
3. Run the id command to check the group to which the user belongs.

Procedure

Step 1 Log in to the FusionInsight Manager portal.

Step 2 Click **O&M > Alarm > Alarm** and check whether the alarm message "Unavailable HDFS service" exists on the alarm page.

- If yes, handle the alarm according to the alarm help.
- If no, go to **Step 3**.

Step 3 Check whether the alarm message "Unavailable Ldap service" exists on the alarm page.

- If yes, handle the alarm according to the alarm help.
- If no, go to **Step 4**.

Step 4 Log in to the faulty FTP server as user **root** , and run the following command to switch to user **omm**:

su - omm

NOTE

Ensure that the following operations are performed as user **omm**.

Step 5 Run the following command:

id -Gn *Username*

Step 6 Check whether the group to which the user belongs exists in the command output.

- If yes, contact the technical support.
- If no, go to **Step 7**.

Step 7 Wait 10 minutes for the sssd service to synchronize user data and then log in to the FTP client again to check whether the login is successful.

- If yes, no further action is required.
- If no, contact the technical support.

----End

Reference Information

None.

2.4.6.2 FTP-Server Uploads Data in a Slow Speed

Symptom

When data is uploaded to the cluster through FTP-Server, the upload speed is slow.

Possible Causes

- The network between the client and the server is faulty.
- The customer's self-developed code has errors.
- HDFS DataNode is faulty.

Fault Locating

1. Run the **ftp** command (manual installation is required) to check whether the problem is caused by the faulty server, customer code, or network.
2. If the server is faulty, check the DataNode running status of the HDFS.

Procedure

Step 1 On a node in the cluster, use **ftp** to access the FTP server and check whether it can be accessed.

ftp *IP Port*

```
[root@192-168-20-162 flink]# ftp 192.168.20.162 22021
Connected to 192.168.20.162 (192.168.20.162).
220 Service ready for new user.
Name (192.168.20.162:root): admintest
331 User name okay, need password for admintest.
Password:
230 User logged in, proceed.
Remote system type is UNIX.
ftp> ls
227 Entering Passive Mode (192,168,20,162,86,220)
150 File status okay; about to open data connection.
drwxrwxrwx    0 flink hadoop            0 Jul 21 10:00 FusionInsight_FlinkServer
drwxr-xr-x    0 admintest supergroup            0 Jun  9 10:09 HiBench
drwxrwxrwx    0 hdfs hadoop            0 May 31 12:04 app-logs
drwxr-xr-x    0 hdfs hadoop            0 May 31 12:04 datasets
drwxr-xr-x    0 hdfs hadoop            0 May 31 12:04 datastore
drwxrwx---    0 flink hadoop            0 May 31 12:04 flink
drwxr-x---    0 flume hadoop            0 May 31 12:04 flume
drwx------    0 admintest supergroup            0 Jun 20 16:06 hudi
drwxrwxrwx    0 mapred hadoop            0 May 31 12:04 mr-history
drwxrwxrwx    0 hdfs hadoop            0 May 31 12:04 mrs
drwxrwxrwt    0 spark hadoop            0 Jun 13 21:07 sparkJobHistory
drwx--x--x    0 admin supergroup            0 May 31 12:04 tenant
drwxrwxrwx    0 hdfs hadoop            0 Jun 20 16:06 tmp
drwxrwxrwx    0 hdfs hadoop            0 Jun 28 20:40 user
drwxr-xr-x    0 sparkuser supergroup            0 Jun  9 11:20 var
226 Closing data connection.
ftp> exit
221 Goodbye.
You have new mail in /var/spool/mail/root
[root@192-168-20-162 flink]#
```

- If it can be accessed, the FTP service is normal. Go to **Step 3**.
- If it cannot be accessed, the HDFS DataNode may be abnormal. Go to **Step 3**.

NOTE

IP indicates the service IP address of the node where FTP-Server is installed.

To obtain the value of **Port**, log in to FusionInsight Manager, choose **Cluster** > **Services** > **FTP-Server**, click **Configurations**, and click **All Configurations**. On the displayed page, search for and check the value of **Port**. The default value is **22021**.

Step 2 Run the **ftp** command on the service node to access the FTP server and check whether it can be accessed.

- If it can be accessed, the problem may be caused by the faulty customer's service code.
- If it cannot be accessed, check the network.

Step 3 Log in to the FusionInsight Manager portal.

Step 4 Choose **O&M** > **Alarm** > **Alarms** and check whether alarms related to HDFS are generated.

- If the alarms are generated, rectify the fault by referring to the alarm help.
- If the alarms are not generated, go to **Step 5**.

Step 5 Choose **O&M** > **Log** > **Download**. Set **Service** to **FTP-Server** of the cluster to be operated.

Step 6 In the upper right corner, select a log time range, or click to specify the period for log collection by setting the start time and end time, and click **Download**.

Step 7 Contact technical support and send the collected fault logs.

----End

Reference Information

None.

2.4.7 GraphBase

2.4.7.1 Common GraphBase Client Faults

2.4.7.1.1 Error Message "Connection timed out: connect" Is Displayed

Symptom

The following information is displayed in the log when the GraphBase client is running: "Connection timed out: connect".

Possible Causes

- The IP address configured on the client for accessing the GraphBase service is different from the value of **loadbalancer.floatip** in the cluster. As a result, the client connection times out.
- CAS login verification failed.

Fault Locating

1. Check whether the IP address configured for accessing the GraphBase service in the running environment of the client is the same as the value of **loadbalancer.floatip** configured on FusionInsight Manager.
2. Check whether the value of **casIp** configured for accessing the GraphBase service in the running environment of the client is the same as the IP address in the URL (**https://IP:28443/web**) for accessing FusionInsight Manager.

Procedure

Step 1 Log in to FusionInsight Manager.

Step 2 Choose **Cluster >** *Name of the desired cluster* **> Service** > **GraphBase** > **Configuration > All Configurations** and check the value of **loadbalancer.floatip**.

Step 3 Use WinSCP to log in to the node where the client is deployed as user **root** and go to the directory **/opt/graphbaseClient/GraphBase/examples/**. Download the sample project graphbase-core-example to the local host, go to the conf directory, check whether the IP address for accessing the GraphBase service in **graphbase.properties** is the same as the value of **loadbalancer.floatip**, and whether the value of **casIp** is the same as the IP address in the URL (**https://***IP:28443***/web**) for accessing FusionInsight Manager.

Step 4 Change the value of the IP address for accessing the GraphBase service in the **graphbase.properties** configuration file to the value of **loadbalancer.floatip**, and ensure that the value of **casIp** is the same as the IP address in the URL (**https://***IP:28443***/web**) for accessing FusionInsight Manager.

Step 5 Run the GraphBase client again.

----End

Reference

None

2.4.7.1.2 Error Message "Connection refused: connect" Is Displayed

Symptom

The following information is displayed in the log when the GraphBase client is running: "Connection refused: connect".

Possible Causes

The port number configured on the client for accessing the GraphBase service is different from the value of **loadbalancer.https.port** in the cluster. As a result, the client connection is refused.

Fault Locating

Check whether the port configured for accessing the GraphBase service in the running environment of the client is the same as the value of **loadbalancer.https.port** configured on FusionInsight Manager.

Procedure

Step 1 Log in to FusionInsight Manager.

Step 2 Choose **Cluster** > *Name of the desired cluster* > **Service** > **GraphBase** > **Configuration** > **All Configurations** and check the value of **loadbalancer.https.port**.

Step 3 Use WinSCP to log in to the node where the client is deployed as user **root** and go to the **/opt/graphbaseClient/GraphBase/examples** directory. Download the sample project graphbase-core-example to the local host, go to the conf directory, and check whether the port number for accessing the GraphBase service in the **graphbase.properties** file is the same as the value of **loadbalancer.https.port**.

Step 4 Change the port number for accessing the GraphBase service in the **graphbase.properties** configuration file to the same as the value of **loadbalancer.https.port**.

Step 5 Run the GraphBase client again.

----End

Reference

None

2.4.7.1.3 Data Occasionally Cannot Be Obtained During the Runtime of the Client

Symptom

When the GraphBase client is running, the log similar to the following is displayed:

```
REQ HEADER: POST https://X.X.X.X:22380/graphbase/graph/graphbase/edge/search HTTP/1.1
REQ BODY:   {"filterList":[{"propertyName":"weight","predicate":"=","values":
[0.6]}],"edgeLabel":"call","limit":1}
RSP BODY:   {
"msg": "The edge full search result does not exist.",
"code": "20506",
"data": {}
}
[FAIL]: search edge [call] fail.
[main] INFO com.huawei.GraphBaseRestExample - null
```

Possible Causes

There is a delay in writing index data. As a result, the latest data cannot be queried. After an external index is created, a short delay occurs in data flash during new index data writing to the external index engine.

The main reason is that the index storage engine (Elasticsearch) data is written to the cache first, and then the data cache is flashed to the disk in a very short time.

Fault Locating

Check whether the edge data can be obtained when it is queried for the second time.

Procedure

Method 1: Run the sample data repeatedly, wait for a short time after the data is written, and then query the data.

Method 2: Disable the Elasticsearch cache. (This function is not recommended, which affects the index data writing performance.)

Step 1 Log in to FusionInsight Manager, choose **Cluster >** *Name of the desired cluster* **> Service** > **Elasticsearch** > **Configurations** > **All Configuration**, add the user-defined parameter **elasticsearch.customized.configs**, set the name to **refresh_interval**, and set the value to **-1**.

Step 2 Restart Elasticsearch.

----End

Reference

None

2.4.7.1.4 Error Message "cas login fail" Is Displayed

Symptom

The following information is displayed in the log when the GraphBase client is running: "cas login fail".

Possible Causes

The username, or keytab file used for accessing the GraphBase service on the GraphBase client is incorrect.

Fault Locating

In the keytab-based authentication, confirm that the username is correct, and download the keytab file.

Procedure

Step 1 Check whether the username and password configured in **graphbase.properties** for accessing the GraphBase service are correct.

```
ip =
port =
userName =
```

Step 2 On FusionInsight Manager, choose **System** > **Permission** > **User**. Locate the row that contains the user and choose **More** > **Download Authentication Credential** to download the user authentication file.

Obtain the **graphtest_***1527219173664***_keytab.tar** package. Decompress the package to obtain the **user.keytab** user authentication file.

Step 3 Run the GraphBase client again.

----End

Reference

None

2.4.7.2 Common GraphBase O&M Faults

2.4.7.2.1 GraphBase Service Fault Caused by ZooKeeper Faults

Symptom

The following alarm information is displayed in the GraphBase service log:

```
[WARN ] [2018-11-22 16:09:20,532] [SendThread] org.apache.zookeeper.ClientCnxn.run(1449) - Session
0x1301125897b33987 for server X.X.X.X:X, unexpected error, closing socket connection and attempting
reconnect
java.net.ConnectException: Connection refused
at sun.nio.ch.SocketChannelImpl.checkConnect(Native Method) ~[?:1.8.0_162]
at sun.nio.ch.SocketChannelImpl.finishConnect(SocketChannelImpl.java:717) ~[?:1.8.0_162]
at org.apache.zookeeper.ClientCnxnSocketNIO.doTransport(ClientCnxnSocketNIO.java:364)
~[zookeeper-3.5.1.jar:EI_Zookeeper_Component_3.5.1.0100.B008_Hadoop_2.7.2.0100.B008]
at org.apache.zookeeper.ClientCnxn$SendThread.run(ClientCnxn.java:1428)
[zookeeper-3.5.1.jar:EI_Zookeeper_Component_3.5.1.0100.B008_Hadoop_2.7.2.0100.B008]
```

Possible Causes

The ZooKeeper service is unavailable or GraphBase is disconnected from the ZooKeeper service.

Fault Locating

- Check whether the ZooKeeper service is running properly.
- Check whether the network connection is normal.

Procedure

Step 1 Check whether the ZooKeeper service is available. If it is unavailable, rectify the ZooKeeper fault. For details, see "ALM-13000 ZooKeeper Service Unavailability" in product documentation.

Step 2 Check whether the GraphBase server can connect to the ZooKeeper server. If the two servers are disconnected from each other, rectify the network fault.

Step 3 If the fault persists, collect the process logs and contact the technical support.

----End

Reference

None

2.4.7.2.2 GraphBase Service Fault Caused by HBase Faults

Symptom

The GraphBase client does not receive any response after sending an operation request.

```
The following alarm information is displayed in the GraphBase service log:
Caused by: java.io.IOException: Failed to get result within timeout, timeout=60000ms
at org.apache.hadoop.hbase.client.ScannerCallableWithReplicas.call(ScannerCallableWithReplicas.java:241)
~[hbase-client-2.2.3.jar:2.2.3]
at org.apache.hadoop.hbase.client.ScannerCallableWithReplicas.call(ScannerCallableWithReplicas.java:60)
~[hbase-client-2.2.3.jar:2.2.3]
at org.apache.hadoop.hbase.client.RpcRetryingCaller.callWithoutRetries(RpcRetryingCaller.java:218) ~[hbase-
client-2.2.3.jar:2.2.3]
at org.apache.hadoop.hbase.client.ClientScanner.call(ClientScanner.java:314) ~[hbase-client-2.2.3.jar:2.2.3]
at org.apache.hadoop.hbase.client.ClientScanner.nextScanner(ClientScanner.java:289) ~[hbase-
client-2.2.3.jar:2.2.3]
at org.apache.hadoop.hbase.client.ClientScanner.initializeScannerInConstruction(ClientScanner.java:164)
~[hbase-client-2.2.3.jar:2.2.3]
at org.apache.hadoop.hbase.client.ClientScanner.<init>(ClientScanner.java:159) ~[hbase-client-2.2.3.jar:2.2.3]
at org.apache.hadoop.hbase.client.HTable.getScanner(HTable.java:796) ~[hbase-client-2.2.3.jar:2.2.]
at com.v5analytics.simpleorm.HBaseSimpleOrmSession.findAll(HBaseSimpleOrmSession.java:118) ~[visallo-
simple-orm-hbase-1.1.jar:?]
... 5 more
```

Possible Causes

The HBase service is unavailable or GraphBase is disconnected from the HBase service.

Fault Locating

- Check whether the HBase service is running properly.
- Check whether the network connection is normal.

Procedure

Step 1 Check whether the HBase service is available. If it is unavailable, rectify the HBase fault.

Step 2 Check whether the GraphBase server can connect to the HBase server. If the two servers are disconnected from each other, rectify the network fault.

Step 3 If the fault persists, collect process logs and contact the technical support.

----End

Reference

None.

2.4.7.2.3 GraphBase Index Query Failure Due to Elasticsearch Mode Switching

Symptom

The following error information is displayed during query using indexes:

```
{"msg":"Could not execute operation due to backend exception","code":"20002","data":{}}
Background logs:
[ERROR] [2018-11-23 17:33:32,534] [https-jsse-nio-10.26.66.144-22388-exec-10]
org.visallo.web.routes.graphbase.vertex.GraphBaseVertexIndexQuery.error(62) - the input parameter query is illegal.
```

Possible Causes

- After the Elasticsearch service is switched from the safe mode to the normal mode, the GraphBase service is not restarted.
- After the Elasticsearch service is switched from the normal mode to the secure mode, the GraphBase service is not restarted.

Fault Locating

- Check whether the Elasticsearch service is running properly.
- After Elasticsearch is switched from the security mode to the normal mode, check whether the upper-layer service is selected during the Elasticsearch service restart.
- After Elasticsearch is switched from the normal mode to the security mode, check whether the upper-layer service is selected during the Elasticsearch service restart.

Procedure

Step 1 Check whether the Elasticsearch service is available. If it is unavailable, rectify the Elasticsearch fault.

Step 2 Log in to FusionInsight Manager, choose **Cluster >** *Name of the desired cluster* **> Service** > **Elasticsearch** > **Configuration** > **All Configurations** > **Security**, set **ELASTICSEARCH_SECURITY_ENABLE** to **false** or **true** as required, and click **Save**. In the displayed **Save Configuration** dialog box, confirm the modification and click **OK**. Wait until the message "Operation succeeded" is displayed, and click **Finish**.

Step 3 The configuration is saved successfully.

After the configuration is saved, restart the expired service or instance for the configuration to take effect.

Step 4 After the service or instance is restarted, perform a query using indexes.

Step 5 If the fault persists, collect process logs and contact the technical support.

----End

Reference

None

2.4.8 HBase

2.4.8.1 Common HBase Client Faults

2.4.8.1.1 Client Login Failure

Symptom

When a user starts a HBase client and log in, a login failure occurs.

Possible Causes

- The krb5 file is not configured correctly in the client environment. This cause occurs only in security mode, but not normal mode.
- The username and password file used to access the HBase cluster are not configured in the hbase-site.xml configuration file of the client environment or the password file has expired. This cause occurs only in security mode, but not normal mode.
- The Jar packages in the client environment are inconsistent with those in the cluster.
- The time of the client environment is inconsistent with the time of the cluster and the difference is more than 3 minutes.

Fault Locating

1. In security mode, if the krb5 configuration file is inconsistent, update the local configuration file.
2. In security mode, if principal, keytab, and other parameters are not configured in the hbase-site.xml file, add them to the file.
3. If the jar packages are inconsistent, replace them with those of the cluster.
4. If the time is inconsistent, synchronize the time on the local machine with time of the cluster. Do not change the time of the cluster. (Changing the cluster time is a critical operation.)
5. After troubleshooting, restart the client. It takes about 10 minutes to rectify the fault.

Procedure

Step 1 (Optional) In security mode, check whether the local krb5 configuration file is consistent with the that in the cluster.

- Configuration file path in the Windows environment: **C:\Windows\krb5.ini**.
- Configuration file path in the Linux environment: **/etc/krb5.conf**.

Step 2 (Optional) In security mode, check whether the kerberos principal and keytab used for login are correct.

Step 3 Check whether the time in the local environment is consistent with the that in the cluster.

Step 4 Check whether the local jar packages are consistent with those of the cluster (especially the jar packages related to HBase, ZooKeeper, and Hadoop)

----End

Reference Information

None.

2.4.8.1.2 "SASL authentication failed" Displayed on a Client

Symptom

In security mode, the client process fails to access the HBase cluster. A log similar to the following is generated:

```
SASL authentication failed. The most likely cause is missing or invalid credentials. Consider 'kinit'.
```

Possible Causes

The client process invokes the User#login method several times for login.

Fault Locating

1. Modify client code to prevent multiple logins in the process.
2. After modifying code, restart the client.
3. It takes about 10 minutes to rectify the fault.

Procedure

Step 1 Check whether the client log file contains multiple logs similar to the following: "Login successful for user XXXXX using keytab file XXXXXX". If yes, there are multiple login attempts.

Step 2 Check the client code to prevent repeated logins in the process.

----End

Reference Information

None.

2.4.8.2 Common HBase Operation Faults

2.4.8.2.1 hbase:meta Cannot Be Found Because of Network or OS Faults

Symptom

When applications such as MapReduce and Spark are run, the following error may occur, resulting in a task execution failure:

```
Caused by: java.net.SocketTimeoutException: callTimeout=60000, callDuration=60304: row ''
on table 'hbase:meta' at region=hbase:meta,,1.1588230740, hostname=host1,21302,1448886113294,
seqNum=0
at org.apache.hadoop.hbase.client.RpcRetryingCaller.callWithRetries(RpcRetryingCaller.java:159)
at org.apache.hadoop.hbase.client.ResultBoundedCompletionService
$QueueingFuture.run(ResultBoundedCompletionService.java:64)
... 3 more
```

Possible Causes

- The HDFS service is unavailable.
- The location of the meta region stored in ZooKeeper is inconsistent with the actual location.

Fault Locating

None.

Procedure

Step 1 Check whether HDFS is available. If the service is unavailable, rectify the HDFS fault.

Step 2 If HDFS is normal, identify the node where the hbase:meta table resides based on the HBase original page. Then restart the RegionServer of the node.

Step 3 If the fault persists, collect the log and contact technical support.

----End

Reference Information

None.

2.4.8.2.2 Active/Standby Switchover of the HMasters Fails

Symptom

During active/standby switchover of HMasters, the standby HMaster fails to become active in 10 minutes. In this case, both HMasters are standby, and the following information is generated in the run log of the HMaster:

```
2015-11-23 08:48:47,643 | INFO  | MASTER_SERVER_OPERATIONS-linux-174:21300-3 | Skip assigning region
in transition on other
server{7630007b8b816b171535a056ae828fcf state=CLOSED, ts=1448239727400,
server=linux-223,21302,1448101490432} |
org.apache.hadoop.hbase.master.handler.ServerShutdownHandler.process(ServerShutdownHandler.java:268)
```

Possible Causes

Services are running during the startup process, which results in an increase in the Region. The increase in the Region triggers the Region split operation, which divides a Region into multiple Regions. When the new HMaster goes online, the RegionServer registered by meta region on the ZooKeeper needs to be re-allocated and the meta table needs to be re-loaded. The HMaster checks the Region status on all RegionServers and places the Regions online. Then the HMaster performs the OFFLINE > PENDING_OPEN > OPENING > OPEN process and executes the split

tasks that have not been completed. If there is a large number of Regions, the time required for placing them online is long. If the time exceeds the value specified by **hbase.master.initializationmonitor.timeout**, the HMaster expected to become active will fail to go online, resulting in an active/standby switchover failure.

Fault Locating

None.

Procedure

Step 1 On FusionInsight Manager, choose **Cluster >** *Name of the desired cluster* > **Services > HBase > Configurations > All Configurations**. Search and modify the value of **hbase.master.initializationmonitor.timeout** .

NOTE

The default value of **hbase.master.initializationmonitor.timeout** is 3600000. The parameter is usually used together with **hbase.master.initializationmonitor.haltontimeout**. Based on the test result, if there are more than 2000 Regions, the HMaster needs 360s to go online in the preceding scenario. You can modify the value based on the actual situation.

Step 2 Choose **Cluster >** *Name of the desired cluster* > **Services > HBase > Instance**, select the HMaster instances and choose **More** > **Restart Instance**. Enter the password and restart the HMaster instances.

----End

Reference Information

None.

2.4.8.2.3 The LoadIncrementalHFiles Tool Failed

Symptom

While trying to load more than 32 Hfiles to one Family of one Region, LoadIncrementalHFiles loading failed with following exception.

```
Exception in thread "main" java.io.IOException: Trying to load more than 32 hfiles to one family of one
region
	at
org.apache.hadoop.hbase.mapreduce.LoadIncrementalHFiles.doBulkLoad(LoadIncrementalHFiles.java:302)
	at org.apache.hadoop.hbase.mapreduce.LoadIncrementalHFiles.run(LoadIncrementalHFiles.java:884)
	at org.apache.hadoop.util.ToolRunner.run(ToolRunner.java:75)
	at org.apache.hadoop.util.ToolRunner.run(ToolRunner.java:90)
	at org.apache.hadoop.hbase.mapreduce.LoadIncrementalHFiles.main(LoadIncrementalHFiles.java:890)
```

Possible Causes

During data loading, the default maximum number of HFiles is 32. This error occurs when a Family in a Region has more than 32 HFiles.

Fault Locating

None.

Procedure

Step 1 Add **hbase.mapreduce.bulkload.max.hfiles.perRegion.perFamily** to the **LoadIncrementalHFiles** command when running it and set this parameter to the largest value. This parameter value indicates the maximum number of HFiles that can be generated under the family.

For example, the system supports 40 HFiles when the following command runs.

```
cd <hbase_client>/HBase/hbase
bin/hbase org.apache.hadoop.hbase.mapreduce.LoadIncrementalHFiles -
Dhbase.mapreduce.bulkload.max.hfiles.perRegion.perFamily=40 <hdfs://storefileoutput> <tablename>
```

Step 2 If the fault persists, collect the process logs and submit to the technical support engineers.

----End

Reference Information

None.

2.4.8.2.4 No HMaster in the Active State Exists in the Cluster

Symptom

On the FusionInsight Manager HBase service page, no HMaster in the Active state exists in the cluster. The HMaster service cannot be provided.

Possible Causes

The communication between the HMaster service and ZooKeeper service is unstable. This occurs because the ZooKeeper service is not running properly.

Fault Locating

The communication between the HMaster service and ZooKeeper service is unstable.

1. On a HMaster node that was in the Active state previously, error information similar to the following is displayed in the logs:
```
Checksum failed.
AuthFailed for /hbase/master
```
2. View the ZooKeeper logs. If information indicating that the quorumpeer instance has been restarted for multiple times exists in the logs, find the faulty quorumpeer instance, and rectify the fault.

Procedure

Find the faulty quorumpeer instance and perform the following operations.

Step 1 Log in to FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **ZooKeeper** > **Instance** > **quorumpeer**, and select the faulty quorumpeer.

Step 2 Choose **More > Restart Instance**, and enter the password to restart the quorumpeer.

----End

Reference Information

None.

2.4.8.2.5 "OutOfMemoryError: Direct buffer memory" Written in RegionServer Log

Symptom

During running a bulkload job or region open operation, a log similar to the following is generated at RegionServer side:

```
"java.lang.OutOfMemoryError: Direct buffer memory"
```

Possible Causes

HBase need a good amount of memory for its various operations. It uses direct buffer memory for I/O operation, so the environment should provide more direct buffer and heap memory to RegionServer for better performance and increasing number of concurrency.

Fault Locating

Check the JVM parameters, increase the heap (-Xms/-Xmx) and direct buffer memory (-XX:MaxDirectMemorySize) as per the use case.

Procedure

Increase the heap and direct buffer memory to avoid OutOfMemory problem.

Step 1 Log in to FusionInsight Manager, choose **Cluster >** *Name of the desired cluster* **> Services > HBase > Configurations > All Configurations**. In the navigation tree, choose **RegionServer** > **System**, config the **GC_OPTS** parameter.

For example:

-Xms32G -Xmx32G -XX:MaxDirectMemorySize=2048M

NOTE

By default, **-XX:MaxDirectMemorySize** is not configured in the **GC_OPTS** parameter. To configure it, you need to add it to the **GC_OPTS** parameter as an custom option.

Modify these GC_OPTS as per the use case. More memory resources are used if more concurrent read/write operations are performed on the RegionServer. According to actual practice, the preceding configuration can support 30 concurrent tasks on the RegionServer in a long term.

Step 2 Restart the RegionServer and client operations.

Step 3 If the fault persists, collect the process logs and submit to technical support.

----End

Reference Information

None.

2.4.8.2.6 Disk Fault Causes Regions to Stay Offline Despite RegionServer Restart

NOTE

This section applies only to the physical machine cluster.

Symptom

After the disk is faulty, the RegionServer is restarted. However, the region remains offline.

Possible Causes

Regions are reallocated when the disk becomes faulty and the related RegionServer is restarted. As a result, the region allocation fails and regions stay offline.

Fault Locating

Identify the cause of the disk fault and the cause of RegionServer restart.

Procedure

Step 1 Clear the disk fault.

Step 2 After the disk fault is rectified and the HBase health status is restored, run the **hbase hbck -j** *${CLIENT_HOME}*/**HBase/hbase/tools/hbase-hbck2-*.jar assigns -o** *<ENCODED_REGIONNAME>* command to bring regions online.

Step 3 If the fault persists, collect process logs and submit them to technical support.

----End

Reference Information

None.

2.4.8.2.7 Multiple Regions Are in RIT Status, An Abnormality Occurs in HMaster, and "Packet len6080218 is out of range" Is Displayed in the Log

Symptom

Multiple Regions are in RIT status, an abnormality occurs in HMaster. The slave and master always switch with each other, but cannot recover. The print information in the log is displayed as follows:

```
Packet len6080218 is out of range!
```

Possible Causes

Multiple Regions are in RIT status. When the Region information of RIT is read, the value exceeds the default value of **jute.maxbuffer**, and the reading fails.

Fault Locating

None.

Procedure

To configure the value of **jute.maxbuffer**, refer to the following information:

Theoretically, 1 MB can hold 6990 Regions at most.

References

None.

2.4.8.2.8 "Found lingering reference file" Is Displayed in the hbck Command Output

Symptom

The residual reference file refers to the reference file that connects to the HFile, which does not exist in HDFS.

The hbck tool reports the following errors ({CLIENT_HOME} in the command indicates the client installation directory):

```
hbase/bin> hbase hbck -j /opt/client/HBase/hbase/tools/hbase-hbck2-1.1.0-h0.cbu.mrs.*.jar filesystem
15:07:33.088 [main] INFO  org.apache.hadoop.hbase.zookeeper.RecoverableZooKeeper - Process
identifier=GlobalIndexTracker-Client: connecting to ZooKeeper
ensemble=host1:24002,host2:24002,host3:24002
Debug is  true storeKey false useTicketCache true useKeyTab false doNotPrompt false ticketCache is null
isInitiator true KeyTab is null refreshKrb5Config is false principal is null tryFirstPass is false useFirstPass is
false storePass is false clearPass is false
Acquire TGT from Cache
Principal is test@HADOOP.COM
Commit Succeeded

15:07:33.115 [main] INFO  org.apache.hadoop.hbase.client.GlobalIndexTracker - GlobalIndexCacheTracker
started successfully
15:07:34.839 [main] INFO  org.apache.hadoop.hbase.zookeeper.RecoverableZooKeeper - Process
identifier=HBCK2 connecting to ZooKeeper ensemble=host1:24002,host2:24002,host3:24002
Debug is  true storeKey false useTicketCache true useKeyTab false doNotPrompt false ticketCache is null
isInitiator true KeyTab is null refreshKrb5Config is false principal is null tryFirstPass is false useFirstPass is
false storePass is false clearPass is false
Acquire TGT from Cache
Principal is test@HADOOP.COM
Commit Succeeded

15:07:35.420 [hbasefsck-0] INFO  org.apache.hadoop.metrics2.impl.MetricsConfig - Loaded properties from
hadoop-metrics2-hbase.properties
15:07:35.443 [hbasefsck-0] INFO  org.apache.hadoop.metrics2.impl.MetricsSystemImpl - Scheduled Metric
snapshot period at 10 second(s).
15:07:35.444 [hbasefsck-0] INFO  org.apache.hadoop.metrics2.impl.MetricsSystemImpl - HBase metrics
system started
15:07:35.495 [hbasefsck-0] INFO  org.apache.hadoop.hbase.metrics.MetricRegistries - Loaded
MetricRegistries class org.apache.hadoop.hbase.metrics.impl.MetricRegistriesImpl
15:07:35.844 [hbasefsck-0] INFO  org.apache.hadoop.io.compress.CodecPool - Got brand-new decompressor
[.snappy]
```

```
15:07:35.939 [hbasefsck-2] INFO  org.apache.hadoop.io.compress.CodecPool - Got brand-new decompressor
[.snappy]
Checked 24 hfiles for corruption
 Corrupt HFiles:                  0
 HFiles moved while checking:     0
HFile Summary: OK
Checked 0 MOB files for corruption
 Corrupt MOB files:               0
 MOB files moved while checking:  0
MOB summary: OK
Debug is  true storeKey false useTicketCache true useKeyTab false doNotPrompt false ticketCache is null
isInitiator true KeyTab is null refreshKrb5Config is false principal is null tryFirstPass is false useFirstPass is
false storePass is false clearPass is false
Acquire TGT from Cache
Principal is test@HADOOP.COM
Commit Succeeded

15:07:36.216 [main] INFO  org.apache.hadoop.hbase.zookeeper.RecoverableZooKeeper - Process
identifier=GlobalIndexTracker-Client: connecting to ZooKeeper
ensemble=host1:24002,host2:24002,host3:24002
Debug is  true storeKey false useTicketCache true useKeyTab false doNotPrompt false ticketCache is null
isInitiator true KeyTab is null refreshKrb5Config is false principal is null tryFirstPass is false useFirstPass is
false storePass is false clearPass is false
Acquire TGT from Cache
Principal is test@HADOOP.COM
Commit Succeeded

15:07:36.239 [main] INFO  org.apache.hadoop.hbase.client.GlobalIndexTracker - GlobalIndexCacheTracker
started successfully
15:07:36.342 [main] INFO  org.apache.hbase.hbck1.HBaseFsck - Loading regioninfos HDFS

15:07:36.663 [main] WARN  org.apache.hbase.hbck1.HBaseFsck - Naming new problem group: 112
ERROR: (region test,112,1705906453389.8d49d498454c1b836cb5c333223868ce.) Multiple regions have the
same startkey: 112
ERROR: (region test,112,1705891425126.7e030e885248d418e0f2efcbc1d72cb4.) Multiple regions have the
same startkey: 112
ERROR: (regions test,112,1705891425126.7e030e885248d418e0f2efcbc1d72cb4. and
test,user5145426939389338463,1705906453389.b7bc7c2b6d72eea00a0ef22efa306fbd.) There is an overlap
in the region chain.
15:07:36.664 [main] WARN  org.apache.hbase.hbck1.HBaseFsck - reached end of problem group: null
ERROR: Found inconsistency in table test
ERROR: Found lingering reference file hdfs://hacluster/hbase/data/default/test/
b7bc7c2b6d72eea00a0ef22efa306fbd/f1/
df110a4c28f54812b6b013954125cef7.7e030e885248d418e0f2efcbc1d72cb4
15:07:36.921 [main] INFO  org.apache.hadoop.hbase.client.ConnectionImplementation - Closing master
protocol: MasterService
15:07:37.027 [main] INFO  org.apache.hadoop.hbase.client.ConnectionImplementation - Connection has
been closed by main.
15:07:37.030 [main] INFO  org.apache.hadoop.hbase.client.ConnectionImplementation - Closing master
protocol: MasterService
15:07:37.133 [main] INFO  org.apache.hadoop.hbase.client.ConnectionImplementation - Connection has
been closed by main.
```

Possible Causes

In a fault scenario, sub-region A has been created in the table directory. However, RegionServer fails during the creation of sub-region B. As a result, the region fails to be split and an isolated sub-directory is left in the file system of the **table** directory.

If only the **.split** directories are deleted in the region but sub-regions are not deleted, the isolated sub-regions may be moved to the table directory during the failed splitting operation. Therefore, if the parent region is split, the HFile that sub-region A refers becomes invalid, and the hbck tool report the error.

Fault Locating

None.

Procedure

Step 1 Run the **-fixReferenceFiles** command provided by the hbck tool to save the residual reference file to another location.

hbase hbck -j ${CLIENT_HOME}/**HBase/hbase/tools/hbase-hbck2-1.1.0-h0.cbu.mrs.*.jar filesystem -fixReferenceFiles** *<tableName>*

Step 2 Run the **hbck** command to check whether the **-fixReferenceFiles** command has removed all inconsistencies.

hbase hbck -j ${CLIENT_HOME}**/HBase/hbase/tools/hbase-hbck2-1.1.0-h0.cbu.mrs.*.jar filesystem** *<tableName>*

If the command outputs are different, implement recovery based on the check items.

----End

Reference Information

Run the following command to obtain the detailed usage of the **hbck** command:

hbase hbck -j ${CLIENT_HOME}**/HBase/hbase/tools/hbase-hbck2-1.1.0-h0.cbu.mrs.*.jar**

2.4.8.2.9 When HBase Is Running the BulkLoad Task, the Error "OutOfMemoryError" Occurs

Symptom

When BulkLoad loads large data amount to HBase table, the error "OutOfMemoryError" occurs. The error information of running the BulkLoad task failure is displayed as shown in **Figure 2-2**.

Figure 2-2 Error information of BulkLoad task execution failure

```
2015-11-25 12:49:23,472 INFO  [main] mapreduce.Job: Task Id : attempt_1448094383919_0012_r_000004_0, Status : FAILED
Error: org.apache.hadoop.mapreduce.task.reduce.Shuffle$ShuffleError: error in shuffle in fetcher#6
        at org.apache.hadoop.mapreduce.task.reduce.Shuffle.run(Shuffle.java:134)
        at org.apache.hadoop.mapred.ReduceTask.run(ReduceTask.java:376)
        at org.apache.hadoop.mapred.YarnChild$2.run(YarnChild.java:180)
        at java.security.AccessController.doPrivileged(Native Method)
        at javax.security.auth.Subject.doAs(Subject.java:422)
        at org.apache.hadoop.security.UserGroupInformation.doAs(UserGroupInformation.java:1673)
        at org.apache.hadoop.mapred.YarnChild.main(YarnChild.java:174)
Caused by: java.lang.OutOfMemoryError: Java heap space
        at org.apache.hadoop.io.BoundedByteArrayOutputStream.<init>(BoundedByteArrayOutputStream.java:56)
        at org.apache.hadoop.io.BoundedByteArrayOutputStream.<init>(BoundedByteArrayOutputStream.java:46)
        at org.apache.hadoop.mapreduce.task.reduce.InMemoryMapOutput.<init>(InMemoryMapOutput.java:59)
        at org.apache.hadoop.mapreduce.task.reduce.MergeManagerImpl.unconditionalReserve(MergeManagerImpl.java:307)
        at org.apache.hadoop.mapreduce.task.reduce.MergeManagerImpl.reserve(MergeManagerImpl.java:297)
        at org.apache.hadoop.mapreduce.task.reduce.Fetcher.copyMapOutput(Fetcher.java:514)
        at org.apache.hadoop.mapreduce.task.reduce.Fetcher.copyFromHost(Fetcher.java:336)
        at org.apache.hadoop.mapreduce.task.reduce.Fetcher.run(Fetcher.java:193)
```

Possible Causes

With large data amount, the map process in running the BulkLoad task generates large shuffle data amount. During the reduce process, specify whether to save the data obtained by fetcher thread in the memory by configuring the Xmx in JVM

progress and parameters related with shuffle (**mapreduce.reduce.shuffle.input.buffer.percent** and **mapreduce.reduce.shuffle.parallelcopies**) If the data is required to save in the memory, when the fetcher thread is started and initialized, available memory of JVM is insufficient to instantiate fetcher due to other reasons, causing the memory overflow.

Table 2-3 Parameter description

Parameter	Description	Default Value
mapreduce.reduce.shuffle.input.buffer.percent	Specifies the percentage of available memory in fetcher thread to the occupied memory of Xmx configuration.	0.70
mapreduce.reduce.shuffle.parallelcopies	Specifies the number of fetcher threads.	10

Fault Locating

None.

Procedure

Before the client submits a task, see the parameter configuration in **Table 2-4**, reduce the configurations of **mapreduce.reduce.shuffle.input.buffer.percent** and **mapreduce.reduce.shuffle.parallelcopies,** and submit the task.

Table 2-4 Parameter configuration guide

Parameter	Recommended Value
mapreduce.reduce.shuffle.input.buffer.percent	0.60
mapreduce.reduce.shuffle.parallelcopies	5

References

None.

2.4.8.2.10 Replication failed caused by table not found in peer cluster

Symptom

During replication following error may occur at RegionServer side:

At active cluster RegionServer, "Can't replicate because of a local or network error", "Table 't1' was not found" are prompted.

```
2016-04-21 20:11:30,240 | WARN  | regionserver/192-168-63-228/192.168.63.228:21302.replicationSource,1 |
Can't replicate because of a local or network error: |
org.apache.hadoop.hbase.replication.regionserver.HBaseInterClusterReplicationEndpoint.replicate(HBaseInter
ClusterReplicationEndpoint.java:319)
java.io.IOException: java.io.IOException: Failed to replicate the data
at
org.apache.hadoop.hbase.replication.regionserver.ReplicationSink.replicateTheEntries(ReplicationSink.java:25
0)
at
org.apache.hadoop.hbase.replication.regionserver.ReplicationSink.replicateEntries(ReplicationSink.java:212)
at org.apache.hadoop.hbase.replication.regionserver.Replication.replicateLogEntries(Replication.java:228)
at org.apache.hadoop.hbase.regionserver.RSRpcServices.replicateWALEntry(RSRpcServices.java:1732)
at org.apache.hadoop.hbase.protobuf.generated.AdminProtos$AdminService
$2.callBlockingMethod(AdminProtos.java:24638)
at org.apache.hadoop.hbase.ipc.RpcServer.call(RpcServer.java:2157)
at org.apache.hadoop.hbase.ipc.CallRunner.run(CallRunner.java:109)
at org.apache.hadoop.hbase.ipc.RpcExecutor.consumerLoop(RpcExecutor.java:133)
at org.apache.hadoop.hbase.ipc.RpcExecutor$1.run(RpcExecutor.java:108)
at java.lang.Thread.run(Thread.java:745)
Caused by: java.util.concurrent.ExecutionException:
org.apache.hadoop.hbase.client.RetriesExhaustedWithDetailsException: Failed 18000 actions: Table 't1' was
not found.: 18000 times,
at java.util.concurrent.FutureTask.report(FutureTask.java:122)
at java.util.concurrent.FutureTask.get(FutureTask.java:192)
at
org.apache.hadoop.hbase.replication.regionserver.ReplicationSink.replicateTheEntries(ReplicationSink.java:24
8)
```

At peer cluster RegionServer, "Cannot get replica 0 location" is prompted.

```
2016-04-22 09:57:21,223 | ERROR | pool-11800-thread-1 | Cannot get replica 0 location for
{"totalColumns":2,"row":"04000000001122214","families":{"f1":[{"qualifier":"c1","vlen":1024,"tag":
[],"timestamp":1461238382720},{"qualifier":"c2","vlen":1024,"tag":[],"timestamp":1461238382720}]}} |
org.apache.hadoop.hbase.client.AsyncProcess
$AsyncRequestFutureImpl.manageLocationError(AsyncProcess.java:927)
```

Possible Causes

In this scenario replication failed because table was not found in peer cluster. Active cluster RegionSever will keep retrying to replicate data until all wal entries finishes, these wal entries may have deleted table data. So peer cluster RegionServer will always fail because table does not exist.

Fault Locating

Check the peer cluster whether table exist.

Procedure

1. If table does not exist in peer cluster then create the same table as earlier.
2. When current wal replication is done then delete the table if it was expected.

References

None.

2.4.8.2.11 An Empty Region Is Displayed on the HMaster Web UI and Same Table Fails to Be Created

Symptom

1. Tables of empty regions may be displayed on the HMaster web UI.

Namespace	Name	State	Regions								Description
			OPEN	OPENING	CLOSED	CLOSING	OFFLINE	FAILED	SPLIT	Other	
default	t1	ENABLED	1	0	0	0	0	0	0	0	't1', {NAME => 'cf1'}

2. When the client retries to create the same table, the following error message is displayed:

```
ERROR: java.io.IOException: the table directory:hdfs://10.18.106.212:25000/hbase/data/default/t1
exists,this may be created by other process,please delete the directory first.
at org.apache.hadoop.hbase.master.handler.CreateTableHandler.prepare(CreateTableHandler.java:131)
at org.apache.hadoop.hbase.master.HMaster.createTable(HMaster.java:1559)
at org.apache.hadoop.hbase.master.MasterRpcServices.createTable(MasterRpcServices.java:468)
at org.apache.hadoop.hbase.protobuf.generated.MasterProtos$MasterService
$2.callBlockingMethod(MasterProtos.java:59779)
at org.apache.hadoop.hbase.ipc.RpcServer.call(RpcServer.java:2171)
at org.apache.hadoop.hbase.ipc.CallRunner.run(CallRunner.java:112)
at org.apache.hadoop.hbase.ipc.RpcExecutor.consumerLoop(RpcExecutor.java:133)
at org.apache.hadoop.hbase.ipc.RpcExecutor$1.run(RpcExecutor.java:108)
at java.lang.Thread.run(Thread.java:745)
```

Possible Causes

When a fault occurs, HMaster has created a table in the file system, but the region information cannot be updated in the **meta** table. Therefore, the table exists in the file system but does not exist in the **meta** table.

During the HMaster active/standby switchover or restart, an empty region is displayed on the HMaster web UI, as shown in the preceding figure. The table is listed based on the file system instead of the **meta** table. Therefore, the region information of the table does not exist in HBase, and the **meta** table is empty.

Fault Locating

Scan the **hbase:meta** table and check whether the table region information exists.

Procedure

There are three fault scenarios:

- The data is complete. The **regioninfo** and **column family** directories exist under the **region** directory. Run the **scan 'hbase:meta', {COLUMNS => ['table:state'], ROWPREFIXFILTER => '***Table name***'}** command in the HBase shell to query data. Run the **addFsRegionsMissingInMeta** command to rectify the fault.

```
10-120-175-11:/srv/tsq/reliability/hbase # hdfs dfs -lsr /hbase/data/default/member
lsr: DEPRECATED: Please use 'ls -R' instead.
16/07/18 16:08:24 INFO hdfs.PeerCache: SocketCache disabled.
drwxr-xr-x - hbase hadoop 0 2016-07-18 09:53 /hbase/data/default/member/.tabledesc
-rw-r--r-- 3 hbase hadoop 534 2016-07-18 09:53 /hbase/data/default/
member/.tabledesc/.tableinfo.0000000001
drwxr-xr-x - hbase hadoop 0 2016-07-18 09:53 /hbase/data/default/member/.tmp
drwxr-xr-x - hbase hadoop 0 2016-07-18 09:56 /hbase/data/default/member/
```

```
6672415aee84564a77a38686789c48d8
-rw-r--r-- 3 hbase hadoop 42 2016-07-18 09:55 /hbase/data/default/member/
6672415aee84564a77a38686789c48d8/.regioninfo
drwxr-xr-x - hbase hadoop 0 2016-07-18 09:55 /hbase/data/default/member/
6672415aee84564a77a38686789c48d8/address
drwxr-xr-x - hbase hadoop 0 2016-07-18 09:55 /hbase/data/default/member/
6672415aee84564a77a38686789c48d8/info
-rw-r--r-- 3 hbase hadoop 4467 2016-07-18 09:55 /hbase/data/default/member/
6672415aee84564a77a38686789c48d8/info/f8962770089342a6bc83e443c872fd8c
drwxr-xr-x - hbase hadoop 0 2016-07-18 10:12 /hbase/data/default/member/
6672415aee84564a77a38686789c48d8/recovered.edits
-rw-r--r-- 3 hbase hadoop 0 2016-07-18 10:12 /hbase/data/default/member/
6672415aee84564a77a38686789c48d8/recovered.edits/17.seqid
```

In this code, **member** indicates the table name, and **address** and **info** indicate the column families.

Recovery procedure:

a. The hbck tool provides the **addFsRegionsMissingInMeta** command to rectify the fault.

   hbase hbck -j ${CLIENT_HOME}**/HBase/hbase/tools/hbase-hbck2-1.1.0-h0.cbu.mrs.*.jar addFsRegionsMissingInMeta** <tableName>

b. Run the **hbck** command to check whether the **-repair** command has rectified all inconsistencies.

   hbase hbck -j ${CLIENT_HOME}**/HBase/hbase/tools/hbase-hbck2-1.1.0-h0.cbu.mrs.*.jar reportMissingRegionsInMeta** <tableName>

   If the **hbck** command output is inconsistent, run the operation in **a** again.

- The data is complete. The **regioninfo** and **column family** directories exist under the **region** directory. No data is found after the **scan 'hbase:meta', {COLUMNS => ['table:state'], ROWPREFIXFILTER => '***Table name***'}** command is executed in the HBase shell. In this case, you can only use the offline repair tool to regenerate all meta table data.

  Recovery procedure:

  a. Copy the JAR file of the repair tool to the **${CLIENT_HOME}/HBase/hbase/lib** directory.

     cp -af ${CLIENT_HOME}**/HBase/hbase/tools/hbase-hbck2-1.1.0-h0.cbu.mrs.*.jar** ${CLIENT_HOME}**/HBase/hbase/lib**

  b. Log in to FusionInsight Manager, choose **Cluster** > **Services**, locate the row that contains the HBase service, and click **Stop Service** to stop it.

  c. Run the following command on the node where the JAR file in **a** is located to restore data:

     hbase org.apache.hbase.hbck1.OfflineMetaRepair

  d. On FusionInsight Manager, choose **Cluster** > **Services**, locate the row that contains the HBase service, and click **Start Service** to start it.

     NOTE

     Before performing this operation, stop the HBase service and regenerate full meta table data, and ensure that services are acceptable.

- The table fails to be created. The HBase data in HDFS is incomplete. The **region** directory has only one **regioninfo** directory and does not have the **column family** directory. The table does not contain data and cannot be

restored by running the **addFsRegionsMissingInMeta** command. In this case, you can only delete the directory in HDFS.

```
10-120-175-11:~ # hdfs dfs -lsr /hbase/data/default/member
lsr: DEPRECATED: Please use 'ls -R' instead.
16/07/16 18:43:19 INFO hdfs.PeerCache: SocketCache disabled.
drwxr-xr-x - hbase hadoop 0 2016-07-16 15:59 /hbase/data/default/member/.tabledesc
-rw-r--r-- 3 hbase hadoop 534 2016-07-16 15:59 /hbase/data/default/
member/.tabledesc/.tableinfo.0000000001
drwxr-xr-x - hbase hadoop 0 2016-07-16 15:59 /hbase/data/default/member/.tmp
drwxr-xr-x - hbase hadoop 0 2016-07-16 15:59 /hbase/data/default/member/
4fb1281998d2aa3814d1416c9b752d74
-rw-r--r-- 3 hbase hadoop 41 2016-07-16 15:59 /hbase/data/default/member/
4fb1281998d2aa3814d1416c9b752d74/.regioninfo
```

Run the **-rmr** command to delete directories.

hdfs dfs -rmr */hbase/data/default/member*

member indicates the table name, and the directory and table name are examples.

NOTE

Deleting a file or folder is a high-risk operation. Ensure that the file or folder is no longer required before performing this operation.

Reference Information

Run the following command to check the usage details of the **hbck** command.

hbase hbck -j ${CLIENT_HOME}**/HBase/hbase/tools/hbase-hbck2-1.1.0-h0.cbu.mrs.*.jar**

2.4.8.2.12 Replication Stuck due to CallQueueTooBigException

Symptom

Replication is stuck in peer cluster if the following message is observed continuously.

Logs of RegionServers in the source cluster:

```
2016-05-26 10:12:00,367 | WARN  | regionserver/192-168-63-228/192.168.63.228:21302.replicationSource,33
| Can't replicate because of an error on the remote cluster:  |
org.apache.hadoop.hbase.replication.regionserver.HBaseInterClusterReplicationEndpoint.replicate(HBaseInter
ClusterReplicationEndpoint.java:275)
org.apache.hadoop.hbase.ipc.RemoteWithExtrasException(org.apache.hadoop.hbase.ipc.RpcServer
$CallQueueTooBigException): Call queue is full on /192.168.154.55:21302, is
hbase.ipc.server.max.callqueue.size too small?
at org.apache.hadoop.hbase.ipc.RpcClientImpl.call(RpcClientImpl.java:1277)
at org.apache.hadoop.hbase.ipc.AbstractRpcClient.callBlockingMethod(AbstractRpcClient.java:223)
at org.apache.hadoop.hbase.ipc.AbstractRpcClient
$BlockingRpcChannelImplementation.callBlockingMethod(AbstractRpcClient.java:324)
at org.apache.hadoop.hbase.protobuf.generated.AdminProtos$AdminService
$BlockingStub.replicateWALEntry(AdminProtos.java:25690)
at
org.apache.hadoop.hbase.protobuf.ReplicationProtbufUtil.replicateWALEntry(ReplicationProtbufUtil.java:79)
at org.apache.hadoop.hbase.replication.regionserver.HBaseInterClusterReplicationEndpoint
$Replicator.call(HBaseInterClusterReplicationEndpoint.java:381)
at org.apache.hadoop.hbase.replication.regionserver.HBaseInterClusterReplicationEndpoint
$Replicator.call(HBaseInterClusterReplicationEndpoint.java:364)
at java.util.concurrent.FutureTask.run(FutureTask.java:266)
at java.util.concurrent.Executors$RunnableAdapter.call(Executors.java:511)
at java.util.concurrent.FutureTask.run(FutureTask.java:266)
at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1142)
```

```
at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:617)
at java.lang.Thread.run(Thread.java:745)
```

Logs of RegionServers in the peer cluster:

```
2016-05-26 10:12:21,971 | INFO  | pool-5614-thread-1 | #2, waiting for 7232  actions to finish |
org.apache.hadoop.hbase.client.AsyncProcess
$AsyncRequestFutureImpl.waitUntilDone(AsyncProcess.java:1572)
2016-05-26 10:12:31,990 | INFO  | pool-5614-thread-1 | #2, waiting for 7232  actions to finish |
org.apache.hadoop.hbase.client.AsyncProcess
$AsyncRequestFutureImpl.waitUntilDone(AsyncProcess.java:1572)
2016-05-26 10:12:42,006 | INFO  | pool-5614-thread-1 | #2, waiting for 7232  actions to finish |
org.apache.hadoop.hbase.client.AsyncProcess
$AsyncRequestFutureImpl.waitUntilDone(AsyncProcess.java:1572)
2016-05-26 10:12:52,029 | INFO  | pool-5614-thread-1 | #2, waiting for 7232  actions to finish |
org.apache.hadoop.hbase.client.AsyncProcess
$AsyncRequestFutureImpl.waitUntilDone(AsyncProcess.java:1572)
```

Possible Causes

If heavy writes to the source cluster are observed, RegionServers in the peer cluster are unable to replicate data over a long period of time either due to RegionServer shutdown, or DataNode faults, or network issues. When the RegionServer functionality is restored, it may receive a replication request with a lot of edits in it. Consequently, RegionServers in the peer cluster takes more time than **hbase.rpc.replication.timeout** to process the replication request. Once the time spent in processing the replication request exceeds the time limit, RegionServer in the source cluster will resend the request, incurring the possibility that the direct buffer memory (default size is 64 MB) gets too full to serve any requests further.

Fault Locating

Check if the data replication is stuck and the mentioned log messages in **Symptom** section are observed in RegionServer logs.

Procedure

Increase the direct buffer memory of each RegionServer process in the peer cluster to 1 GB. The default value is 64 GB. The process is as follow:

Add **-XX\:MaxDirectMemorySize\=1024m** to the **GC_OPTS** attribute in the **<HBASE_CONF_DIR>/ENV_VARS** of each RegionServer process in peer cluster and then restart all these processes.

NOTE

By default, **-XX:MaxDirectMemorySize** is not configured in the **GC_OPTS** parameter. To configure it, you need to add it to the **GC_OPTS** parameter as an custom option.

References

None.

2.4.8.2.13 "Region X on HDFS, but not listed in hbase:meta or deployed on any region server" Is Displayed in the hbck Report

Symptom

Region splitting sometimes fails due to RegionServer interruption or HMaster active/standby switchover (failover). These failures may generate some extra useless HDFS directories. The following is the error message displayed in the hbck report:

```
hbase/bin> hbase hbck -j /opt/client/HBase/hbase/tools/hbase-hbck2-1.1.0-h0.cbu.mrs.*.jar
extraRegionsInMeta
.....................
.....................
2016-06-23 21:02:35,419 INFO  [main-EventThread] zookeeper.ClientCnxn: EventThread shut down for
session: 0x10055fdee6900fe
2016-06-23 21:02:35,419 DEBUG [main] ipc.AbstractRpcClient: Stopping rpc client
2016-06-23 21:02:35,419 INFO  [main] util.HBaseFsck: Checking and fixing region consistency
ERROR: Region { meta => null, hdfs => hdfs://hacluster/hbase/data/default/testSplitFlow/
921ad89687a245138dd14953ae14e5e5, deployed => , replicaId => 0 } on HDFS, but not listed in
hbase:meta or deployed on any region server
ERROR: Region { meta => null, hdfs => hdfs://hacluster/hbase/data/default/testSplitFlow/
c2167918b0f0403f17f864a660008945, deployed => , replicaId => 0 } on HDFS, but not listed in hbase:meta
or deployed on any region server
2016-06-23 21:02:35,421 DEBUG [main] util.HBaseFsck: There are 5 region info entries
2016-06-23 21:02:35,422 DEBUG [main] util.FSTableDescriptors: Fetching table descriptors from the
filesystem.
2016-06-23 21:02:35,449 INFO  [main] util.HBaseFsck: Computing mapping of all store files
...................
...................
```

Possible Causes

In the fault scenario, the sub-region directory is created in the table directory during region splitting. However, the RegionServer breaks down before the **hbase:meta** table is updated. Then, the HMaster active/standby switchover (failover) cannot delete the incomplete split subdirectories. The hbck reports this error.

Fault Locating

None.

Procedure

Step 1 The hbck tool provides the **extraRegionsInMeta** command option to clear these HDFS directories.

hbase hbck -j *${CLIENT_HOME}*/**HBase/hbase/tools/hbase-hbck2-1.1.0-h0.cbu.mrs.*.jar extraRegionsInMeta -f** *<tableName>*

Step 2 Run the **hbck** command to check whether the **extraRegionsInMeta** command option fixes the inconsistency mentioned above.

hbase hbck -j *${CLIENT_HOME}*/**HBase/hbase/tools/hbase-hbck2-1.1.0-h0.cbu.mrs.*.jar extraRegionsInMeta**

----End

Reference Information

Run the following command to learn about the usage details of the **hbck** command:

hbase hbck -j *${CLIENT_HOME}*/**HBase/hbase/tools/hbase-hbck2-1.1.0-h0.cbu.mrs.*.jar**

2.4.8.2.14 hbck Reports that a Region Is Allocated to Multiple RegionServers

Symptom

In a fault scenario, a region may contain multiple RegionServers.

The hbck tool of HBase reports the following error:

```
ERROR: Region { meta =>
cdrtable1,1860051495220150101,1464768981639.eb3203617c76a2dd649c2d295e384fde., hdfs => hdfs://
hacluster/hbase/data/default/cdrtable1/eb3203617c76a2dd649c2d295e384fde, deployed => ???????
192-168-137-242,21302,1465872900854;cdrtable1,1860051495220150101,1464768981639.eb3203617c76a2
dd649c2d295e384fde.,
192-168-56-46,21302,1465872903247;cdrtable1,1860051495220150101,1464768981639.eb3203617c76a2dd
649c2d295e384fde., replicaId => 0 } is listed in hbase:meta on region server
192-168-56-46,21302,1465872903247 but is multiply assigned to region servers
192-168-137-242,21302,1465872900854, 192-168-56-46,21302,1465872903247
```

Possible Causes

During region allocation, the status update of RegionServer and HMaster may time out due to high load. As a result, the region status recorded by HMaster is inconsistent with that recorded by RegionServer.

In a fault scenario, if CallTimeoutException occurs during region allocation, the regions are re-allocated based on the new plan of HMaster. Therefore, HMaster may allocate the region to another RegionServer. If the old RegionServer (that is, the RegionServer where CallTimeoutException occurs) opens the region and reports the status to HMaster, double allocation may occur if the reporting request times out or fails due to other reasons.

Fault Locating

Trace regions in HMaster or RegionServer logs and find out the root cause of repeated allocation.

Procedure

Check and rectify the network fault.

Step 1 Restart the RegionServer that fails to report the regions it brings online.

----End

NOTE

If the fault persists, collect program logs and submit them to technical support.

Reference Information

None.

2.4.8.2.15 InvalidToken Error Occurs of Network Faults

Symptom

In security mode, when applications such as Mapreduce and Spark are run, the following error may occur, resulting in a task execution failure:

```
2015-12-07 12:46:17,607 WARN [htable-pool1-t1] org.apache.hadoop.hbase.ipc.AbstractRpcClient:
Exception encountered while connecting to the server :
org.apache.hadoop.ipc.RemoteException(org.apache.hadoop.security.token.SecretManager$InvalidToken):
Unknown master key for token (id=7)
```

Possible Causes

The tokens of the client and server are inconsistent because of network faults.

Fault Locating

None.

Procedure

Step 1 Restart the RegionServer and client that incur the fault.

Step 2 If the fault persists, collect the log and contact the technical support engineers.

----End

Reference Information

None.

2.4.8.2.16 Rolling Restart Fails When the Balancer Operation of a Service Is Performed

Symptom

Failed to perform rolling restart because HBase is performing the balancer operation.

The following error is reported:

```
Failed to perform this operation before rolling restart of role RegionServer on hotsIP
Operation succeeded after rolling restart of role RegionServer on hostIP
```

Possible Causes

During the balancer operation process, regions are in the migration state. When the rolling restart is performed, regions are also migrated. As a result, regions fail to be migrated during the rolling restart, and the rolling restart fails.

Fault Locating

Trace the region in the HMaster/RegionServer logs and check whether the balancer is enabled.

Procedure

Step 1 Log in to the node where the HBase client is installed. Perform security authentication using the **hbase** user.

Step 2 Run the following commands to access **hbase shell** and disable the automatic balancer:

hbase shell

balance_switch false

NOTE

After the **balance_switch false** command is executed successfully, the previous balancer status is returned.

```
hbase(main):003:0> balance_switch false
true
0 row(s) in 0.0820 seconds
```

You can run the **balancer_enabled** command in **hbase shell** to query the current balancer status which should be **false**.

```
hbase(main):004:0> balancer_enabled
false
0 row(s) in 0.0030 seconds
```

Step 3 Check whether any region is in Region in Transition (RIT) state.

- If yes, rectify the fault. For details, see **Multiple Regions Are in RIT Status, An Abnormality Occurs in HMaster, and "Packet len6080218 is out of range" Is Displayed in the Log**.
- If the alarm is not cleared, go to step **Step 4**.

Step 4 Perform the rolling restart again.

Step 5 After the execution in **Step 4** is successful, run the following command to enable the automatic balancer:

hbase shell

balance_switch true

NOTE

After the **balance_switch true** command is executed successfully, the previous balancer status is returned.

```
hbase(main):003:0> balance_switch true
false
0 row(s) in 0.0820 seconds
```

You can run the **balancer_enabled** command in **hbase shell** to query the current balancer status which should be **true**.

```
hbase(main):004:0> balancer_enabled
true
0 row(s) in 0.0030 seconds
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 6 If the fault persists, collect program logs and submit them to technical support.

----End

Reference Information

None.

2.4.9 HDFS

2.4.9.1 Common HDFS Service Faults

2.4.9.1.1 HDFS Service Is Always Abnormal

Symptom

On the HDFS service page, unavailable services, HBase, Hive, and Mapreduce faults or startup failures are displayed.

Possible Causes

- The HDFS is in safe mode.
- ZooKeeper that the HDFS depends on are abnormal.

Fault Locating

1. Check whether the HDFS is in safe mode.
2. Check whether the ZooKeeper services are running properly.

Procedure

Step 1 Check whether the HDFS is in safe mode.

- If yes, exit the HDFS safe mode directly.
- If no, go to **Step 2**.

Step 2 Log in to the FusionInsight Manager system, go to the ZooKeeper service pages to check whether the service is running properly, and go to **O&M > Alarm > Alarm**, check whether fault alarms exist on the ZooKeeper alarm pages.

Step 3 Restore the services based on the alarm restoration guidance, and ensure that the ZooKeeper service is running properly.

Step 4 Restart HDFS and check whether this service is running properly.

- If yes, no further action is required.
- If not, go to **Step 5**.

Step 5 Check whether NameNode is faulty. If yes, restore NameNode.

----End

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Reference Information

HDFS safe mode exit methods. For more details, see **https://hadoop.apache.org/docs/r3.1.1/hadoop-project-dist/hadoop-common/CommandsManual.html**.

2.4.9.1.2 HDFS Block Loss

Symptom

- The Hadoop Distributed File System (HDFS) is in the safe mode and HDFS is unavailable.
- The value of the block loss item on the HDFS service page is greater than zero.
- HDFS cannot be started, but role instances can be started successfully.

Possible Causes

- The data copy is lost because of data node hard disk faults or node faults.
- The HDFS enters the safe mode in the following situations:
  a. NameNode is started and is waiting for DataNode to report the copy.
  b. The space of the disk where NameNode locates is insufficient.

     The threshold of the HDFS block loss is too high. After the HDFS enters the safe mode in one of the preceding situations, it requires a long period of time and strict conditions for the HDFS to exit the safe mode.
  c. After NameNode data is restored, the metadata and service data cannot be matched.
- All copies of the HDFS files are lost.

Fault Locating

1. Check whether node alarms or hard disk fault alarms exist on the FusionInsight Manager alarm page.
2. Check whether the block loss threshold of NameNode **dfs.namenode.safemode.threshold-pct** is too high.

Procedure

Step 1 Log in to the FusionInsight Manager portal, click **O&M** > **Alarm** > **Alarm** to check whether HDFS alarms, node faults, and hard disk faults exist.

- If yes, clear alarms and rectify faults by following steps provided in related sections.
- If not, go to **Step 2**

Step 2 Install the HDFS client. On the client, run fsck as user **hdfs** to check whether files in the HDFS are complete.

Command example:

hdfs fsck /

Step 3 If the fsck check only displays the copy loss, but no file loss (check whether the number of existing copies is greater than zero), run ***hdfs dfsadmin -safemode leave*** to exit the HDFS security mode. Then the fault can be rectified.

Step 4 If files are lost, check whether NameNode data is restored.

- If yes, no service data block corresponding to the metadata can be found. Run ***hdfs dfsadmin -safemode leave*** to exit the HDFS security mode, and go to **Step 5**
- If no, files are lost. Go to **Step 5**

Step 5 If any file is lost, check the file path of the lost file and whether the lost file is an important file.

- You can delete unimportant files after exiting the safe mode. (MapReduce files are unimportant files.)

  Command example:

  hdfs fsck [path-to-file] -delete

- After NameNode data is restored, the metadata and service data may not be matched, so you need to delete incorrect data from the check results.

  hdfs fsck / -delete

  NOTE

  - If lost files are important files, you must restore these files. Contact the technical support if necessary.
  - Deleting a file or folder is a high-risk operation. Ensure that the file or folder is no longer required before performing this operation.

Step 6 Check whether the block loss threshold of NameNode is too high.

On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services** > **HDFS** > **Configurations** > **All Configurations** > **NameNode** > **High Availability**, and set **dfs.namenode.safemode.threshold-pct**.

If there are only three nodes in the cluster, you are advised to set **dfs.namenode.safemode.threshold-pct to 0.66**.

Step 7 Restart HDFS.

----End

Reference Information

None.

2.4.9.1.3 Failed to Exit the HDFS Safe Mode

Symptom

- The Hadoop Distributed File System (HDFS) is in the safe mode and HDFS is unavailable.
- The safe mode cannot be automatically restored.

Possible Causes

- The data copy is lost because of data node hard disk faults or node faults.
- The HDFS enters the safe mode in the following situations:
  a. NameNode is started and is waiting for DataNode to report the copy.
  b. The space of the disk where NameNode locates is insufficient.

  The threshold of the HDFS block loss is too high. After the HDFS enters the safe mode in one of the preceding situations, it requires a long period of time and strict conditions for the HDFS to exit the safe mode.
- All copies of the HDFS files are lost.

Fault Locating

1. Check whether node alarms or hard disk fault alarms exist on the FusionInsight Manager alarm page.
2. Check whether the block loss threshold of NameNode **dfs.namenode.safemode.threshold-pct** is too high, The default value is **0.999999**.
3. Check whether the safe mode exit command is properly run.

Procedure

Step 1 Restore the HDFS safe mode by following the **HDFS Block Loss** exception guidance.

Step 2 Exit the safe mode by following the safe mode operation guidance in the common operation guidance.

Step 3 Check the usage of the disk where NameNode exists and rectify the fault.

----End

Reference Information

HDFS safe mode exit methods. For more details, see **https://hadoop.apache.org/docs/r3.1.1/hadoop-project-dist/hadoop-common/CommandsManual.html**.

2.4.9.1.4 Failed to Start HDFS When SafeMode Is On

Symptom

When HDFS is being started, the following problem occurs.

Figure 2-3 Failure details

```
[2014-11-26 18:49:00] RoleInstance check validity failure [{ScriptExecutionResult=ScriptExecutionResult [exitCode=1, output=,
errMsg=log4j:WARN Failed to set property [maxBackupIndex] to value "",
log4j:WARN Failed to set property [maxBackupIndex] to value "",
ls: '/hdfsServiceCheck-vm-219': No such file or directory
log4j:WARN Failed to set property [maxBackupIndex] to value "",
put: org.apache.hadoop.hdfs.server.namenode.SafeModeException: Cannot create file/hdfsServiceCheck-vm-219._COPYING_. Name node is
in safe mode.
}]} for NameNode#10.91.8.219@vm-219.
[2014-11-26 18:49:00] RoleInstance check validity failure for ROLE[name: NameNode].
[2014-11-26 18:49:00] Check validity of role for ROLE[name: NameNode].
[2014-11-26 18:49:00] Check validity of roleInstance for NameNode#10.91.8.219@vm-219.
[2014-11-26 18:50:36] RoleInstance check validity failure [{ScriptExecutionResult=ScriptExecutionResult [exitCode=1, output=,
```

Possible Causes

SafeMode of HDFS is On due to certain operations in the current cluster. In this case, the failure information is displayed when you start HDFS, but the HDFS process has been started.

For details about SafeMode, visit the official website: **http://hadoop.apache.org/docs/r3.1.1/hadoop-project-dist/hadoop-hdfs/HdfsUserGuide.html#Safemode**

Fault Locating

Among the background processes displayed by running commands, HDFS has been started.

Procedure

Step 1 On the HDFS WebUI, check whether "Safe mode is ON" is displayed. If yes, the safe mode is enabled.

Figure 2-4 Safe mode is on

Step 2 In the cluster, run the ***jps*** command to view existing processes and check whether HDFS is running.

In the following information, **127400 NameNode** and **238821 NameNode** indicates that NameNode is started; **131879**, **242298**, and **78053** indicates that DataNode is started.

If the following information is displayed, HDFS has been started and can provide services even though the page displays a service startup failure message. In this case, only operations allowed when Safe Mode is On can be performed.

```
omm@vm-218:~> jps
 27977 NodeAgent
 169978 HMaster
 31208 EsperMain
 20921 QuorumPeerMain
 175185 ThriftServer
 7438 HRegionServer
 228482 Jps
 123267 DFSZKFailoverController
 189961 JobHistoryServer
 119586 JournalNode
 215506 AosMainProcess
 215233 ControllerService
 31087 PMSMain
 21398 FmsMain
 214170 ApplicationMain
 215474 Bootstrap
 191164 SparkSubmit
 190755 HistoryServer
 127400 NameNode131879
 169255 ResourceManager
 169048 NodeManager
 214388 AccountServiceMain
omm@vm-219:~> jps
 59390 Main
 242298
 148479 HMaster
 99207 QuorumPeerMain
 77977 Main
 1217 HRegionServer
 43189 NodeAgent
 65284 FsShell
 231921 JournalNode
 152289 ThriftServer
 148041 ResourceManager
 147672 NodeManager
 235351 DFSZKFailoverController
 168021 CoarseGrainedExecutorBackend
 238821 NameNode
 81834 Jps
 166502 ExecutorLauncher
omm@vm-220:~> jps
 120134 Jps
 113686 HRegionServer
 55076 CoarseGrainedExecutorBackend
 78053
 239667 NodeAgent
 73407 JournalNode
 44873 NodeManager
 47546 ThriftServer
 21071 QuorumPeerMain
```

Step 3 It is recommended that all the HDFS faults in the cluster be rectified based on the actual situation to ensure that Safe Mode is Off. For example, check that the number of lost HDFS blocks is less than the threshold. After all the faults are rectified, run the command for the HDFS to exit the safe mode.

Step 4 On FusionInsight Manager, restart HDFS.

----End

Reference Information

HDFS safe mode exit methods. For more details, see **https://hadoop.apache.org/docs/r3.1.1/hadoop-project-dist/hadoop-common/CommandsManual.html**.

2.4.9.1.5 HDFS Startup Progress Bar Does Not Move

Symptom

During the startup of the HDFS service on FusionInsight Manager, the startup progress bar does not move for a long time or a startup failure is reported 1 hour later. This affects other cluster operations.

Possible Causes

The HDFS service is abnormal, but the HDFS health check timeout interval is 1 hour.

Fault Locating

1. There is information input in the service startup progress bar on the FusionInsight Manager portal.
2. Fault recovery takes about 1 minute.

Procedure

Step 1 On FusionInsight Manager, click the progress bar to view the details .In the progress bar details, find the name of the role for which the health check is performed, and check the IP addresses of all nodes on which the role is installed.

Step 2 Log in to each node queried in **Step 1** as user **omm** , and perform **Step 3** to **Step 4**.

Step 3 Change the name of the **start-agent.sh** script.

mv ${BIGDATA_HOME}/om-agent/nodeagent/bin/start-agent.sh ${BIGDATA_HOME}/om-agent/nodeagent/bin/start-agent.sh.bak

Step 4 Run the script **${BIGDATA_HOME}/om-agent/nodeagent/bin/stop-agent.sh** to stop the agent.

cd ${BIGDATA_HOME}/om-agent/nodeagent/bin/

./stop-agent.sh

Step 5 View the progress bar on FusionInsight Manager. About 1 minute later, when a message is displayed indicating that the service fails to be started, restore the **start-agent.sh** script of each node queried in **Step 1**.

mv ${BIGDATA_HOME}/om-agent/nodeagent/bin/start-agent.sh.bak ${BIGDATA_HOME}/om-agent/nodeagent/bin/start-agent.sh

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 6 Find the HDFS health check failure cause. After the problem is resolved, restart the HDFS service.

----End

Reference Information

None.

2.4.9.1.6 Failed to Add the HDFS Service After Cross-AZ HA Is Enabled for a Cluster

Symptom

The HDFS service fails to be added to the cluster where the cross-AZ HA function is enabled.

```
[2020-06-23 14:09:06]RoleInstance configuration failure [{ActionFailureMessage=Failed to configure process: 2_24_NameNode, error details: Since AZ is enabled, the value of dfs.block.replicator.classname is invalid, it must be set to org.apache.hadoop.hdfs.server.blockmanagement.BlockPlacementPolicyWithAZExpression.}]
```

Possible Causes

Some default parameters of HDFS do not meet HA requirements, causing the installation failure.

Fault Locating

Some default HDFS parameters do not meet HA requirements. As a result, the service fails to be installed.

Procedure

Step 1 On FusionInsight Manager, choose **Cluster** > **Services** > **Add Service** and add the HDFS service again as prompted.

Step 2 On the **Configuration** page, search for and change the values of the following parameters. For details about the parameters, see **Table 2-5**.

Table 2-5 HDFS configuration parameters

Parameter	Value
dfs.block.replicator.classname	org.apache.hadoop.hdfs.server.blockmanagement.BlockPlacementPolicyWithAZExpression
net.topology.impl	org.apache.hadoop.hdfs.net.DFSNetworkTopologyWithAZ
dfs.use.dfs.network.topology	false

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 3 Click **Next**. Check whether the configurations are correct, then click **Submit** and wait until the service installation is complete.

----End

Reference Information

None.

2.4.9.2 Common HDFS Client Faults

2.4.9.2.1 OutOfMemoryError Exception Occurs on the HDFS Maintenance Client

Symptom

OutOfMemoryError is reported when the Hadoop Distributed File System (HDFS) maintenance client runs the maintenance command.

If the HDFS maintenance client runs ***hdfs dfs -ls /user/*/*/*/****, the following information is displayed.

```
#
# java.lang.OutOfMemoryError: Java heap space
# -XX:OnOutOfMemoryError="kill -9 %p"
#   Executing /bin/sh -c "kill -9 74251"...
Killed
```

Possible Causes

The default memory size of the HDFS client program is too small. The HDFS client program runs out of memory and logs out because the memory required exceeds the default memory. During the directory query, the HDFS client requires a large amount of memory to cache the directory if the directory to be queried contains too many files. If the memory is insufficient, OutOfMemoryError is reported.

Fault Locating

None.

Procedure

This fault can be rectified by setting the environment variable of the HDFS client.

Step 1 Before starting the client, you can change the GC value in the **-Xmx** parameter of **HADOOP_CLIENT_OPTS** in the *client installation directory*/**HDFS/component_env** and run the **source component_env** command to make the modified parameter take effect. Alternatively, you can run the following command:

export *HADOOP_CLIENT_OPTS*=**"$HADOOP_CLIENT_OPTS -Xmx512m"**

NOTE

Increase memory if there are too many files or a filename is too long. Formula for calculating the required minimal memory size:

Required minimal memory size (KB) = (3 + 0.02 * Average filename length) * File quantity + Memory size (KB) required by jvm to run basic operations

The average filename length is the length of the filename plus the length of the pathname. For example, if the /dir/file1.txt filename is 14 characters in length, and the memory size required by jvm to run basic operations is 128 MB, consider increasing the memory required by jvm to run basic operations.

For example: To run the ***hdfs dfs -ls*** command to query 300,000 files whose filename is 100 characters in total, then the required minimal memory is approximately 1.5 GB, namely, (3 + 0.02 x 100) * 300000 + 128 * 1024 = 1631072/1024 ≈ 1593 MB. In this case, you need to run the following command to update the "-Xmx" GC parameter in HADOOP_CLIENT_OPTS to 1593m:

```
export HADOOP_CLIENT_OPTS="$HADOOP_CLIENT_OPTS -Xmx1593m"
```

Step 2 Configure the parameters in the command, and reduce the memory required by the HDFS maintenance client for running maintenance commands.

If OutOfMemoryError is reported when ***hdfs dfs -ls /user/*/*/*/**** is executed, you can run other similar commands to obtain the directory, for example, ***hdfs dfs -ls -R /user***.

----End

Reference Information

None.

2.4.9.2.2 HDFS Client Cannot Connect to HDFS Cluster

Symptom

The HDFS client cannot connect to HDFS clusters.

Possible Causes

- Kerberos authentication is not successful.
- NameNode IP address is incorrect.
- The Hadoop Distributed File System (HDFS) service is not running properly.

Fault Locating

First, check whether the HDFS service is running properly. Then, check whether the HDFS client is properly installed. Finally, check whether the client is properly used.

Procedure

Step 1 Log in to the FusionInsight Manager portal, and check whether the HDFS service is running properly on the service list page and alarm page. If any exception exists, perform related operations according to the alarm help.

Step 2 Log in to the server node as user root, and install the HDFS client.

Step 3 Run the following command to enter the client installation directory, for example, **/opt/hadoopclient**:

cd /opt/hadoopclient

Step 4 Run the **source bigdata_env** command to configure the environment variables.

Step 5 If the cluster uses the security mode, run the **kinit hdfs** command to log in to the HDFS client using the service account.

Please contact Administrator obtain the service account and password.

----End

Reference Information

None.

2.4.9.3 Common HDFS NameNode Faults

2.4.9.3.1 NameNodes Are Always in the Standby State

Symptom

On the FusionInsight Manager HDFS service page, the two NameNodes are always in the Standby state and cannot provide services.

Possible Causes

- Active NameNode selection fails because the old data that controls the active/standby status of NameNodes remains in ZooKeeper.
- The session ID of the ZooKeeper client ZKFC is inconsistent with that of the ZooKeeper server, resulting in connection deadlock.
- JournalNode is abnormal and an active/standby switchover occurs on the NameNodes. When editlog is being restored on the NameNodes, an editlog synchronization failure occurs.

Fault Locating

- In the ZKFC logs, if information similar to **java.lang.IllegalArgumentException: Unable to determine service address for namenode '1781'** exists, the old data remains in ZooKeeper.
- In the logs of the two ZKFCs, if the "Active > Standby" and "Standby > Active > Standby" NameNode status switchovers exist, the ZooKeeper client ZKFC and the ZooKeeper server are in deadlock connection.
- On the NameNodes, write editlog and restore editlog failures exist.
  a. In the logs of the NameNode that is supposed to be in the Active state, if the following error information exists:
  ```
  Got too many exceptions to achieve quorum size 2/3.
  ```
  a write editlog failure occurs, the NameNode restarts, and the "Active > Standby" NameNode status switchover exists.
  b. In the logs of the NameNode that is supposed to be in the Standby state, if the following error information exists:

```
recoverUnfinalizedSegments failed for required journal
```

a restore editlog failure occurs, the NameNode restarts, an Active status preemption failure occurs, and the NameNode is in the Standby state.

Procedure

- The old data remains in ZooKeeper.
  a. Log in to the node where the ZooKeeper client is located as user **root**.
  b. Run the following command to export the environment variables:

     cd *ZooKeeper client installation directory*

     source bigdata_env
  c. In security mode, run the following command to log in to Kerberos as user **hdfs** (skip this step in normal mode).

     kinit hdfs

     NOTE

     For details about the default password of user **hdfs**, see ***Huawei Cloud Stack 8.3.1 Account List*** or consult the system administrator.
  d. Use the ZooKeeper client to access the CLI.

     zkCli.sh -server *service IP address of any functioning ZooKeeper node*:**24002**
  e. Run the following command to delete the old data:

     deleteall /hadoop-ha/hacluster/ActiveBreadCrumb
  f. Check whether the active/standby status of NameNodes is recovered.
- The ZooKeeper client and server are in deadlock connection.
  a. Log in to FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **HDFS** > **Instance** > **NameNode,** and select the NameNode in the Standby > Active > Standby state.
  b. Choose **More** > **Restart Instance** to restart the NameNode.
- On the NameNodes, write editlog and restore editlog failures exist.

  Perform the following operations on the two NameNodes to restore editlog.
  a. On FusionInsight Manager, stop HDFS.
  b. Log in the new NameNode node as user **root**, run the **su - omm** command to switch to user **omm**.
  c. Run the following commands to export the environment variables:

     EXECUTABLE_HOME="${CONTROLLER_HOME}/kerberos_user_specific_binay/kerberos"

     LD_LIBRARY_PATH=${EXECUTABLE_HOME}/lib:$LD_LIBRARY_PATH

     PATH=${EXECUTABLE_HOME}/bin:$PATH
  d. (Optional) In security mode, run the kinit command to obtain a security certificate.

     kinit hdfs
  e. Go to the **${BIGDATA_HOME}/FusionInsight_HD_8.3.1/1_6_NameNode** directory, and copy the environment variable script to the directory. The number 1_6 in the directory changes as the environment changes.

NOTE

The version 8.3.1 is used as an example. Replace it with the actual version number.

- In security mode, run the following commands:

  cd ${BIGDATA_HOME}/FusionInsight_HD_8.3.1/1_6_NameNode

  cp ${BIGDATA_HOME}/FusionInsight_HD_8.3.1/install/FusionInsight-Hadoop-3.3.1/hadoop/sbin/exportENV_VARS.sh ./

- In normal mode, run the following commands:

  cd ${BIGDATA_HOME}/FusionInsight_HD_8.3.1/1_6_NameNode

  cp ${BIGDATA_HOME}/FusionInsight_HD_8.3.1/install/FusionInsight-Hadoop-3.3.1/hadoop/sbin/exportENV_VARS.sh ./

f. Run the following command for the environment variables to take effect.

   source exportENV_VARS.sh

g. Run the following command to restore editlog.

   cd $HADOOP_HOME/bin

   ./hdfs namenode -recover

h. Enter **y** as prompted.

i. On FusionInsight Manager, start HDFS.

Reference Information

None.

2.4.9.3.2 Failed to Switch Namenode to Active

Symptom

When NameNode instance is re-added after deletion NameNode, the Namenode does not switch to active, following exception is logged in ZKFC.

```
2019-11-20 17:41:59,203 | WARN | Health Monitor for NameNode at HOST-10-18-51-160/10.1.1.0:25500-EventThread
| Exception handling the winning of election |
org.apache.hadoop.ha.ActiveStandbyElector.becomeActive(ActiveStandbyElector.java:809)
java.lang.IllegalArgumentException: Unable to determine service address for namenode '66'
```

Possible Causes

When Namenode instance is deleted, IP and ID are not updated in the ZooKeeper. Hence on re-addition of instance, cluster startup fails.

As shown in **Figure 2-5**, first delete the Node 2, then add the Node 3 as NameNode.

Figure 2-5 Cluster

Fault Locating

Need to format ZKFC and copy meta data from active node to newly added Namenode.

Procedure

The client has obtained the security authentication. To restore this cluster, perform following steps:

NOTICE

Seek help from HDFS experts before doing this operation since it is a critical operation.

Step 1 Stop HDFS service from FusionInsight Manager.

Step 2 Run the command as follows to format ZKFC.

1. Run the **su - omm** command to switch to user **omm**.
2. Run the following commands to export the environment variables:

   EXECUTABLE_HOME="${CONTROLLER_HOME}/kerberos_user_specific_binay/kerberos"

   LD_LIBRARY_PATH=${EXECUTABLE_HOME}/lib:$LD_LIBRARY_PATH

   PATH=${EXECUTABLE_HOME}/bin:$PATH
3. If the cluster uses the security mode, run the **kinit** command to obtain a security certificate:

   kinit hdfs
4. Go to **${BIGDATA_HOME}/FusionInsight_HD_8.3.1/1_6_Zkfc**, copy the environment variables shell to the current path.

   cd ${BIGDATA_HOME}/FusionInsight_HD_8.3.1/1_6_Zkfc

   cp ${BIGDATA_HOME}/FusionInsight_HD_8.3.1/install/FusionInsight-Hadoop-3.3.1/adapter/bin/exportENV_VARS.sh ./
5. Run the command, the environment variables will take effect.

   source exportENV_VARS.sh
6. Run the following commands to format ZKFC:

   cd $HADOOP_HOME/bin

   ./hdfs zkfc -formatZK

Input **y** after the messages, then the operation finished.

Step 3 Start JournalNode and old Namenode. The old NameNode means the Active NameNode, such as the Node 1 in **Figure 2-5**.

Step 4 For the new NameNode, execute ***bootstrapStandby*** command to copy the information from the active NameNode. The new NameNode means the one we added, such as the Node 3 in **Figure 2-5**.

1. Run the **su - omm** command to switch to user **omm**.
2. Run the following commands to export the environment variables:

   EXECUTABLE_HOME="${CONTROLLER_HOME}/kerberos_user_specific_binay/kerberos"

   LD_LIBRARY_PATH=${EXECUTABLE_HOME}/lib:$LD_LIBRARY_PATH

   PATH=${EXECUTABLE_HOME}/bin:$PATH
3. If the cluster uses the security mode, run the **kinit** command to obtain a security certificate:

   kinit hdfs
4. Go to **${BIGDATA_HOME}/FusionInsight_HD_8.3.1/1_6_NameNode**, copy the environment variables shell to the current path.

   cd ${BIGDATA_HOME}/FusionInsight_HD_8.3.1/1_6_NameNode

   cp ${BIGDATA_HOME}/FusionInsight_HD_8.3.1/install/FusionInsight-Hadoop-3.3.1/adapter/bin/exportENV_VARS.sh ./
5. Run the command, the environment variables will take effect.

   source exportENV_VARS.sh
6. Run the following commands to copy the information:

   cd $HADOOP_HOME/bin

   ./hdfs namenode -bootstrapStandby -force

Step 5 Start HDFS service from FusionInsight Manager.

----End

Reference Information

None.

2.4.9.3.3 NameNode Is Always in the Restoring State

Symptom

On the FusionInsight Manager HDFS service page, NameNode is always in the **Restoring** state and cannot provide services.

Possible Causes

- The configuration is not synchronized to the node.
- A host name or IP address conflict exists in the cluster.
- The IP address 127.0.0.2 exists in the **/etc/hosts** node in the cluster.

Fault Locating

1. First, synchronize the configuration of the NameNode service using FusionInsight Manager and restart the service.
2. Check whether a host name or IP address conflict exists in the cluster.
3. Then check whether the IP address 127.0.0.2 exists in the machine where the faulty node locates. If yes, delete the IP address.

Procedure

Step 1 Log in to the FusionInsight Manager portal, and choose **Cluster** > *Name of the desired cluster* > **Services** > **HDFS** > **More** > **Synchronize Configuration** to synchronize the cluster service configuration.

Step 2 In the service list, click **More** > **Restart Service** to restart the HDFS service.

Step 3 Log in to the operating system (OS) where the faulty service is located as user **root**.

Step 4 Run **cat /etc/hosts | grep 127.0.0.2** to check whether any result exists. If yes, delete the lines containing 127.0.0.2 in the **/etc/hosts** file.

Step 5 Check whether the NameNode run log file (the default file is **/var/log/Bigdata/hdfs/nn/hadoop-omm-namenode-hostname.log**) whose status is **Restoring** contains the following similar logs.

If the following logs exist, the **/etc/hosts** file is incorrect.

```
Caused by: GSSException: No valid credentials provided (Mechanism level: Server not found in Kerberos database (7) - UNKNOWN_SERVER)
 Caused by: KrbException: Server not found in Kerberos database (7) - UNKNOWN_SERVER
        at sun.security.krb5.KrbTgsRep.<init>(KrbTgsRep.java:73)
        at sun.security.krb5.KrbTgsReq.getReply(KrbTgsReq.java:192)
        ... 27 more
 Caused by: KrbException: Identifier doesn't match expected value (906)
2015-04-20 08:54:43,764 | WARN  | 1771906083@qtp-1569927211-2146 | Authentication exception: GSSException: Failure unspecified at GSS-API level (Mechanism level: Invalid argument (400) - Cannot find key of appropriate type to decrypt AP REP - AES256 CTS mode with HMAC SHA1-96) | org.apache.hadoop.security.authentication.server.AuthenticationFilter.doFilter(AuthenticationFilter.java:401)
 org.apache.hadoop.security.authentication.client.AuthenticationException: GSSException: Failure unspecified at GSS-API level (Mechanism level: Invalid argument (400) - Cannot find key of appropriate type to decrypt AP REP - AES256 CTS mode with HMAC SHA1-96)
  Caused by: KrbException: Invalid argument (400) - Cannot find key of appropriate type to decrypt AP REP - AES256 CTS mode with HMAC SHA1-96
```

Step 6 Run **cat /etc/hosts** to check whether IP addresses conflict in the node of the cluster one by one. Check whether an IP address corresponds to multiple host names or a host name corresponds to multiple IP addresses. If yes, modify the IP address.

Step 7 Resolve the content conflict problem in the **/etc/hosts** file, and then restart the NameNode.

----End

Reference Information

None.

2.4.9.3.4 HDFS Enters the Safe Mode Due to Resource Exceptions

Symptom

The HDFS enters the safe mode during the verification on the performance indicators in the performance environment.

The NameNode log file contains the following information:

```
WARN org.apache.hadoop.hdfs.server.namenode.NameNodeResourceChecker: Space available on volume 'null' is 0,
WARN org.apache.hadoop.hdfs.server.namenode.FSNamesystem: NameNode low on available disk space. Entering safe mode.
```

Possible Causes

1. The fault is caused by insufficient space of the directory specified by the parameter **dfs.namenode.name.dir.**
2. The fault is caused by the unavailability of the underlying network file system. For example, the network is unstable.

Fault Locating

1. Check whether the space of the directory specified by the parameter **dfs.namenode.name.dir** is sufficient.
2. Check whether the underlying network file system is abnormal. For example, the network is unstable.
3. Check whether the NameNode logs contain information similar to " NameNode low on available disk space. Entering safe mode."

Procedure

1. Check whether the space of the directory specified by the parameter **dfs.namenode.name.dir** is sufficient.
2. Repair the underlying network file system (after the network is stable) and manually exit the safe mode.

   Run the following command to manually exit the safe mode:

   hdfs dfsadmin -safemode leave

Reference Information

None.

2.4.9.3.5 NameNode Becomes Faulty Because HDFS editlogs Are Damaged

Symptom

After the cluster node is powered off and powered on, or the disk capacity is expanded, NameNode fails to start.

Possible Causes

The JournalNode editlog is damaged, causing data on each JournalNode to be inconsistent.

Fault Locating

1. The following error is found in the NameNode logs:

```
2019-06-27 17:30:23,434 | FATAL | IPC Server handler 6 on 25006 | Error: recoverUnfinalizedSegments
failed for required journal (JournalAndStream(mgr=QJM to [192.169.1.166:25012,
192.168.1.204:25012, 192.168.1.239:25012], stream=null)) | JournalSet.java:396
java.io.IOException: Timed out waiting 120000ms for a quorum of nodes to respond.
at
org.apache.hadoop.hdfs.qjournal.client.AsyncLoggerSet.waitForWriteQuorum(AsyncLoggerSet.java:138)
at
org.apache.hadoop.hdfs.qjournal.client.QuorumJournalManager.createNewUniqueEpoch(QuorumJourn
alManager.java:223)
at
org.apache.hadoop.hdfs.qjournal.client.QuorumJournalManager.recoverUnfinalizedSegments(QuorumJ
ournalManager.java:459)
at org.apache.hadoop.hdfs.server.namenode.JournalSet$6.apply(JournalSet.java:622)
at
org.apache.hadoop.hdfs.server.namenode.JournalSet.mapJournalsAndReportErrors(JournalSet.java:391)
at
org.apache.hadoop.hdfs.server.namenode.JournalSet.recoverUnfinalizedSegments(JournalSet.java:619)
at org.apache.hadoop.hdfs.server.namenode.FSEditLog.recoverUnclosedStreams(FSEditLog.java:1611)
at
org.apache.hadoop.hdfs.server.namenode.FSNamesystem.startActiveServices(FSNamesystem.java:1231)
at org.apache.hadoop.hdfs.server.namenode.NameNode
$NameNodeHAContext.startActiveServices(NameNode.java:1925)
at org.apache.hadoop.hdfs.server.namenode.ha.ActiveState.enterState(ActiveState.java:61)
at org.apache.hadoop.hdfs.server.namenode.ha.HAState.setStateInternal(HAState.java:65)
at org.apache.hadoop.hdfs.server.namenode.ha.StandbyState.setState(StandbyState.java:59)
at org.apache.hadoop.hdfs.server.namenode.NameNode.transitionToActive(NameNode.java:1768)
at
org.apache.hadoop.hdfs.server.namenode.NameNodeRpcServer.transitionToActive(NameNodeRpcServe
r.java:1747)
at
org.apache.hadoop.ha.protocolPB.HAServiceProtocolServerSideTranslatorPB.transitionToActive(HAServi
ceProtocolServerSideTranslatorPB.java:112)
at org.apache.hadoop.ha.proto.HAServiceProtocolProtos$HAServiceProtocolService
$2.callBlockingMethod(HAServiceProtocolProtos.java:5409)
at org.apache.hadoop.ipc.ProtobufRpcEngine$Server
$ProtoBufRpcInvoker.call(ProtobufRpcEngine.java:530)
at org.apache.hadoop.ipc.RPC$Server.call(RPC.java:1036)
at org.apache.hadoop.ipc.Server$RpcCall.run(Server.java:928)
at org.apache.hadoop.ipc.Server$RpcCall.run(Server.java:863)
at java.security.AccessController.doPrivileged(Native Method)
at javax.security.auth.Subject.doAs(Subject.java:422)
at org.apache.hadoop.security.UserGroupInformation.doAs(UserGroupInformation.java:1729)
at org.apache.hadoop.ipc.Server$Handler.run(Server.java:2792)
2019-06-27 17:30:23,436 | INFO  | IPC Server handler 6 on 25006 | Exiting with status 1: Error:
recoverUnfinalizedSegments failed for required journal (JournalAndStream(mgr=QJM to
[192.169.1.166:25012, 192.168.1.204:25012, 192.168.1.239:25012], stream=null)) | ExitUtil.java:210
```

2. The JournalNode logs are as follows:

```
2019-06-27 17:33:36,354 | WARN  | IPC Server handler 0 on 25012 | Caught exception after scanning
through 0 ops from /srv/BigData/journalnode/hacluster/current/
edits_inprogress_0000000000000000808 while determining its valid length. Position was 1028096 |
FSEditLogLoader.java:1292
java.io.IOException: Can't scan a pre-transactional edit log.
at org.apache.hadoop.hdfs.server.namenode.FSEditLogOp
$LegacyReader.scanOp(FSEditLogOp.java:5295)
at
org.apache.hadoop.hdfs.server.namenode.EditLogFileInputStream.scanNextOp(EditLogFileInputStream.j
ava:261)
at org.apache.hadoop.hdfs.server.namenode.FSEditLogLoader.scanEditLog(FSEditLogLoader.java:1288)
at
org.apache.hadoop.hdfs.server.namenode.EditLogFileInputStream.scanEditLog(EditLogFileInputStream.j
ava:345)
at org.apache.hadoop.hdfs.server.namenode.FileJournalManager
$EditLogFile.scanLog(FileJournalManager.java:566)
at org.apache.hadoop.hdfs.qjournal.server.Journal.scanStorageForLatestEdits(Journal.java:234)
at org.apache.hadoop.hdfs.qjournal.server.Journal.<init>(Journal.java:175)
at org.apache.hadoop.hdfs.qjournal.server.JournalNode.getOrCreateJournal(JournalNode.java:106)
```

```
at org.apache.hadoop.hdfs.qjournal.server.JournalNode.getOrCreateJournal(JournalNode.java:151)
at
org.apache.hadoop.hdfs.qjournal.server.JournalNodeRpcServer.getEditLogManifest(JournalNodeRpcServ
er.java:228)
at
org.apache.hadoop.hdfs.qjournal.protocolPB.QJournalProtocolServerSideTranslatorPB.getEditLogManife
st(QJournalProtocolServerSideTranslatorPB.java:230)
at org.apache.hadoop.hdfs.qjournal.protocol.QJournalProtocolProtos$QJournalProtocolService
$2.callBlockingMethod(QJournalProtocolProtos.java:28984)
at org.apache.hadoop.ipc.ProtobufRpcEngine$Server
$ProtoBufRpcInvoker.call(ProtobufRpcEngine.java:530)
at org.apache.hadoop.ipc.RPC$Server.call(RPC.java:1036)
at org.apache.hadoop.ipc.Server$RpcCall.run(Server.java:928)
at org.apache.hadoop.ipc.Server$RpcCall.run(Server.java:863)
at java.security.AccessController.doPrivileged(Native Method)
at javax.security.auth.Subject.doAs(Subject.java:422)
at org.apache.hadoop.security.UserGroupInformation.doAs(UserGroupInformation.java:1729)
at org.apache.hadoop.ipc.Server$Handler.run(Server.java:2792)
```

Procedure

Step 1 Stop the HDFS service.

Step 2 Locate the JournalNode on which the editlog is not damaged.

NOTE

If the JournalNode run log does not contain the error log java.io.IOException: Can't scan a pre-transactional edit log, the editlog is not damaged.

Step 3 Copy the editlogs on the normal JournalNode to the JournalNode with the damaged editlog.

NOTE

1. View the value of **dfs.journalnode.edits.dir** to obtain the storage directory of editlogs on JournalNode. The default value is **/srv/BigData/journalnode**.
2. Back up the editlogs on the JournalNode on which the editlog is damaged.

   cp -r /srv/BigData/journalnode/hacluster/current /backup

   rm -rf /srv/BigData/journalnode/hacluster/current
3. Copy the editlogs of the normal node to the abnormal node.

   scp -r /srv/BigData/journalnode/hacluster/current root@xxx.xxx.xxx.xxx:/srv/BigData/journalnode/hacluster
4. On the abnormal node, change the owner group of the copied file to **omm:wheel**.

   chown -R omm:wheel /srv/BigData/journalnode/hacluster/current

Step 4 Restart the HDFS service.

----End

Related Information

None

2.4.9.3.6 Client Access to the NameNode Becomes Slow Due to the Shutdown of the Standby NameNode

Symptom

After a cluster node is powered off or the process does not respond, the client accesses the NameNode slowly.

If the following error message is displayed during client connection, the NameNode instance is abnormal. After the connection is retried for 20 times, the NameNode will be switched over for reconnection.

```
INFO retry.RetryInvocationHandler: No Route to Host from  xx.xx.xx.xx to xx.xx.xx.xx:25000 failed on socket timeout exception: java.net.NoRouteToHostException: No route to host; For more details see:  http://wiki.apache.org/hadoop/NoRouteToHost, while invoking ClientNamenodeProtocolTranslatorPB.getFileInfo over 192-168-64-81/192.168.64.81:25000 after 1 failover attempts. Trying to failover after sleeping for 592ms.
```

Possible Causes

After a client's access to the standby NameNode times out, the request is routed to the active NameNode. As a result, the client access duration is prolonged.

Procedure

Step 1 Log in to the client installation node as the client installation user and run the following command to modify the configuration file.

vim *client installation path*/**HDFS/hadoop/etc/hadoop/hdfs-site.xml**

Step 2 Change the value of **dfs.client.failover.max.attempts** to **5** and save the file.

```
</property>
<property>
<name>dfs.client.failover.max.attempts</name>
<value>5</value>
</property>
<property>
<name>dfs.mover.auto.hdfsfiles_or_dirs</name>
```

Step 3 Retry the client request.

----End

2.4.9.4 Common HDFS DataNode Faults

2.4.9.4.1 Uneven Distribution of HDFS Data

Symptom

System reports alarms indicating insufficient disk space after the system runs for a long period or the faulty disk is replaced.

Possible Causes

- Services are centrally running on some nodes after the cluster runs for a long period.

- The disk capacity of nodes in the cluster is uneven.
- The hard disk has been replaced.

Fault Locating

Balance the data in the cluster using the Hadoop Distributed File System (HDFS) disk balancing tool.

Procedure

Balance the data by following steps provided in the common HDFS maintenance commands.

Step 1 Install the HDFS client and connect it to the HDFS.

Step 2 Run the following command to balance the data.

Command example

bash /opt/hadoopclient/HDFS/hadoop/sbin/start-balancer.sh -threshold 1

In the command, **/opt/hadoopclient** is the client installation directory.

You can query logs in the hadoop-root-balancer-*host name*.out log file under the **/opt/hadoopclient/HDFS/hadoop/logs** directory of the client.

----End

Reference Information

HDFS data balancer. For more details, see **https://hadoop.apache.org/docs/r3.1.1/hadoop-project-dist/hadoop-hdfs/HdfsUserGuide.html#Balancer**.

2.4.9.4.2 DataNode logs InvalidProtocolBufferException

Symptom

DataNode unable to send block reports to NameNode. Following is the DataNode logs:

```
java.lang.IllegalStateException: com.google.protobuf.InvalidProtocolBufferException:
Protocol message was too large.  May be malicious.  Use CodedInputStream.setSizeLimit()
to increase the size limit exception
```

Possible Causes

This exception is encountered while block reporting from DataNode to NameNode. HDFS is designed for large files, so in case if it is being used for small files, the block reporting per volume may go beyond limit, to fit in a single message.

Fault Locating

To avoid this, we can specify multiple **dfs.datanode.data.dir** so that the blocks are split in many volumes and the block report message size is smaller.

In case if it is encounter in a running environment, Hadoop currently does not have a method to do this automatically.

Procedure

Step 1 Shutdown the DataNode involved.

Step 2 Use the **mv** command to move the individual block replica and meta pairs from one directory (**dfs.datanode.data.dir**) to the new directory. Also need to ensure the subdir-named directory structure remains exactly the same when moving the blocks across the disks.

For example, if the block replica and its meta pair were under **/data/1/dfs/dn/current/BP-1788246909-10.10.1.202-1412278461680/current/finalized/subdir0/subdir1/**, and you wanted to move it to **/data/5/disk**, then it MUST be moved into the same subdirectory structure underneath that, i.e. **/data/5/dfs/dn/current/BP-1788246909-10.10.1.202-1412278461680/current/finalized/subdir0/subdir1/**.

If this is not maintained, the DataNode will no longer be able to locate the replicas after the move.

Step 3 Restart the DataNode.

----End

Reference Information

None.

2.4.9.4.3 File Write Operation Failed due to DataNode unavailable for Replication

Symptom

Exception "*Failed to place enough replicas: expected...*" while client tries to perform write operation on the HDFS.

Possible Causes

- Data receivers are not available at DataNode.
- Not enough Hard Disks space at DataNode.
- Heartbeats are delayed from DataNode.

Fault Locating

Understand the current throughput of the cluster and based on the requirement, increase the resources (example, Disk, CPU, or Network).

Procedure

Step 1 Check the DataNode log. If the log contains "java.io.IOException: Xceiver count 8193 exceeds the limit of concurrent xcievers: 8192", then it indicates that data receivers are not available at DataNode.

Log in to FusionInsight Manager and choose **Cluster** > *Name of the desired cluster* > **Services** > **HDFS** > **Configurations** > **All Configurations**. Search for **dfs.datanode.max.transfer.threads** and change the parameter value to a number larger than 8192, for example, 16384.

NOTE

dfs.datanode.max.transfer.threads is used to Specify the maximum number of threads to use for transferring data in and out of the DataNode.

Step 2 If not enough hard disk space or CPU, try adding new data node or ensure the resource availability (disk space or CPU).

Step 3 If network issues, ensure the network availability.

----End

Reference Information

None.

2.4.10 HetuEngine

2.4.10.1 Message "yarn error with state [FAILED]" Is Displayed on the Client

Symptom

When an HSBroker instance is normal, run the **hetu-cli** command on the client or use the JDBC to drive the compute instance connection using the secondary development sample code. However, the compute instance fails to be created and the error message "yarn error with state [FAILED]" is displayed. The details are as follows:

```
Exception in thread "main" java.lang.IllegalArgumentException: Get uri from hsbroker error. Error code :
10000005 Message : Failed to create cluster [default]. Reason: yarn error with state [FAILED].
    at io.prestosql.cli.ClientOptions.parseServer(ClientOptions.java:284)
    at io.prestosql.cli.ClientOptions.toClientSession(ClientOptions.java:183)
    at io.prestosql.cli.Console.run(Console.java:88)
    at io.prestosql.cli.Presto.main(Presto.java:31)
```

- On the HSConsole page, the compute instance status is **ERROR**.

  Figure 2-6 Computing instance status

- On the native Yarn page, an error indicating that the virtual memory usage exceeds the limit is reported in the application corresponding to Coordinator.

Figure 2-7 Excessive virtual memory usage

```
ne):
tics:  Application application_1607676566783_0006 failed 2 times due to AM Container for appattempt_1607676566783_0006_000002 exited with exitCode: -103
       Failing this attempt.Diagnostics: [2020-12-11 17:09:25.964]Container [pid=55300,containerID=container_e03_1607676566783_0006_02_000001] is running 16928808968 beyond the 'VIRTUAL' memory limit. Current
       usage: 352.2 MB of 1 GB physical memory used; 6.6 GB of 5 GB virtual memory used. Killing container.
       Dump of the process-tree for container_e03_1607676566783_0006_02_000001 :
       |- PID PPID PGRPID SESSID CMD_NAME USER_MODE_TIME(MILLIS) SYSTEM_TIME(MILLIS) VMEM_USAGE(BYTES) RSSMEM_USAGE(PAGES) FULL_CMD_LINE
       |- 55300 55297 55300 55300 (bash) 1 0 5787648 719 /bin/bash -c /home/        Bigdata/common/runtime0/jdk1.8.0_242//bin/java -Djava.net.preferIPv4Stack=true -Djava.awt.headless=true -
       Djava.net.preferIPv4Stack=true -Djava.net.preferIPv6Addresses=false -Djava.security.krb5.conf=/home/        Bigdata/FusionInsight_BASE_8.0.2.1/1_31_KerberosClient/etc/kdc.conf -
       Djava.security.auth.login.config=/home/        /Bigdata/FusionInsight_HD_8.0.2.1/1_9_NodeManager/etc/jaas-zk.conf -Xmx768m -Dlog4j.configuration=yarnservice-log4j.properties -
       DLOG_DIR=/srv/BigData/hadoop/data1/nm/containerlogs/application_1607676566783_0006/container_e03_1607676566783_0006_02_000001 org.apache.hadoop.yarn.service.ServiceMaster -yarnfile
       hdfs://hacluster/user/hetuserver/.yarn/services/default-coordinator/default-coordinator.json -service_name default-coordinator -keytab hdfs://hacluster/user/hetuserver/8.0.0/hetuserver.keytab -principal_name
       hetuserver/hadoop.hadoop.com@HADOOP.COM -D hadoop.registry.zk.root=/registry -D hadoop.registry.zk.quorum=8.99.33.104:24002,8.99.33.105:24002,8.99.33.106:24002
       1>/srv/BigData/hadoop/data1/nm/containerlogs/application_1607676566783_0006/container_e03_1607676566783_0006_02_000001/serviceam-out.txt
       2>/srv/BigData/hadoop/data1/nm/containerlogs/application_1607676566783_0006/container_e03_1607676566783_0006_02_000001/serviceam-err.txt
       |- 55318 55300 55300 55300 (java) 1039 108 7055802368 89432 /home/        /Bigdata/common/runtime0/jdk1.8.0_242//bin/java -Djava.net.preferIPv4Stack=true -Djava.awt.headless=true -
       Djava.net.preferIPv4Stack=true -Djava.net.preferIPv6Addresses=false -Djava.security.krb5.conf=/home/        /Bigdata/FusionInsight_BASE_8.0.2.1/1_31_KerberosClient/etc/kdc.conf -
       Djava.security.auth.login.config=/home/        /Bigdata/FusionInsight_HD_8.0.2.1/1_9_NodeManager/etc/jaas-zk.conf -Xmx768m -Dlog4j.configuration=yarnservice-log4j.properties -
       DLOG_DIR=/srv/BigData/hadoop/data1/nm/containerlogs/application_1607676566783_0006/container_e03_1607676566783_0006_02_000001 org.apache.hadoop.yarn.service.ServiceMaster -yarnfile
       hdfs://hacluster/user/hetuserver/.yarn/services/default-coordinator/default-coordinator.json -service_name default-coordinator -keytab hdfs://hacluster/user/hetuserver/8.0.0/hetuserver.keytab -principal_name
       hetuserver/hadoop.hadoop.com@HADOOP.COM -D hadoop.registry.zk.root=/registry -D hadoop.registry.zk.quorum=8.99.33.104:24002,8.99.33.105:24002,8.99.33.106:24002
       [2020-12-11 17:09:25.987]Container killed on request. Exit code is 143
       [2020-12-11 17:09:26.051]Container exited with a non-zero exit code 143.
       For more detailed output, check the application tracking page: https://8-99-33-104:26022/applicationhistory/app/application_1607676566783_0006 Then click on links to logs of each attempt.
       . Failing the application.
ged    false
```

Possible Causes

- The ratio of the virtual memory to the physical memory of a task is too low in Yarn.

Fault Locating

1. Modify the ratio of the virtual memory to the physical memory of a task in Yarn.
2. Restart Yarn and the HetuEngine compute instance.

Procedure

Step 1 Log in to FusionInsight Manager, choose **Yarn** > **Configurations** > **All Configurations**, search for **yarn.nodemanager.vmem-pmem-ratio**, change its value to **20**, and save the configuration. Restart the Yarn service.

Step 2 After Yarn is restarted, run the **hetu-cli** command on the client to start the compute instance again, or restart the compute instance on the HSConsole page.

```
source /opt/hadoopclient/bigdata_env
hetu-cli --catalog hive
```

----End

2.4.10.2 Dynamic Scaling Function of the HetuEngine Compute Instance Does Not Take Effect

Symptom

On the HSConsole page, the dynamic scaling function of the HetuEngine compute instance is enabled. The instance is in the **Scaling out** or **Scaling in** state. After a period of time, the instance is in the **Running** state, but the number of workers remains unchanged. That is, the dynamic scaling function does not take effect.

Possible Causes

- The Yarn NodeAgent node is faulty. As a result, the AM of the worker or coordinator on the node is restarted. The number of workers restarted is different from that before the restart.
- Failed to update the number of workers to the database during scale-in or scale-out due to a database read/write fault.

Fault Locating

1. You can log in to the HetuEngine metabase and check whether the number of workers in the cluster with dynamic scaling enabled is the same as that displayed on the native page.

2. Disable the dynamic scaling function and enable it again.

Procedure

Step 1 Log in to FusionInsight Manager and select the HetuEngine service. On the **Dashboard** page, click the HSConsole link to go to the HSConsole page.

Step 2 For an instance whose dynamic scaling is invalid, click **Configure** and set **Scaling** from **ON** to **OFF**.

Figure 2-8 Setting **Scaling** to **OFF**

Figure 2-9 Checking whether the configuration takes effect

Step 3 Enable dynamic scaling again. Set **Scaling** from **OFF** to **ON**, and set the parameters based on the site requirements.

----End

2.4.10.3 Residual Yarn Container Process Exists After HetuEngine Is Uninstalled and Reinstalled

Symptom

1. A compute instance is running in the HetuEngine service.
2. A coordinator or worker is running on a NodeManager. The NodeManager is faulty and the fault is not rectified.
3. The HetuEngine service is uninstalled, and the HetuEngine applications on Yarn are stopped.

4. After the HetuEngine service is reinstalled and the compute instance is started, the container process of the HetuEngine service exists in the background. Run the **ps** *pid* command to check whether the task corresponding to the process is a Yarn container and whether the task is an application of the instance started by the HetuEngine service.

Figure 2-10 Residual PrestoServer process in the background

```
  PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
67225 omm       20   0 6520264 1.612g  87556 S 100.66 2.573  92:46.11 java
25769 omm       20   0 10.863g 909240  34612 S 27.815 1.384  13:25.79 java
 1661 root      20   0 1234648  32168  23684 S  6.291 0.049  32:58.85 messageservice
36811 omm       20   0 10.653g 599804  21332 S  5.629 0.913   0:35.98 java
72519 hetuser+  20   0 7984660 1.461g 111680 S  3.974 2.332  31:26.19 presto-server
  495 root      20   0  225856 127224 123724 S  3.311 0.194  11:59.42 systemd-journal
33900 omm       20   0 12.016g 997136  48884 S  2.649 1.518  33:48.67 java
 1425 message+  20   0   68572   7108   5512 S  2.318 0.011  10:06.74 dbus-daemon
22969 omm       20   0 3295256 1.268g  11964 S  1.656 2.024  16:19.34 slapd
63899 omm       20   0 6356716 541056  40992 S  1.656 0.824  46:05.86 java
```

Possible Causes

- After the NodeManager node is faulty, the container running on the NodeManager node cannot be managed and cannot be stopped even if applications are stopped once the HetuEngine service is uninstalled.

Fault Locating

Manually stop the container process that is no longer managed.

Procedure

Step 1 Run the **top** command to check the PrestoServer task on the node and obtain the PID of the task.

Step 2 Run the **kill -9** *pid* command to stop the task.

----End

2.4.11 Hive

2.4.11.1 "authentication failed" Displayed on a Shell Client

Symptom

In a cluster of the secure edition, HiveServer is normal. However, after the **beeline** command is run on a Shell client, the login fails, and **authentication failed** is displayed. The detailed information is as follows:

```
Debug is true storeKey false useTicketCache true useKeyTab false doNotPrompt false ticketCache is null
isInitiator true KeyTab is null refreshKrb5Config is false principal is null tryFirstPass is false useFirstPass is
false storePass is false clearPass is false
Acquire TGT from Cache
Credentials are no longer valid
Principal is null
null credentials from Ticket Cache
[Krb5LoginModule] authentication failed
No password provided
```

Possible Causes

- Kerberos authentication for the account is not performed.
- Kerberos authentication account expires.

Fault Locating

1. Perform Kerberos authentication again for the client user.
2. Log in to the client again after the authentication.
3. It takes about 1 minutes to rectify the fault.

Procedure

Step 1 Log in to the node where the Hive client is installed as user **root**.

Step 2 Run the following command to enter the client installation directory, for example, **/opt/hadoopclient**.

cd /opt/hadoopclient

Step 3 Run the **source bigdata_env** command to configure the environment variables.

Step 4 Run the following command:

kinit *component service user*

NOTE

The component service user can be created by the system administrator as required. Change the password of the component service user at the first login.

Step 5 Run the **beeline** command to log in to the Hive client.

----End

Reference Information

None.

2.4.11.2 "The ZooKeeper client is AuthFailed" Displayed When Client Authentication Failed

Symptom

In a cluster of the secure edition, HiveServer is normal. However, HiveServer fails to be logged in from a Shell client or secondary development tool, and **The ZooKeeper client is AuthFailed** is displayed. The detailed information is as follows:

```
14/05/19 10:52:00 WARN utils.HAClientUtilDummyWatcher: The ZooKeeper client is AuthFailed
 14/05/19 10:52:00 INFO utils.HiveHAClientUtil: Exception thrown while reading data from znode.The possible reason may be connectionless. This is recoverable. Retrying..
 14/05/19 10:52:16 WARN utils.HAClientUtilDummyWatcher: The ZooKeeper client is AuthFailed
 14/05/19 10:52:32 WARN utils.HAClientUtilDummyWatcher: The ZooKeeper client is AuthFailed
 14/05/19 10:52:32 ERROR st.BasicTestCase: Exception: Could not establish connection to active hiveserver
 java.sql.SQLException: Could not establish connection to active hiveserver
```

Possible Causes

- Authentication Failed when the client obtains the HiveServer address from ZooKeeper because the KeyTab file used by the client is incorrect.
- The system time of the client is inconsistent with that of the cluster.

Fault Locating

1. When you log in to the Hive client, you need to obtain the HiveServer address from ZooKeeper. When the HiveServer service is running properly, the client cannot connect to HiveServer because the HiveServer address cannot be obtained.
2. When the secure edition is used, the Hive client can obtain the address of the HiveServer from ZooKeeper only after passing the Kerberos authentication. According to related logs, if the authentication fails, check the Kerberos authentication information.
3. Log in to the Hive client again after the authentication, which takes less than 1 minute.

Procedure

Step 1 Confirm with the administrator to ensure that the information of the keytab used by the client.

Step 2 Check that the client system time is the same as the cluster system time.

----End

Reference Information

None.

2.4.11.3 "Read timed out" Displayed When a Client Fails to Be Connected

Symptom

In a cluster of the secure edition, HiveServer is normal. However, HiveServer fails to be logged in from a Shell client or secondary development tool, and **Read timed out** is displayed. The detailed information is as follows:

```
org.apache.hadoop.hive.ha.client.HAConnectMonitor.<init>(HAConnectMonitor.java:54)
 at org.apache.hadoop.hive.ha.client.HATTransport.open(HATTransport.java:158)
 at org.apache.hadoop.hive.jdbc.ha.HAHiveConnection.<init>(HAHiveConnection.java:60)
 ... 6 more
 Caused by: java.net.SocketTimeoutException: Read timed out
 at java.net.SocketInputStream.socketRead0(Native Method)
 at java.net.SocketInputStream.read(SocketInputStream.java:152)
 at java.net.SocketInputStream.read(SocketInputStream.java:122)
 at org.apache.thrift.transport.TIOStreamTransport.read(TIOStreamTransport.java:127)
```

Possible Causes

The socket connection times out when a Hive client is connected to the HiveServer due to network problems.

Fault Locating

1. A socket connection is to be created when the Hive client connects to the HiveServer. If packet loss occurs on the network, the socket connection times out and the Hive client fails to connect to the HiveServer.
2. Run the **ping** command to check the network between the Hive client and HiveServer.
3. Connect the Hive client to the server again when the network condition is better, which takes less than 1 minute.

Procedure

Step 1 Run **ping** *HiveServer IP address* to check the network condition from the Hive client.

If the ping test fails or the failure rate is high, the network is not stable.

Contact the network administrator to restore the network communication to meet the service requirements.

Step 2 Use the application layer of the Hive client, and add a failure retry mechanism in the application layer.

----End

Reference Information

None.

2.4.11.4 "Unable to determine if xxx encryptede" Displayed When a Shell Client Accesses a Table

Symptom

When the HiveServer service is running properly and user **poctest** accesses the **checkpoint** table, the following error information is displayed in the CLI:

```
0: jdbc:hive2://ha-cluster/default>  select * from checkpoint;
Error: Error while compiling statement: FAILED: SemanticException Unable to determine if hdfs://hacluster/
user/hive/warehouse/checkpointis encrypted: org.apache.hadoop.security.AccessControlException:
Permission denied: user=poctest, access=READ, inode="/user/hive/warehouse/
checkpoint":pocown:hive:drwx------
```

Possible Causes

If the access permission on the **checkpoint** table is not assigned to user **poctest**, the user cannot access the table.

Fault Locating

1. Check whether user **poctest** has the access permission on the **checkpoint** table.
2. On FusionInsight Manager, assign user **poctest** the access permission on the **checkpoint** table.

3. This operation takes less than 1 minute.

Procedure

Step 1 Log in to FusionInsight Manager.

Step 2 Choose **System** > **Permission** > **User** to view the role bound to user **poctest**. You can choose **System** > **Permission** > **Role** to check whether the role has the SELECT permission on the **checkpoint** table.

Step 3 Choose **System** > **Permission** > **Role**.

Step 4 Click **Create Role** and set **Role Name** and **Description**.

Step 5 Assign the role the SELECT permission on the **checkpoint** table.

Step 6 On **User**, bind user **poctest** to the role.

Step 7 Log in to the CLI as the **poctest** user, and run the following command:

beeline

select * from checkpoint;

If the result is displayed, other Hive users have the read permission.

----End

Reference Information

None.

2.4.11.5 Garbled Characters Displayed When the SELECT Statement Is Run for ARC4-encrypted Textfile

Symptom

Garbled characters are displayed when the SELECT statement is run for the compressed and archived Hive query result table which is encrypted by the alleged Rivest Cipher 4 (ARC4) encryption algorithm.

Possible Causes

The textfile file which is not a blocked file is encrypted by using ARC4.

Fault Locating

1. Encrypt the textfile file by using org.apache.hadoop.io.encryption.arc4.ARC4BlockCodec.
2. This operation takes less than 1 minute.

Procedure

1. If garbled characters are displayed during the query, run the following command on the beeline client:

set mapreduce.output.fileoutputformat.compress.codec=org.apache.hadoop.io.encryption.arc4.ARC4BlockCodec;

set hive.exec.compress.output=true.

Enter the admin user password.

2. Run the following command to import the data to the result table:

   insert overwrite table tbl_result select * from tbl_source;

3. Check whether the garbled characters are displayed by running the following command:

   select * from tbl_result.

   If no garbled character is displayed, the fault is solved.

Reference Information

None.

2.4.11.6 "File does not exist" Is Displayed in Hive Server Logs

Symptom

When the HiveServer service is normal, a user enables the Hive local mode and performs operations, such as querying data, on a Hive_over_HBase table (storing data on HBase). An execution error is displayed on the Hive client, and "File does not exist" is displayed in the subprocess logs of the Hive server.

The execution error on the Hive client is as follows:

```
0: jdbc:hive2://10.64.35.144:21066/default> select count(*) from default__tb_1_index_3__;
 Error: Error while processing statement: FAILED: Execution Error, return code 1 from
org.apache.hadoop.hive.ql.exec.mr.MapRedTask (state=08S01,code=1)
```

Go to **/var/log/Bigdata/hive/hiveserver/hive.log** and view the subprocess logs of the Hive server. "File does not exist" is displayed, as shown below:

NOTE

The version 8.3.1 is used as an example. Replace it with the actual version number.

```
2019-03-30 14:17:34,586 ERROR [main]: mr.ExecDriver (SessionState.java:printError(548)) - Job Submission
failed with exception 'java.io.FileNotFoundException(File does not exist: hdfs://hacluster/opt/huawei/
Bigdata/FusionInsight_HD_8.3.1/install/FusionInsight-Hive-3.1.0/hive-3.1.0/lib/hive-hbase-handler-3.1.0.jar)'
 java.io.FileNotFoundException: File does not exist:hdfs://hacluster/opt/huawei/Bigdata/
FusionInsight_HD_8.3.1/instal/FusionInsight-Hive-3.1.0/hive-3.1.0/lib/hive-hbase-handler-3.1.0.jar
```

Possible Causes

When a MapReduce job is run in the cluster mode, the third-party jar package is stored in the distributed cache. The jar package is released after the job is executed. In local mode, the third-party jar package must be obtained from a local computer. Currently, however, MapReduce does not support acquisition of the third-party jar package from a local computer. After Hive submits a job, MapReduce forcibly converts the path of the third-party jar package to an HDFS path that does not exist in local mode. As a result, the system cannot obtain the jar package for running the job and an error occurs.

For example, the third-party jar package is stored in **file:/opt/huawei/BigData/hive/lib/hbase-exec.jar**. Before running a MapReduce job, the system forcibly converts the path to an unavailable path, **hdfs:/opt/huawei/BigData/hive/lib/hbase-exec.jar**.

Troubleshooting Method

To resolve this problem, upload the third-party jar package to a specified HDFS path before performing operations on the Hive_over_HBase table.

Procedure

NOTE

In the following commands, {version} indicates the Hive version, for example, 1.1.0, and {jar version} indicates the version of each jar package. Enter the actual Hive and jar package versions when running the commands.

1. Log in to the active or standby Hive node as user **root**.
2. Initialize the environment variable to ensure that HDFS shell commands can be run.
   a. Run the following command to configure the environment variable:

      source bigdata_env

   b. If the cluster uses the security mode, run the following command to perform user authentication:

      kinit *Component service user*

   c. Run the following command to check whether HDFS shell commands can be run:

      hdfs

      If the following information is displayed, HDFS shell commands can be run.

```
Usage: hdfs [--config confdir] COMMAND
       where COMMAND is one of:
  dfs                  run a filesystem command on the file systems supported in Hadoop.
  namenode -format     format the DFS filesystem
  secondarynamenode    run the DFS secondary namenode
  namenode             run the DFS namenode
  journalnode          run the DFS journalnode
  zkfc                 run the ZK Failover Controller daemon
  datanode             run a DFS datanode
  dfsadmin             run a DFS admin client
  haadmin              run a DFS HA admin client
  colocationadmin      run a DFS Colocation Admin client
  fsck                 run a DFS filesystem checking utility
  balancer             run a cluster balancing utility
  jmxget               get JMX exported values from NameNode or DataNode.
  oiv                  apply the offline fsimage viewer to an fsimage
  oiv_legacy           apply the offline fsimage viewer to an legacy fsimage
  oev                  apply the offline edits viewer to an edits file
  fetchdt              fetch a delegation token from the NameNode
  getconf              get config values from configuration
  groups               get the groups which users belong to
  snapshotDiff         diff two snapshots of a directory or diff the
                       current directory contents with a snapshot
  lsSnapshottableDir list all snapshottable dirs owned by the current user
Use -help to see options
  portmap              run a portmap service
  nfs3                 run an NFS version 3 gateway
```

```
cacheadmin      configure the HDFS cache

Most commands print help when invoked w/o parameters.
```

3. Run the following commands to create HDFS paths:

   hdfs dfs -mkdir -p ${BIGDATA_HOME}/FusionInsight/hive/hive-3.1.0/lib/

   hdfs dfs -mkdir -p ${BIGDATA_HOME}/FusionInsight/hive/hadoop/share/hadoop/common/lib

   hdfs dfs -mkdir -p ${BIGDATA_HOME}/FusionInsight/hive/hadoop/share/hadoop/mapreduce

4. Run the following commands to upload related jar packages of Hive.

   hdfs dfs -copyFromLocal ${BIGDATA_HOME}/FusionInsight_Current/*_HiveServer/install/hive-3.1.0/lib/hive-hbase-handler-3.1.0*jar ${BIGDATA_HOME}/FusionInsight/hive/hive-3.1.0/lib/

   hdfs dfs -copyFromLocal ${BIGDATA_HOME}/FusionInsight_Current/*_HiveServer/install/hive-3.1.0/lib/hbase-server-2.2.3*jar ${BIGDATA_HOME}/FusionInsight/hive/hive-3.1.0/lib/

   hdfs dfs -copyFromLocal ${BIGDATA_HOME}/FusionInsight_Current/*_HiveServer/install/hive-3.1.0/lib/htrace-core-3.1.0-incubating*jar ${BIGDATA_HOME}/FusionInsight/hive/hive-3.1.0/lib/

   hdfs dfs -copyFromLocal ${BIGDATA_HOME}/FusionInsight_Current/*_HiveServer/install/hive-3.1.0/lib/hbase-protocol-2.2.3*jar ${BIGDATA_HOME}/FusionInsight/hive/hive-3.1.0/lib/

   hdfs dfs -copyFromLocal ${BIGDATA_HOME}/FusionInsight_Current/*_HiveServer/install/hive-3.1.0/lib/hbase-client-2.2.3*jar ${BIGDATA_HOME}/FusionInsight/hive/hive-3.1.0/lib/

   hdfs dfs -copyFromLocal ${BIGDATA_HOME}/FusionInsight_Current/*_HiveServer/install/hive-3.1.0/lib/hbase-common-2.2.3*jar ${BIGDATA_HOME}/FusionInsight/hive/hive-3.1.0/lib/

   hdfs dfs -copyFromLocal ${BIGDATA_HOME}/FusionInsight_Current/*_HiveServer/install/hive-3.1.0/lib/hbase-hadoop-compat-2.2.3*jar ${BIGDATA_HOME}/FusionInsight/hive/hive-3.1.0/lib/

   hdfs dfs -copyFromLocal ${BIGDATA_HOME}/FusionInsight_Current/*_HiveServer/install/hive-3.1.0/lib/hive-exec-3.1.0*jar ${BIGDATA_HOME}/FusionInsight/hive/hive-3.1.0/lib

5. Run the following commands to upload related jar packages of MapReduce:

   hdfs dfs -copyFromLocal ${BIGDATA_HOME}/FusionInsight_Current/*_HiveServer/install/hadoop/share/hadoop/mapreduce/hadoop-mapreduce-client-core-3.3.1*jar ${BIGDATA_HOME}/FusionInsight/hive/hadoop/share/hadoop/mapreduce/

   hdfs dfs -copyFromLocal ${BIGDATA_HOME}/FusionInsight_Current/*_HiveServer/install/hadoop/share/hadoop/common/lib/netty-3.10.6.Final.jar ${BIGDATA_HOME}/FusionInsight/hive/hadoop/share/hadoop/common/lib/

   hdfs dfs -copyFromLocal ${BIGDATA_HOME}/FusionInsight_Current/*_HiveServer/install/hadoop/share/hadoop/common/lib/protobuf-java-2.5.0.jar ${BIGDATA_HOME}/FusionInsight/hive/hadoop/share/hadoop/common/lib/

   hdfs dfs -copyFromLocal ${BIGDATA_HOME}/FusionInsight_Current/*_HiveServer/install/hadoop/share/hadoop/common/hadoop-

common-3.3.1*jar ${BIGDATA_HOME}/FusionInsight/hive/hadoop/share/hadoop/common/

hdfs dfs -copyFromLocal ${BIGDATA_HOME}/FusionInsight_Current/*_HiveServer/install/hadoop/share/hadoop/common/lib/zookeeper-*jar ${BIGDATA_HOME}/FusionInsight/hive/hadoop/share/hadoop/common/lib/

hdfs dfs -copyFromLocal ${BIGDATA_HOME}/FusionInsight_Current/*_HiveServer/install/hadoop/share/hadoop/common/lib/guava-11.0.2.jar ${BIGDATA_HOME}/FusionInsight/hive/hadoop/share/hadoop/common/lib/

6. Log in to the server where the Hive client is installed, and run the following command to enter the local mode:

   set hive.exec.mode.local.auto=true;

7. Run the following command to query the Hive_over_HBase table. If query results are displayed, the fault is rectified.

   select count(*) from *Hive_over_HBase table name;*

   For example, the table name is default__tb_1_index_3_.

   select count(*) from default__tb_1_index_3__;

   If information similar to the following is displayed, the fault is rectified.

```
0: jdbc:hive2://ha-cluster/default> select count(*) from default__tb_1_index_3__;
+------+
| _c0  |
+------+
| 0  |
```

Reference Information

None.

2.4.11.7 Failed to Download a Large Amount of Result Data on the Hue WebUI

Symptom

In **Query Editor** > **Hive** on the Hue WebUI, the error message **The data volume of the returned query result is too large. It is recommended that LIMIT or TABLESAMPLE keywords be added to SQL statements** or **500 Internal Server Error** is displayed when a user clicks the download button after running the query statement.

Possible Causes

In the query result, the data amount of a single line exceeds 16 KB. When the data amount of 1000 lines exceeds 16777215 B (16 MB), the result data amount exceeds the system threshold and the download fails.

Fault Locating

1. After the keyword LIMIT is added at the end of the statement, a data record is queried. Estimate the size of the data record and multiply the size by 1000 to check whether the total size exceeds the system threshold 16777215 B (16 MB).

   SELECT col_name FROM table_name LIMIT 1

   NOTE

   In **Query Editor** > **Hive** on the Hue WebUI, a maximum of 30000 lines of data can be downloaded. (The size of each line of data cannot exceed 16 KB.)

2. If the number exceeds the system threshold, the Hue client cannot download large amount of data sets. You need to use either of the following methods to store the result sets to the HDFS or Hive intermediate tables, and then use HDFS commands to download the data sets to a node in the cluster.
   - Use the **INSERT OVERWRITE [LOCAL] DIRECTORY SELECT col_name FROM table_name** statement to export the query result to the HDFS or local node.
   - Use the **CREATE TABLE table_name1 AS SELECT col_name FROM table_name** statement to create a CSV table and import the query result to the table.
3. If the size does not exceed the threshold, contact the technical support.

Procedure

- **Exporting data to the HDFS**
  a. Log in to Hue, choose **Query Editor** > **Hive**, and run **INSERT OVERWRITE [LOCAL] DIRECTORY** to export the query result to the HDFS.

     For example, run the following statement to export the query result to **/tmp/result** on the HDFS:

     insert overwrite directory "/tmp/result" select * from test;

  b. Log in to the node where the HDFS client locates and run the ***get*** command of the HDFS to download the result from the HDFS.

     For example, run the following statement to download the files in **/tmp/result** to **/home/omm/result** on the local node:

     hdfs dfs -get /tmp/result /home/omm/result/

- **Exporting data to the CSV table**
  a. Log in to Hue, choose **Query Editor** > **Hive**, and run the SQL statement of the created CSV table to export the query result to the Hive table.

     For example, run the following statement to store the query result to the tt table of the CSV format:

     CREATE TABLE *TT* ROW FORMAT SERDE 'org.apache.hadoop.hive.serde2.OpenCSVSerde' STORED AS TEXTFILE AS SELECT col_name FROM table_name ;

  b. The SELECT statement can be used to query the CSV table that stores the query result.

     SELECT * FROM TT LIMIT *XX*

NOTE

XX indicates the number of lines to be queried.

c. To directly download data files, run the SHOW statement to view the storage path of the TT table. The command is as follows:

SHOW CREATE TABLE *TT*;

```
+----------------------------------------------------------------+
|                        createtab_stmt                          |
+----------------------------------------------------------------+
| CREATE TABLE `TT`(                                             |
|   `id` string,                                                 |
|   `name` string,                                               |
|   `address` string)                                            |
| ROW FORMAT SERDE                                               |
|   'org.apache.hadoop.hive.serde2.OpenCSVSerde'                 |
| STORED AS INPUTFORMAT                                          |
|   'org.apache.hadoop.mapred.TextInputFormat'                   |
| OUTPUTFORMAT                                                   |
|   'org.apache.hadoop.hive.ql.io.HiveIgnoreKeyTextOutputFormat' |
| LOCATION                                                       |
|   'hdfs://hacluster/user/hive/warehouse/tt'                    |
| TBLPROPERTIES (                                                |
|   'bucketing_version'='2',                                     |
|   'transient_lastDdlTime'='1712479321')                        |
+----------------------------------------------------------------+
```

d. Log in to the node where the HDFS client is located and run the get command of the HDFS to download the query result from the HDFS, or log in to the HDFS WebUI to download the query result.

hdfs dfs -get *hdfs://hacluster/user/hive/warehouse/tt*

Reference Information

None.

2.4.11.8 Hive Table Is Created in a Specified Path

Symptom

The HiveServer service is running properly, but an error occurs when a Hive table is created in a specified path. The HQL command is as follows:

```
create external table exttbl_bad(id int, name string) row format delimited fields terminated by ',' stored as textfile location '/tmp/tmptbl';
```

NOTE

/tmp/tmptbl is the HDFS directory in which the Hive table is to be created.

The error information is as follows:

```
Error: Error while compiling statement: FAILED: HiveAccessControlException Permission denied. Principal [name=admin, type=USER] does not have following privileges on Object [type=DFS_URI, name=/tmp/tmptbl] for operation CREATETABLE : [SELECT, INSERT, DELETE, OBJECT OWNERSHIP] (state=42000,code=40000)
```

Possible Causes

To create a Hive table in a specified HDFS directory, the current Hive user must be the owner of the HDFS directory and have the read, write, and execute permission of the directory. The possible cause is as follows:

- The current Hive user is not the owner of the HDFS directory and does not have read, write, and execute permission.
- The HDFS directory does not exist.

Fault Locating

1. Check whether the HDFS directory in which the Hive table is to be created exists.
2. Check whether the current Hive user is the owner of the HDFS directory and has read, write, and execute permission of the directory.

Procedure

The following procedure assumes that the HDFS directory is **/tmp/tmptbl** and the Hive user is **hive-test**.

Step 1 Log in to the HDFS client.

Step 2 Run the following command to go to the client installation directory, for example, **/opt/hadoopclient**:

cd /opt/hadoopclient

Step 3 Run the following command to configure environment variables:

source bigdata_env

Step 4 If the cluster uses the security mode, run the following command to perform user authentication:

kinit *component service user*

Step 5 Run the following command to check whether the HDFS directory, such as **/tmp/tmptbl**, exists:

hdfs dfs -ls /tmp/tmptbl

If the following information is displayed, the directory does not exist:

```
ls: `/tmp/tmptbl': No such file or directory
```

- If the directory exists, go to **Step 7**.
- If the directory does not exist, go to **Step 6**.

Step 6 Run the following command to create the HDFS directory. If no error message is displayed, the directory is created successfully.

hdfs dfs -mkdir -p /tmp/tmptbl

Step 7 Run the following command to check whether the current Hive user is the owner of the HDFS directory and has the read, write, and execute permission of the directory.

hdfs dfs -ls -d /tmp/tmptbl

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If yes, the information about the Hive user is displayed.

  ```
  drwx------ - hive-test hadoop-d      0 2015-10-10 15:12 /tmp/tmptbl
  ```

  In the information, **hive-test** is the name of the Hive user, and **hadoop-d** is the user group of the Hive user. The preceding information shows that the owner of **/tmp/tmptbl** is **hive-test**.
- If no, run the following command to change the owner and assign the read, write, and execute permission to the owner.

  hdfs dfs -chown hive-test:hadoop-d /tmp/tmptbl

  hdfs dfs -chmod 700 /tmp/tmptbl

----End

Reference Information

None.

2.4.11.9 No Information Is Displayed When a SQL Statement Fails to Be Run on the Hue WebUI

Symptom

A SQL statement fails to be run in **Query Editor** > **Hive** on the Hue WebUI, but no error information is displayed.

As shown in the following figure:

There should be the following information in normal cases:

Possible Causes

The possible cause is that the browser cache is not cleared. This problem rarely occurs.

Fault Locating

None

Procedure

Clear the browser cache to resolve this problem.

Reference Information

None

2.4.11.10 "SemanticException Error while configuring input job properties" Displayed When Operations Are Performed on a Hive_over_HBase Table

Symptom

hbase_t is a Hive_over_HBase table (data is stored in the **test_hbase** table of HBase). When the HiveServer service is running properly and user **test** performs operations (such as query) on **hbase_t**, an execution error occurs on the Hive client and the following information is displayed:

```
0: jdbc:hive2://10.10.151.99:21066/> select * from hbase_t;
Error: Error while compiling statement: FAILED: SemanticException Error while configuring input job properties (state=42000,code=40000)
```

Possible Causes

User **test** does not have rights on the HBase table.

Fault Locating

1. Check whether user **test** has related rights on the HBase table.
2. Assign the user related HBase rights.

Procedure

Step 1 Log in to FusionInsight Manager, choose **System > Permission** > **User** to view the role bound to user **test**, and choose **System > Permission** > **Role** to check whether the role has related rights on the HBase table.

Step 2 On the role management page of FusionInsight Manager, create a role, for example, **hive_hbase_select**, and assign the role the rights to query the Hive table **hbase_t** and the HBase table **test_hbase**.

1. In the **Configure Resource Permission** table, choose **HBase** > **HBase Scope** > **global** > **default**, and select **read** of the **test_hbase** table, and click **OK** to assign table query rights to the role.

2. Edit the role, in the **Configure Resource Permission** table, choose **HBase** > **HBase Scope** > **global** > **hbase**, and select **execute** of the **hbase:meta** table, and click **OK**.
3. Edit the role, in the **Configure Resource Permission** table, choose **Hive** > **Hive Read Write Privileges** > **default**, select **SELECT** of the **hbase_t** table, and click **OK**.

Step 3 On the user management page, bind user **test** to the **hive_hbase_select** role to enable the user to query the Hive table and the HBase table.

Step 4 Run the following command to query the Hive_over_HBase table. If query results are displayed, the fault is rectified.

select * from hbase_t;

----End

Reference Information

None

2.4.11.11 An Error Is Reported when the rename Operation Is Performed on a Large Partition Table

Symptom

When the Hive service is running properly, the **rename** operation is performed on a large partition table. An error message is displayed, indicating that the task fails. The following error message is displayed on the client:

```
Execution Error, return code 1 from org.apache.hadoop.hive.ql.exec.DDLTask. Unable to alter table. New location for this table ... already exists: ...
```

The new table name can be queried on HDFS, but no service data exists. After a period of time, the new table name is restored to the old table name, and the service data is restored.

Possible Causes

The rename operation is actually to create a new table and to delete the old table. Because the large partition table contains too many partitions, the task times out and an error is reported. After the task fails, the name and data of the old table are restored after a period of time. The MetaStore and HiveServer parameters need to be adjusted to prevent task timeout. Then, the **rename** operation can be successfully executed.

NOTE

You need to configure MetaStore parameters and HiveServer parameters according to the data volume. The following parameter values are for reference only. You need to adjust them according to the actual situation.

hive.metastore.million.partition.optimizer.batch.retrieve.max indicates the number of partitions loaded at a time when partitions in a large partitioned table are queried. **hive.metastore.million.partition.optimizer.batch.delete.max** indicates the number of partitions of a large partitioned table deleted at a time. **hive.metastore.client.socket.timeout** indicates the timeout interval of the MetaStore client.

Procedure

Step 1 Log in to FusionInsight Manager and choose **Cluster >** *name of the desired cluster* **> Services** > **Hive** > **Configurations**.

Step 2 On the page that is displayed, click **All Configurations** and set **Role** to **MetaStore** and **HiveServer** respectively. Search for the **hive.metastore.customized.configs** and **hive.server.customized.configs** parameters respectively for the two roles. Perform **Step 3**-**Step 5** to add the following three configuration items.

Step 3 In the **Name** textbox, enter **hive.metastore.million.partition.optimizer.batch.retrieve.max** and set **Value**, for example, to **2500**.

Step 4 Click the "+" icon to add a parameter configuration line. In the **Name** textbox, enter **hive.metastore.million.partition.optimizer.batch.delete.max** and set **Value**, for example, to **1000**.

Step 5 Click the "+" icon to add a parameter configuration line. In the **Name** text box, enter **hive.metastore.client.socket.timeout** and set **Value**, for example, to **10800s**.

Step 6 Click **Save**, then click **OK**. Restart services or instances with expired configurations to make the configurations take effect.

Step 7 Restart the service and perform the failed operation again. If the same task timeout error still occurs, repeat the preceding steps to adjust the preceding three parameters.

----End

2.4.11.12 "java.lang.OutOfMemoryError: GC overhead limit exceeded" Is Reported in MapReduce Logs When Partitions Are Inserted Dynamically

Symptom

When the HiveServer service is running properly and partitions are inserted dynamically, the **java.lang.OutOfMemoryError: GC overhead limit exceeded** error is reported in MapReduce logs.

Possible Causes

The out-of-memory (OOM) error occurs because too many partitions need to be processed by a single task. The number of partitions processed by a single task needs to be reduced based on specific scenarios.

Fault Locating

Perform operations according to the following example:

Run the following statements to create a table:

create table test(idint)partitioned by (dt int);

create table test1(id int, dt int);

Run the following statement to insert a partition dynamically:

insert overwrite table test partition (dt) selectid, dt from test;

Procedure

Step 1 **dt** is a partition field, so you need to distribute the partition field to different tasks to reduce the number of partitions processed by a single task.

The modified statement is as follows:

insert overwrite tabletest partition (dt) select id, dt from test1 distribute by dt;

Step 2 When data skew exists in the partition fields of **distribute by**, for example, fields whose value is null take a big proportion, you can disorder the data for processing.

When skew fields whose value is null exist, the statement is optimized as follows:

insert overwrite tabletest partition (dt) select id, dt from test1 distribute by nvl(dt,round(rand()*50));

NOTE

The NVL function is a user-defined function (UDF) embedded in Hive. This function can convert a null value into a desired value. For details about the usage of the embedded UDF, visit https://cwiki.apache.org/confluence/display/Hive/LanguageManual+UDF. A random digit from 0 to 1 is returned by using the rand function and then multiplied by constant 50 (the constant can be another digit and needs to be selected based on task concurrency and proper processing time). Then the result is rounded by using the round function. Partitions whose value is null are distributed to multiple tasks for processing.

----End

Reference Information

None

2.4.11.13 "Error 10011" Is Displayed on the Client When a UDF Is Used

Symptom

When a user-defined function (UDF) created by Spark is used in Hive, the **Error 10011** error is displayed on the client if metadata information is not synchronized in a timely manner.

For example, when a UDF named **test_udf** is created in Spark, the Hive client is used to connect to HiveServer, and **test_udf** is used, the following error information is displayed:

```
Error: Error while compiling statement: FAILED: SemanticException [Error 10011]: Line 1:7 Invalid function 'test_udf' (state=42000,code=10011)
```

This problem occurs when a UDF is used between multiple HiveServers. For example, when the UDF created by HiverServer2 is used on HiveServer1, the preceding error information is displayed on the client connected to HiveServer1 if metadata information is not synchronized in a timely manner.

Possible Causes

Shared metadata between multiple HiveServers or between Hive and Spark is not synchronized, and memory data becomes inconsistent. As a result, the UDF does not take effect.

Fault Locating

On the HiveServer where the UDF cannot be used, run **reload function** to synchronize the UDF information that is newly added to MetaStore to the HiveServer memory.

Procedure

Step 1 Log in to the Hive client where the UDF is used.

Step 2 Check whether the client is connected to the HiveServer where the UDF does not take effect.

NOTE

If the client is a beeline client, you can perform this step using the host name in the beeline prompt.

- If yes, go to **Step 3**.
- If no, exit the client and go to **Step 1**.

Step 3 Check whether the **using jar** keyword is included in the statement used to create the UDF.

- If yes, go to **Step 4**.
- If no, run the following command:

  add jar hdfs:///*jar_path***/***jar_name***.jar;**

NOTE

- *jar_path* specifies the storage path on HDFS of the JAR package used by the UDF.
- *jar_name* specifies the name of the JAR package used by the UDF.

Step 4 Run the following command to synchronize metadata:

reload function;

----End

Reference Information

None

2.4.11.14 When Permissions Are Granted for a Hive Database on the Interface, a Message Is Displayed Stating "Failed to modify role. Operation failed."

Symptom

If a role is granted permissions for a Hive database when Hive is working correctly and the permission granting is not completed in 10 minutes, a message is displayed stating **Failed to modify role. Operation failed.**.

Possible Causes

Excessive tables and partitions exist in the database, causing permission granting timeout.

NOTE

Within the permission granting timeout period, a database supports a maximum of 5000 tables and 1 million partitions. It is recommended that no location be specified for the partitions. If the partition directories are not under the table directories, at most 5000 partitions are supported.

Impact

The role for which permissions are granted has incorrect permissions for HDFS of some tables. Therefore, users who match the role cannot use the tables correctly.

Procedure

Step 1 Log in to FusionInsight Manager and choose **System > Permission** > **Role**. Click **Modify** to modify the permissions.

Step 2 Choose **Hive** > **Hive Read Write Privileges**. On the database permission granting page, click the database that fails to be granted permissions. The table permission granting page is displayed.

Step 3 Change the number of items displayed on each page from **10** to **300** and select all granted permissions. Then click **OK**.

Step 4 Repeat **Step 3** to cancel all permissions granted to the database.

Step 5 Use **Step 3** to grant the required permissions for all tables.

----End

Reference Information

None.

2.4.11.15 Error Message "task timeout set: 600s, taskTimedOut: true; task stuck timeout set: 600s, taskStuck: false" Is Displayed During Hive Task Execution

Symptom

When the HiveServer service is running properly and a MapReduce task is executed, the error message "task timeout set: 600s, taskTimedOut: true; task stuck timeout set: 600s, taskStuck: false" is reported.

Possible Causes

- After mapjoin is enabled, the execution statement contains the Cartesian product during task execution.
- Due to data distribution problems, severe data divergence occurs. Cyclic operations are performed on subtasks for a long time, but communication with ApplicationMaster times out. As a result, an error is reported.

Fault Locating

1. Check the Cartesian product.

   Check whether the join statement has association fields or non-equivalent associations, for example:

   select * from test1 t1 join test2 t2;

   select * from test1 t1 join test2 t2 on t1.id<> t2.id;

2. Check data divergence.

   On the Yarn WebUI, check the statistical counters information in the current Map task execution phase. If the number of Map output records is significantly greater than the number of Map input records, severe data divergence may occur.

Procedure

Step 1 Check whether the HQL statement is correct.

Step 2 View the data distribution of the associated fields in the HQL statement and check whether there is a large amount of duplicate data.

Step 3 When submitting a task, increase values of **mapreduce.task.timeout** and **mapreduce.task.stuck.timeout-ms** (unit: ms).

set mapreduce.task.timeout=3600000;

set mapreduce.task.stuck.timeout-ms=3600000;

Step 4 If the problem persists, stop the mapjoin.

set hive.auto.convert.join=false;

NOTE

If the problem still persists, adjust the service logic based on the actual situation.

----End

Related Information

None

2.4.11.16 admin User Fails to Submit the Hive on Spark Task in an Insecure Environment

Symptom

In an insecure environment, user **admin** fails to submit the Hive on Spark task, and the **org.apache.hadoop.security.AccessControlException: Permission denied** error is reported in MapReduce logs.

Possible Causes

Before the statement is executed, the **admin** user does not have permissions to access the **/user/admin** directory created by the **root** user when starting the Hive on Spark task because the directory has been used

Fault Locating

View the MapReduce logs to check whether the **Exception in thread "main" org.apache.hadoop.security.AccessControlException: Permission denied: user=admin, access=WRITE, inode="/user/admin":root:hadoop:drwxr-xr-x** error is reported.

Procedure

Step 1 Log in as a user who has the read and write permissions on the HDFS directory **/user/admin**.

Step 2 Run the following command to manually delete the **/user/admin** directory:

hdfs dfs -rm -r /user/admin

Step 3 Log in to the system as the **admin** user and execute the Hive On Spark task again.

----End

Reference Information

None

2.4.11.17 "java.lang.IllegalStateException: unread block data" Is Displayed When Running Hive on Spark After Third-Party JAR Files Are Added

Symptom

After the user adds third-party JAR files to Hive, uses JBDC to connect to HiveServer, and sets Spark as the Hive execution engine, the "java.lang.IllegalStateException: unread block data" exception is reported during the execution of Spark executor.

Possible Causes

Generally, if the Spark task deserialization fails and data cannot be read, the possible cause is that the JAR files references are inconsistent during serialization and deserialization. You can check whether the user-defined third-party JAR files conflict with the JAR files of Hive on Spark.

Fault Locating

Check whether the third-party JAR directory contains common open-source JAR packages. If the JAR packages are contained, compare the JAR packages with that in the Hive directory and that in the Spark directory, and delete the repeated packages in the third-party JAR directory.

Procedure

Step 1 Search for the host where the HiveServer instance is located.

Step 2 Go to the third-party JAR package directory: *cluster installation directory*/**third_lib**/*component name*.

Step 3 Decompile the JAR packages in the preceding directory and check whether common JAR files such as **org.apache.*** and **com.google** exist. If common JAR files exist, move them to another directory (for example, **/tmp**) and restart HiveServer.

Step 4 If the problem persists, contact the Spark contact person.

----End

Reference Information

None

2.4.11.18 When HBase Is Not Installed, Hive on Spark Tasks Do Not Respond

Symptom

When HBase is not installed, Hive on Spark tasks do not respond for about 10 minutes.

Possible Causes

The default value of **spark.security.credentials.hbase.enabled** in Spark is **true**, the HBase user is used for authentication during task execution. If the HBase

service does not exist or is stopped, the authentication fails and the tasks do not respond.

Procedure

Step 1 Choose **Cluster >** *Name of the desired cluster* **> Services** > **Hive** > **Configurations** > **All Comfiguration** > **HiveServer** > **Customization**, add the parameter named **spark.security.credentials.hbase.enabled** to the **hive.server.customized.configs** configuration item, and set the value to **true**.

Step 2 Save the configuration and restart the Hive service.

----End

2.4.11.19 Query Fails Due to Duplicate Names in the Hive Struct Field

Symptom

1. If the Hive table contains fields of the struct type, check whether duplicate keys exist in the field definition. You can run the following command to view the table description:

   desc *table_name*;

   NOTE

   In the preceding command, *table_name* indicates the table name.

   If duplicate keys are displayed in the query result, for example, ***struct<a int, a string, b string>***, the name of **a** is a duplicate key.

2. The HiveServer log contains the following error information:

```
java.io.EOFException: Read past end of RLE integer from compressed stream Stream for column 3 kind
LENGTH position: 6 length: 6 range: 0 offset: 12 limit: 12 range 0 = 0 to 6 uncompressed: 3 to 3
```

Possible Causes

Fields of the struct type cannot contain duplicate key names.

Procedure

Step 1 Contact the customer service personnel to modify the table and rename the fields of the struct type.

----End

Related Information

None

2.4.11.20 Some HBase Classes Fail to Be Loaded When Hive on Spark Executes HBase Data Source

Symptom

When Hive on Spark executes the HBase data source, some HBase classes are loaded inconsistently. The error log "Job failed with java.lang.LinkageError: loader

constraint violation: when resolving method" is displayed. As a result, the task fails.

Possible Causes

The Spark class loader loads JAR packages in different sequences.

Procedure

Step 1 Log in to the FusionInsight Manager.

Step 2 Choose **Cluster** > **Services** > **Hive** > **Configurations** > **All Configurations** > **HiveServer** > **Customization** and add the **spark.executor.userClassPathFirst** and **spark.driver.userClassPathFirst** parameters to **hive.server.customized.configs**. Set their values to **false**.

Example:

Step 3 Save the configuration and restart the HiveServer instance.

----End

2.4.11.21 An Error Is Reported During LOAD Execution When Hive Interconnects with OBS Using the Wrapper Solution

Symptom

In the storage-compute decoupling scenario, Hive interconnects with OBS using the Wrapper solution. When the Hive LOAD SQL statement is executed, an error message "java.lang.UnsupportedOperationException: can not support rename across filesystem" is displayed. As a result, the LOAD statement fails to be executed.

Possible Causes

The possible cause is that the HDFS path in the LOAD statement is not configured to map to the OBS wrapper. As a result, the schema of the HDFS path in the LOAD statement is inconsistent with that of the location in the table.

Procedure

Step 1 Log in to the FusionInsight Manager portal.

Step 2 Choose **Cluster** > **Service** > **Hive** > **Configurations** > **HiveServer**, and add the following two parameters to **hdfs.site.customized.configs**:

- Set **fs.hdfs.impl** to **com.huawei.hadoop.MRSHDFSWrapperFileSystem**.
- Set **fs.hdfs.mounttable.hacluster.link./***Path used by LOAD* to **obs://obs-test/***Mapped OBS path*.

See the following figure.

NOTE

For details, see "Interconnecting Hive with OBS" in *MapReduce Service (MRS) 3.3.1-LTS User Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Usage Guide (for Huawei Cloud Stack 8.3.1)*.

Step 3 Save the configuration and restart the HiveServer instance.

----End

2.4.11.22 An SQL Error Is Reported When the CBO of Hive Is Disabled

Symptom

When the CBO of Hive is disabled, that is, **hive.cbo.enable** is set to **false**, an error is reported when a SQL statement that meets one of the following conditions is executed:

- The **where** clause contains the field condition of the nested subquery and the statement involves at least two tables. An example of the SQL statement is as follows:

  select ... from table1 , table2, ... where column... in (select column... from table2) ...;
- The GROUP BY statement is followed by the ORDER BY syntax and the SELECT field does not contain the ORDER BY field. Such a SQL statement fails to be parsed when CBO is disabled. An example of the SQL statement is as follows:

  select count(distinct id), [columns...] FROM table1 GROUP BY id,... ORDER BY id desc;

Possible Causes

The symptom of this problem is the same in versions from Hive-1.2.1 to Hive-3.1.0. When the CBO is disabled, the SQL statements in the preceding two scenarios are not supported. You need to enable the CBO to support the SQL statements.

Procedure

Add **set hive.cbo.enable=true** before the SQL statement to be executed.

2.4.11.23 Hive on Spark Failed to Insert Data into a Bucketed Table

Symptom

When Hive on Spark inserts data into a bucketed table, if the number of buckets in the inserted table exceeds 1000, an NEP exception is reported in the log of the Spark executor and the task fails.

Possible Causes

The symptom of this problem is the same in versions from Hive-1.2.1 to Hive-3.1.0. When a table with more than 1000 buckets is inserted, the task fails. The cause is that the bucketId of the bucket table calculated by shuffle is incorrect during Hive and Spark engine adaptation. In this case, data is in disorder after Spark shuffle.

Procedure

Change the execution engine to MR or Tez and add **set hive.execution.engine=mr;** or **set hive.execution.engine=tez;** before the SQL statement to be executed.

2.4.11.24 An Error Is Reported When msck repair table table_name Is Run on Hive

Symptom

When the **msck repair table table_name** command is run on Hive, the error message "FAILED: Execution Error, return code 1 from org.apache.hadoop.hive.ql.exec.DDLTask (state=08S01,code=1)" is displayed.

Possible Causes

A directory in the HiveServer log file **/var/log/Bigdata/hive/hiveserver/hive.log** does not comply with the partition format.

```
2020-07-15 15:38:10,427 | WARN  | HiveServer2-Background-Pool: Thread-10905216 | Failed to run metacheck:  | org.apache.hadoop.hive.ql.exec.DDLTask.msck(DDLTask.java:2023)
org.apache.hadoop.hive.ql.metadata.HiveException: Repair: Cannot add partition ads_marketing.t_marketing_telemarketing_order_list:dtime=2020-04-24 17%3A55%3A00 due to invalid characters in the name
    at org.apache.hadoop.hive.ql.exec.DDLTask.msck(DDLTask.java:1986) [hive-exec-2.3.3-mrs-1.9.0.jar:2.3.3-mrs-1.9.0]
    at org.apache.hadoop.hive.ql.exec.DDLTask.execute(DDLTask.java:424) [hive-exec-2.3.3-mrs-1.9.0.jar:2.3.3-mrs-1.9.0]
    at org.apache.hadoop.hive.ql.exec.Task.executeTask(Task.java:199) [hive-exec-2.3.3-mrs-1.9.0.jar:2.3.3-mrs-1.9.0]
    at org.apache.hadoop.hive.ql.exec.TaskRunner.runSequential(TaskRunner.java:100) [hive-exec-2.3.3-mrs-1.9.0.jar:2.3.3-mrs-1.9.0]
    at org.apache.hadoop.hive.ql.Driver.launchTask(Driver.java:2185) [hive-exec-2.3.3-mrs-1.9.0.jar:2.3.3-mrs-1.9.0]
    at org.apache.hadoop.hive.ql.Driver.execute(Driver.java:1841) [hive-exec-2.3.3-mrs-1.9.0.jar:2.3.3-mrs-1.9.0]
    at org.apache.hadoop.hive.ql.Driver.runInternal(Driver.java:1527) [hive-exec-2.3.3-mrs-1.9.0.jar:2.3.3-mrs-1.9.0]
    at org.apache.hadoop.hive.ql.Driver.run(Driver.java:1238) [hive-exec-2.3.3-mrs-1.9.0.jar:2.3.3-mrs-1.9.0]
    at org.apache.hadoop.hive.ql.Driver.run(Driver.java:1233) [hive-exec-2.3.3-mrs-1.9.0.jar:2.3.3-mrs-1.9.0]
    at org.apache.hive.service.cli.operation.SQLOperation.runQuery(SQLOperation.java:266) [hive-service-2.3.3-mrs-1.9.0.jar:2.3.3-mrs-1.9.0]
    at org.apache.hive.service.cli.operation.SQLOperation.access$800(SQLOperation.java:93) [hive-service-2.3.3-mrs-1.9.0.jar:2.3.3-mrs-1.9.0]
    at org.apache.hive.service.cli.operation.SQLOperation$BackgroundWork$1.run(SQLOperation.java:379) [hive-service-2.3.3-mrs-1.9.0.jar:2.3.3-mrs-1.9.0]
    at java.security.AccessController.doPrivileged(Native Method) ~[?:1.8.0_232]
    at javax.security.auth.Subject.doAs(Subject.java:422) [?:1.8.0_232]
    at org.apache.hadoop.security.UserGroupInformation.doAs(UserGroupInformation.java:1840) [hadoop-common-2.8.3-mrs-1.9.0.jar:?]
    at org.apache.hive.service.cli.operation.SQLOperation$BackgroundWork.run(SQLOperation.java:393) [hive-service-2.3.3-mrs-1.9.0.jar:2.3.3-mrs-1.9.0]
    at java.util.concurrent.Executors$RunnableAdapter.call(Executors.java:511) [?:1.8.0_232]
    at java.util.concurrent.FutureTask.run(FutureTask.java:266) [?:1.8.0_232]
    at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1149) [?:1.8.0_232]
    at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:624) [?:1.8.0_232]
    at java.lang.Thread.run(Thread.java:748) [?:1.8.0_232]
```

Procedure

- Method 1: Delete the incorrect file or directory.
- Method 2: Run the **set hive.msck.path.validation=skip** command to skip invalid directories.

2.4.11.25 An Error Message "Invalid ACL: ACL has 33 access entries, which exceeds maximum of 32" Is Displayed When Hive Creates a Table

Symptom

An error is reported when Hive creates a table. The error information is as follows: Invalid ACL: ACL has 33 access entries, which exceeds maximum of 32.

Possible Causes

- Cause 1: This version may be upgraded from C70/C80. Check whether the ACL of the location of the database to which the created table belongs contains some authorization groups whose permissions are 0.

```
group:aaaa_1623210398123:---
group:hadoopmanager:r-x
```

- Cause 2: The location permission of the database to which the current table belongs and the user group to which the current table creation user belongs exceeds 32 characters.

Procedure

- Method 1: If a group without permission information exists, delete the group.
  a. Run the **hdfs dfs -getfacl {***HDFS path***}** command to query the ACL permission of **location**.
  b. Run the **hdfs dfs -setfacl -x group:**{*User group*} {*HDFS path*} command to delete the user group without permission information.

  NOTE

  In the preceding command, *{HDFS path}* indicates the HDFS path for storing the new table, and *{User group}* indicates the user group to which the user who creates the table belongs and whose permission information is empty.

- Method 2: Configure the 32-bit permission combination mode for Hive. For details, see "Authorizing Over 32 Roles in Hive" in *Component Operation Guide*.

2.4.11.26 Number of Buckets Is Inconsistent with the Number of Files When a Bucket Table Is Executed on Hive on Spark

Symptom

An error message "Bucketed table metadata is not current. Fix the metadata or don't use bucketed mapjoin" is displayed when Hive on Spark is used to query bucketed tables.

Possible Causes

Data is not stored by bucket when being imported to the bucket table. As a result, the number of buckets does not match the number of files, and sortmerge cannot be used for optimization.

Procedure

Run the following command before running the SQL statement on the client:

set hive.auto.convert.sortmerge.join=false;

2.4.11.27 Connection Timeout During SQL Statement Execution on the Client

Symptom

The SQL statement fails to be executed on the client, and the error message "Timed out waiting for a free available connection" is displayed.

Possible Causes

A large number of DBService connections exist, and obtaining connections times out.

Procedure

Step 1 Check whether the client uses the Spark-SQL client to execute SQL statements.

- If yes, check the timeout parameter in the URL, change the value to **600**, and go to **Step 7**.
- If the alarm is not cleared, go to **Step 2**.

Step 2 Log in to FusionInsight Manager, choose **Cluster** > **Services** > **Hive** > **Configuration** > **All Configurations**, search for **javax.jdo.option.ConnectionURL**, and check whether the value of the timeout parameter is less than **600**.

NOTE

This parameter exists in Hive, HiveServer, MetaStore, and WebHCat. Ensure that the parameter values are the same.

- If yes, go to **Step 3**.
- If no, go to **Step 7**.

Step 3 Check whether the value of **javax.jdo.option.ConnectionURL** is **${javax.jdo.option.ConnectionURL.default}**.

- If yes, go to **Step 4**.
- If no, change the timeout parameter in the URL to **600**, click **Save**, and go to **Step 7**.

Step 4 Click **Instance**, select any HiveServer instance, and log in to the instance node as user **root**.

Step 5 Open the **${BIGDATA_HOME}/FusionInsight_Current/*HiveServer/etc/hivemetastore-site.xml** configuration file, find the **javax.jdo.option.ConnectionURL** parameter, and copy its value.

Step 6 Log in to FusionInsight Manager, choose **Cluster** > **Services** > **Hive** > **Configuration** > **All Configurations**, search for **javax.jdo.option.ConnectionURL**, change its value to the URL copied in **Step 5**, change the timeout parameter to **600**, and click **Save**.

NOTE

This parameter exists in Hive, HiveServer, MetaStore, and WebHCat. Ensure that the parameter values are the same.

Step 7 Choose **Cluster** > **Services** > **Hive** > **Configuration** > **All Configurations**, search for **maxConnectionsPerPartition**, and check whether its value is less than **100**.

- If yes, change the value to **100**, click **Save**, and go to **Step 8**.
- If no, go to **Step 8**.

Step 8 If parameters are modified in the preceding steps, choose **Cluster** > **Services** > **Hive** > **Dashboard** and choose **More** > **Service Rolling Restart**. If the parameters are not modified, skip this step.

----End

2.4.11.28 A UDF Runs Successfully on Hive on MR but Fails on Hive on Tez and Hive on Spark

Symptom

A user-defined function (UDF) runs successfully on the Hive on MR engine. However, **Caused by: java.lang.ClassNotFoundException** is reported when it runs on the Hive on Tez engine.

Possible Causes

The UDF is developed based on Hadoop2.x and has introduced Hadoop2.x JAR packages, which may conflict with the JAR packages of the platform, and cause task running failures.

Procedure

Step 1 Check the execution engine type.

- If the execution engine is Hive on Tez, perform **Step 2** to **Step 5**.
- If the execution engine is Hive on Spark, go to **Step 6**.

Step 2 If Hive on Tez is used, log in to FusionInsight Manager, choose **Cluster** > **Services** > **Hive**, choose **Configuration** > **All Configurations**, and search for the **hive.security.authorization.sqlstd.confwhitelist** parameter.

Step 3 Append **,tez.user.classpath.first** to the value of **hive.security.authorization.sqlstd.confwhitelist**.

Step 4 Save the setting and restart the HiveServer instance.

Step 5 Run the following command before Hive on Tez runs the UDF:

set tez.user.classpath.first=false;

Step 6 Run the following commands before Hive on Spark runs the UDF:

set spark.executor.userClassPathFirst=false;

set spark.driver.userClassPathFirst=false;

----End

2.4.12 Hue

2.4.12.1 Hue Page Cannot Be Opened

Symptom

The Hue WebUI page of the service component cannot be opened.

Possible Causes

- The port is not opened for external users.
- The floating IP address is not correctly set.

Fault Locating

1. On the local machine where the browser locates, run the **telnet** command in the command-line interface (CLI) to check whether the port is opened.
2. Run **ifconfig** in the node where the Hue locates to check whether the floating IP address that is set takes effect.
3. It takes about 10 minutes to rectify the fault.

Procedure

Step 1 Log in to the FusionInsight Manager portal.

Step 2 Choose **Cluster** > *Name of the desired cluster* > **Services** > **Hue** > **Instance** to check whether the Hue service is running properly on the active and standby nodes.

- If yes, go to **Step 7**.
- If no, go to **Step 3**.

Step 3 Click **Configuration** and check whether the Hue configuration items **HUE_FLOAT_IP** and **HTTP_PORT** are correctly configured.

- If yes, go to **Step 4**.
- If no, correct the floating IP address and port of the Hue service.

Step 4 On the service network, run **telnet** *HUE node IP HTTP_PORT* or **telnet** *HUE_FLOAT_IP HTTP_PORT* to check whether the port is opened externally.

- If yes, ensure that the port is opened and then continue to rectify the fault.
- If no, go to **Step 5**.

Step 5 On the FusionInsight Manager portal, choose **Cluster** > *Name of the desired cluster* > **Services** > **Hue** , click **Stop Service**.

Step 6 Log in to the management node as user **root** ,, and run **ping** *HUE_FLOAT_IP* to check whether the Hue floating IP address can be pinged successfully.

- If yes, the floating IP is in use. Configure another IP address.
- If no, go to **Step 7**.

Step 7 Contact the technical support.

----End

Reference Information

None.

2.4.12.2 Hue Reports a Document2 Exceeding Error

Symptom

1. The newly created user is used to trigger multithreading with Python to simulate Hue, concurrently log in to Hive, and create tables.
2. The following error is displayed when the user logs in to Hue using a browser.

Possible Causes

The **Document2.objects.create** method is triggered in multiple locations, and the same user repeatedly adds **Document2**.

Fault Locating

1. Check the codes based on the error information. It is found that two **Document2** records are read from the database. However, the codes specify that only one record can exist.
2. Log in to the Hue database. It is found that the user has two records and multiple codes invoke the **Document2.objects.create** method to add **Document2**. The adding operation is triggered at the same time.

Procedure

Step 1 Back up the database (the testing environment is used to prevent accidents).

Step 2 Log in to the active DBService node, switch to user **omm**, and run the **gsql -p 20051 -d hue -W ****** -U hue** (* indicates the password of the Hue user) command.

Step 3 Search **owner_id** from the **auth_user** table and run the SQL statement to query the user records. In normal cases, the number of user records is 2.

Example:

select * from "auth_user" where "username" = 'admin001';

select * from "desktop_document2" where "owner_id" = 3 and "type" = 'directory';

Step 4 Delete the redundant records by ID.

Example:

delete from "desktop_document2" where "id" = 52

----End

Reference

None.

2.4.12.3 "Proxy Error" Is Displayed When the Hue Page Is Opened

Symptom

"Proxy Error" is displayed when the Hue page is opened.

Possible Causes

- Httpd does not receive packets or receives incorrect packets due to network faults, such as the high packet error rate and high latency.
- The authentication relationship between the Httpd service and the Hue service fails because of clock change or other reasons.

Fault Locating

1. Check whether a network fault or clock change occurs.
2. Check whether alarms related to the Hue service have been generated or still exist.

Procedure

Step 1 Log in to FusionInsight Manager to check whether any network fault, clock change, or Hue service alarm exists. If yes, contact the administrator to rectify the fault. Then, check whether the Hue page can be normally opened.

- If yes, no further action is required.
- If no, go to **Step 2**.

Step 2 Obtain the address of the current Httpd server, which is the host address in the URL of the Hue page. That is, if the URL of Hue is https://192.168.0.1:21201, the Httpd service address is 192.168.0.1.

Step 3 Log in to the Httpd server and check logs in **/var/log/Bigdata/httpd/error_log**.

Step 4 Check whether the error message "AH01102: error reading status line from remote server" or "AH00898: Error reading from remote server" exists in the **error_log** file. (You can open the Hue page for several times to confirm the error.)

- If yes, restart the Hue service on FusionInsight Manager and go to **Step 5**.
- If no, go to **Step 6**.

Step 5 Restart the Hue service and open the Hue page again.

- If yes, no further action is required.
- If no, go to **Step 6**.

Step 6 Contact the technical support.

----End

2.4.12.4 Alarm "Hue Service Unavailable" Is Reported and Is Not Cleared for a Long Time

Symptom

A user logs in to FusionInsight Manager and finds that alarm "Hue Service Is Unavailable" persists. The user checks the Hue instance and finds that the node status is **Unknown**. The alarm persists even after the Hue service is restarted.

Possible Causes

Exceptions (for example, full load of CPUs and exhaustion of server I/Os) occur because the service node is fully loaded. The Hue service cannot exchange information with DBService occasionally. As a result, alarm "Hue Service Is Unavailable" is generated.

Fault Locating

1. Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Alarm**. Check whether other alarms are generated before and after the point in time when alarm "Hue Service Is Unavailable" is generated.
2. Check whether the **/var/log/Bigdata/hue/hue-ha-status.log** file on the Hue server contains **The account has been locked**.

Procedure

Step 1 Log in to FusionInsight Manager and check whether other alarms are generated before and after the point in time when alarm "Hue Service Is Unavailable" is generated. If such alarms exist, a service fault occurs in the cluster. In this case,

further locate the fault. If no such alarms exist, the service account may be locked due to misoperations.

Step 2 Log in to any Hue server and check whether the **/var/log/Bigdata/hue/hue-ha-status.log** file contains **The account has been locked**.

- If yes, the alarm is generated because the Hue account is locked. Go to **Step 3**.
- If no, go to **Step 6**.

Step 3 Log in to the active DBService node as user **omm** and run the following command to connect to the GaussDB database of DBService.

source ${DBSERVER_HOME}/.dbservice_profile

gsql -p 20051 -d postgres -W *Password of user omm for logging in to the GaussDB database in DBService* **-U omm**

Step 4 Run the **alter role hue account unlock;** command. After the command is executed successfully, run the **\q** command to exit gsql. Run the **gsql -p 20051 -d hue -W** *Password of user hue for Hue to connect to the DBService database* **-U hue** command to check whether the account is unlocked.

- If yes, go to **Step 5**.
- If no, retry **Step 4**. If the problem persists, go to **Step 6**.

Step 5 Log in to FusionInsight Manager and restart the Hue service. Check whether alarm "Hue Service Is Unavailable" is automatically cleared and whether the Hue page is accessed properly.

- If yes, no further action is required.
- If no, go to **Step 6**.

Step 6 Contact the technical support.

----End

2.4.12.5 Failed to View Job Information in Job Browser

Symptom

1. The Mapreduce is installed with two nodes.
2. On the Hue page, choose Job Browser and click a job to view job information. An error message is displayed.

Possible Causes

In RedHat 6.x and CentOS 6.x, a compatibility problem occurs when Hue is used to access JobHistoryServer. As a result, the correct result cannot be returned.

Procedure

You can view logs by using the Mapreduce on a single node.

2.4.13 IoTDB

2.4.13.1 Data of a Storage Group Deleted on the IoTDB Client Is Not Deleted from the Data Node

Issue

When a user runs the **delete storage group** command on the IoTDB client to delete a storage group, the data files of this storage group are not deleted from the data node.

Symptom

In the scenario with a large amount of data, after a storage group is deleted on the IoTDB client, data files in the storage group on the data node are not deleted.

Cause Analysis

Some regions of the deleted storage group do not exist on the data node.

Procedure

Manually delete the data of the specified storage group from the data node.

Step 1 Log in to FusionInsight Manager, choose **Cluster** > **Services** > **IoTDB**, click the **Instance** tab, and view the management IP address of the node where the IoTDBServer instance is located.

Step 2 Log in to any IoTDBServer node as user **root**.

Step 3 Run the following command to go to the IoTDB data node directory:

cd $BIGDATA_DATA_HOME/iotdb/iotdbserver

Step 4 Run the following command to query the paths of the deleted storage group:

find ./ -type d -name '*Name of the deleted storage group****'**

For example, if the deleted storage group is **root.test.g_0**, run the following command:

find ./ -type d -name 'root.test.g_0*'

The command output is as follows:

```
./data1/data/unsequence/root.test.g_0
./data1/data/sequence/root.test.g_0
./data1/system/schema/root.test.g_0
./data1/system/databases/root.test.g_0
./data2/wal/root.test.g_0-241
```

Step 5 Run the following command to delete all paths found in **Step 4**:

rm -rf '*Path of the deleted storage group***'**

For example:

rm -rf ./data1/data/unsequence/root.test.g_0

rm -rf ./data1/data/sequence/root.test.g_0

rm -rf ./data1/system/schema/root.test.g_0

rm -rf ./data1/system/databases/root.test.g_0

rm -rf ./data2/wal/root.test.g_0-241

Step 6 Log in to other IoTDBServer nodes and repeat **Step 2** to **Step 5**.

----End

2.4.13.2 ReadOnly Status of the IoTDB Instance Is Triggered and Cannot Be Automatically Restored

Symptom

Due to insufficient disk space, operations such as data merge trigger the ReadOnly status of the IoTDB instance. As a result, data cannot be written.

Possible Causes

The node status is set to ReadOnly.

Fault Locating

On the client, run the **show cluster** command to check the node status and set the node status from **ReadOnly** to **Running**.

Procedure

Step 1 Log in to the node where the IoTDB client is installed as the client installation user.

Step 2 Run the following commands to switch to the client installation directory and configure environment variables:

cd *Client installation directory*

source bigdata_env

kinit *Component service user* (Skip this step if Kerberos authentication is not enabled for the cluster.)

Step 3 Run the following command to switch to the directory where the IoTDB client running script is stored:

cd /opt/client/IoTDB/iotdb/sbin

Step 4 If Kerberos authentication is disabled for the cluster (the cluster is in normal mode), invoke the **alter-cli-password.sh** script to change the default password of the default user **root**.

sh alter-cli-password.sh *IP address of the IoTDBServer instance RPC port number*

NOTE

- The default RPC port number of IoTDBServer is **22260**, which can be configured in the **IOTDB_SERVER_RPC_PORT** parameter.
- For the default password of user **root**, see ***Huawei Cloud Stack 8.3.1 Account List*** .

Step 5 Run the following command to log in to the client:

./start-cli.sh -h *IP address of the IoTDBServer instance node* **-p** *IoTDBServer RPC port*

After running this command, specify the service username as required. The **root** user is used for login if Kerberos authentication is disabled for the cluster (the cluster is in normal mode).

Step 6 Run the following command to check the node status:

show cluster

```
IoTDB@[illegible]:22260> show cluster
+------+----------+--------+---------------+------------+
|NodeID|  NodeType|  Status|InternalAddress|InternalPort|
+------+----------+--------+---------------+------------+
|     0|ConfigNode| Running|[illegible]|       22259|
|     1|ConfigNode| Running|[illegible]|       22259|
|     2|ConfigNode| Running|[illegible]|       22259|
|     3|  DataNode|ReadOnly|[illegible]|       22250|
|     4|  DataNode|ReadOnly|[illegible]|       22250|
|     5|  DataNode|ReadOnly|[illegible]|       22250|
+------+----------+--------+---------------+------------+
Total line number = 6
It costs 0.004s
```

Step 7 Run the following command to set the node status to **Running**:

SET SYSTEM TO RUNNING

```
IoTDB@[illegible]:22260> SET SYSTEM TO RUNNING
```

The node status is changed.

```
IoTDB@1[redacted]:22260> show cluster
+------+----------+-------+---------------+------------+
|NodeID|  NodeType| Status|InternalAddress|InternalPort|
+------+----------+-------+---------------+------------+
|     0|ConfigNode|Running|[redacted]|       22259|
|     1|ConfigNode|Running|[redacted]|       22259|
|     2|ConfigNode|Running|[redacted]|       22259|
|     3|  DataNode|Running|[redacted]|       22250|
|     4|  DataNode|Running|[redacted]|       22250|
|     5|  DataNode|Running|[redacted]|       22250|
+------+----------+-------+---------------+------------+
Total line number = 6
It costs 0.005s
```

----End

2.4.14 Kafka

2.4.14.1 Broker Instance Status Is Restoring After Kafka Node Disk Usage Reaches 100%

Symptom

After the disk usage of the Kafka data directory reaches 100%, the Broker instance on the node is in the **Restoring** state and the node cannot provide Kafka services.

Possible Causes

- Topic partitioning is improper, due to which the usage of some disks reaches 100%.
- The local disk store other data in addition to the Kafka data, due to which the disk usage reaches 100%.

Fault Locating

1. Locate the reason why the disk usage reaches 100%.
2. Move data to other idle disks and restart the Broker instance.
3. Resolve the disk capacity insufficiency problem according to the handling method of "ALM-38001 Insufficient Kafka Disk Space".

Procedure

Step 1 Log in to FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Kafka** > **Instance**, stop the Broker instance whose status is **Restoring**, record the management IP address of the node where the Broker instance is located, and record **broker.id**. The value can be obtained by using the following method: Click the role name. On the **Configurations** page, select **All Configurations**, and search for the **broker.id** parameter.

Step 2 Log in to the recorded management IP address as user **root**, and run the **df -lh** command to view the mounted directory whose disk usage is 100%, for example, **${BIGDATA_DATA_HOME}/kafka/data1**.

Step 3 Go to the directory, run the **du -sh *** command to view the size of each file in the directory,check whether files other than **kafka-logs** exist, and determine whether these files can be migrated.

- If yes, migrate related data and go to **Step 8**.
- If no, go to **Step 4**.

Step 4 Go to the **kafka-logs** directory, run the **du -sh *** command, select a partition folder to be moved. The naming rule is **Topic name-Partition ID**. Record the topic and partition.

Step 5 Modify the **recovery-point-offset-checkpoint** and **replication-offset-checkpoint** files in the **kafka-logs** directory in the same way.

1. Decrease the number in the second line in the file. (To remove multiple directories, the number deducted is equal to the number of files to be removed.)
2. Delete the line of the to-be-removed partition. (The line structure is "Topic name Partition ID Offset". Save the data before deletion. Subsequently, the content must be added to the file of the same name in the destination directory.)

Step 6 Modify the **recovery-point-offset-checkpoint** and **replication-offset-checkpoint** files in the destination data directory. For example, **${BIGDATA_DATA_HOME}/kafka/data2/kafka-logs** in the same way.

- Increase the number in the second line in the file. (To move multiple directories, the number added is equal to the number of files to be moved.)
- Add the to-be moved partition to the end of the file. (The line structure is "Topic name Partition ID Offset". You can copy the line data saved in **Step 5**.)

Step 7 Move the partition to the destination directory. After the partition is moved, run the **chown omm:wheel -R** *Partition directory* command to modify the directory owner group for the partition.

Step 8 Log in to FusionInsight Manager and choose **Cluster** > *Name of the desired cluster* > **Services** > **Kafka** > **Instance** to stop the Broker instance.

Step 9 Wait for 5 to 10 minutes and check whether the health status of the Broker instance is **Normal**.

- If yes, resolve the disk capacity insufficiency problem according to the handling method of "ALM-38001 Insufficient Kafka Disk Space" after the alarm is cleared.
- If no, contact the technical support.

----End

Reference Information

ALM-38001 Insufficient Kafka Disk Space

2.4.15 KrbServer

2.4.15.1 KrbServer Service Unavailability

Symptom

This alarm is reported when the KrbServer service is unavailable.

Possible Causes

The KrbServer service depends on the LdapServer service. This fault may be caused by the unavailable LdapServer service.

Fault Locating

1. The KrbServer service depends on the LdapServer service. You need to handle the LdapServer service unavailability alarm first, and then restart the KrbServer service.
2. It takes about 10 minutes to rectify the fault.

Procedure

Step 1 Log in to FusionInsight Manager.

Step 2 Choose **O&M > Alarm** , check whether an alarm indicating unavailable LdapServer service exists. If yes, handle the alarm according to the related alarm guide.

Step 3 Choose **Cluster >** *Name of the desired cluster* **> Services** > **KrbServer** > **More** > **Restart Service**. On the displayed **Verify Identity** dialog box, enter the password and click **OK**. On the displayed **Restart Service** dialog box, select **Restart upper-layer services** as required, and click **OK** to restart the KrbServer service.

NOTE

The KrbServer service is unavailable during the restart. Upper-layer services that depend on the KrbServer service are also affected.

----End

Reference Information

None.

2.4.15.2 Running Status of the KrbServer Service Is Unknown

Symptom

In the service list on FusionInsight Manager, the running status of the KrbServer service is **Unknown**.

Possible Causes

Service status information cannot be uploaded because network resources are exhausted.

Fault Locating

Check whether exceptions such as **java.net.ConnectException: Connection refused** exist in the heartbeat log files of the agent on the node where KrbServer is deployed.

The log file path is **/var/log/Bigdata/nodeagent/agentlog/heartbeat_trace.log**.

Procedure

Step 1 Log in to any node in the cluster as user **root**.

Step 2 Install the FusionInsight client, run the **kinit admin** command.

Step 3 If the **kinit** command runs successfully, the KrbServer service is available; otherwise, contact the technical support.

----End

Reference Information

None.

2.4.15.3 An Error Occurred When Changing a Component Password

Symptom

During the component password changing, the following message is displayed:

```
Password change rejected: New password was used previously.Please choose a different password.. Please try again
```

Possible Causes

The message is displayed due to KrbServer internal problems. The password has been changed successfully.

Fault Locating

Log in to a component using the new password.

Procedure

Step 1 Enter in to the client installation directory.

Step 2 Run the **source bigdata_env** command to configure the environment variables for the client.

Step 3 Run the **kinit** *Component user name* command to perform authentication.

Step 4 Enter the new password of the component to check whether the authentication is successful.

- If yes, no further action is required. Ignore the error message.
- If no, go to **Step 5**.

Step 5 Contact the technical support.

----End

Reference Information

None.

2.4.15.4 Failed to Update a Ticket

Symptom

The ticket fails to be updated after the **kinit -R** command is run in the cluster or on the KrbServer client. An error message stating "kinit:KDC can't fulfill requested option while renewing credentials" is reported.

Possible Causes

The KrbServer service does not support the **-R** parameter.

Fault Locating

Check whether the value of configuration item **kdc_renew_lifetime** of the KrbServer service is 0 and whether the value of **kdc_renewable** is **false**.

Procedure

Step 1 Log in to FusionInsight Manager.

Step 2 Choose **Cluster** > *Name of the desired cluster* > **Services** > **KrbServer** > **Configurations**. Search **kdc_renew_lifetime** in the **Search** and set it to a value that is not **0**. Then **search kdc_renewable** and set it to **true**. Click **Save**.

Step 3 Click **More** > **Restart Service** and click **OK** to restart service.

Step 4 Download the client again and run the **kinit -R** command after running the **kinit** *username* command to update the authenticated and valid ticket.

----End

2.4.16 LdapServer

2.4.16.1 System Reports an Alarm Indicating That the LdapServer Service Is Unavailable

Symptom

The system reports an alarm indicating that the LdapServer service is unavailable when the node where LdapServer locates is faulty or the LdapServer instance is not working properly.

Possible Causes

The LdapServer process is abnormal due to faults of the node where LdapServer locates or other reasons.

Fault Locating

1. If the LdapServer instance is not working properly, deploy this instance on another node. Delete the faulty LdapServer instance, and then add a new LdapServer service to the cluster.
2. If the node where LdapServer locates is faulty, rectify the node fault according to related alarm recovery guidance.
3. It takes about 10 minutes to rectify the fault.

Procedure

Step 1 Log in to the FusionInsight Manager system.

Step 2 Choose **Cluster >** *Name of the desired cluster* **> Services** > **LdapServer** > **Instance**, and check the IP addresses of the nodes where the two SlapdServer instances locate.

Step 3 On the FusionInsight Manager portal, choose **O&M > Alarm > Alarms** > **Advanced Search**, search for "12006", and check whether alarms of the nodes where the SlapdServer instances locate exist.

- If yes, handle the alarms by using the methods provided in section "ALM-12006 NodeAgent Process Is Abnormal" in the alarm documentation. After the alarms are handled, go to **Step 4**.
- If no, go to **Step 5**.

Step 4 Check whether the alarm indicating that the LdapServer service is unavailable is cleared.

- If yes, no further action is required.
- If no, go to **Step 5**.

Step 5 Contact the technical support.

----End

Reference Information

None.

2.4.16.2 FusionInsight Manager Is Unavailable Due to LdapServer Data Exception

Symptom

The LdapServer component fails to start due to data exception, which results in unavailable FusionInsight Manager functions.

Verification method:

Run the following command on any node in the cluster:

ldapsearch -H ldaps://*OMS_Float_IP_address*:*OLdap_port* **-LLL -x -D cn=root,dc=hadoop,dc=com -W -b ou=Peoples,dc=hadoop,dc=com**

Enter the password of LDAP administrator and the following error occurs:

```
Other (e.g., implementation specifice) error (80)
Additional information: internal error
```

Possible Causes

The functions of FusionInsight Manager become unavailable due to an OKerberos exception caused by abnormal OLDAP data.

Fault Locating

1. Restore the Manager backup data.
2. It takes about 10 minutes to rectify the fault.

Procedure

Step 1 Check whether you have logged in to the current page.

- If yes, go to **Step 2**.
- If no, go to **Step 3**.

Step 2 Use the backup of Manager data to recover the Manager data. For details, see "Recovering Manager Data" in *MapReduce Service (MRS) 3.3.1-LTS User Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Usage Guide (for Huawei Cloud Stack 8.3.1).*

Step 3 Contact the O&M personnel.

----End

Reference Information

None.

2.4.16.3 Health Status of the LdapServer Service Is Unknown

Symptom

In the service list on FusionInsight Manager, the running status of the LdapServer service is **Unknown**.

Possible Causes

Service status information cannot be uploaded because network resources are exhausted.

Fault Locating

Check whether exceptions such as **java.net.ConnectException: Connection refused** exist in the heartbeat log files of the agent on the node where LdapServer is deployed.

The log file path is **/var/log/Bigdata/nodeagent/agentlog/heartbeat_trace.log**.

Procedure

Step 1 Log in to any node where LdapServer is deployed as user **root**.

Step 2 Check whether exceptions such as **java.net.ConnectException: Connection refused** exist in the heartbeat log files of the agent on the node where LdapServer is deployed.

- If yes, go to **Step 3**.
- If no, go to **Step 4**.

Step 3 Run the **ldapsearch -H ldaps://***ldap_IP:ldap_port* **-LLL -x -D cn=root,dc=hadoop,dc=com -W -b ou=Peoples,dc=hadoop,dc=com** command, enter the password of LDAP administrator to check whether LdapServer is normal. The query result is shown in the following figure.

```
dn: ou=Peoples,dc=hadoop,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Peoples

dn: cn=admin,ou=Peoples,dc=hadoop,dc=com
uid: admin
uidNumber: 20000
cn: admin
homeDirectory: /home/admin
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
description: [userName:"admin"]
```

- If yes, no further action is required.
- If no, go to **Step 4**.

Step 4 Contact the technical support.

----End

Reference Information

None.

2.4.16.4 The OS User Conflicts with the FusionInsight User, Causing a Component Service Authentication Failure

Symptom

userA added on FusionInsight Manager is assigned the permission to use FusionInsight components. When the user submits a component service execution request, the execution fails. The system displays a message indicating that the permission is insufficient and the authentication fails.

Possible Causes

1. The FusionInsight username is the same as the operating system (OS) username.
2. The OS user ID is the same as the FusionInsight user ID.
3. The OS user group ID is the same as the FusionInsight user group ID.

Fault Locating

Check whether the username, user ID, and user group ID of the OS are the same as those of FusionInsight, respectively.

Procedure

Step 1 Log in to the node where the services fail as user **root**, and run the following command to check whether the user with the same name as *userA* exists in the OS:

cat /etc/passwd | grep -w *userA*

- If yes, go to **Step 2**.
- If no, go to **Step 3**.

Step 2 If services are not affected, you are advised to delete FusionInsight user *userA*..

NOTICE

To prevent the name of the FusionInsight user from being the same as that of the OS user, check whether a user with the same name exists in the OS before adding a FusionInsight user.

Step 3 Run the **id -u userA** command to obtain the UID of *userA*. Run the following command to check whether the user with the same ID as *userA* exists in the OS:

cat /etc/passwd | grep -w *userA UID*

- If yes, go to **Step 4**.
- If no, go to **Step 5**.

Step 4 Delete OS user *userA* if the services and OS are not affected.

NOTICE

To prevent the OS user ID from being the same as the FusionInsight user ID, specify the user ID when adding an OS user.

useradd -u<uid>: specifies the user ID. (The recommended ID range is 500 to 8000.)

Step 5 Run the **id -Gn** *userA* command to check the owner group of *userA*. Compare the user group and role of *userA* in FusionInsight to check whether there are user groups that do not belong to FusionInsight (except the **ficommon** group).

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

NOTE

The user group corresponding to the FusionInsight role consists of the role name, underlines (_), and role creation time.

- If yes, go to **Step 6**.
- If no, go to **Step 8**.

Step 6 Run the following command to check whether the user group that does not belong to the FusionInsight in **Step 5** is an OS user group:

cat /etc/group |grep -w *User group name*

- If yes, go to **Step 7**.
- If no, go to **Step 8**.

Step 7 Delete the OS user group if the services and OS are not affected.

NOTICE

To prevent the OS user group ID from being the same as the FusionInsight user group ID, specify the user group ID when adding an OS user group.

groupadd -g<gid>: specifies the user group ID. (The recommended ID range is 500 to 8000.)

Step 8 Contact the technical support.

----End

Reference Information

None

2.4.17 Loader

2.4.17.1 Failed to Obtain a Connection

Symptom

- When Secure File Transfer Protocol (SFTP) import or export tasks are performed, an error message is displayed, as shown in **Figure 2-11**.

Figure 2-11 SFTP data import or export failure

Status	Failed Reason
Submission failed	Failed to get sftp session. cause: 172.16.0.1 (caused by: java.net.ConnectException: Connection timed out)

- When File Transfer Protocol (FTP) import or export tasks are performed, an error message is displayed, as shown in **Figure 2-12**.

Figure 2-12 FTP data import or export failure

Status	Failed Reason
Submission failed	Failed to login the ftp server. cause: Failed to login ftp server. Server: 172.16.0.1 ; port: 21 . (caused by: Connection timed out)

- When RDB import or export tasks are performed, an error message is displayed, as shown in **Figure 2-13**.

Figure 2-13 RDB data import or export failure

Possible Causes

- Some parameters about the connection of the Loader job are incorrect.
- The password contains invalid special characters that are not supported by Loader.

Fault Locating

1. Check whether the parameters of connection are incorrect.
2. Check whether invalid characters are contained in the password.

Procedure

The test function of the connection is used to locate parameter configuration errors. The following uses importing RDB data to the HDFS as an example:

Step 1 On the **Loader Jobs** page, click **Job ID**, and select to go to the page displayed in **Figure 2-14**

Figure 2-14 sftp job editing page

Step 2 Click **Edit** on the page displayed in **Figure 2-14** to go to the page displayed in **Figure 2-15**.

Figure 2-15 Connection editing page

Step 3 After confirming that all the parameters are correctly configured, click **Test** at the lower part of the page to test the connectivity of this connection.

- If the test succeeds, Click **OK** to save the connection configuration information. After saving the configuration information of connection, go to the **To** page of the job, and click **Save** to save the configuration information of the job or click **Save and run** to execute the job again.
- If the test fails, contact the technical support.

NOTE

The password of the SFTP or FTP server cannot contain the plus symbol (+). In addition, the password of each server cannot contain semicolons (;).

----End

Reference Information

None.

2.4.17.2 Failed to Import Data by Using HBASE_BULKLOAD

Symptom

Failed to import data from other data resources to a HBase table by using HBASE_BULKLOAD, and no error message is displayed on the Loader Jobs page.

Possible Causes

The user who had logged in to the Loader does not have the permission to perform such operation on the HBase table.

Fault Locating

1. Check whether the user has the permission to perform such operation on the HBase table.
2. It takes about 20 minutes to rectify the fault.

Procedure

Step 1 Log in to the FusionInsight Manager portal, click **O&M > Alarm > Alarms** to check whether alarms indicating that the HBase, Mapreduce, and HDFS services are unavailable exist during the running of job.

- If yes, handle the alarms by following the steps provided in related sections.
- If not, go to **Step 2**.

Step 2 Log in to the HBase client as user **hbase**.

Log in to the node host using PuTTY, go to the client installation directory on the FusionInsight Manager portal, and run the following command:

source bigdata_env

kinit *component service user* (If the cluster uses the security mode.)

hbase shell

NOTE

The component service user can be created by the system administrator as required. Change the password of the component service user at the first login.

Step 3 Run **user_permission 'OM_ROLES'**. OM_ROLES indicates the name of the HBase table to which data is to be imported. The command output is as follows:

Figure 2-16 Operation permission of the HBase table

```
hbase(main):003:0> user_permission 'OM_ROLES'
User                                       Table,Family,Qualifier:Permission
 hbase                                     OM_ROLES,,: [Permission: actions=READ,WRITE,EXEC,CREATE,ADMIN]
1 row(s) in 0.3640 seconds
```

Step 4 Check the command output, as shown in **Figure 2-16**:

- If the HDFS user is not in the User list, go to **Step 5**.
- If the HDFS user exists but has no READ, WRITE, or EXEC permission, go to **Step 5**.
- If the HDFS user exists and has READ, WRITE, and EXEC permissions, go to **Step 7**.

Step 5 Run the **grant 'HDFS', 'RWX', 'OM_ROLES'** command in the HBase client.

In the command, HDFS is the username for logging in to Loader, RWX is the read, write, and execute permissions, and OM_ROLES is the name of the Hbase table to which data is to be imported.

Step 6 Run the Job again on the Loader Jobs page. Observe whether the job was run successful.

- If yes, no further action is required.
- If no, go to **Step 7**.

Step 7 Contact the technical support.

----End

Reference Information

None.

2.4.17.3 Failed to Import or Export Data by Using SFTP

Symptom

Failed to import or export data (Job Description contains the SFTP string) by using SFTP. No error message is displayed on the Loader Jobs page.

Possible Causes

The SFTP server configuration file is incorrect, which results in failure to obtain connections when a large number of Maps connect to the SFTP server.

Fault Locating

1. Check whether the configuration file of SFTP server is correct.
2. It takes about 5 minutes to rectify the fault.

Procedure

Step 1 Use PuTTY to log in to SFTP server node as **root** user.

Step 2 If the SFTP server is deployed in the RedHat OS, check two configuration files **/etc/pam.d/password-auth-ac** and **/etc/pam.d/system-auth-ac** in the RedHat system. If the SFTP server is deployed in SuSE OS, check the **/etc/pam.d/common-auth-pc** configuration file.

Check whether auth required pam_tally2.so is configured in these configuration files (policy for locking accounts after authentication failure). For example, the following configuration item indicates that an account will be locked for 300 seconds if the authentication fails for three consecutive times:

```
auth required pam_tally2.so onerr=fail deny=3 unlock_time=300 even_deny_root root_unlock_time=300
```

- If yes, go to **Step 3**.
- If no, go to **Step 6**.

Step 3 Check whether the policy for locking accounts after authentication failure includes serialize:

```
auth required pam_tally2.so onerr=fail deny=3 unlock_time=300 even_deny_root root_unlock_time=300
serialize
```

- If yes, go to **Step 5**.
- If no, go to **Step 4**.

Step 4 Add serialize and restart the sshd service.

service sshd restart

Step 5 Run the job again. Observe whether the operation was successful.

- If yes, no further action is required.
- If no, go to **Step 6**.

Step 6 Contact the technical support.

----End

Reference Information

None.

2.4.17.4 Phoenix Table is Empty After Data is Imported

Symptom

When data is imported to the Phoenix table, the Loader page displays that the import is successful but the Phoenix table does not contain data.

Possible Causes

- When the Loader job is configured, the input file content is empty.
- When the Loader job is configured, the input directory is empty.
- When the Loader job is configured, the conversion step configuration is incorrect.

Fault Locating

1. Check whether the input file content is empty.
2. Check whether the input directory is empty
3. Check whether the conversion configuration item is correct.
4. It takes about 5 minutes to rectify the fault.

Procedure

Step 1 During the process of configuring Loader job, if file name is entered, check whether the file content entered is empty; if path is entered, check whether the path is invalid.

- If yes, no further action is required.
- If no, go to **Step 2**.

Step 2 On the Loader Jobs page, select Job ID, click , and edit the job.

Step 3 Click **Transform** and click the conversion step (such as HBaseOutput) twice, as shown in **Figure 2-17**

Figure 2-17 Edit button of the conversion steps

Step 4 Check whether the **table name** and **column name** contain lowercase letters on the pop-up configuration page of the conversion step, as shown in **Figure 2-18**.

Figure 2-18 Conversion step configuration of HBaseOutput

- If yes, change all the lowercase letters into the uppercase and restart the job.
- If no, go to **Step 5**.

Step 5 The column name in **Figure 2-18** is consistent with that in the phoenix table. Check whether these characters are contained in the phoenix table.

- One or some values do not exist in phoenix table which result in the column name value configuration is incorrect. Enter the right one.
- If all the values of column name exist in the phoenix table, contact the technical support.

----End

Reference Information

None.

2.4.17.5 Failed to Query Data If the Data Is Imported Before the Hive Table Is Created

Symptom

The user uses the Loader tool to import data to HDFS, and then creates a Hive table. No data is found when the Hive table is queried.

Possible Causes

- The content of the file specified during Loader job configuration is empty.
- The directory specified during Loader job configuration is empty.
- The conversion step is not correctly configured during Loader job configuration.
- An internal table is created, but data is not stored in the HDFS path specified for Hive.
- The imported data is partitioned, the partition information does not exist in the metadata of Hive.

Fault Locating

1. Check whether the content of the specified file is empty.
2. Check whether the specified directory is empty.
3. Check the conversion configuration item.
4. Check whether the imported data is stored in the HDFS path specified for Hive.
5. Check whether partition columns are configuration for the configuration item of the job conversion step.

Procedure

Step 1 On the **From** tab page, check whether the file in **Input path** is empty if a file name is entered during job creation, or check whether the path is empty if a path is entered during job creation.

- If yes, create new content.
- If no, go to **Step 2**.

Step 2 Open **view history** of the current job to check whether all the data are filtered as dirty data.

- If yes, check the configuration of each conversion step of the current job, especially check whether values of **field name**, **type**, **decimal Formate**, and **length** of adjacent steps are consistent.
  - If yes, go to **Step 3**.
  - If no, correct the configuration information.

- If no, go to **Step 3**.

Step 3 On the **to** page, check whether **Output directory** is correctly set to the HDFS path designated for Hive.

- If yes, go to **Step 4**.
- If no, check whether the created Hive table is an internal table. If it is an internal table, create an external table.

Step 4 Check whether one or more partition columns are specified for the hive output conversion step.

position	field name	type	decimal Format	length	is partitionkey
1	q1	INTEGER			☑
2	q2	VARCHAR		20	☑
3	q3	CHAR		1	☑
4	q4	INTEGER			☐
5	q5	DATE			☑

- If yes, the current output data is partitioned. After the table is created, run **MSCK REPAIR TABLE table_name** on the Hive client to synchronize the partition information in the table directory to the metadata.
- If no, contact the technical support.

----End

Reference Information

None.

2.4.17.6 An Error Occurred When Creating an SFTP Connection

Symptom

An error as shown in the following figure occurred when running a Loader job for creating an SFTP connection.

Possible Causes

An exception occurred when the Loader service verifies the encryption algorithm supported by the SFTP connector.

Fault Locating

Modify the daemon process configuration file **/etc/ssh/sshd_config** of the SSH server. That is, set **Ciphers** to the encryption algorithms supported by SSH. (Use commas (,) to separate multiple encryption algorithms.)

The encryption algorithms supported by MRS include aes128-cbc, aes192-cbc, aes256-cbc, aes128-ctr, aes192-ctr, and aes256-ctr.

Procedure

Step 1 Use PuTTY to log in to the server that corresponds to **Sftp server IP** in the figure as user **root**.

Step 2 Edit the **/etc/ssh/sshd_config** file to set **Ciphers** to the preceding encryption algorithms listed.

vi /etc/ssh/sshd_config

```
...
Ciphers aes128-cbc,aes192-cbc,aes256-cbc,aes128-ctr,aes192-ctr,aes256-ctr,3des-cbc
```

Step 3 Save the configuration file and run the **service sshd restart** command to restart the SSH service.

----End

Reference Information

None.

2.4.17.7 Loader Client WCC Encryption Failed and FileNotFound Is Reported

Symptom

When the Loader client is used to obtain the plaintext ciphertext, the following error is reported.

```
[root@node-master1Amtu loader-tools-1.99.3]# sh encrypt_tool 123
Internal error org.wcc.framework.AppRuntimeException: org.wcc.framework.AppRuntimeException: FileNotFound
```

Possible Causes

In Euler 2.9 and Kylin Linux Advanced Server release V10 (Tercel), the **t** permission cannot be granted to the **/tmp** directory. Otherwise, users outside the **omm/ficommon** group will fail to encrypt or decrypt data through WCC.

Security hardening has been performed on the Euler system. Users outside the owner group are not allowed to use it, and files in the directories with the **t** permission cannot be opened in read and write mode.

Fault Locating

Check the permissions of the **/tmp** directory.

```
[root@          tmp]# ll -d /tmp
drwxrwxrwt 35 root root 1200 Dec 16 15:46 /tmp
[root@          tmp]# ll
total 2432
-rw-rw---- 1 omm    ficommon       0 Dec 12 18:26 2431D845C6781B1A5674FD45A0DE13D1BBD54615700E0177C00771C378159F57.plock
-rw-rw-rw- 1 omm    wheel          0 Dec 13 21:07 248D9E715A1437E225F805917779FEE93503A78ABC53A9A564F3DBCE230A67B5.plock
-rw-rw---- 1 omm    ficommon       0 Dec 12 18:26 D55E11D4CE9921E3AF1110943F8AF3CCE7431BC9FBEF5B2B5D8354DDF193823C
-rw-rw-rw- 1 omm    wheel          0 Dec 15 15:30 D9A91B013191E13CE0D1D33DDCECA0F50BAF480383949C73E2323946B943472E.plock
-rw------- 1 root   root       75205 Dec 16 14:58 debug.log
drwx------ 2 root   root          60 Dec 15 15:34 diskmgt
-rw------- 1 omm    wheel          0 Dec 16 15:46 dntrash_lockfile
drwx------ 2 omm    wheel         40 Dec 15 21:30 elasticsearch-116356950099966644
drwx------ 3 omm    wheel         60 Dec 15 21:10 embedded-jetty-jsp
-rw------- 1 omm    wheel        424 Dec 14 10:18 executor-reconfig.log
-rw------- 1 root   root       28820 Dec 15 15:34 fi-preinstall.log
drwxr-x--- 4 omm    wheel         80 Dec 16 12:51 flink-web-f13058ae-0fb1-448a-9c24-f6ac716cfc5e
drwx------ 4 omm    wheel         80 Dec 16 14:19 FusionInsight-Client
-rw-r----- 1 omm    wheel     198568 Dec 16 14:32 hadoop132828556088239791.tmp
drwx------ 3 omm    wheel         60 Dec 12 19:33 hadoop-omm
drwx------ 4 omm    wheel         80 Dec 16 14:45 hadoop-unjar3583691701179822109
drwx------ 5 omm    wheel        100 Dec 16 14:46 hadoop-unjar3733753828558240593
drwx------ 3 root   root          60 Dec 16 14:29 HBase
drwxr-x--- 2 omm    wheel        920 Dec 16 15:46 hsperfdata_omm
drwxr-x--- 2 ommdba wheel         60 Dec 16 15:46 hsperfdata_ommdba
drwx------ 2 root   root          60 Dec 16 15:45 hsperfdata_root
drwx------ 2 omm    wheel         40 Dec 15 20:06 jetty-8-99-8-7-25013-journal-_-any-9132888559714302336
drwx------ 2 omm    wheel         40 Dec 15 20:05 jetty-8-99-8-7-25021-router-_-any-3926309382281159720
drwx------ 3 omm    wheel         60 Dec 15 20:58 jetty-8-99-8-7-26006-hadoop-yarn-commom-3_1_1-hw-ei-302053_jar-_-any-2373450907
drwx------ 2 omm    wheel         40 Dec 15 20:41 jetty-localhost-25016-datanode-_-any-1281595840763214320
-rw------- 1 omm    wheel        146 Dec 12 19:03 KerberosClient
-rw------- 1 omm    wheel        424 Dec 14 10:18 knox-reconfig.log
-rw------- 1 root   root         875 Dec 16 15:41 krb5cc_0
-rw------- 1 omm    wheel      77859 Dec 15 20:12 liblz4-java-6105954007771057054.so
-rw------- 1 omm    wheel          0 Dec 15 20:12 liblz4-java-6105954007771057054.so.lck
-rw------- 1 root   root           0 Dec 14 10:17 mountdisk_success
drwxr-x--- 2 omm    wheel         40 Dec 16 15:45 omm
-rw------- 1 root   root          90 Dec 15 15:28 preset_temp.tar.gz.sha256.temp
-rw------- 1 omm    wheel         74 Dec 15 21:43 PRESTART_LOG
-rw------- 1 omm    wheel       9658 Dec 16 15:45 report.json
drwx------ 3 root   root          60 Dec 16 14:29 root
-rw-r----- 1 omm    wheel     133104 Dec 16 14:32 snappy918899074705917354.tmp
drwx------ 3 root   root          60 Dec 15 17:19 systemd-private-dfd7cca37c3e44508f3b78e05c24befa-ntpd.service-W2kNMS
drwx------ 3 root   root          60 Dec 12 18:18 systemd-private-dfd7cca37c3e44508f3b78e05c24befa-systemd-logind.service-IJEpas
-rw------- 1 omm    wheel          0 Dec 16 15:46 tmp_error
drwx------ 3 omm    wheel         60 Dec 15 21:44 tomcat.4114272991010493119.29861
drwx------ 3 omm    wheel         60 Dec 15 21:43 tomcat.4496489467618032617.29880
drwx------ 3 omm    wheel         60 Dec 12 19:33 tomcat.6667174223875379994.29861
drwx------ 3 omm    wheel         60 Dec 12 19:33 tomcat.7552101220935832663.29880
drwx------ 2 omm    wheel         40 Dec 12 19:33 tomcat-docbase.1422917257033642362.29880
drwx------ 2 omm    wheel         40 Dec 15 21:44 tomcat-docbase.2854779939139656220.29861
drwx------ 2 omm    wheel         40 Dec 15 21:43 tomcat-docbase.6947113845883371222.29880
drwx------ 2 omm    wheel         40 Dec 12 19:33 tomcat-docbase.7761033508875374815.29861
-rw-rw---- 1 omm    ficommon       0 Dec 12 18:25 _wcc_file_locker_
-rw-r----- 1 omm    wheel    1181776 Dec 16 14:32 zstd2846212490659482034.tmp
```

Procedure

Run the following command to delete the permission on the **/tmp** directory:

chmod o-t /tmp

2.4.17.8 Data Is Lost After the Job for Importing Data to HBase Is Successfully Executed

Symptom

Data fails to be committed when being imported to HBase. As a result, the data is lost.

Possible Causes

There is a high possibility that job committing will fail if it takes a long time. Once it fails, data is stuck in an intermediate state and cannot meet data consistency requirements.

Fault Locating

Yarn log analysis: The entire data import process involves three rename operations. The number of files in the first rename operation is greater than that in the second rename operation. Consequently, only the number of files in the second rename operation is available in the source directory **/hbase/staging/** during bulkload and is imported to the HBase table. As a result, data is lost. The process of moving files is as follows:

First time: The **hflie** generated by Reduce is moved from **/hbase/extdata/loader_tmp/HBase/364_1678533666029_8656372993603390770/_temporary/1/_temporary/attempt_1662650274123_33118_r_005647_0/0/** to **/hbase/extdata/loader_tmp/HBase/364_1678533666029_8656372993603390770/0/**.

Second time: Files in the **/hbase/extdata/loader_tmp/HBase/364_1678533666029_8656372993603390770/0/** directory are moved to the **/hbase/staging/** directory.

Third time: Files in **/hbase/staging/** are loaded to **/hbase/data/default/T85_ACT_ACT_TRX_EVT** in bulkload mode.

According to the code analysis, the second and third file movement operations are performed in ApplicationMaster. The Yarn web UI shows that ApplicationMaster has been started twice.

Procedure

Step 1 On FusionInsight Manager, choose **Cluster** > **Services** > **Loader** > **Configurations** > **All Configurations**, and set **mapreduce.am.max-attempts** to **1** to disable ApplicationMaster from retrying upon failures.

Step 2 Save and synchronize the configuration.

Step 3 Restart the job.

----End

2.4.17.9 Garbled Characters Are Displayed When Loader Reads Rarely-used Oracle Characters

Symptom

Oracle characters are encrypted using ALT32UFT8. When Loader is used to write Oracle data to Hive or HDFS, rarely-used characters are garbled.

Possible Causes

The data in Oracle JDBC driver is garbled and the compliant encoding format cannot be transferred into the Oracle JDBC driver. As a result, this problem persists on Loader.

Procedure

Step 1 To solve this problem, the code needs to be converted using the CONVERT function of Oracle.

Select **Table SQL statement** and enter the following SQL statement:

select convert(name,'AL32UTF8','UTF8') as name from zw_test where ${CONDITIONS}

Step 2 Restart the job after you complete the configuration. The problem of garbled characters is solved.

----End

2.4.17.10 sqoop-shell Is Unavailable Due to Encryption and Decryption Errors

Symptom

The Euler environment supports sticky bits. When a directory's sticky bit is set, only the directory's owner can modify the directory. If the permission on the **/tmp** directory is not modified, the Loader client fails to decrypt data using WCC. As a result, the password in the configuration file generated by sqoop-shell is incorrect and each retry fails.

Possible Causes

WCC generates lock files in the **/tmp** directory. If the sticky bit of the **/tmp** directory is set, an error indicating that the files do not exist is reported. As a result, encryption and decryption fail.

Procedure

Step 1 Run the following command to change the permission on the **/tmp** directory to **777**:

chmod 777 /tmp

Step 2 Delete the **sqoop-shell.properties** and **sqoop-shell-trustore.jks** files from the **sqoop-shell** directory.

Step 3 Change the **truststore** name generated in the **sqoop2-shell** script to be different from the existing name.

```
shellStart() {
    local shellDir="${BASEDIR}/sqoop-shell"
    local randompassword
    local encryptpassword
    local truststore="sqoop-shell-truststore.jks"
    local loadershellpro="sqoop-shell.properties"

    local capath="${ROOTPATH}/ca.crt"
    if [ -f  "${shellDir}/${loadershellpro}" ]; then
        encryptpassword=$(readFromEtc "password" "" "${shellDir}/${loadershellpro}")
    fi


    if [ ! -f "${shellDir}/${truststore}" ]; then
        randompassword=$(head /dev/urandom | tr -dc 0-9 | head -c 20)
        encryptpassword=$(${BASEDIR}/encrypt_tool ${randompassword})
        rm -f ${shellDir}/${loadershellpro}
        echo "password = ${encryptpassword}" >> ${shellDir}/${loadershellpro}

        if [ -f "$capath" ];then
      keytool -import -alias sqoop-shell -file ${capath}  -keystore ${shellDir}/${truststore} > /dev
$randompassword
$randompassword
yes
EOF
        fi
    fi
```

Step 4 Run the script again.

----End

2.4.18 Manager

2.4.18.1 Upgrade Faults

2.4.18.1.1 Failed to Upgrade an Manager Due to Abnormal HA-Monitored Resource

Symptom

An error indicating abnormal resource is displayed when you upgrade Manager.

Possible Causes

Resources monitored by the HA process are abnormal.

Fault Locating

1. Check **/var/log/Bigdata/upgrade/upgrade.log_*** to find the upgrade failure cause.
2. The fault rectification time depends on the actual condition.

Procedure

Step 1 Log in to the Manager installation node as user **omm**.

Step 2 Run the **${BIGDATA_HOME}/om-server/om/sbin/status-oms.sh** script to check the resource usage status of the active and standby nodes.

Step 3 Analyze resources in Exception one by one.

- Check **/var/log/Bigdata/controller/acs/acs.log** of the faulty node to view the acs resource information.
- Check **/var/log/Bigdata/controller/aos/aos.log** of the faulty node to view the aos resource information.
- Check **/var/log/Bigdata/controller/controller.log** of the faulty node to view the controller resource information.
- Check **/var/log/Bigdata/omm/oms/ha/scriptlog/floatip.log** of the faulty node to view the floatip resource information.
- Check **/var/log/Bigdata/omm/oms/fms/fms.log** of the faulty node to view the fms resource information.
- Check **/var/log/Bigdata/omm/oms/db/omm_gaussdba.log** of the faulty node to view the GaussDB resource information.
- Check **/var/log/Bigdata/httpd/error_log** of the faulty node to view the httpd resource information.
- Check **/var/log/Bigdata/omm/oms/iam/iam.log** of the faulty node to view the iam resource information.
- Check **/var/log/Bigdata/omm/oms/ha/scriptlog/ha_ntp.log** of the faulty node to view the ntp resource information.
- Check **/var/log/Bigdata/okerberos/checkservice-detail.log** of the faulty node to view the okerberos resource information.
- Check **/var/log/Bigdata/oldapserver/ldapserver_chk_service.log** of the faulty node to view the oldap resource information.
- Check **/var/log/Bigdata/omm/oms/pms/pms.log** of the faulty node to view the pms resource information.
- Check **/var/log/Bigdata/tomcat/catalina.log** and **/var/log/Bigdata/tomcat/catalina.out** of the faulty node to view the tomcat resource information.
- Check **/var/log/Bigdata/omm/oms/heartBeatCheck/scriptlog/heartbeatcheck_ha.log** of the faulty node to view the heartBeatCheck resource information.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 4 Rectify the faults based on the exception logs. Upgrade the Manager after the Manager resources are in proper states.

----End

Reference Information

None.

2.4.18.1.2 A Message Indicating Upgrade Package Check Error Displayed During Manager Upgrade

Symptom

The following error message is displayed during Manager upgrade.

```
Check upgrade package failed, No upgrade adaptation package.
```

Possible Causes

- The current version cannot be upgraded using the upgrade package.
- The current system version is the target version.

Fault Locating

Check the upgrade package and ensure that it is correct.

Procedure

1. Check related documentation of the upgrade package to verify whether the package can be used to upgrade the current version. If it cannot be used, choose the correct upgrade package.
2. Check whether the current system version is the target version. If an upgrade has been performed in the system, you do not need to upgrade the system again.

Reference Information

None.

2.4.18.1.3 Clearing Redundant Tenant Data

Symptom

After the OMS is successfully upgraded upon a previous upgrade and rollback failure, some redundant tenant management data remains in the system. The remaining data includes the Yarn queue and role that are not associated with any tenant.

Possible Causes

During the OMS upgrade, a default queue and role by default for tenant management. When the OMS is rolled back, the system clears the queue and role.

When the OMS upgrade and rollback fail, the default queue and role are not cleared. During the next upgrade, the system detects the default queue and role and creates a new queue and role.

Fault Locating

1. On FusionInsight Manager, click **System** > **Permission** >**Role**. On the displayed page, check whether there is the role created for tenant. Also there is no users or groups associated with the role. In **Tenant Resources Management**, there is no tenant have the same name with the role. These roles are redundant data needs to be cleared.
2. Click **Audit**. On the displayed page, check whether there are audit logs recording upgrade and rollback failures in the cluster.

Procedure

Step 1 Log in to the active OMS node as user **omm**.

Step 2 Go to the **${BIGDATA_HOME}/om-server/om/sbin** directory and run **delete-RoleInfo.sh** to delete the specified role name.

cd ${BIGDATA_HOME}/om-server/om/sbin

./delete-RoleInfo.sh *role_name*

The role is deleted successfully if the following information is displayed:

```
Delete role successfully.
```

----End

Reference Information

None.

2.4.18.2 Other Faults

2.4.18.2.1 Failed to Install a NameNode Instance

Symptom

A message indicating NameNode instance installation failure is displayed.

Possible Causes

The mapping between the host name and IP address is incorrect in **/etc/hosts**.

Fault Locating

1. Check **/var/log/Bigdata/controller/controller.log** to find the failure cause.
2. It takes about 1 minute to rectify the fault.

Procedure

Step 1 Log in to the active management node as user **root**.

Step 2 Check whether the error information indicating that the agent is installed exists in the active management node logs.

Path to the log files: **/var/log/Bigdata/controller/controller.log**

Command: **vi /var/log/Bigdata/controller/controller.log**

If agent is already installed, log files contain the following information:

```
...is found with existing node agent installation.
```

Run the script **${BIGDATA_ROOT_HOME}/Bigdata_setup/nodesetup/setup/uninstall.sh/uninstall.sh** to forced uninstall the agent.

Step 3 Log in to the node where the NameNode instance installation fails as the **root** user, run the **vi /etc/hosts** command to modify the mapping between the host name and the IP address, and save the modification.

Step 4 Try to expand the NameNode instance to see whether the problem is solved.

- If yes, no further action is required.
- If no, contact the technical support

----End

Reference Information

None.

2.4.18.2.2 JPA Error Displayed During Instance Adding or Removing

Symptom

A JPA error occurs when you add or remove an instance on the FusionInsight Manager portal.

```
Could open JPA EntityManager for transaction; nested exception is javax.persistence.persisitenceException:
org.hibernate.exception.JDBCConnectionException: Could not open connection
```

Possible Causes

The GaussDB database is abnormal.

Fault Locating

Try to execute active/standby switchover to see if it can clear the faults.

Procedure

Step 1 Log in to the active management node as user **root**.

Step 2 Run **$OMS_RUN_PATH/workspace0/ha/module/hacom/tools/ha_client_tool --ip=127.0.0.1 --port=20013 --switchover --name=forceswap** command for active/standby switchover.

NOTE

In IPv6 mode, run the following command to switch over the active and standby OMS nodes: **$OMS_RUN_PATH/workspace0/ha/module/hacom/tools/ha_client_tool --ip=::1 --port=20013 --switchover --name=forceswap**

Step 3 Wait for the switch to succeed, see if the fault is resolved.

- If yes, no further action is required.
- If no, go to **Step 4**.

Step 4 On the FusionInsight Manager, choose **O&M > Log > Download**. Select **Manager** from the **Service** to collect Manager logs and contact the technical support.

----End

Reference Information

None.

2.4.18.2.3 Failed to Start Components Due to Database Connection Failures

Symptom

Some components that depends on DBService, such as Hive and Loader, fail to be started when you add or restart them on FusionInsight Manager.

Possible Causes

DBService components are running abnormally, causing database connection failures.

Fault Locating

1. Check **/var/log/Bigdata/controller/controller.log** on the active management node.
2. It takes about 10 minutes to rectify the fault.

Procedure

Step 1 Log in to the active management node as user **root**.

Step 2 Run the following command to view the contents of **/var/log/Bigdata/controller/controller.log** and check the startup failure cause:

vi /var/log/Bigdata/controller/controller.log

Step 3 Log in to the FusionInsight Manager portal, and choose **Services** > **DBService** > **Instances** to view the abnormal DBServer instances.

Step 4 Log in to the node where the running status of DBService is abnormal as user **root**, and rectify the fault by performing the operations for troubleshooting in **DBService**.

----End

Reference Information

None.

2.4.18.2.4 Failed to Decommission a DataNode Instance

Symptom

Decommissioning a DataNode instance fails.

Possible Causes

- The number of installed DataNode instances is less than the number of block backups (This parameter can be configured by **dfs.replication**. Choose **Cluster** > *Name of the desired cluster* > **Services** > **HDFS** > **Configurations**, click **All Configurations**, search the **dfs.replication** parameter. The default value is 3, and the following uses 3 as an example).
- The mapping between the host name and the IP address is incorrect.

Fault Locating

1. Check the number of DataNode instances.
2. Check the mapping between the host name and the IP address.
3. It takes about 2 minutes to rectify the fault.

Procedure

Step 1 Log in to the FusionInsight Manager portal.

Step 2 Choose **Cluster** > *Name of the desired cluster* > **Services** > **HDFS** > **Instance** to check whether more than three DataNode instances are installed.

- If yes, go to **Step 3**.
- If no, the number of remaining DataNode instance nodes is smaller than the number of data block replicas, it is normal that a decommissioning failure occurs.

Step 3 Log in to the node where the DataNode instance to be decommissioned is located as user **root**.

Step 4 Run the following command to check whether the configuration of **/etc/hosts** is correct:

vi /etc/hosts

Step 5 Correct the mapping between the host name and the IP address.

```
10.10.10.11 mgtomsdat-sh-3-01-1
10.10.10.12 mgtomsdat-sh-3-01-2
10.10.10.13 mgtdat-sh-3-01-3
```

Step 6 On the **Services** page of the FusionInsight Manager portal, restart the HDFS service.

----End

Reference Information

None.

2.4.18.2.5 Failed to Log In to a Native Window

Symptom

You cannot log in to the native window of each component.

Possible Causes

- The password is incorrect.
- The initial password is not changed.

Fault Locating

1. Check whether the password is correct.
2. Check whether the initial password is changed.
3. It takes about 1 minute to rectify the fault.

Procedure

Step 1 Change the initial password. You cannot log in to the native window by using the default password.

1. Log in to any node of the cluster as user root, and then run the following command to switch to user **omm**:

   su - omm

2. Run the following commands to export the environment variables:

   EXECUTABLE_HOME="${CONTROLLER_HOME}/kerberos_user_specific_binay/kerberos"

   LD_LIBRARY_PATH=${EXECUTABLE_HOME}/lib:$LD_LIBRARY_PATH

   PATH=${EXECUTABLE_HOME}/bin:$PATH

3. Run **kinit** *component service user* to change the password.

   For example, run **kinit hdfs**.

   NOTE

   The component service user can be created by the system administrator as required. Change the password of the component service user at the first login.

Step 2 Check whether the new password is correct if the login failure occurs again after you change the initial password.

----End

Reference Information

None.

2.4.18.2.6 Database User Password Being Forgotten

Symptom

A user forgets the database user password, and needs to reset it.

Possible Causes

None.

Fault Locating

1. Forcibly change the database password using a command.
2. It takes about 2 minutes to rectify the fault.

Procedure

Step 1 Log in to the node of DBServer(Active) instance as user root.

NOTE

Go to **${BIGDATA_HOME}/FusionInsight_BASE_8.3.1/install/FusionInsight-dbservice-2.7.0/sbin/**, on any node where DBService is installed as user **omm** and run the **status-dbserver.sh** script. The node whose **HAActive** status is **active** is the active DBService node.

The version 8.3.1 is used as an example. Replace it with the actual version number.

Step 2 Run the **su - omm** command to switch to the **omm** user.

Step 3 Go to **${BIGDATA_HOME}/FusionInsight_BASE_8.3.1/install/FusionInsight-meta-2.7.0/common/scripts**, and run the **forceModifyPwd.sh** script to forcibly change the database user password. The user needs to know the administrator's username and password.

The parameters in the

./forceModifyPwd.sh *logDir ip port dbName dbUser* command are as follows:

- logDir: specifies the log output directory.
- ip: specifies the IP address for active DBServer.
- port: specifies the port for connecting to the database (20051).
- dbName: specifies the name of the database whose password needs to be reset.
- dbUser: specifies the user name of the database whose password needs to be reset.

The following describes how to run the command:

cd ${BIGDATA_HOME}/FusionInsight_BASE_8.3.1/install/FusionInsight-meta-2.7.0/common/scripts

./forceModifyPwd.sh /var/log/Bigdata/ 127.0.0.1 20051 hivemeta hive

Enter the username and password of the GaussDB database administrator in the DBService component(omm) as prompted.

```
Please input DB super userName :
Please input DB super user password:
Please input new user password for user hive:
STEP : Start to set log...
The Log: [/var/log/Bigdata//forceModifyPwd_2016-12-20.log]
STEP : Finished setting log succesfully.                    [done]
STEP : forceModifyPwd to Database System...
STEP : forceModifyPwd to Database System successfully.          [done]
```

----End

Reference Information

None.

2.4.18.2.7 Abnormality Caused by Component Database User Password Change

Symptom

- After a user changes the database user password, the component that is added after being removed cannot be started.
- The user account is locked when a user changes the database user password over the WebUI.

Possible Causes

- After the password changes, the user uses the initial database user password to connect the reinstalled component to the database for several consecutive times, and the database user account is locked.
- The user enters an incorrect password for several consecutive times, the database user account is locked.

Fault Locating

1. Change the password on the window of FusionInsight Manager (choose **Cluster** > *Name of the desired cluster* > **Services** > **Hive** > **More** > **Reset Database Password** for example), and enter the correct password. The database user account is locked.
2. It takes about 2 minutes to rectify the fault.

Procedure

Step 1 Log in to the node of DBServer(Active) instance as user **root**.

Step 2 Run the **su - omm** command to switch to the **omm** user.

Step 3 Go to **${BIGDATA_HOME}/FusionInsight_BASE_8.3.1/install/FusionInsight-meta-2.7.0/common/scripts**, and run **unlockUser.sh** to unlock the user account. The user needs to know the database administrator's username and password.

The parameters in the

./unlockUser.sh *logDir ip port dbName dbUser* command are follows:

- logDir: specifies the log output directory.
- ip: specifies the IP address for active DBServer.

- port: specifies the port for connecting to the database (20051).
- dbName: specifies the database whose user account needs to be unlocked.
- dbUser: specifies the user name of the database whose user account needs to be unlocked.

The following describes how to run the command:

cd ${BIGDATA_HOME}/FusionInsight_BASE_8.3.1/install/FusionInsight-meta-2.7.0/common/scripts

./unlockUser.sh/var/log/Bigdata/ 127.0.0.1 20051 hivemeta hive

Enter the username and password of the GaussDB database administrator in the DBService component(**omm**) as prompted.

```
Please input DB super userName :
Please input DB super user password:
STEP : Start to set log...
The Log: [/var/log/Bigdata//unLockDBUser_2016-12-20.log]
STEP : Finished setting log succesfully.                    [done]
STEP : unLockDBUser to Database System...
STEP : unlockUser to Database System successfully.          [done]
```

----End

Reference Information

None.

2.4.18.2.8 Monitoring Indicator Display Error

Symptom

When users view the real-time or historical curve of an indicator on the monitoring page, curve changes that rarely occur during the proper operation occur. For example, the indicator value becomes zero instantly and the monitoring curve jitters abnormally. Then the display recovers after a short period of time.

Possible Causes

- The active and standby instances of the service are switched.
- The cluster or service process is restarted.
- The service process is abnormal.

Fault Locating

1. Check whether alarms of the service to which this indicator belongs are generated during this period.
2. Check whether the process of the service to which this indicator belongs is restarted or active/standby switchover occurs.
3. Check whether the cluster is restarted.
4. Check whether the service process is abnormal.
5. It takes about 10 minutes to rectify the fault.

Procedure

Step 1 Log in to the FusionInsight Manager portal.

Step 2 On the **Alarms** page, check whether alarms related to the indicator are generated during the period when the monitoring indicator is abnormal.

- If yes, handle the alarms by following steps provided in the alarm help document.
- If no, go to **Step 3**.

Step 3 On the **Alarms** page, check whether events indicating the active/standby switchover of the service to which the indicator belongs are generated.

- If yes, no further action is required.

  NOTE

  During the service active and standby switchover process, the indicator value that the monitoring plug-in collects may be abnormal.

- If no, go to **Step 4**.

Step 4 On the **Audit** page, check whether audit logs recording the cluster, service, or instance restart exist.

- If yes, no further action is required.

  NOTE

  During the cluster, service, or instance restart process, the indicator value that the monitoring plug-in collects may be abnormal.

- If no, go to **Step 5**.

Step 5 Log in to the node where the indicator value cannot be properly collected.

Step 6 Check whether records indicating process restart exist in the service run logs.

- If yes, no further action is required.

  NOTE

  During the restart process, the indicator value that the monitoring plug-in collects may be abnormal.

- If no, go to **Step 7**.

Step 7 Check whether error logs exist in the service run logs.

- If yes, the process is abnormal. Collect the logs and contact maintenance personnel to analyze the fault.
- If no, go to **Step 8**.

Step 8 Contact the technical support.

----End

Reference Information

None.

2.4.18.2.9 Failed to Start the GaussDB Due to Inconsistent Logs and Data

Symptom

- After the server powers off abnormally or restarts, FusionInsight Manager cannot be logged in. (The login page can be displayed, but the login fails after entering the user name and password).
- Log in to the active and standby management nodes of the cluster, run the **ps -ef | grep "gaussdb/bin/gaussdb -M"** command on the two nodes to check the related process. On both nodes, no similar process exists, or the process pid keeps changing.(This operation is to check whether the process exists, regardless of whether the process status is **primary** or **pending**.)

```
ommdba 82669 1  0 07:02 ?  00:00:00 ${BIGDATA_ROOT_HOME}/Bigdata_gaussdb/workspace0/gaussdb/bin/gaussdb -M primary
```

Possible Causes

- To ensure strict data consistency, the database records a log each time when a data record is submitted or modified, and the log and data must match exactly. In this way, the database service can work properly and ensure data restoration. The database records a log first, and then writes data. This mechanism theoretically allows the log to be written to the disk before the data, which ensures consistency during data restoration.
- When the logs and data are updated from the disk cache to disk, the order of logs and data may be reversed. That is, the data is written before the logs. If the abnormal power-off or restart occurs after the data is updated but before the log is updated, the data can be found but the matched log cannot be found during the data restoration after the server is restarted. In this case, the database fails to be started to ensure strict consistency.
- This fault occurs under the two conditions:
  - The disk cache function is enabled for the disk on which GaussDB data is stored. There is no RAID card with cache or the cache of the RAID card is invalid.
  - This fault occurs on the GaussDB processes of the active and standby management nodes. Therefore, the restoration cannot be performed by reconstruction. (If the GaussDB process of only one node is faulty, the GaussDB process of the other node can be used to restore the faulty one by certain reconstruction mechanism.)

Fault Locating

Step 1 Log in to the active and standby management nodes of the cluster as user **root**, run the **ps -ef | grep "gaussdb/bin/gaussdb -M"** command on the two nodes to check the related process. On both nodes, no similar process exists, or the process pid keeps changing.

```
ommdba 82669 1  0 07:02 ?  00:00:00 ${BIGDATA_ROOT_HOME}/Bigdata_gaussdb/workspace0/gaussdb/bin/gaussdb -M primary
```

NOTE

Check whether the GaussDB process does not exist or is unstable. To avoid incorrect judgment, do not perform this operation when the server is restarting or is not completely started. Perform this operation when the server starts and runs stably for a period.

If the GaussDB process does not exist or is unstable, the GaussDB process is abnormal.(This operation is to check whether the process exists, regardless of whether the process status is **primary** or **pending**.)

Step 2 Run the **cd /var/log/Bigdata/omm/oms/db** command to go to the GaussDB error log directory on the active and standby management nodes, respectively. Find the error log file **gaussdb-*.log** (* indicates the day when the fault occurs. For example, if the fault occurs on December 03, the file name is **gaussdb-03.log**), locate the time when the fault occurs, and check whether the subsequent logs repeatedly record error information similar to the following:

```
[2021-10-31 01:50:59.468 GMT]  startup 104922  LOG:  could not open file "pg_xlog/
000000010000000F000000ED" (log file 15, segment 237): No such file or directory
```

This fault results in startup failure of the GaussDB service.

Step 3 If the error information in **Step 2** exists on both nodes, see **Procedure** to rectify the fault; otherwise, you need to locate the fault cause and do not use this Fault Locating.

----End

Procedure

Step 1 Log in to the active management node as user **root**, run the **su - ommdba** command to switch to user **ommdba**, run the **vi $GAUSSDATA/postgresql.conf** command to open the GaussDB configuration file, and set **enable_minrecovery_check** to **off** for the GaussDB to start properly.

Step 2 Check whether the GaussDB on the node starts properly. If the GaussDB start properly, restore the data on the node. After the data restoration is complete, set **enable_minrecovery_check** to **on**.

Step 3 Repeat the **Step 1** to **Step 2** operations on the standby management node to restore the data on the standby management node.

Step 4 Run the **gs_ctl restart** command to restart the GaussDB on the active and standby management nodes. Check that the gaussDB is running properly on both nodes, and the processing is complete.

----End

Reference Information

None.

2.4.18.2.10 Database Connection Error

Symptom

- A database connection error is reported during alarm threshold modification.
- No progress information is displayed during health check.
- The alarm information indicates that a database connection error occurs.

Possible Causes

The database resources lock ordering is performed during data table update to ensure data validity. During the system startup, a database update operation (such

as setting alarm thresholds and performing health checks) is performed before the previous system data update operation is complete. In this case, the database lock ordering is confusing and database resources cannot be accessed.

Fault Locating

1. Database-related operations, such as querying alarms and setting alarm thresholds, cannot be performed successfully on FusionInsight Manager.
2. No progress information is displayed during health check.
3. FusionInsight Manager login may fail after many database-related operations are performed.

Procedure

Step 1 Log in to the active management node as user **omm**.

Step 2 Run the script **${BIGDATA_HOME}/om-server/om/sbin/restart-controller.sh** to restart the controller process.

Step 3 It is recommended that subsequent database-related operations (such as setting alarm thresholds and performing health checks) be performed 3 minutes after the cluster is installed or the controller process is restarted.

----End

Reference Information

None.

2.4.18.2.11 Slow Manager Page Loading

Symptom

During the login to FusionInsight Manager, the page loading is slow and has long delay.

Possible Causes

A network intermittent disconnection fault occurs on the external management network.

Fault Locating

1. Check whether the management node HA resource is normal.
2. Check the external management network status.

Procedure

Step 1 Log in to the active management node as user omm and go to the **$ {BIGDATA_HOME}/om-server/om/sbin/** directory.

cd ${BIGDATA_HOME}/om-server/om/sbin/

Step 2 Run the **./status-oms.sh** command to view the resource status and check whether the resource status in **ResStatus** switches between **non-steady** and **Normal** for a long time.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 Run the **ping** command to check the network status of the external management network, and check whether any timeout occurs.

ping *WebService floating IP address of the FusionInsight Manager system*

```
Request timed out
Request timed out
```

- If yes, go to **Step 4**.
- If no, go to **Step 5**.

Step 4 Contact the network administrator to resolve the external management network problem.

Step 5 Contact the technical support.

----End

Reference Information

None.

2.4.18.2.12 Incorrect Display on the Manager Portal

Symptom

During the login to FusionInsight Manager, the portal is displayed abnormally. For example, the page is blank, the data is incomplete, or the element locations are incorrect.

Possible Causes

- The browser has been used to access FusionInsight Manager of other versions or the cache is not cleared after the upgrade.
- The floatip resource in Manager is abnormal.

Fault Locating

- Clear the browser cache and access again.
- Check whether the HA resources of the active and standby management nodes are normal.

Procedure

Step 1 Open the browser window and press **Ctrl+Shift+Delete**.

Step 2 In the displayed dialog box, clear the browser cache.

- Internet Explorer: Select **Temporary Internet File** and **Cookies**, and click **Delete**.

- Chrome: Select **Cookies and other site and plug-in data** and **Cached images and files**, and click **Clear browsing data**.

Step 3 Log in to FusionInsight Manager again to check whether the fault is rectified.

- If yes, no further action is required.
- If no, go to **Step 4**.

Step 4 Log in to the active OMS node as user **omm** and run the following command to query the active/standby HA resource status on the Manager portal:

sh ${BIGDATA_HOME}/om-server/om/sbin/status-oms.sh

Check whether the value of **ResHAStatus** of the **floatip** resource is in the **Exception** status and whether the node is the standby OMS node

- If yes, go to **Step 5**.
- If no, contact the technical support.

Step 5 Log in to the node recorded in **Step 4** as user **root** and run the **ifconfig** command to check whether the floating IP addresses (including the floating IP addresses of OM and WS) can be queried.

```
eth0:oms  Link encap:Ethernet  HWaddr 28:6E:D4:89:37:E6
          inet addr:192.168.1.35  Bcast:192.168.1.255  Mask:255.255.254.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Interrupt:45

eth0:web  Link encap:Ethernet  HWaddr 28:6E:D4:89:37:E6
          inet addr:192.168.1.34  Bcast:192.168.1.255  Mask:255.255.254.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Interrupt:45
```

- If yes, go to **Step 6**.
- If no, the floating IP addresses of the OM and WebService cannot be queried. Contact the technical support. The system displays a message indicating that the execution of the **ifconfig** command is abnormal, go to **Step 7**.

Step 6 Log in to the node recorded in **Step 4** as user **root**, run the ifconfig command to manually unbind the queried floating IP addresses from the NIC, wait for 1 minute, and go to **Step 3**.

Ifconfig *floating IP address device name* down

```
[root@szvphicpra14411 opt]#ifconfig eth0:web down
```

Step 7 Log in to the node recorded in **Step 4** as user **root** and run the **ip addr | grep *floating IP address*** to check whether the floating IP address can be queried.

ip addr | grep *floating IP address*

- If yes, go to **Step 8**.
- If no, contact the technical support.

Step 8 Log in to the node recorded in **Step 4** as user **root** and run the following command to unbind the floating IP address:

ip addr del *floating IP address* dev *NIC name*

For example: **ip addr del 192.168.1.35 dev eth0**

```
[root@szvphicpra14411 opt]#ip addr del 192.168.1.35 dev eth0
```

- If yes, the operation is successful. Wait for 1 minute and go to **Step 3**.
- If no, contact the technical support.

----End

Reference Information

None.

2.4.18.2.13 Failed to Add a User on the FusionInsight Manager Portal

Symptom

On the FusionInsight Manager portal, the users, such as **admin**, exist in the user list on the user management page accessed by choosing **System** > **Permission** > **User**, but an error message is displayed after **Create User** is clicked.

Possible Causes

- The disk space of active management node is insufficient.
- The active LdapServer in the cluster is stopped.
- The node where the active LdapServer service locates is faulty.

Fault Locating

1. Check whether the **ALM-12017 Insufficient Disk Capacity** alarm exists.
2. Check whether the **ALM-12004 OLdap Resource Abnormal** alarm exists .
3. Fault recovery takes about 1 minutes.

Procedure

Step 1 Log in to FusionInsight Manager, and check whether the **ALM-12017 Insufficient Disk Capacity** alarm persists.

Step 2 Click **O&M > Alarm > Alarms** to check whether there is **ALM-12004 OLdap Resource Abnormal** alarm.

- If yes, go to **Step 3**.
- If no, go to **Step 4**.

Step 3 Handle the alarm according to the alarm handling procedure.

Step 4 Contact the technical support.

----End

Reference Information

None.

2.4.18.2.14 Failed to Uninstall Manager

Symptom

Manager fails to be uninstalled by running the script **${BIGDATA_ROOT_HOME}/Bigdata_setup/om/inst/uninstall.sh**.

The following provides an example:

```
[root@host1 inst]# ./uninstall.sh
.../om/inst/uninstall.sh: line 608: ...om/inst/oss/interface/interface.sh: No such file or directory
```

Possible Causes

Some files do not exist in **${BIGDATA_ROOT_HOME}**, due to which the script cannot be run properly.

Fault Locating

If Manager fails to be uninstalled, forcibly uninstall it by using commands.

Procedure

Step 1 Log in to the standby Manager node as user **root**.

Step 2 Run the **pkill -9 gaussdb** command to stop the gaussdb process.

Step 3 Run the **su - omm** command to switch to user **omm**. Run the following commands to stop all the processes of user **omm**:

NOTE

If the accounts do not exist, ignore this operation, go to **Step 4**.

pkill -9 java -u omm

ps -ef | grep omm

Run the following command to stop all the queried processes of user **omm**:

kill -9 *pid*

Step 4 Run the **su - root** command and enter the password to switch to user **root**.

Step 5 Run the following command to move or delete the MRS cluster log directory, installation directory, and data directory to other directories (the following directories are only examples and the actual directories must be consistent with those in the cluster):

mv ${BIGDATA_DATA_HOME} */tmp/backup*

mv ${BIGDATA_ROOT_HOME} */tmp/backup1*

mv /var/log/Bigdata */tmp/backup2*

Step 6 Delete the **omm** and **ommdba** accounts in the system.

NOTE

If the accounts do not exist, ignore this operation.

userdel omm

userdel ommdba

rm -rf /home/omm

rm -rf /home/ommdba

Step 7 Run **ifconfig** command to delete the OMSServer floating IP address and OMWebService floating IP address.

NOTE

If the IP address do not exist, ignore this operation.

For example:

ifconfig eth0:oms down

ifconfig eth0:ws down

Step 8 Log in to the active Manager node, repeat **Step 2** to **Step 7** to uninstall the active Manager.

----End

Reference Information

None.

2.4.18.2.15 Hosts Page of Manager Cannot Monitor Host State Normally

Symptom

In the host list on the Hosts page of FusionInsight Manager, "Not available" is displayed in CPU, memory, and disk usage items.

Possible Causes

- The status of the monitoring process is abnormal.
- Script h**ost_metric_collect.sh** for collecting host monitoring indicators is hung.
- The permission or size of the shared memory is modified by mistake.
- The **omm_agent.bin** permission is modified by mistake.
- Cluster switchover occurs.
- The cluster or service process is restarted.

Fault Locating

1. Check whether the status of the monitoring process is normal.
2. Check whether script **host_metric_collect.sh** is successfully executed.
3. Check whether the permission and size of the shared memory are correct.
4. Check whether the **omm_agent.bin** permission is correct.
5. Check whether the status of the cluster or service is normal.
6. Fault recovery takes about 10 minute.

Procedure

Step 1 If "Not available" is displayed, wait for 5 minutes and check whether the problem can be resolved automatically. If the problem persists after 5 minutes, go to **Step 2**.

After the system is restarted, monitoring data cannot be obtained temporarily.

Step 2 Go to a monitoring page of a host that is not available, click **Customize**, modify the indicators in the displayed list box, and click **OK**. 5 minutes later, check whether the problem is resolved. If the problem persists after 5 minutes, go to **Step 3**.

During repeated cluster switchover or restart, performance data delivery may be abnormal. This operation is to redeliver the performance data.

Step 3 Log in to the active management node as user **omm**, and run the following command to restart pms:

restart_app pms

Restart NodeAgent:

sh ${BIGDATA_HOME}/om-agent/nodeagent/bin/stop-agent.sh

sh ${BIGDATA_HOME}/om-agent/nodeagent/bin/start-agent.sh

If the problem persists after 5 minutes, go to **Step 4**.

Step 4 Log in to the node on which "Not available" is displayed as user **omm**. Run the following command to check whether the script for collecting host monitoring indicators is hung:

sh ${BIGDATA_HOME}/om-agent/nodeagent/bin/pluginScript/host_metric_collect.sh

If running script **host_metric_collect.sh** is not complete within 10 seconds, the script is abnormal. Stop running the script and run the following command:

sh -x ${BIGDATA_HOME}/om-agent/nodeagent/bin/pluginScript/host_metric_collect.sh

Check the collection command that causes the script to hang and analyze the failure cause according to the collection command that fails to be executed.

If the script for collecting the monitoring indicators runs properly, go to **Step 5**.

Step 5 Log in to the node on which "Not available" is displayed as user **omm**. Run **ipcs -m | grep 0x54376801** to check whether the permission and size of the shared memory are correct. The correct shared memory information is as follows:

```
0x54376801 65536      omm        600        125760048  2
```

In the command output, if the permission of the shared memory is **root** or the nattch count is less than 2, the shared memory is abnormal. If the shared memory is abnormal, run **ipcrm -M 0x54376801** to delete the old shared memory, and restart NodeAgent and omm_agent.

Command for restarting NodeAgent:

sh ${BIGDATA_HOME}/om-agent/nodeagent/bin/stop-agent.sh

sh ${BIGDATA_HOME}/om-agent/nodeagent/bin/start-agent.sh

Command for restarting omm_agent:

${BIGDATA_HOME}/om-agent/OMA/tools/restart_oma_app

If the problem persists after 5 minutes, go to **Step 6**.

Step 6 Check whether the **omm_agent.bin** permission is correct. Run the following command:

ll ${BIGDATA_HOME}/om-agent/OMA/bin/omm_agent.bin

Check whether the **omm_agent.bin** permission is correct. The permission must be **omm:wheel**. If the permission is not **omm:wheel**, change it to omm:wheel and restart the omm_agent.

Command for restarting omm_agent:

${BIGDATA_HOME}/om-agent/OMA/tools/restart_oma_app

If the problem persists after 5 minutes, go to **Step 7**.

Step 7 Contact the technical support.

----End

Reference Information

None.

2.4.18.2.16 Failed to Change the Password

Symptom

Users fail to change passwords in the following scenarios:

- A user cannot change the password upon re-login after the password expires.
- A newly created user tries to change the password upon first login but fails.
- An error message indicating that the password fails to be changed is displayed in other password changing scenarios.

Possible Causes

The **kadmin** process occasionally connects to the standby Ldap due to a Kerberos open-source bug. As the result, the password of the FusionInsight system cannot be changed and a message indicating that the username or password is incorrect is displayed.

Fault Locating

1. Log in the active management node as user **omm**.
2. Check whether **/var/log/Bigdata/controller/acs/acs.log** contains the following error message:
```
Server error: Password not changed.
Kerberos database constraints violated while trying to change password.
```
3. Log in to the active management node as user **omm**, and run **ps -ef | grep kerberos|grep oms** to check whether the omskerberos process exists.
4. If the process exist, perform the following operations to rectify the fault. If the fault persists, contact the technical support.

Procedure

Step 1 Log in to the active management node as user **omm**.

Step 2 Check whether **/var/log/Bigdata/controller/acs/acs.log** contains the following error message:
```
Server error: Password not changed.
Kerberos database constraints violated while trying to change password.
```

Step 3 Run **ps -ef |grep kerberos|grep oms** to view the ID of the omskerberos process, and record the ID as **ID1** and **ID2**.

Step 4 Run **kill -9** *ID1 ID2*, wait 2 minutes, and change the password again. If the password cannot be changed, on the FusionInsight Manager, choose **O&M** > **Log** > **Download**, select **Controller** and **OmsKerberos**, Set time for log collection to 10 minutes ahead and 10 minutes behind the trouble generation time and click **Download**. Collect logs and contact the technical support.

----End

Reference Information

None.

2.4.18.2.17 Kerberos Secondary Authentication Is 20s Slower After the DNS Is Installed

Symptom

On the FusionInsight Manager portal, the ZooKeeper service running status automatically switches between **Faulty** and **Normal**, and the ZooKeeper instance running status also switches between **Restoring** and **Normal**.

Possible Causes

- The configuration of **/etc/hosts** on the node where the ZooKeeper locates is incorrect.
- The DNS is deployed on the node where ZooKeeper locates.

Fault Locating

1. Check whether the IP address and host name configuration is correct in **/etc/hosts** on the ZooKeeper nodes, that is, whether one IP address corresponds to multiple host names or one host name corresponds to multiple IP addresses.
2. Check whether the DNS is installed on the node where ZooKeeper locates.

Procedure

Step 1 Log in to the FusionInsight Manager portal.

Step 2 Choose **Cluster** > *Name of the desired cluster* > **Services** > **ZooKeeper** > **Instance** to check the faulty ZooKeeper instance.

Step 3 Log in to the node where the faulty ZooKeeper locates as user **root.**

Step 4 Check whether the configuration in **/etc/hosts** is correct.

- If yes, go to **Step 5**.
- If no, correct the configuration in **/etc/hosts** and restart the ZooKeeper service. The fault can be rectified.

Step 5 Run the following command to check whether the DNS server is installed on the node:

service named status

The following information indicates that the DNS server is installed and enabled.

```
Checking for nameserver BIND
version: 9.6-ESV-R7-P4
CPUs found: 8
worker threads: 8
number of zones: 17
debug level: 0
xfers running: 0
xfers deferred: 0
soa queries in progress: 0
query logging is ON
recursive clients: 4/0/1000
tcp clients: 0/100
server is up and running
```

Step 6 If the DNS server is installed and enabled on the node, run the following command to disable the DNS server:

service named stop

The following information indicates that the DNS server disabled.

```
Shutting down name server BIND waiting for named to shut down (28s)
```

Step 7 If the DNS service is required, add the following configuration to the **/etc/hosts** file on the node:

Any unreachable IP address hadoop.*System domain*

For example, add the following content:

```
10.10.10.10 hadoop.XXX.com
```

Step 8 Run the following command to check whether the DNS client is installed on the node:

cat /etc/resolv.conf

The following information indicates that the DNS client is installed and enabled.

```
namesever 10.10.8.8
namesever 10.10.4.4
```

Step 9 If the DNS client is installed and enabled on the node, run the following command to disable the DNS client:

vi /etc/resolv.conf

Comment all the content by "#" and save the file.

```
# namesever 10.10.8.8
# namesever 10.10.4.4
```

Step 10 If the DNS client service is installed and enabled on the node, to use the DNS client service, add the following configuration to the **/etc/hosts** file on the node and the node where the DNS service is deployed:

Any unreachable IP address hadoop.*System domain*

For example, add the following content:

```
10.10.10.10 hadoop.XXX.com
```

Step 11 Log in to FusionInsight Manager, choose **Cluster >** *Name of the desired cluster* **> Services** > **ZooKeeper** > **Instance**, select the faulty ZooKeeper instance, choose **More** > **Restart Instance** to restart the instance, and check whether ZooKeeper is restored.

- If yes, no further action is required.
- If no, contact the technical support.

----End

Reference Information

None.

2.4.18.2.18 Some Operations on Manager Fail After Standby OMS Power-off

Symptom

When a standby OMS is powered off, some operations (e.g. start or stop the services) on Manager fail in 1 minutes.

Possible Causes

After a standby OMS is powered off, the database mode is switched from the synchronous mode to the asynchronous mode. Therefore, accessing the database fails during the mode switchover.

- Synchronous mode: When the client sends a connection request to the active node and commits the transactions, such as, addition, deletion, modification, and query on the database, the active node sends the record logs to the standby node and after receiving the logs the standby node sends response messages to the active node. Then the active node returns success messages to the client.
- Asynchronous mode: When the client sends a connection request to the active node and commits the transactions, such as, addition, deletion, modification, and query on the database, the active node sends the record logs to the standby node and returns success messages to the client. Then the standby node updates its database based on the received logs, so as to synchronize database data with the active node.

Fault Locating

1. Check and verify that the standby OMS has been powered off.
2. Check that files **/var/log/Bigdata/omm/oms/pms/pms.log**, **/var/log/Bigdata/omm/oms/fms/fms.log**, and **/var/log/Bigdata/omm/oms/iam/iam.log** of the active OMS contain the following logs generated near the time when power-off happened:
```
[MiniConnectionPoolManager:connectionErrorOccurred 478] connectionErrorOccurred
```

Procedure

Step 1 The system can recover automatically after 1 minute and do not perform any operation before the recovery. If you perform some operations and the operations fail, determine the failure cause based on the troubleshooting method and retry after 1 minute.

Step 2 If the retry fails multiple, choose **O&M** > **Log > Download** on the FusionInsight Manager, select **OmmServer** from the **Services** to collect the OmmServer logs and contact the technical support.

----End

Reference Information

None.

2.4.18.2.19 Troubleshooting Dual Active Manager Nodes

Symptom

When logging in to the cluster management interface, users can view that the cluster service status is normal. However, a large number of alarms indicating node faults and unavailable services cannot be cleared.

Possible Causes

- Dual active nodes exist in an HA cluster.
- When the original active OMS switches to the standby node, HA does not stop the relevant component services on the original active OMS.

Fault Locating

Step 1 Log in to the management node as user **omm**.

Step 2 Run the **${BIGDATA_HOME}/om-server/om/sbin/status-oms.sh** script to view the active/standby status of the management node. Check whether dual active nodes exist in the HA cluster.

- If yes, rectify the fault by performing required operation in section "Dual active nodes exist in the HA cluster"
- If no, perform **Step 3**.

Step 3 Log in to the standby management node as user **root** (determine the standby management node based on the query result of **Step 2**). Run **ps -ef | grep** *process name* to determine whether the aos, controller, fms, httpd, iam, pms, and tomcat processes or services are running.

Alternatively, run **ifconfig** to check whether the OMS floating IP address exists.

- If yes, HA does not stop the relevant component services on the active node when the active node switches to the standby node. Rectify the fault by performing required operations in section "HA does not stop the relevant component services on the node."
- If no, the fault is not caused by dual active nodes. You can analyze other causes.

----End

Procedure

Dual active nodes exist in the HA cluster.

Step 1 Log in to the two management nodes as user **omm** and ping each other on both nodes to check whether they can be pinged.

- If yes, check the firewall. Check whether the iptables prohibits the heartbeat port (20012). If the port is prohibited, cancel the prohibition, wait for 5 minutes, and continue with the processing.
- If no, the network is faulty. Solve the network problem. After ensuring that the ping test is successful, wait for 5 minutes and continue with the processing.

Step 2 Run the **${BIGDATA_HOME}/om-server/om/sbin/status-oms.sh** script to view the active/standby status of the OMS node. Check whether the dual active problem in the HA cluster is resolved.

- If yes, go to **Step 3**.
- If no, contact the technical support.

Step 3 Log in to the active and standby management nodes respectively as user **root**. Run **ps -A -opid,lstart,cmd | grep controller** to view the start time of the controller process and compare the time (the time that maps to **-Dprocess.name=controller** in the query result). The later start time is the time when the standby node becomes the active one. Take note of the time.

Step 4 Log in to FusionInsight Manager as user **admin** to view the alarms generated after the time when dual active nodes exist on OMS. Check the node status and service status on the cluster management page and manually clear alarms reported by mistake.

----End

HA does not stop the relevant component services on the node.

Step 1 Log in to the standby management node as user **root** and run **reboot** to restart the node.

NOTE

If the node deploys a service instance, restarting the node causes the instances to be temporarily unavailable.

Step 2 Check the standby node again after restarting it to verify whether any AOS, controller, FMS, httpd, IAM, PMS, and Tomcat processes or service are running.

- If yes, contact the technical support.
- If no, go to **Step 3**.

Step 3 Log in to the active management node as user **root**. Run **ps -A -opid,lstart,cmd | grep controller** to view the start time of the controller progress (the time that maps to **-Dprocess.name=controller** in the query result). The start time is the time when the standby node becomes the active one. Take note of the time.

Step 4 Log in to FusionInsight Manager as user **admin** to view the alarms generated after the time when the OMS become the active node. Check the node status and service status on the Manager page and manually clear alarms reported by mistake.

----End

Reference Information

None.

2.4.18.2.20 Manager Database Is Abnormal Because Directories or Files Are Deleted Incorrectly

Symptom

- The GaussDB data or program directory of the standby management node is damaged.
- The GaussDB service of the active and standby management nodes is abnormal and cannot automatically recover.
- The GaussDB data or program directories on the active or standby management nodes are damaged and cannot be automatically restored.
- If there is no data or the program directory is damaged, the exception is caused only by the inconsistency between active and standby data. In this case, skip this operation.

Prerequisites

- You have been assigned the permission of user **root**.
- You have logged in to the active management node as user **omm** and copied the latest available OMS backup package from **${BIGDATA_DATA_HOME}/LocalBackup**.
- You have logged in to the active management node as user **ommdba** and manually backed up the **$GAUSSDATA** directory.

Possible Causes

- The GaussDB program directory is damaged.
- The GaussDB data directory is damaged.
- The GaussDB metadata is damaged and cannot be restored.

Fault Locating

1. Log in to the faulty node as user **ommdba**.
2. Run the **ls -l "${GAUSSHOME}"** command to check whether the **$GAUSSHOME** directory exists.
3. Run the **ls -l "${GAUSSDATA}"** command to check whether the **$GAUSSDATA** directory exists.
4. Fault recovery takes about 180 minutes.

Procedure

Step 1 Log in to the standby management node as user **omm**.

Step 2 Stop the OMS.

sh ${CONTROLLER_HOME}/sbin/stop-oms.sh

Step 3 After the OMS is stopped, run the following command as user **root** to check whether the GaussDB process is stopped.

ps -ef|grep ommdba

If the process is found, run the **kill -9** *pid* command to stop it.

Step 4 Switch to user **omm**, decompress the OMS installation package to **$BIGDATA_TMP** and create a GaussDB installation directory.

tar -xf "${CONTROLLER_HOME}/omm/OMS-V100R001C00.x86_64.tar" -C "${BIGDATA_TMP}"

mkdir -p "${BIGDATA_TMP}/OMS-V100R001C00.x86_64/package/software/GSDB/"

Step 5 Run the **cat /etc/*-release** command to check the OS version.

- For Red Hat, EulerOS, or versions earlier than CentOS 7.0, run the following command:

  tar -zxf "${BIGDATA_TMP}/OMS-V100R001C00.x86_64/package/software/redhat/"GaussDB-*.tar.gz -C "${BIGDATA_TMP}/OMS-V100R001C00.x86_64/package/software/GSDB/"

- For CentOS 7.0 or later, run the following commands:

  tar -zxf "${BIGDATA_TMP}/OMS-V100R001C00.x86_64/package/software/centos/"GaussDB-*.tar.gz -C "${BIGDATA_TMP}/OMS-V100R001C00.x86_64/package/software/GSDB/"

- For SUSE, run the following commands:

  tar -zxf "${BIGDATA_TMP}/OMS-V100R001C00.x86_64/package/software/suse/"GaussDB-*.tar.gz -C "${BIGDATA_TMP}/OMS-V100R001C00.x86_64/package/software/GSDB/"

Step 6 Switch to user **root**. Grant the group permission to the **${BIGDATA_HOME}/tmp/OMS-V100R001C00.x86_64** directory.

su - root

chmod 770 -R "${BIGDATA_HOME}/tmp/OMS-V100R001C00.x86_64/"

Step 7 Go to the restoration script directory.

cd "${BIGDATA_HOME}/tmp/OMS-V100R001C00.x86_64/package/tools"

NOTE

${BIGDATA_HOME} is the FusionInsight Manager installation directory.

Step 8 Check whether the **$GAUSSHOME** program directory is deleted.

- If yes, go to **Step 11**.
- If no, go to **Step 9**.

Step 9 Check whether files in the **$GAUSSHOME** directory are deleted by mistake.

- If yes, go to **Step 12**.
- If no, go to **Step 10**.

Step 10 Check whether the **$GAUSSDATA** data directory is deleted or some files under the directory are lost.

- If yes, go to **Step 13**.
- If no, go to **Step 23**.

Step 11 If the program directory does not exist, install it. Run the **sh repair_gaussdb.sh -i** command to install GaussDB.

The installation is successful if the following information is displayed:

```
Please use setLogFile to set log file first.
Setting the log file:[/var/log/Bigdata/omm/oms/install_oms.log]...[done]
Installing GaussDB start...
Succeed to Install GaussDB.
Init GaussDB start...                                    [done]
Succeed to init GaussDB start...
```

- If yes, go to **Step 15**.
- If no, go to **Step 14**.

Step 12 If the program directory exists but the following files are deleted by mistake, uninstall and then install the program. Run the **sh repair_gaussdb.sh -u && sh repair_gaussdb.sh -i** command to uninstall and install GaussDB.

The uninstallation and installation are successful if the following information is displayed:

```
Please use setLogFile to set log file first.
Setting the log file:[/var/log/Bigdata/omm/oms/install_oms.log]...[done]
Uninstalling GaussDB start...
Succeed to uninstall GaussDB.
Please use setLogFile to set log file first.
Setting the log file:[/var/log/Bigdata/omm/oms/install_oms.log]...[done]
Installing GaussDB start...
Succeed to Install GaussDB.
Init GaussDB start...                                    [done]
Succeed to init GaussDB start...
```

- If yes, go to **Step 15**.
- If no, go to **Step 14**.

Step 13 Run the **sh repair_gaussdb.sh -r** command to initialize GaussDB and restore the installation directory and configuration of GaussDB.

The initialization is successful if the following information is displayed:

```
Please use setLogFile to set log file first.
Setting the log file:[/var/log/Bigdata/omm/oms/install_oms.log]...[done]
Init GaussDB start...                                    [done]
Succeed to init GaussDB start...
```

If yes, go to **Step 15**.

If no, go to **Step 14**.

NOTE

After the reinstallation is complete, the **${GAUSSDATA}/postgresql.conf** and **${GAUSSDATA}/pg_hba.conf** files will be reset. As a result, the GaussDB on the current node may generate an alarm indicating that data is not synchronized between the GaussDB on the other node. Check whether the **${GAUSSDATA}/postgresql.conf** and **${GAUSSDATA}/pg_hba.conf** are the same on the two nodes.

Generally, the IP addresses (**localhost** and **remotehost**) of **replconninfo1** in the **${GAUSSDATA}/postgresql.conf** file are the same as those of the active and standby nodes, other configuration items are the same.

Step 14 Collect the **${BIGDATA_LOG_HOME}/omm/oms/install_oms.log** file and contact the technical support.

Step 15 Switch to user **omm**.

su - omm

Step 16 Start the OMS.

sh ${CONTROLLER_HOME}/sbin/start-oms.sh

Step 17 Check whether the active and standby nodes are abnormal because files are deleted by mistake.

- If yes, go to **Step 18**.
- If no, go to **Step 22**.

Step 18 Log in to the active node as user **omm** and repeat **Step 2** to **Step 16**.

Step 19 Query which node is the active node and run the **${CONTROLLER_HOME}/sbin/huaweibigdata_backup.sh -r** *OMS backup file* on the active node to restore OMS service data.

The restoration is successful if the following information is displayed:

```
Start OMS restore.
Warning: Permanently added '10.39.234.124' (RSA) to the list of known hosts.
Warning: Permanently added '10.39.234.58' (RSA) to the list of known hosts.
Warning: Permanently added '10.39.234.181' (RSA) to the list of known hosts.
Warning: Permanently added '10.39.234.58' (RSA) to the list of known hosts.
Start to restore database.
Restore OMS successfully, please manually restart OMS.
```

- If yes, go to **Step 21**.
- If no, go to **Step 20**.

Step 20 Collect the **${BIGDATA_LOG_HOME}/controller/scriptlog/backup.log** file and contact the technical support.

Step 21 Restart the active and standby OMS nodes.

sh ${CONTROLLER_HOME}/sbin/restart-oms.sh

Step 22 Check whether the OMS status is normal.

Run the **sh ${BIGDATA_HOME}/om-server/om/sbin/status-oms.sh** command to check whether **HAAllResOK** of the active and standby management nodes is **Normal**.

- If yes, go to **Step 23**.
- If no, contact the technical support.

Step 23 After a period of time or the space is insufficient, delete the temporary directory on the faulty node.

rm -rf ${BIGDATA_TMP}/OMS-V100R001C00.x86_64

----End

2.4.18.2.21 Standby Database Is Abnormal Due to Improper Configuration of Transaction Log Parameters in the Manager Database

Symptom

A user runs the **sh ${CONTROLLER_HOME}/sbin/status-oms.sh** command to query the OMS status. The GaussDB resource on the standby management node is in the **Exception** state for a long time and cannot automatically restore, as shown in **Figure 2-19**.

Figure 2-19 Abnormal status of the standby GaussDB process

```
ResName                         ResStatus          ResHAStatus        ResType
acs                             Stopped            Normal             Single_active
aos                             Stopped            Normal             Single_active
cep                             Stopped            Normal             Single_active
controller                      Stopped            Normal             Single_active
feed_watchdog                   Normal             Normal             Double_active
floatip                         Stopped            Normal             Single_active
fms                             Stopped            Normal             Single_active
gaussDB                         Repairing          Exception          Active_standby
heartBeatCheck                  Stopped            Normal             Single_active
httpd                           Stopped            Normal             Single_active
iam                             Stopped            Normal             Single_active
ntp                             Standby_normal     Normal             Active_standby
okerberos                       Normal             Normal             Double_active
oldap                           Standby_normal     Normal             Active_standby
pms                             Stopped            Normal             Single_active
tomcat                          Stopped            Normal             Single_active
acs                             Normal             Normal             Single_active
aos                             Normal             Normal             Single_active
cep                             Normal             Normal             Single_active
controller                      Normal             Normal             Single_active
feed_watchdog                   Normal             Normal             Double_active
floatip                         Normal             Normal             Single_active
fms                             Normal             Normal             Single_active
gaussDB                         Active_normal      Normal             Active_standby
heartBeatCheck                  Normal             Normal             Single_active
httpd                           Normal             Normal             Single_active
```

Possible Causes

The value of the **wal_keep_segments** parameter for the Manager database is small. When database read and write operations are frequent, transaction log files are updated quickly. When the standby node needs to copy the earlier transaction log file from the active node, the transaction log file has been deleted. As a result, the standby node cannot obtain the complete data flow, causing the database exception.

NOTE

wal_keep_segments: Set the minimum number of transaction log files to be retained in **$ {BIGDATA_DATA_HOME}/dbdata_om/db/pg_xlog**. The standby node obtains host logs for flow replication. The size of a transaction log file is 16 MB.

Fault Locating

Log in to the standby management node as user **ommdba** and check whether the **${BIGDATA_LOG_HOME}/omm/oms/db/gaussdb-xxx.log** file contains the following error information:

```
[2017-12-19 06:09:33 GMT]    FATAL:  failed to identify consistence at 2/AB8A6F50: FATAL:  could not open file "pg_xlog/000000000000000200000AB" (log file 2, segment 171): No such file or directory (libpqwalreceiver.c:493)
[2017-12-19 06:09:33 GMT]    LOG:  wal receiver shutting down (walreceiver.c:679)
```

Procedure

Step 1 Log in to the active management node as user **ommdba**.

Step 2 Run the **ls -l ${BIGDATA_DATA_HOME}/dbdata_om/db/pg_xlog** command. In the command output, select the earliest and latest time points of the transaction log file to obtain the storage duration (latest time point - earliest time point) of transaction logs, convert the time to minutes, and record the result as T.

```
# ls -l $BIGDATA_DATA_HOME/dbdata_om/db/pg_xlog
total 1966084
-rw-------. 1 ommdba wheel 16777216 Apr 10 10:47 000000010000000A0000003D
-rw-------. 1 ommdba wheel 16777216 Apr 10 10:47 000000010000000A0000003E
-rw-------. 1 ommdba wheel 16777216 Apr 10 10:47 000000010000000A0000003F
-rw-------. 1 ommdba wheel 16777216 Apr 10 10:48 000000010000000A00000040
```

```
-rw-------. 1 ommdba wheel 16777216 Apr 10 10:48 000000010000000A00000041
-rw-------. 1 ommdba wheel 16777216 Apr 10 10:48 000000010000000A00000042
-rw-------. 1 ommdba wheel 16777216 Apr 10 10:50 000000010000000A00000043
-rw-------. 1 ommdba wheel 16777216 Apr 10 10:50 000000010000000A00000044
-rw-------. 1 ommdba wheel 16777216 Apr 10 10:50 000000010000000A00000045
-rw-------. 1 ommdba wheel 16777216 Apr 10 10:51 000000010000000A00000046
-rw-------. 1 ommdba wheel 16777216 Apr 10 10:51 000000010000000A00000047
-rw-------. 1 ommdba wheel 16777216 Apr 10 10:51 000000010000000A00000048
-rw-------. 1 ommdba wheel 16777216 Apr 10 10:51 000000010000000A00000049
-rw-------. 1 ommdba wheel 16777216 Apr 10 10:51 000000010000000A0000004A
-rw-------. 1 ommdba wheel 16777216 Apr 10 10:51 000000010000000A0000004B
-rw-------. 1 ommdba wheel 16777216 Apr 10 10:51 000000010000000A0000004C
-rw-------. 1 ommdba wheel 16777216 Apr 10 10:53 000000010000000A0000004D
-rw-------. 1 ommdba wheel 16777216 Apr 10 10:53 000000010000000A0000004E
-rw-------. 1 ommdba wheel 16777216 Apr 10 10:53 000000010000000A0000004F
-rw-------. 1 ommdba wheel 16777216 Apr 10 10:55 000000010000000A00000050
-rw-------. 1 ommdba wheel 16777216 Apr 10 10:55 000000010000000A00000051
-rw-------. 1 ommdba wheel 16777216 Apr 10 10:55 000000010000000A00000052
-rw-------. 1 ommdba wheel 16777216 Apr 10 10:56 000000010000000A00000053
-rw-------. 1 ommdba wheel 16777216 Apr 10 10:56 000000010000000A00000054
-rw-------. 1 ommdba wheel 16777216 Apr 10 10:56 000000010000000A00000055
drwx------ 2 ommdba wheel     4096 Dec 19 18:03 archive_status
```

Step 3 Run the **ls -l ${BIGDATA_DATA_HOME}/dbdata_om/db/pg_xlog | wc -l** command to calculate the total number of reserved transaction log files. The result is C.

```
# ls -l ${BIGDATA_DATA_HOME}/dbdata_om/db/pg_xlog | wc -l
19
```

Step 4 Based on the calculation results of **Step 2** and **Step 3**, estimate the number of transaction log files generated by the current cluster every minute. The result is N.

Number of transaction log files generated every minute (N) = Total number of transaction log files (C)/Duration for storing transaction logs (T)

Step 5 Set the transaction log files of the current cluster to be retained for 12 hours. The parameter value is equal to the number of transaction log files generated every minute (N) x 720 (minutes). Run the following command to change the value of the **wal_keep_segments** parameter:

gs_guc reload -c wal_keep_segments=parameter value

NOTE

1. The **wal_keep_segments** parameter takes effect dynamically. You do not need to restart the database process.
2. The disk space occupied by transaction log files cannot be greater than the remaining disk space of the data directory. The size of a transaction log file is 16 MB. Therefore, the maximum value of **wal_keep_segments** cannot exceed the available disk space of the data directory divided by 16 MB. Run the **df -m ${BIGDATA_DATA_HOME}/dbdata_om/db** command to query the remaining disk space of the data directory.

   ```
   # df -m ${BIGDATA_DATA_HOME}/dbdata_om/db
   Filesystem     1M-blocks  Used Available Use% Mounted on
   /dev/xvda2         36285  7321     27121  22% /
   ```

3. Run the **grep wal_keep_segments ${BIGDATA_DATA_HOME}/dbdata_om/db/postgresql.conf** command to check whether the parameter value takes effect.

Step 6 Log in to the standby management node as user **omm** and run the **$ {CONTROLLER_HOME}/sbin/stop-oms.sh** command to stop the standby OMS:

```
# ${CONTROLLER_HOME}/sbin/stop-oms.sh
[2017-12-19 18:39:54] [INFO] Enter into stop-oms.sh with user omm
stop HA successfully.
[2017-12-19 18:40:08] [INFO] End stop-oms.sh with user omm
```

Step 7 Switch to user **ommdba** and run the following commands to restore the database for the standby management node. This step may take several hours.

gs_ctl build

```
# gs_ctl build
gs_ctl: connect to server, build started.
xlog start point: D/6EF36D0
gs_ctl: starting background WAL receiver
640156/640156 kB (100%), 1/1 tablespace
xlog end point: D/EDCC6F8
gs_ctl: waiting for background process to finish streaming...
gs_ctl: build completed.
server starting..... done
server started
```

NOTE

During the restoration, you can run the **gs_ctl querybuild** command as user **ommdba** to view the database restoration progress.

```
# gs_ctl querybuild
 Ha state:
        LOCAL_ROLE                  : Standby
        STATIC_CONNECTIONS          : 1
        DB_STATE                    : Building
        DETAIL_INFORMATION          : 10%
```

Step 8 Switch to user **omm** and run the **${CONTROLLER_HOME}/sbin/start-oms.sh** command to start the standby OMS.

```
# $CONTROLLER_HOME/sbin/start-oms.sh
[2017-12-19 18:44:31] [INFO] Enter into start-oms.sh with user omm
start HA successfully.
[2017-12-19 18:45:35] [INFO] End start-oms.sh with user omm
```

Step 9 Run the **${CONTROLLER_HOME}/sbin/status-oms.sh** command to check OMS status. Check whether GaussDB is restored.

- If yes, go to **Step 10**.
- If no, contact the technical support.

Step 10 Log in to the active management node as user **ommdba** and run the following command to restore the default value of the **wal_keep_segments** parameter:

gs_guc reload -c wal_keep_segments=500

NOTE

The database transaction log files occupy a large amount of disk space. After the fault is rectified, restore the default value of the **wal_keep_segments** parameter.

----End

2.4.18.2.22 Trust of User omm Fails Because the expect Process Stops Responding

Symptom

After a node is powered on and off, the trust relationship between the node and the **omm** user of other nodes in the cluster fails. After the **ps ux | grep ssh** command is executed, it is found that the **expect** process stops responding, as shown in the following figure.

```
omm@linuxSp2Host4:~> ps ux|grep ssh
omm       9934  0.0  0.0  12872  1800 ?        S    10:26   0:00 bash /opt/huawei/Bigdata/om-server/om/sbin/ssh-agent-monitor-startup.sh
omm      10477  0.0  0.0  12888  1784 ?        S    10:26   0:00 bash /opt/huawei/Bigdata/om-server/om/sbin/ssh-agent-monitor.sh
omm      10631  0.0  0.0  54024   808 ?        Ss   10:26   0:00 ssh-agent -a /home/omm/.ssh/agent.pid
omm      10782  0.0  0.0  59660  3424 ?        S    10:26   0:00 /usr/bin/expect -c ?    spawn ssh-add?    expect {?       "Enter passphraso for " {send "Yq0yBpfvso9Dr
hkj7I812vCZPa8RQ02\n";}?    }?    interact?    foreach {pid spawnid os_error_flag value} [wait] break?    if {$os_error_flag == 0} {?       exit $value?    }  else {?
      exit $value?    }?
omm      11101  0.0  0.0  58280  2528 pts/0    Ss+  10:26   0:00 ssh-add
omm      60108  0.0  0.0   5708   804 pts/3    S+   11:19   0:00 grep ssh
omm@linuxSp2Host4:~> ssh 192.168.131.66
```

Procedure

Step 1 Log in to the faulty node as user **omm**.

Step 2 Run the **ps ux | grep ssh** command to query the PID of the expect process that stops responding.

Step 3 Run the **kill -9 PID** command to stop the expect process.

Step 4 Wait 1 minute for the daemon process to automatically register the key again to restore the trust relationship.

----End

2.4.18.2.23 Installation Package Fails to Be Distributed After OpenSSH Upgrade

Symptom

After the OpenSSH of the operating system is upgraded, (for example, upgraded to 7.9), the installation package fails to be distributed during cluster installation or capacity expansion.

Possible Causes

After the OpenSSH is upgraded, the default format of the Rivest-Shamir-Adleman (RSA) file generated by the **ssh-keygen** command is changed. As a result, mutual trust between **omm** users of nodes fails.

Fault Locating

Check whether the private key file (/**home/omm/.ssh/id_rsa**) of user **omm** contains the ENCRYPTED field. If it does not, this problem is located. In this case, perform the following steps.

Procedure

Step 1 Log in to the faulty node as user **root**.

Step 2 Roll back the OpenSSH to the source version.

rpm -Uvh -oldpackage *path of the OpenSSH RPM package*

For example: **rpm -Uvh --oldpackage /opt/openssh-7.4p1-11.el7.x86_64.rpm**

Step 3 Create a test user, for example, user **test**.

useradd test -m -d /home/test

Step 4 Switch to user **test**.

su - test

Step 5 Generate a private key file for user **test**.

ssh-keygen -t rsa -f /home/test/.ssh/id_rsa -P 1234567890

Step 6 Check whether the generated private key file (/**home/test/.ssh/id_rsa**) contains the ENCRYPTED field. If it does not, roll back the OpenSSH to an earlier version (for example, 7.4). If it does, roll back the OpenSSH of other nodes and reinstall the cluster or expand the capacity.

Step 7 Delete user **test**.

userdel -rf test

----End

Related Information

None

2.4.18.2.24 Analyzing Failures of the Audit Dump Configuration

Scenario

When an audit dump is configured, the error "**Failed to connect to the SFTP service. Please check the network connection or parameter settings.**" is reported.

Possible Causes

- The entered username and password for logging to the peer SFTP node are incorrect.
- The encryption negotiation algorithm of OpenSSH of the operating system is missing.

Procedure

Step 1 Use the username and password to log in to the SFTP node and check whether you can log in to the node.

- If yes, go to **Step 2**.
- If no, ensure that the username and password are correct and perform the configuration again.

Step 2 Log in to the SFTP node as the **root** user, run the **vim /etc/ssh/sshd_config** command to edit the **sshd_config** configuration file, add the configuration item **KexAlgorithms diffie-hellman-group1-sha1,diffie-hellman-group14-sha1,diffie-hellman-group-exchange-sha1,diffie-hellman-group-exchange-sha256,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group1-sha1,curve25519-sha256@libssh.org**. Save the configuration and exit. Then run the **service sshd restart** command to restart the SSH service, and reconfigure the audit dump function.

----End

2.4.18.2.25 Failed to Synchronize Configuration After the IP Address Is Changed

Scenario

After the IP address of OMSServer is changed, configuration synchronization fails.

Prerequisites

The nodeagent configuration file is abnormally cleared. As a result, the node is faulty and the configuration synchronization fails.

Precautions

1. Change the IP address of OMSServer and perform configuration synchronization. Check whether the synchronization fails.
2. If the synchronization fails, log in to the faulty node as user **omm** and check whether the nodeagent configuration file is empty.

   cd ${NODE_AGENT_HOME}/etc/agent

   ll nodeagent.properties

   If the value of file size in the fifth column is **0**, the configuration file is cleared abnormally.

   ```
   ...
   -rw------- 1 omm wheel 0 Jul  8 10:33 nodeagent.properties
   ...
   ```

Procedure

Step 1 Log in to the faulty node as user **omm** and copy the configuration file of other normal node to this node.

cd ${NODE_AGENT_HOME}/etc/agent

scp *IP address of the node where the configuration file is normal*:**$ {NODE_AGENT_HOME}/etc/agent/nodeagent.properties ./**

Step 2 Change the value of **om.nodeagent.nodeid** in the configuration file to the local node ID.

The node ID is in the format of *IP address*@*host name*. You can run the **hostname** command to view the host name of the node.

For example, if the IP address of the faulty node is **192.168.60.2** and the configuration file is copied from the node whose IP address is **192.168.60.1**, the node ID before the change is:For example, if the IP address of the faulty node is 192.168.60.2, the configuration file is copied from the 192.168.60.1 node.

```
om.nodeagent.nodeid=192.168.60.1@node1
```

The node ID after the change is:

```
om.nodeagent.nodeid=192.168.60.2@node2
```

Step 3 On FusionInsight Manager, wait for about 5 minutes until the faulty node is automatically recovered, and synchronize the configuration again.

----End

Related Information

None

2.4.18.2.26 Failed to Add or Reinstall Hosts Because of the Changed HOSTKEY

Symptom

1. Failed to add a host, and the following information is prompted:
```
#Node DISCOVERY incomplete# Could not verify `ecdsa-sha2-nistp256` host key with fingerprint `31:90:be:5c:92:a4:62:90:7d:9a:d2:c2:4e:4f:d6:2a` for `xxx.xxx.xxx.xxx` on port 22 while Connecting via SSH to xxx.xxx.xxx.xxx using username root.
```
2. Failed to reinstall a host, and the following information is prompted:
```
Failed to reinstall the nodes. Error details: Failed to verify nodes connection. Maybe the password is incorrect or the network is abnormal.
```

Possible Cause

The HOSTKEY of the node to be added or reinstalled is changed. (Reinstalling the OS or regenerating the HOSTKEY may change the HOSTKEY.)

Procedure

Step 1 Log in to the active and standby OMS nodes as user **omm** and perform the following operations.

Step 2 Run the **vi /var/log/Bigdata/controller/controller_nodesetup.log** command and search for the keyword **HOST_KEY_NOT_VERIFIABLE**. The following error information is displayed:

```
2019-10-14 23:01:47,867 ERROR [pool-101-thread-1] SSH Command Exectuion failed, Error details: com.huawei.bigdata.om.controller.agent.nodesetup.SshActionChannelHandler.recordException(SshActionChannelHandler.java:465)  net.schmizz.sshj.transport.TransportException: [HOST_KEY_NOT_VERIFIABLE] Could not verify `ecdsa-sha2-nistp256` host key with fingerprint `31:90:be:5c:92:a4:62:90:7d:9a:d2:c2:4e:4f:d6:2a` for `xxx.xxx.xxx.xxx` on port 22  at net.schmizz.sshj.transport.KeyExchanger.verifyHost(KeyExchanger.java:211)  at net.schmizz.sshj.transport.KeyExchanger.handle(KeyExchanger.java:365)  at net.schmizz.sshj.transport.TransportImpl.handle(TransportImpl.java:503)  at net.schmizz.sshj.transport.Decoder.decode(Decoder.java:102)  at net.schmizz.sshj.transport.Decoder.received(Decoder.java:170)  at net.schmizz.sshj.transport.Reader.run(Reader.java:59)  2019-10-14 23:01:47,868 INFO  [pool-101-thread-1] SSH Connection to xxx.xxx.xxx.xxx Not initialized due to error so no need to disconnect. com.huawei.bigdata.om.controller.agent.nodesetup.SshActionChannelHandler.disconnectSSH(SshActionChannelHandler.java:418)
```

Step 3 Run the **vi ${BIGDATA_HOME}/om-server/om/etc/om/known_hosts** command to delete the lines that contain the host name or IP address of the node to be added or reinstalled.

Step 4 Log in to the active OMS node as user **omm**, run the **sh ${BIGDATA_HOME}/om-server/om/sbin/restart-controller.sh** command to restart the controller node, and add or reinstall the host.

You do not need to restart the controller on the standby OMS node.

----End

2.4.18.2.27 Authentication of the Peer Domain Users Is Slow After Mutual Trust Is Configured

Fault Scenario

After mutual trust is configured on the FusionInsight GUI, authentication of the peer cluster domain users on the local cluster client is slow or times out.

Handling Suggestion

Configure the domain information of the peer cluster in the **/etc/hosts** file of all nodes in the cluster. For example, if the peer cluster domain name is **CLUSTER1.COM**, configure **cluster1.com** *10.10.10.10* in the **/etc/hosts** file of all nodes in the cluster. **cluster1.com** is a lower-case peer domain name, and *10.10.10.10* can be any unreachable IP address.

2.4.18.2.28 Some Nodes in the MRS Service Cluster Are Faulty After the MRS Is Powered Off and then Powered On

Symptom

After the cluster is powered off and then powered on, the node status in the cluster is faulty. However, the FusionInsight Manager page can be properly accessed.

The error information is as follows:

```
ERROR [main] SecurityUtils: Authentication failed.
javax.security.sasl.SaslException: Failure to initialize security context [Caused by GSSException: No valid
credentials provided (Mechanism level: Failed to find any Kerberos credentails)]
at com.sun.security.sasl.gsskerb.GssKrb5Server.<init>(GssKrb5Server.java:125)
at com.sun.security.sasl.gsskerb.FactoryImpl.createSaslServer(FactoryImpl.java:85)
at javax.security.sasl.Sasl.createSaslServer(Sasl.java:524)
at org.apache.thrift.transport.TSaslServerTransport.handleSaslStartMessage(TSaslServerTransport.java:141)
at org.apache.thrift.transport.TSaslTransport.open(TSaslTransport.java:265)
at org.apache.thrift.transport.TSaslServerTransport.open(TSaslServerTransport.java:42)
at org.apache.thrift.transport.TSaslServerTransport$Factory.getTransport(TSaslServerTransport.java:217)
at com.huawei.bigdata.om.common.rpc.KrbServiceTransport.lambda$getTransport
$0(KrbServiceTransport.java:31)
at java.security.AccessController.doPrivileged(Native Method)
at javax.security.auth.Subject.doAs(Subject.java:360)
at com.huawei.bigdata.om.common.rpc.KrbServiceTransport.getTransport(KrbServiceTransport.java:30)
at org.apache.thrift.server.TThreadPoolServer$WorkerProcess.run(TThreadPoolServer.java:293)
at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1149)
at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:624)
at java.lang.Thread.run(Thread.java:748)
Caused by: GSSException: No valid credentials provided (Mechanism level: Failed to find any Kerberos
credentails)
at sun.security.jgss.krb5.Krb5AcceptCredential.getInstance(Krb5AcceptCredential.java:87)
at sun.security.jgss.krb5.Krb5MechFactory.getCredentialElement(Krb5MechFactory.java:129)
at sun.security.jgss.GSSManagerImpl.getCredentialElement(GSSManagerImpl.java:193)
at sun.security.jgss.GSSCredentialImpl.add(GSSCredentialImpl.java:427)
at sun.security.jgss.GSSCredentialImpl.<init>(GSSCredentialImpl.java:62)
at sun.security.jgss.GSSManagerImpl.createCredential(GSSManagerImpl.java:154)
at com.sun.security.sasl.gsskerb.GssKrb5Server.<init>(GssKrb5Server.java:108)
... 14 more
```

Possible Causes

The underlying services such as Ldap and Kerberos are being started, and the upper-layer service Controller has been started. As a result, Controller authentication fails.

Fault Locating

Open the **/var/log/Bigdata/controller/controller_root.log** file and check whether the preceding error information exists.

Procedure

Step 1 Use PuTTY to log in to the active management node as user **omm**.

Step 2 Run the **sh ${BIGDATA_HOME}/om-server/om/sbin/restart-controller.sh** command to restart the Controller.

Step 3 After the restart is successful, check whether the faulty node is restored.

----End

2.4.18.2.29 Login Occasionally Fails After MRS Manager Exits Due to Timeout

Symptom

Login occasionally fails after MRS Manager exits due to timeout.

Possible Causes

After the timeout, the JS and CSS files of the page fail to be loaded.

Procedure

Step 1 Clear the browser cache.

Step 2 Refresh the current page and log in again.

----End

2.4.18.2.30 Threshold Monitoring Alarms for New Services Are Not Reported

NOTE

This section applies only to monitoring alarms of the spacial aggregation calculation.

Symptom

After a service is added, the threshold monitoring alarm of the service is not reported, and alarms cannot be triggered even if the default threshold is changed.

Possible Causes

When a service is added, its monitoring metrics of spacial aggregation calculations may fail to be loaded to the PMS memory.

Procedure

The solution is as follows:

Step 1 On FusionInsight Manager, choose **O&M** > **Alarm** > **Thresholds** and check whether the threshold of the monitoring metric is greater than or less than the configured alarm threshold.

- If yes, change the alarm threshold and check whether alarm reporting is normal. If it is not, go to **Step 2**.
- If no, go to **Step 2**.

Step 2 Log in to the active OMS node as user **root** and run the following command to switch to user **omm**:

su - omm

Restart the OMS or PMS service.

- Restart the OMS service.

  sh ${BIGDATA_HOME}/om-server/om/sbin/restart-oms.sh

- Restart the PMS service.

  sh $BIGDATA_HOME/om-server/OMS/tools/restart_app pms

----End

2.4.18.2.31 An Error Reported During Client Authentication for a New User

Symptom

When a new user is authenticated on the client for the first time, the password needs to be changed. After the password is changed, the following error message is displayed:

```
kinit: Password has expired while getting initial credentials
```

Fault Locating

The error message is displayed, but the actual user password has been changed successfully. In this case, use the new password for authentication again.

Procedure

Run the user authentication command again and enter the new password.

kinit *user name*

2.4.18.2.32 Alarm Faults Are Rectified, but Alarms in the Manager Alarm List Are Not Automatically Cleared

Symptom

For alarms that can be automatically cleared, the alarm fault has been rectified, but the alarms on the **O&M** > **Alarm** > **Alarms** page on FusionInsight Manager are not automatically cleared.

Possible Causes

The OMA fails to process the cached message. As a result, the clear alarm fails to be reported.

Procedure

Step 1 Log in to the node for which the alarm is generated as user **omm**.

Step 2 Run the following command to check whether alarms that are not cleared exist in the cache.

cat ${NODE_AGENT_HOME}/etc/agent/alarmSupression.properties | grep "^*Alarm ID***"**

Step 3 If information can be found, delete the matching line information from the **$ {NODE_AGENT_HOME}/etc/agent/alarmSupression.properties** file.

Step 4 After a while, choose **O&M > Alarm > Alarms** on the FusionInsight Manager page. The alarm is automatically cleared.

----End

2.4.18.2.33 After a Node Is Powered Off and Then Powered On, the OMS Node Cannot Be Automatically Started or an Alarm "Trust Relationships Between Nodes Become Invalid" Is Reported

Symptom

After a host is powered off and then powered on, the OMS node does not automatically start, or an alarm "Trust Relationships Between Nodes Become Invalid" is generated.

Possible Causes

- The OMS node is manually stopped before the power-off.
- During the power-off and power-on operations, the scheduled tasks of user **omm** are lost.

Fault Locating

- If the OMS node has been stopped before power-off, you need to determine whether to start the OMS node after power-on. Manually stopping the OMS node will clear the scheduled tasks automatically configured by the OMS node.

- The OS may clear the scheduled tasks of user **omm**.

Procedure

Step 1 Log in to the faulty node as user **root** and check whether the **/var/spool/cron/omm** file is empty.

- If yes, the file is empty. View the **/var/log/cron** file and check the scheduled task information before the faulty node is powered off. Add scheduled tasks in the **/var/spool/cron/omm** file on other normal nodes. Then go to **Step 3**.

  NOTE

  The **/var/log/cron** file is the system scheduled task log file. After the system is powered off, you can view the scheduled task information before the system is powered off when the scheduled task is cleared by user **omm**. Add the missing scheduled tasks to the **/var/spool/cron/omm** directory.

- If no, go to **Step 2**.

Step 2 Check whether the **start_ha_monitor.sh** and **ssh-agent-monitor-startup.sh** scheduled tasks are missing in the **/var/spool/cron/omm** file.

- If yes, the **start_ha_monitor.sh** and **ssh-agent-monitor-startup.sh** scheduled tasks are missing. You can supplement the scheduled tasks in the **/var/spool/cron/omm** file by referring to other normal nodes.

  For example, the content to be supplemented is as follows:

```
*/1 * * * * bash ${BIGDATA_HOME}/om-server/om/sbin/ssh-agent-monitor-startup.sh > /dev/null 2>&1
* * * * * source /home/omm/.profile;sh ${BIGDATA_HOME}/om-server/OMS/workspace/ha/module/hamon/script/start_ha_monitor.sh > /dev/null 2>&1 &
```

- If no, contact technical support.

Step 3 After the modification, wait for the scheduled task to automatically start the OMS or mutual trust process.

----End

2.4.19 Mapreduce

2.4.19.1 JobHistoryServer Node Faults

Symptom

The MapReduce is successfully started, but the NodeManager and JobHistoryServer are in the **Restoring** state, indicating that the services are unavailable.

Possible Causes

- The Hadoop Distributed File System (HDFS) is not started, or the HDFS is in safe mode and cannot provide services.
- The YARN configuration items **yarn.nodemanager.local-dirs** and **yarn.nodemanager.log-dirs** do not have sufficient space.

Fault Locating

Check whether alarms indicating unavailable services occur in the YARN service, and check the alarm causes.

Procedure

Step 1 Log in to the FusionInsight Manager system.

Enter the address to be accessed in the address box. The address format is https://*WebService floating IP address of the FusionInsight Manager system*:28443/web.

Step 2 Choose **Cluster >** *Name of the desired cluster* **> Services** > **HDFS** > **More > Restart Service**, and restart HDFS.

Step 3 If the cause of unavailable services is **All nodemanagers are lost**, check the space of the disk where **yarn.nodemanager.local-dirs** and **yarn.nodemanager.log-dirs** locate.

----End

Reference Information

None.

2.4.19.2 HDFS Directory Fails to Be Deleted After the Related Job Is Deleted

Symptom

After a user runs the following command to delete a MapReduce job after the job execution, the HDFS directory created by job is not deleted.

yarn application -kill *<app ID>*

Possible Causes

After the job is executed, the user runs the preceding command to delete the job, but the HDFS directory is not deleted.

Fault Locating

None.

Procedure

The ***yarn application -kill*** *<app ID>* command is not recommended. You are advised to use the following command to delete the job:

./mapred job -kill *<Job-Id>*

If the ***yarn application -kill*** *<app ID>* command is used, you can perform the following operation to delete the HDFS directory:

Step 1 Log in to the node on which the client is installed as the client installation user.

Step 2 Run the following command to go to the client installation directory:

cd /opt/hadoopclient

Step 3 Run the following command to configure environment variables:

source bigdata_env

Step 4 If the cluster uses the security mode. Run the following command to perform user authentication. If the cluster uses the normal mode, user authentication is not required.

kinit *component service user*

Step 5 Run the command as follows to check the exist files under the **/tmp/hadoop-yarn/staging** path.

hadoop fs -ls -R /tmp/hadoop-yarn/staging

Step 6 Run the following command to delete the HDFS directory:

hadoop fs -rm -r -f *<path-to-job data>*

For example, ***hadoop fs -rm -r -f /tmp/hadoop-yarn/staging/hdfs/staging/job_1418213163174_0005***

----End

Reference Information

None.

2.4.19.3 java.io.IOException Error Occurs During Job Execution

Symptom

The following error occurs when a MapReduce job is executed:

```
java.io.IOException: java.io.IOException: Could not find Job details for JobId:job_1417092389329_0004 in JobHistoryServer.
	at org.apache.hadoop.mapreduce.v2.hs.HistoryClientService$HSClientProtocolHandler.verifyAndGetJob(HistoryClientService.java:216)
	at org.apache.hadoop.mapreduce.v2.hs.HistoryClientService$HSClientProtocolHandler.getTaskAttemptCompletionEvents(HistoryClientService.java:277)
	at org.apache.hadoop.mapreduce.v2.api.impl.pb.service.MRClientProtocolPBServiceImpl.getTaskAttemptCompletionEvents(MRClientProtocolPBServiceImpl.java:173)
	at org.apache.hadoop.yarn.proto.MRClientProtocol$MRClientProtocolService$2.callBlockingMethod(MRClientProtocol.java:283)
	at org.apache.hadoop.ipc.ProtobufRpcEngine$Server$ProtoBufRpcInvoker.call(ProtobufRpcEngine.java:585)
	at org.apache.hadoop.ipc.RPC$Server.call(RPC.java:928)
	at org.apache.hadoop.ipc.Server$Handler$1.run(Server.java:2013)
	at org.apache.hadoop.ipc.Server$Handler$1.run(Server.java:2009)
	at java.security.AccessController.doPrivileged(Native Method)
	at javax.security.auth.Subject.doAs(Subject.java:415)
	at org.apache.hadoop.security.UserGroupInformation.doAs(UserGroupInformation.java:1612)
	at org.apache.hadoop.ipc.Server$Handler.run(Server.java:2007)
```

Possible Causes

During the MapReduce job execution, if the HDFS recovers after a fault is rectified, this error occurs.

Fault Locating

Check whether the job execution is complete. If the job execution is complete, the error is caused by the HDFS fault rectification. No further action is required.

If the job execution is not complete, check the MapReduce job application.

Procedure

None.

Reference Information

None.

2.4.19.4 MapReduce Tasks with Large Data Amount Run Slowly

Symptom

Reduce tasks run slowly when MapReduce tasks with large data amount are running. The native WebUI logs continuously records the following information:

```
2015-05-20 23:32:17,527 INFO [fetcher#29] org.apache.hadoop.mapreduce.task.reduce.Fetcher: fetcher#29
- MergeManager returned status WAIT ...
2015-05-20 23:32:17,545 INFO [fetcher#13] org.apache.hadoop.mapreduce.task.reduce.Fetcher: fetcher#13
- MergeManager returned status WAIT ...
2015-05-20 23:32:17,549 INFO [fetcher#29] org.apache.hadoop.mapreduce.task.reduce.Fetcher: fetcher#29
- MergeManager returned status WAIT ...
```

Some data is read every 5 to 6 hours and the following information is recorded:

```
2015-05-21 05:34:16,257 INFO [fetcher#14]
org.apache.hadoop.mapreduce.task.reduce.InMemoryMapOutput: Read 1720474 bytes from map-output for
attempt_1431609106966_0153_m_002488_0
```

The preceding two types of logs are recorded in an alternate manner.

Possible Causes

During the reduce data processing, data needs to be copied to the local computer for reduce operations. In reducer, the data copy tasks and data merge tasks are performed concurrently. If the memory usage of the data copy tasks does not reach the threshold, write operations may not be triggered and the remaining memory are used by the data merge tasks.

NOTE

Set the parameter **mapreduce.reduce.shuffle.input.buffer.percent** to the buffer size of the data. The default buffer allocated is 70% of the memory.

Set the parameter **mapreduce.reduce.shuffle.merge.percent** to ensure that data is written to the disk after the memory usage of the data copy tasks reaches the threshold. The default value is 66%.

Fault Locating

1. Check whether the value of **mapreduce.reduce.shuffle.parallelcopies** meets the configuration requirement. For details, see **Table 2-6**.

2. Check whether the value of **mapreduce.reduce.memory.mb** of the tasks of reduce meets the configuration requirement. For details, see **Table 2-6**.

Procedure

1. Set **mapreduce.reduce.shuffle.parallelcopies** to a value in the recommended range.
2. Set **mapreduce.reduce.memory.mb** to a value in the recommended range.

Reference Information

Table 2-6 MapReduce task parameter configuration

Parameters	Description	Formula
mapreduce.reduce.memory.mb	Indicates the memory size configured for reduce tasks.	A/B*1.4+(C*50MB) In the formula: A indicates the total input data volume of reduce. B indicates the value of **mapred.reduce.tasks**, C indicates the value of **mapreduce.reduce.shuffle.parallelcopies**.
mapreduce.reduce.shuffle.parallelcopies	Indicates the number of threads started by the reduce fetch data.	The recommended value range is [5,15].

2.4.19.5 Map or Reduce Process Being Terminated Due to Memory Overflow

Symptom

During the running of MapReduce tasks on the YARN, some Map or Reduce tasks are killed. When "Task Failed" occurs, the following logs are displayed on the native WebUI of JobHistoryServer:

```
Container [pid=143419,containerID=container_1432208368012_0016_01_000066] is running beyond virtual memory limits.
Current usage: 769.8 MB of 1 GB physical memory used; 3.8 GB of 2.5 GB virtual memory used. Killing container.
```

Possible Causes

According to logs, the container is killed because the virtual memory usage exceeds the threshold. The NodeManager of YARN detects that the memory usage exceeds the threshold and forcibly stop the container process.

Fault Locating

1. Check whether the task fails due to physical memory overflow or virtual memory overflow.
2. Check the memory configuration of the failed Map or Reduce task. The configuration items to be check include **mapreduce.map.memory.mb**, **mapreduce.reduce.memory.mb** and **yarn.nodemanager.vmem-pmem-ratio**.

Procedure

Step 1 If the fault cause is physical memory overflow, adjust the values of **mapreduce.map.memory.mb** and **mapreduce.reduce.memory.mb** to proper values based on the physical memory values in the error logs. For details about the parameter configuration, see **Table 2-7**.

Step 2 If the fault cause is virtual memory overflow, adjust the configuration using the following formula: **yarn.nodemanager.vmem-pmem-ratio > actual used virtual memory/Map or Reduce physical memory**. For details about the parameter configuration, see **Table 2-7**.

----End

Reference Information

Table 2-7 MapReduce task parameter configuration

Parameters	Description
mapreduce.reduce.memory.mb	Indicates the memory size configured for a reduce container.
mapreduce.map.memory.mb	Indicates the memory size configured for a map container.
yarn.nodemanager.vmem-pmem-ratio	Indicates the ratio of the maximum available virtual memory to physical memory of a container.

NOTE

The physical memory size in the actual running environment must be greater than the values of **mapreduce.reduce.memory.mb** and **mapreduce.map.memory.mb**.

2.4.19.6 Many Fetch Failures Occur During Reduce Phase of Running Task

Symptom

A physical machine with 500 nodes fails to run a 100TB terasort task, and logs of the reduce task indicate many fetch failures have occurred.

Possible Causes

Data fetch during shuffle fails due to insufficient switch bandwidths. If many fetch failures occur, the terasort task may fail.

Fault Locating

- The terasort task fails because the number of fetch failures exceeds the maximum limit.
- The fetch failures are probably due to:
  - High disk I/O usage when writing fetched data into a local disk
  - Insufficient switch bandwidths for fetching data
- Run the terasort task and start monitoring.
  - Use iostat to monitor the local dir of NodeManager. The monitoring result shows that the I/O usage of terasort task is not always 100%, which means that the I/O is not congested. Therefore, the fetch failures are not due to high disk I/O usage.
  - The Reduce task encounters a read timeout during shuffle. The timeout problem may be due to the network.
  - Switch usage statistics show that the switch has run out of bandwidths for a long period of time.

Procedure

- Increase switch bandwidths.
- Decrease the Reduce task concurrency to alleviate the network burden created by concurrent data reads/writes.
- Compress intermediate results to reduce the total size of transmitted data.

  Configure the compress function in the client configuration file mapred-site.xml. For details about the compress parameters, see **Table 2-8**.

Reference Information

Table 2-8 Parameters relating to compress

Parameter	Description	Default Value
mapreduce.map.output.compress	Specified whether to enable compression of map outputs.	true
mapreduce.map.output.compress.codec	Indicates the algorithm for compressing map outputs.	org.apache.hadoop.io.compress.SnappyCodec

2.4.20 MemArtsCC

2.4.20.1 MemArtsCC Reads Data Slowly

Symptom

After Spark is interconnected with MemArtsCC, the data reading speed is slow.

Possible Causes

- OBSA does not pre-read data from MemArtsCC and instead generates multiple small I/O operations.
- Other performance bottlenecks.

Fault Locating

1. Change the value of **spark.hadoop.fs.obs.memartscc.inputstream.buffer.type** to **bind** and retry the task.
2. Check the time required for end-to-end read I/O processing after the network receives a read I/O request.

Procedure

Step 1 When submitting the task, add the **conf spark.hadoop.fs.obs.memartscc.inputstream.buffer.type** parameter and set it to **bind**. Assess whether the read speed improves.

spark.hadoop.fs.obs.memartscc.buffer.size specifies the I/O size, and increasing it will enhance the speed but also raise the memory usage of the worker's I/O read buffer.

Formula for calculating the memory usage of the worker's I/O read buffer: (26*128+20000 - 3000)/2 * IO size

Step 2 Change the OBSA log level to **DEBUG**.

Add the following information to the Hadoop directory file **/etc/hadoop/log4j.properties** on the client and the Spark client file **$Spark_Client/conf/log4j-executor.properties**:

```
log4j.logger.org.apache.hadoop.fs.obs=DEBUGlog4j.logger.com.obs.services=DEBUG
```

Step 3 After the task is executed again, examine the executor log in Spark for the following logs: **OREAD**, which indicates the number of times OBSA reads data from OBSA along with the time consumed and file size; and **MREAD**, which also represents the number of times OBSA reads data from OBSA, the time consumed, and the file size.

```
SUMMARY: OREAD[count=0,time=0,size=0], MREAD[count=728,time=21960168424,size=5961178]
SUMMARY: OREAD[count=0,time=0,size=0], MREAD[count=728,time=21960168424,size=5961178]
```

----End

2.4.20.2 MemArtsCC CCSidecar or CCWorker Process Fault

Symptom

The MemArtsCC CCSidecar or CCWorker process is faulty.

Possible Causes

- The health check fails.
- The process does not exist.

Fault Locating

1. Check whether the process is available.
2. Run the health check command.
3. View the health check script result.

Procedure

Step 1 Log in to the node where the CCSidecar instance is faulty and run the following command to check the status of the CCSidecar process:

ps -ef|grep sidecar

There are three sidecar processes in the normal state, as shown in the following figure. If the CCSidecar is faulty and there are residual processes, you'll need to manually terminate them.

```
[omm@192-168-13-175 ~]$ ps -ef|grep sidecar
omm        56325   36331  0 15:37 pts/0    00:00:00 grep sidecar
omm      3185925       1  0 Jan31 ?        00:00:44 MemArtscc-sidecar_main_service
omm      3187412 3185925  0 Jan31 ?        00:00:30 MemArtscc-sidecar_zookeeper_query
omm      4143607 3185925  0 15:34 ?        00:00:00 MemArtscc-sidecar_background_task
```

Step 2 Log in to the node where the CCWorker instance is faulty and run the following command to check the CCWorker process status:

ps -ef|grep ccworker

```
[omm@192-168-13-175 ~]$ ps -ef|grep ccworker
omm       233217  232901  3 15:41 ?        00:00:01 /opt/huawei/Bigdata/FusionInsight_MemArtsCC_8.3.0/install/FusionInsight-MemArtsCC-3.22/cc-worker/bin/ccworker -f /opt/hua
wei/Bigdata/FusionInsight_MemArtsCC_8.3.0/install/FusionInsight-MemArtsCC-3.22/memartscc/worker.json
omm       265545   36331  0 15:42 pts/0    00:00:00 grep ccworker
[omm@192-168-13-175 ~]$
```

If the CCWorker process does not exist, go to the **/var/log/Bigdata/memartscc/worker** directory to review the worker run logs and assess the CCWorker status. Based on the identified causes, address the issue.

Step 3 Switch to user **omm** and run the following command to check the health check status:

${BIGDATA_HOME}/tmp/python3/bin/cc-sidecar show hc

```
+------------+--------+
| proc       | status |
+------------+--------+
| cc-sidecar | True   |
| cc-worker  | True   |
+------------+--------+
```

The CCSidecar reports the CCWorker status; however, if the CCSidecar itself is faulty, obtaining the CCWorker status becomes impossible, resulting in the process being flagged as faulty. In such cases, refer to the worker run logs in the **/var/log/Bigdata/memartscc/worker** directory to determine the CCWorker status and rectify the fault accordingly.

Step 4 Go to the log directory and view the health check script execution result in **check-sidecar-instance.log** and **check-worker-instance.log**.

----End

2.4.21 MOTService

2.4.21.1 MOTService Fails to Be Installed During Preinstallation

Symptom

On the FusionInsight Manager component installation page, a message is displayed indicating that services and instances fail to be initialized and the component fails to be installed.

Possible Causes

- The Python version of the installation and running environment does not match.
- The related dynamic library dependencies are missing, and Python lacks related modules.

Fault Locating

Check whether related modules are missing in the **/var/log/Bigdata/motservice/script/install.log** file.

The Python versions displayed in the results of commands **python3 -V** and **/usr/bin/python3 -V** should be the same, and the Python version should be later than 3.6 and earlier than 3.9.

Troubleshooting

Step 1 Log in to the active MOTService node as user **omm**.

Step 2 Run the following command to view the error log:

vim /var/log/Bigdata/motservice/script/install.log

- If the log does not contain **security module**, the current Python version is earlier than 3.6. Install Python whose version is later than 3.6 and earlier than 3.9.
- If the log does not contain **ctype module**, the **libffi-devel** library is missing when Python is installed. Run the **yum** command to add the library, and then compile and install Python again.

----End

2.4.21.2 MOTService Fails to Be Installed Due to Service and Instance Startup Failure

Symptom

On the FusionInsight Manager component installation page, a message is displayed indicating that services and instances fail to be started and the component fails to be installed.

The **postgresql.log** file contains message "allocate memory failed", indicating that memory fails to be allocated.

Possible Causes

MOTService is an in-memory database and consumes more memory than other components. Therefore, more memory (at least 2 GB) needs to be allocated to MOTService.

Fault Locating

Check whether the percentage of the total and available memory of the OS, and MOTService memory is proper.

Troubleshooting

Step 1 Log in to the active MOTService node as user **omm**.

Step 2 Run the **free -h** command to check the available memory of the system.

Step 3 Log in to FusionInsight Manager, choose **Cluster** > **Services** > **MOTService**, click **Configuration**, and then **All Configurations**. Check the memory usage of MOTService, that is, the value of **motservice.database.max.process.memory** to determine whether the current memory is sufficient.

Step 4 If the memory is insufficient, decrease the value of **motservice.database.max.process.memory** or increase the cluster memory.

----End

2.4.21.3 "command not found" Is Displayed If gsql Is Used to Connect to the Database

Symptom

The database cannot be connected using the **gsql** command, and message "command not found" is displayed.

Possible Causes

The environment variable script is not loaded.

Fault Locating

The **gsql** file can be found only through the PATH environment variable.

Troubleshooting

Step 1 Log in to the active MOTService node as user **omm**.

Step 2 Run the following command to load environment variables:

source "$MOTSERVER_HOME"/.motservice_profile

Step 3 Run the **gsql** command.

----End

2.4.21.4 An Error Indicating Too Many Client Connections Is Reported When a User Connects to the MOTService Database

Symptom

When the **gsql** command or JDBC client is used to connect to the database, message "Too many clients" or "Too many clients" is displayed.

Possible Causes

The upper limit of connections is set when the user is created.

Fault Locating

Check the number of active and non-active connections and check whether there are too many non-active connections. Change the maximum number of database connections or the session timeout duration to solve the problem.

Troubleshooting

Method 1: changing the maximum number of database connections

Step 1 Log in to FusionInsight Manager, choose **Cluster** > **Services** > **MOTService**, click **Configurations**, and then **All Configurations**.

Step 2 Search for parameter **motservice.database.max.connections** and check whether its value is too small. Default value **5000** is recommended. If the value is too small, increase the value and click **Save**.

Step 3 On the **Dashboard** page, click **More** and select **Restart Service**. Enter the password of the current user to restart the MOTService service.

----End

Method 2: configuring the session timeout duration

Step 1 Log in to the active MOTService node as user **omm**.

Step 2 Run the following command to load environment variables:

source "$MOTSERVER_HOME"/.motservice_profile

Step 3 Log in to the background as user **gsql** and run the following command to check the current parameter settings. If the value of **session_timeout** is **0**, the timeout is canceled. It is recommended to change this value to **10 min**.

SHOW session_timeout;

Step 4 Exit the **gsql** client and run the following command to change the session timeout duration:

gs_guc reload -Z coordinator -Z datanode -N all -I all -c "session_timeout=600"

----End

2.4.21.5 An Error Is Reported During Cluster Connection, Indicating that the Account Is Locked

Symptom

Error message "The account has been locked" is reported when the cluster is connected.

Possible Causes

The account will be locked if the number of incorrect password attempts exceeds the maximum. The default value is 10.

Fault Locating

Unlock the account as the cluster administrator.

Troubleshooting

Step 1 Log in to the active management node as user **omm**.

Step 2 Run the following command to load environment variables:

source ${MOTSERVER_HOME}/.motservice_profile

Step 3 Run the following command to log in to MOTService and enter the password of the MOTService database user **omm**:

gsql -d postgres -p 20105

NOTE

For details about how to obtain the **omm** password of the MOTService database, see ***Huawei Cloud Stack 8.3.1 Account List*** .

Step 4 Run the unlock command.

ALTER USER *user_name* **ACCOUNT UNLOCK;**

NOTE

user_name indicates the account to be unlocked.

----End

2.4.21.6 An Error Message Is Reported During Statement Execution, Indicating That the User Does Not Have the Required Permission

Symptom

Message "ERROR: permission denied for *xxx* " is displayed after the statement is executed.

Possible Causes

The user does not have the corresponding permission.

Fault Locating

Grant the corresponding permission to the current user. The following operations show how to assign the permission of user **tom** to user **jerry**.

Troubleshooting

Step 1 Log in to the active management node as user **omm**.

Step 2 Run the following command to load environment variables:

source "$MOTSERVER_HOME"/.motservice_profile

Step 3 Run the following command to log in to the MOTService database and enter the password of user **omm**:

gsql -d postgres -p 20105

NOTE

For details about how to obtain the **omm** password of the MOTService database, see *Huawei Cloud Stack 8.3.1 Account List* .

Step 4 Grant the schema permissions of user **tom** to user **jerry**.

grant usage on schema tom to jerry;

Step 5 Grant the schema table query permission of user **tom** to user **jerry**.

grant select on all tables in schema tom to jerry;

Step 6 Grant the **SELECT** permission on the tables created by user **tom** in the schema with the same name to user **jerry**.

alter default privileges for user tom in schema tom grant select on tables to jerry;

----End

2.4.21.7 LOCK_WAIT_TIMEOUT Is Displayed During SQL Execution

Symptom

During SQL execution, lock wait timeout (LOCK_WAIT_TIMEOUT) is reported.

Possible Causes

Lock wait timeout is generally caused by the fact that another SQL statement has held the lock. The current SQL statement can be executed only after the SQL statement that holds the lock is successfully executed and releases the lock. If the lock wait time exceeds the specified value of GUC parameter **lockwait_timeout**, the system reports the LOCK_WAIT_TIMEOUT error.

Fault Locating

Find the PID of the deadlocked session and forcibly release the session. It is recommended to optimize the value of **lockwait_timeout**.

Troubleshooting

Step 1 Run the following SQL statements to find the related information, such as the PID of the session that causes the deadlock:

```
SELECT w.query as waiting_query,
w.pid as w_pid,
w.username as w_user,
l.query as locking_query,
l.pid as l_pid,
l.username as l_user,
t.schemaname || '.' || t.relname as tablename
from pg_stat_activity w join pg_locks l1 on w.pid = l1.pid
and not l1.granted join pg_locks l2 on l1.relation = l2.relation
and l2.granted join pg_stat_activity l on l2.pid = l.pid join pg_stat_user_tables t on l1.relation
= t.relid
where w.waiting;
```

Step 2 Release the deadlocked session and change the value of **lockwait_timeout**.

- Run the following statement to forcibly end the session that has the corresponding PID:

  ```
  SELECT PG_TERMINATE_BACKEND(PID);
  ```

- Set the **lockwait_timeout** parameter to control the maximum waiting time of a single lock.
  a. Log in to the active MOTService node as user **omm**.
  b. Run the following command to load environment variables:

     source "$MOTSERVER_HOME"/.motservice_profile

  c. Run the following command to set parameter **lockwait_timeout**:

     gs_guc reload -Z coordinator -Z datanode -N all -I all -c "lockwait_timeout=600000"

     NOTE

     The unit of the value of **lockwait_timeout** is millisecond and the default value is 20 minutes.

----End

2.4.21.8 Database Enters the Read-Only Mode

Symptom

Message "cannot execute xxx in a read-only transaction" is displayed when the SQL statement is executed.

Possible Causes

As shown in the error message, the current database is in read-only mode. Users can query data in the database, but cannot insert or delete data.

Fault Locating

The database may enter the read-only mode manually or automatically. If the disk or memory usage reaches the threshold, the read-only mode will be triggered by MOTService. The following operations show how to disable the read-only mode of the database if the disk or memory usage reaches the threshold.

Troubleshooting

Step 1 Log in to FusionInsight Manager, choose **Cluster** > **Services** > **MOTService**, and click **Dashboard**. On the chart page, check whether the **MOT Used Memory Percentage** exceeds 70%. If the MOT memory usage chart does not exist, click ▾ in the upper right corner, click **Customize**, select **MOT Used Memory Percentage**, and click **OK** to customize the chart.

- If the usage exceeds 70%, go to **Step 2**.
- If the usage does not exceed 70%, go to **Step 4**.

Step 2 Click **Configuration**, click **All Configurations**, search for **motservice.database.max.process.memory**, and check whether the percentage of the maximum process memory of the MOTService database to the system memory is 90%.

- If yes, calculate the ratio of the maximum process memory of the MOTService database to the system memory. If the ratio exceeds 90%, stop the current node, expand the capacity, and go to **Step 4**.
- No: Change the value to **90** and save the configuration. Then, go to **Step 3**.

Step 3 Restart MOTService for the settings to take effect.

Step 4 Log in to the active management node as user **omm**.

Step 5 Run the following command to load environment variables:

```
source "$MOTSERVER_HOME"/.motservice_profile
```

Step 6 Run the following command to disable the read-only mode. If no error is reported, the read-only mode is disabled successfully.

```
gs_guc reload -Z datanode -N all -I all -c "default_transaction_read_only=off"
```

----End

2.4.22 Redis

2.4.22.1 Cluster Instances Are Offline Due to Abnormal Redis Slot Migration

Symptom

Some Redis cluster instances are offline.

Possible Causes

Slot update commands are frequently sent during the Redis migration. Node configuration cannot be synchronized to each node in a timely manner due to the hysteresis of the Redis internal heartbeat mechanism. After the slot configuration changes, one or some nodes detect the speed difference, and the status is marked failed due to incomplete slots, while the cluster keys are complete.

Fault Locating

None.

Procedure

Step 1 Log in to a node where a failed Redis instance locates.

The R1 instance on the 10-122-105-11 node is used as an example.

Step 2 Run the **redis-cli** client command to access the faulty Redis instance node.

NOTE

You need to install the client before running the command.

Step 3 Run the **cluster nodes** command to view the IP addresses and port numbers of the disconnected instances in the cluster.

```
10.122.105.11:22400> cluster nodes
a0f1ddf16cb4c04787ef580bcfc666589cacc4c2 10.122.104.237:22400@24350 master - 0 1436269523159 1
connected 10922-14042
7510ea6016c7988b0eea451e5b80aa7660c1a2e8 10.122.105.237:22403@24353 master - 0 1436269525161
14 connected 14043-16383
b0288a6e1987dec71c59e3d2cd300b5ff4951b67 10.122.105.11:22402@24352 slave
a0f1ddf16cb4c04787ef580bcfc666589cacc4c2 0 1436269522657 1 connected
04e7c368aa976e06bd6049c974851abd7574e33e 10.122.104.176:22402@24354 slave
7d376b5bda015db014438ca935042faaf0cb939d 0 1436269524161 2 connected
0ff497f9b629eac20b30ba723e7f98c146f1ac42 10.122.105.176:22401@24351 master,fail -
1436269522156 1435339121670 13 disconnected 2730
7d376b5bda015db014438ca935042faaf0cb939d 10.122.105.11:22400@24350 myself,master - 0 0 2
connected 5461-10921
......
```

In this example, 2730 is the lost slot.

Step 4 Log in to FusionInsight Manager, view the R4 instance, that is, the master instance that is upgraded from the slave instance of the failed instance on 10-122-104-237. The following figure shows all the instances.

```
10.122.105.11:22400> cluster nodes
a0f1ddf16cb4c04787ef580bcfc666589cacc4c2 10.122.104.237:22400@24350 master - 0 1436269523159 1
connected 10922-14042
7510ea6016c7988b0eea451e5b80aa7660c1a2e8 10.122.105.237:22403@24353 master - 0
1436269525161 14 connected 14043-16383
b0288a6e1987dec71c59e3d2cd300b5ff4951b67 10.122.105.11:22402@24352 slave
a0f1ddf16cb4c04787ef580bcfc666589cacc4c2 0 1436269522657 1 connected
04e7c368aa976e06bd6049c974851abd7574e33e 10.122.104.176:22402@24354 slave
7d376b5bda015db014438ca935042faaf0cb939d 0 1436269524161 2 connected
0ff497f9b629eac20b30ba723e7f98c146f1ac42 10.122.105.176:22401@24351 master,fail -
1436269522156 1435339121670 13 disconnected 2730
7d376b5bda015db014438ca935042faaf0cb939d 10.122.105.11:22400@24350 myself,master - 0 0 2
connected 5461-10921
......
```

Check the IP address, port number, and instance ID of the R4 instance, and use the redis-cli tool to log in to the instance.

redis-cli -h 10.122.105.237 -p 22403

NOTE

If channel encryption is enabled for Redis, run **redis-cli -h 10.122.105.237 -p 22403 --tls.**

To enable channel encryption for Redis, log in to Manager, choose **Cluster > Services > Redis > Configurations > All Configurations**, search for **REDIS_SSL_ON**, and change the parameter value to **true** to enable SSL channel encryption.

Step 5 Send the **cluster setslot** command to the R4 instance on 10-122-105-237.

cluster setslot 2730 node 7510ea6016c7988b0eea451e5b80aa7660c1a2e8

Step 6 When the command returns OK, check the cluster status.

----End

Reference Information

None.

2.4.22.2 Master Instances Exist After the Original Master Instance Restarts Due to Abnormal Redis Slot Migration

Symptom

In the Redis cluster, two same master instances exist. As shown in the figure, 10-122-104-237:R2 and 10-122-105-11:R4 are in master-slave mode previously. After abnormal migration, both instances become master instances.

Possible Causes

Slot update commands are frequently sent during the Redis migration. Node configuration cannot be synchronized to each node in a timely manner due to the

hysteresis of the Redis internal heartbeat mechanism. After the slot configuration changes, one or some nodes detect the speed difference, and the status is marked failed due to incomplete slots, while the cluster keys are complete.

Fault Locating

None.

Procedure

Step 1 Log in to a node where a failed Redis instance locates.

R2 on 10-122-104-237 and R4 on 10-122-105-11 are used as an example.

Step 2 Run the **redis-cli** client command to access instance R2.

NOTE

You need to install the client before running the command.

Step 3 Run the **keys *** command to view the number of keys and find the Redis instance that has empty result.

```
10.122.104.237:22401> keys *
(empty list or set)
```

Step 4 Run the **cluster nodes** command to view the slot range of the instance (R2 on 10-122-104-237 as an example) that has empty key count.

In this example, the slot range of R2 on10-122-104-237 is 5692 to 5694.

```
10.122.104.237:22401> cluster nodes
a0f1ddf16cb4c04787ef580bcfc666589cacc4c2 10.122.104.237:22400@24350 master - 0 1436269523159 1
connected 10922-16383
7510ea6016c7988b0eea451e5b80aa7660c1a2e8 10.122.104.237:22401@24351 myself,master - 0
1436269525161 14 connected 5692-5694
b0288a6e1987dec71c59e3d2cd300b5ff4951b67 10.122.105.11:22402@24352 slave
a0f1ddf16cb4c04787ef580bcfc666589cacc4c2 0 1436269522657 1 connected
04e7c368aa976e06bd6049c974851abd7574e33e 10.122.104.237:22402@24352 slave
7d376b5bda015db014438ca935042faaf0cb939d 0 1436269524161 2 connected
b9ccaeac898d5d3a59d7bb36c835ac95592db270 10.122.105.11:22403@24353 master - 0 1435339121670 13
connected 2730-5459
7d376b5bda015db014438ca935042faaf0cb939d 10.122.105.176:22400@24350 master - 0 0 2 connected
5461-10921
......
```

In this example, 2730 is the lost slot.

Step 5 Send the **setslot** command to R4 on 10-122-105-11. A slot number range within 5692 to 5694 is adopted.

cluster setslot 5692 node b9ccaeac898d5d3a59d7bb36c835ac95592db270

.....

cluster setslot 5694 node b9ccaeac898d5d3a59d7bb36c835ac95592db270

NOTE

b9ccaeac898d5d3a59d7bb36c835ac95592db270 is the ID of R4 on 10-122-105-11.

Step 6 Use the redis-cli tool to log in to R2 on 10-122-104-237 again and send the **replicate** command.

cluster replicate b9ccaeac898d5d3a59d7bb36c835ac95592db270

Step 7 When the command returns OK, check the cluster status.

Redis Cluster Status

master slave Bad master-slave relationship

Host Name	R1	R2	R3	R4
10-122-104-237	M1	S4	S3	S6
10-122-105-11	M2	M5	S1	M4
10-122-105-176	M3	M6	S2	S5

10 Total Records: 3 1

----End

Reference Information

None.

2.4.22.3 Redis Cluster Becomes Unreliable When a Redis Node or Instance Is Disconnected

Symptom

- An instance in a Redis cluster is disconnected, the slave instance becomes the master instance, and there is no slave instance. Therefore, all clusters become unreliable. Then the clusters are in the following state.

Redis Cluster Status

master slave Bad master-slave relationship

Host Name	R1	R2	R3	R4
10-121-16-165	M1	M4	S3	--
10-121-16-237	M2		S1	S4
10-121-17-188	--	M3	S2	M5

- An instance in a Redis cluster is disconnected, and capacity reduction cannot meet reliability requirements because the cluster scale is small. Therefore, cluster stability cannot be ensured by capacity reduction and then expansion. Reliability requirements indicate that any pair of master and slave instance does not exist on a same node, master and slave instances must co-exist, and more than one half of master instances in a Redis cluster cannot exist on a same node.

Redis Cluster Status

master slave Bad master-slave relationship

Host Name	R1	R2
10-121-16-165	M1	M3
10-121-16-237	M2	S1
10-121-17-188		S2

Possible Causes

A Redis node or instance is disconnected.

Fault Locating

If the faulty instance cannot be recovered, reduce and then expand the capacity of the instance to recover the fault. If the cluster scale is small and capacity reduction cannot meet reliability requirements, manual operations are necessary.

Procedure

Reduce and then expand capacity.

Step 1 Log in to FusionInsight Manager and choose **Cluster**, click the name of the desired cluster, and choose **Service** > **Redis** > **Redis Management**.

Step 2 Reduce the capacity of the Redis cluster to ensure that the cluster reliability requirements are met.

Step 3 After the capacity reduction is successful, add two master and two slave instances or more to ensure cluster reliability. The following figure shows the expanded cluster.

If cluster capacity cannot be reduced, manually recover the cluster.

Step 4 Log in to the node (node 10-121-17-188 in this example) on which the faulty instance resides as user **root** and change the value of **cluster-enable** in **$ {BIGDATA_HOME}/FusionInsight_HD_8.3.1/install/FusionInsight-redis-*/redis/config/redis.conf** to **yes**.

NOTE

The version 8.3.1 is used as an example. Replace it with the actual version number.

Step 5 Select an instance (R3 instance on 10-121-17-188 node) that does not exist in the cluster, restart the R3 instance, and run the **redis-cli** client command to access instance R3.

NOTE

You need to install the client before running the command.

Step 6 Add IP addresses of all nodes in the cluster to a whitelist.

cluster setwhitelist <10.121.16.165> <10.121.16.237> <...>

Step 7 Use the redis-cli CLI to send the **meet** command to any instance in the cluster.

cluster meet <ip> <port>

Step 8 After the output OK of the **meet** command is displayed, run the **replicate** command to set a master-slave relationship with the R2 instance (separate master instance) on 10.121.16.165 node. You can obtain the ID of the R2 instance by running the **cluster nodes** command.

cluster replicate <ID of the R2 instance>

Step 9 Check whether the cluster is restored.

Redis Cluster Status

master slave Bad master-slave relationship

Host Name	R1	R2	R3
10-121-16-165	M1	S3	--
10-121-16-237	M2	S1	--
10-121-17-188	--	M3	S2

----End

Reference Information

None.

2.4.22.4 Redis Cluster Exists in the Newly Added Redis Service

Symptom

After the Redis service is added by using FusionInsight Manager, a Redis cluster already exists on the **Redis Manager** page, and the cluster is in **Bad** state.

Possible Causes

The Redis service is deleted by deleting all Redis instances, and the residual data in Redis is not cleared.

Fault Locating

Delete the Redis cluster manually.

Procedure

Step 1 Log in to FusionInsight Manager.

Step 2 Choose **Cluster** > *Name of the desired cluster* > **Services** > **Redis** > **Redis Manager**.

Step 3 Click **Delete** in the **Operation** column of the faulty Redis cluster in the Redis cluster list, enter the administrator password, and delete the Redis cluster.

NOTE

Exercise caution when performing this operation because residual data will be lost after the Redis cluster is deleted.

----End

Reference Information

None.

2.4.22.5 Redis Instances Fail to Start After Node Reboot or Fault Recovery

Symptom

After Redis nodes are manually restarted or faults recover, some Redis instances fail to be started.

Role	Running Status	Configuration Status
Redis_1	Normal	Synchronized
Redis_1	Normal	Synchronized
Redis_1	Faulty	Synchronized

Possible Causes

The system is not shut down when the Redis writes data to disks. As a result, persistent files are damaged.

Fault Locating

Use PuTTY to log in to the node where the faulty instance resides as user **root** and view **redis.log** in **/var/log/Bigdata/redis/redis_n**.

```
[2018-09-10 21:02:43][202544][M][warning] Wrong RDB checksum. Aborting now.[rdb.c:1231]
```

Procedure

Step 1 Log in to the node where the faulty instance is located as user **root** using PuTTY.

Step 2 Delete the dump*****.rdb file in ***$BIGDATA_DATA_HOME*/redis/Redis_n** directory.

Step 3 Choose **Cluster** > *Name of the desired cluster* > **Services** > **Redis**, select the faulty instance, and click **Start Instance**.

----End

Reference Information

None.

2.4.22.6 Redis Scale-Out Failed But Some Instances Are in the Normal State

Symptom

Redis scale-out failed but the displayed status of some instances is still normal. An alarm is reported, indicating that the slot distribution of Redis master instances is uneven.

Possible Causes

Data migration and slot allocation failed during Redis scale-out. As a result, slots have not been allocated to some master instances that are just added, and therefore the status is incorrectly displayed. However, this issue has no adverse impacts on the service running.

Fault Locating

Manually balance load.

Procedure

Step 1 Log in to FusionInsight Manager.

Step 2 Choose **Cluster** and click the name of the desired cluster. Then choose **Services** > **Redis** > **Redis Manager**.

Step 3 In the Redis cluster list, locate the row that contains the Redis cluster that failed scale-out, click **Balance** in the **Operation** column, enter the password, and wait until the cluster balancing is complete.

----End

Reference Information

None.

2.4.22.7 Error Message "unknown command" Is Displayed When High-Risk Commands Are Executed on the Redis Client

Symptom

Error message "unknown command" is displayed when a user executes a high-risk command on the client, for example, **FLUSHALL**, **FLUSHDB**, **EVAL**, **KEYS**, **SAVE** and **DEBUG**.

```
8.5.213.14:22405> FLUSHALL
(error) ERR unknown command `FLUSHALL`, with args beginning with:
8.5.213.14:22405> save
(error) ERR unknown command `save`, with args beginning with:
8.5.213.14:22405> keys *
(error) ERR unknown command `keys`, with args beginning with: `*`,
8.5.213.14:22405> FLUSHDB
(error) ERR unknown command `FLUSHDB`, with args beginning with:
8.5.213.14:22405> DEBUG OBJECT
(error) ERR unknown command `DEBUG`, with args beginning with: `OBJECT`,
8.5.213.14:22405>
```

Possible Causes

Redis high-risk commands are prohibited.

Fault Locating

Change the value of Redis configuration parameter **HIGHT_RISK_COMMAND_ENABLE** to **false** to allow high-risk commands.

Procedure

Step 1 Log in to FusionInsight Manager.

Step 2 Choose **Cluster** and click the name of the target cluster. Then choose **Services** > **Redis** > **Configurations**. Click **All Configurations** in the left pane, search for **HIGHT_RISK_COMMAND_ENABLE**, change the value to **false**, and click **Save**.

Step 3 Click **Dashboard**, choose **More**, and select **Restart Service** in the upper-right corner to restart the Redis service.

----End

NOTICE

Restarting Redis will interrupt user services. Therefore, stop user services first before restarting the Redis.

Reference Information

None.

2.4.22.8 Frequent Active/Standby Switchover Caused by Insufficient Storage Space of the Redis Buffer

Symptom

The insufficient storage space of the Redis buffer causes frequent active/standby switchover. Log in to the node where the faulty instance resides as user **root** and check the **redis.log** file in the **/var/log/Bigdata/redis/redis_N** directory. The following error information is displayed:

```
148054:M 25 Jul 16:54:02.786 * Synchronization with slave 10.136.169.48:33504 succeeded
148054:M 19 Sep 14:37:05.672 # Client id=11774588 addr=10.114.2.22:55968 fd=276 name= age=0 idle=0 flags=N db=0 sub=0 psub=0 multi=-1 qbuf=0 qbuf-fr
e=32768 obl=16378 oll=4090 omem=67108870 events=r cmd=hgetall scheduled to be closed ASAP for overcoming of output buffer limits.
148054:M 19 Sep 14:37:30.510 # Connection with slave 10.136.169.48:33504 lost.
148054:M 19 Sep 14:37:32.990 # Client id=11774590 addr=?:0 fd=76 name= age=0 idle=0 flags=N db=0 sub=0 psub=0 multi=-1 qbuf=14 qbuf-free=32754 obl=1
378 oll=4090 omem=67108870 events=r cmd=hgetall scheduled to be closed ASAP for overcoming of output buffer limits.
148054:M 19 Sep 14:37:58.130 # Client id=11774625 addr=?:0 fd=309 name= age=0 idle=0 flags=N db=0 sub=0 psub=0 multi=-1 qbuf=14 qbuf-free=32754 obl=
6378 oll=4090 omem=67108870 events=r cmd=hgetall scheduled to be closed ASAP for overcoming of output buffer limits.
148054:M 19 Sep 14:38:20.301 # Failover auth denied to d05842ddde2279be6a15d98e4a1fde211cf33edb: its master is up
148054:M 19 Sep 14:38:20.301 # Configuration change detected. Reconfiguring myself as a replica of d05842ddde2279be6a15d98e4a1fde211cf33edb
148054:S 19 Sep 14:38:20.301 * Before turning into a slave, using my master parameters to synthesize a cached master: I may be able to synchronize w
th the new master with just a partial transfer.
148054:S 19 Sep 14:38:21.252 * Connecting to MASTER 10.136.169.48:33504
148054:S 19 Sep 14:38:21.253 * MASTER <-> SLAVE sync started
148054:S 19 Sep 14:38:21.253 * Non blocking connect for SYNC fired the event.
148054:S 19 Sep 14:38:22.587 * FAIL message received from 0d3b87d8b6006b1a4958551792119dc8974f0d22 about d05842ddde2279be6a15d98e4a1fde211cf33edb
```

Possible Causes

The storage space of the Redis buffer for active and standby nodes is insufficient.

Fault Locating

1. Log in to the node where the faulty instance resides as user **root**, and check the error information in the **redis.log** file in the **/var/log/Bigdata/redis/redis_N** directory.
2. On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Services** > **Redis** and choose **Configuration** > **All Configurations**. Enter **client-output-buffer-limit-replica** in the search box to search for the configuration item and check whether the parameter value is **client-output-buffer-limit replica 512mb 80mb 60**.

Procedure

Step 1 Log in to FusionInsight Manager.

Step 2 Choose **Cluster** > *Name of the desired cluster* > **Services** > **Redis** and choose **Configuration** > **All Configurations**. Enter **client-output-buffer-limit-replica** in the search box to search for the configuration item, change the parameter value to **client-output-buffer-limit replica 512mb 80mb 60**, and click **Save** in the upper left corner.

Step 3 Click **Dashboard**, choose **More**, and select **Restart Service** in the upper-right corner to restart the Redis service.

----End

Reference Information

None.

2.4.23 RTDService

2.4.23.1 RTDService Is Faulty

Symptom

On the **Services** page, the **Running Status** of RTDService is not **Normal**.

Possible Causes

- RTDService is faulty.
- Tomcat on the OMS node is faulty.

Fault Locating

1. Restart RTDService.
2. Restart Tomcat on the OMS node.

Troubleshooting

Step 1 Log in to FusionInsight Manager.

Step 2 Choose **Cluster** > **Services** to restart RTDService, enter the administrator password, and wait until the service is restarted.

Step 3 Use PuTTY to log in to the active management node as user **root**.

Step 4 Run the **su - omm** command to switch to user **omm**.

Step 5 Run the following commands to query and stop related processes:

ps -ef | grep apache-tomcat-*

kill -9 *Process ID*

Step 6 Run the **startup.sh** script to restart Tomcat.

cd ${BIGDATA_HOME}/om-server/apache-tomcat-*/bin

./startup.sh

----End

Related Information

None

2.4.23.2 Failed to Add a RTDService Executor BLU

Symptom

Log in to FusionInsight Manager, choose **Cluster** > **Services** > **Containers**, and click **Business Manager**. On the page that is displayed, the **Healthy Status** of RTDService Executor BLU is not **Good** or the **Function Status** is not **Started**.

Possible Causes

RTD Executor goes offline due to MOTService, or RTD Executor fails to be automatically deployed due to other problems such as network problems.

Fault Locating

Check whether the Containers and MOTService services are normal, and then add a BLU again.

Troubleshooting

Step 1 Add the RTD Executor BLU on the RTD Portal again.

1. Log in to the RTDPortal management page.
2. On the RTDPortal page, bring all event source dimension mappings contained in the event source corresponding to the abnormal BLU offline.
3. Bring the event source dimension mappings online again and check whether the BLU can be automatically added.

Step 2 Manually add the RTD Executor BLU.

NOTE

You are not advised to manually perform this operation because the configuration file of the RTD Executor BLU contains many complex configurations. If you want to manually rectify the fault, ensure that the RTD Executor BLU has been successfully added. That is, the **Deployment Status** of the RTD-related BLU component on the service management page is **Deployed**. Then, perform the following operations.

1. Log in to FusionInsight Manager, choose **Cluster** > **Services** > **Containers**, and click **Business Manager**.
2. Click on the right of the group, click **Config Set**, click next to the faulty BLU in the operation column, and download the configuration file of the BLU.
3. Use WinSCP to log in to the OMS node and download the BLU WAR package from **${BIGDATA_HOME}/FusionInsight_FARMER_RTD_*/install/FusionInsight-RTD-*/package/RTD_eventSourceType-*.war** (* indicates the RTD version).
4. Change the WAR package name to the name of the BLU to be manually deployed. For example, if the name of the faulty BLU is **RTD_transaction**, change the WAR package name to **RTD_transaction-*.war**.
5. After the WAR package and configuration file of the BLU are prepared, delete the faulty BLU and add the BLU again by referring to the procedure for manually adding the BLU.

----End

Related Information

None

2.4.23.3 Tenant Password Becomes Invalid After DBService Data Is Restored in an Upgrade

Symptom

After the RTD is reinstalled and DBService data is restored, the RTD service cannot be started.

Possible Causes

The tenant password restored by DBService is invalid.

Fault Locating

The Manager uses a key to encrypt and decrypt the password. Each time the Manager is reinstalled, a different key is generated. After the Manager is reinstalled, you need to use the new key to update the password.

Troubleshooting

Step 1 Use PuTTY to log in to the active RTD node.

Run the following commands:

su - omm

cd ${BIGDATA_HOME}/FusionInsight_FARMER_RTD_*/install/FusionInsight-RTD-*/sbin

sh updatepassword.sh

Enter the ID and password of the tenant to be updated.

Step 2 Log in to FusionInsight Manager and restart the RTD service.

----End

Related Information

None

2.4.23.4 Model Status Becomes Incorrect Due to a ZooKeeper Fault During Model Creation

Symptom

If ZooKeeper of a Farmer cluster becomes faulty, the model is successfully created and is ready. After ZooKeeper is recovered, the model status cannot be switched to the ready state through automatic switchover or model query.

Possible Causes

When ZooKeeper becomes faulty, the model status information of the BLU fails to be written to ZooKeeper. After ZooKeeper is recovered, the BLU does not write the model status information again.

Fault Locating

During model creation, the RTDService delivers the configuration set to each BLU node, triggers BLU model file reload, and reports signaling (model status) to ZooKeeper.

During model query, the RTDService interacts with ZooKeeper to obtain the signaling (model status) from ZooKeeper and then updates the model status in the metadata database.

ZooKeeper becomes faulty during model creation, and the signaling of the BLU node cannot be reported. After ZooKeeper is recovered, the RTDService model cannot query the model information in ZooKeeper, and the model is still in the ready state.

Troubleshooting

Create a model file to trigger status update.

Related Information

None

2.4.23.5 RTDService Becomes Abnormal After It Is Manually Added on the Console

Symptom

When you manually add the RTDService service for an ECS/BMS cluster on the MRS console, the service fails to be added for the first time. After you try again, the RTDService service is successfully added.

However, the RTDService service becomes abnormal, and the RTD web UI cannot be accessed.

Fault Locating

Check the run logs of the RTD service. It is found that the fault is caused by the DBServer connection failure.

```
aused by: org.postgresql.util.PSQLException: FATAL: Invalid username/password,login denied.
        at org.postgresql.core.v3.ConnectionFactoryImpl.doAuthentication(ConnectionFactoryImpl.java:414) ~[gsjdbc4-V100R003C10SPC129.jar:?]
        at org.postgresql.core.v3.ConnectionFactoryImpl.openConnectionImpl(ConnectionFactoryImpl.java:195) ~[gsjdbc4-V100R003C10SPC129.jar:?]
        at org.postgresql.core.ConnectionFactory.openConnection(ConnectionFactory.java:65) ~[gsjdbc4-V100R003C10SPC129.jar:?]
        at org.postgresql.jdbc2.AbstractJdbc2Connection.<init>(AbstractJdbc2Connection.java:124) ~[gsjdbc4-V100R003C10SPC129.jar:?]
        at org.postgresql.jdbc3.AbstractJdbc3Connection.<init>(AbstractJdbc3Connection.java:29) ~[gsjdbc4-V100R003C10SPC129.jar:?]
        at org.postgresql.jdbc3g.AbstractJdbc3gConnection.<init>(AbstractJdbc3gConnection.java:21) ~[gsjdbc4-V100R003C10SPC129.jar:?]
        at org.postgresql.jdbc4.AbstractJdbc4Connection.<init>(AbstractJdbc4Connection.java:31) ~[gsjdbc4-V100R003C10SPC129.jar:?]
        at org.postgresql.jdbc4.Jdbc4Connection.<init>(Jdbc4Connection.java:29) ~[gsjdbc4-V100R003C10SPC129.jar:?]
        at org.postgresql.Driver.makeConnection(Driver.java:394) ~[gsjdbc4-V100R003C10SPC129.jar:?]
        at org.postgresql.Driver.connect(Driver.java:267) ~[gsjdbc4-V100R003C10SPC129.jar:?]
        at java.sql.DriverManager.getConnection(DriverManager.java:664) ~[?:1.8.0_332]
        at java.sql.DriverManager.getConnection(DriverManager.java:208) ~[?:1.8.0_332]
        at org.springframework.jdbc.datasource.DriverManagerDataSource.getConnectionFromDriverManager(DriverManagerDataSource.java:155) ~[spring-jdbc-5.3.20.jar:5.3.20]
        at org.springframework.jdbc.datasource.DriverManagerDataSource.getConnectionFromDriver(DriverManagerDataSource.java:146) ~[spring-jdbc-5.3.20.jar:5.3.20]
        at org.springframework.jdbc.datasource.AbstractDriverBasedDataSource.getConnectionFromDriver(AbstractDriverBasedDataSource.java:205) ~[spring-jdbc-5.3.20.jar:5.3.20]
        at org.springframework.jdbc.datasource.AbstractDriverBasedDataSource.getConnection(AbstractDriverBasedDataSource.java:169) ~[spring-jdbc-5.3.20.jar:5.3.20]
        at org.hibernate.engine.jdbc.connections.internal.DatasourceConnectionProviderImpl.getConnection(DatasourceConnectionProviderImpl.java:122) ~[hibernate-core-5.6.9.Final.jar:5.6.9.Final]
        at org.hibernate.engine.jdbc.env.internal.JdbcEnvironmentInitiator$ConnectionProviderJdbcConnectionAccess.obtainConnection(JdbcEnvironmentInitiator.java:181) ~[hibernate-core-5.6.9.Final.jar:5.6.9.
inal]
        at org.hibernate.resource.transaction.backend.jdbc.internal.DdlTransactionIsolatorNonJtaImpl.getIsolatedConnection(DdlTransactionIsolatorNonJtaImpl.java:44) ~[hibernate-core-5.6.9.Final.jar:5.6.9.F
nal]
        at org.hibernate.tool.schema.internal.exec.ImprovedExtractionContextImpl.getJdbcConnection(ImprovedExtractionContextImpl.java:63) ~[hibernate-core-5.6.9.Final.jar:5.6.9.Final]
        at org.hibernate.tool.schema.extract.spi.ExtractionContext.getQueryResults(ExtractionContext.java:43) ~[hibernate-core-5.6.9.Final.jar:5.6.9.Final]
        at org.hibernate.tool.schema.extract.internal.SequenceInformationExtractorLegacyImpl.extractMetadata(SequenceInformationExtractorLegacyImpl.java:39) ~[hibernate-core-5.6.9.Final.jar:5.6.9.Final]
        at org.hibernate.tool.schema.extract.internal.DatabaseInformationImpl.initializeSequences(DatabaseInformationImpl.java:66) ~[hibernate-core-5.6.9.Final.jar:5.6.9.Final]
        at org.hibernate.tool.schema.extract.internal.DatabaseInformationImpl.<init>(DatabaseInformationImpl.java:60) ~[hibernate-core-5.6.9.Final.jar:5.6.9.Final]
        at org.hibernate.tool.schema.internal.Helper.buildDatabaseInformation(Helper.java:183) ~[hibernate-core-5.6.9.Final.jar:5.6.9.Final]
        at org.hibernate.tool.schema.internal.AbstractSchemaMigrator.doMigration(AbstractSchemaMigrator.java:104) ~[hibernate-core-5.6.9.Final.jar:5.6.9.Final]
        at org.hibernate.tool.schema.spi.SchemaManagementToolCoordinator.performDatabaseAction(SchemaManagementToolCoordinator.java:196) ~[hibernate-core-5.6.9.Final.jar:5.6.9.Final]
        at org.hibernate.tool.schema.spi.SchemaManagementToolCoordinator.process(SchemaManagementToolCoordinator.java:85) ~[hibernate-core-5.6.9.Final.jar:5.6.9.Final]
        at org.hibernate.internal.SessionFactoryImpl.<init>(SessionFactoryImpl.java:335) ~[hibernate-core-5.6.9.Final.jar:5.6.9.Final]
        at org.hibernate.boot.internal.SessionFactoryBuilderImpl.build(SessionFactoryBuilderImpl.java:471) ~[hibernate-core-5.6.9.Final.jar:5.6.9.Final]
        at org.hibernate.cfg.Configuration.buildSessionFactory(Configuration.java:728) ~[hibernate-core-5.6.9.Final.jar:5.6.9.Final]
        at org.hibernate.cfg.Configuration.buildSessionFactory(Configuration.java:746) ~[hibernate-core-5.6.9.Final.jar:5.6.9.Final]
        at org.springframework.orm.hibernate5.LocalSessionFactoryBean.buildSessionFactory(LocalSessionFactoryBean.java:616) ~[spring-orm-5.3.20.jar:5.3.20]
        at org.springframework.orm.hibernate5.LocalSessionFactoryBean.afterPropertiesSet(LocalSessionFactoryBean.java:600) ~[spring-orm-5.3.20.jar:5.3.20]
        at org.springframework.beans.factory.support.AbstractAutowireCapableBeanFactory.invokeInitMethods(AbstractAutowireCapableBeanFactory.java:1863) ~[spring-beans-5.3.20.jar:5.3.20]
        at org.springframework.beans.factory.support.AbstractAutowireCapableBeanFactory.initializeBean(AbstractAutowireCapableBeanFactory.java:1800) ~[spring-beans-5.3.20.jar:5.3.20]
        ... 21 more
7:41:07.504 [localhost-startStop-1] ERROR org.apache.catalina.core.StandardContext - One or more listeners failed to start. Full details will be found in the appropriate container log file
7:41:07.508 [localhost-startStop-1] ERROR org.apache.catalina.core.StandardContext - Context [/rtdservice] startup failed due to previous errors
7:41:07.517 [localhost-startStop-1] INFO  org.apache.catalina.core.ContainerBase.[Catalina].[localhost].[/rtdservice] - Closing Spring root WebApplicationContext
7:41:07.527 [localhost-startStop-1] WARN  org.apache.catalina.loader.WebappClassLoaderBase - The web application [rtdservice] registered the JDBC driver [org.postgresql.Driver] but failed to unregister it
hen the web application was stopped. To prevent a memory leak, the JDBC Driver has been forcibly unregistered.
7:41:07.529 [localhost-startStop-1] WARN  org.apache.catalina.loader.WebappClassLoaderBase - The web application [rtdservice] appears to have started a thread named [fileExistenceProcess-1] but has failed
o stop it. This is very likely to create a memory leak. Stack trace of thread:
sun.misc.Unsafe.park(Native Method)
java.util.concurrent.locks.LockSupport.parkNanos(LockSupport.java:215)
java.util.concurrent.locks.AbstractQueuedSynchronizer$ConditionObject.awaitNanos(AbstractQueuedSynchronizer.java:2084)
java.util.concurrent.ScheduledThreadPoolExecutor$DelayedWorkQueue.take(ScheduledThreadPoolExecutor.java:1093)
```

Troubleshooting

Step 1 Log in to the MRS console.

Step 2 Choose **Clusters** > **Active Clusters** and click a cluster name to go to its details page.

Step 3 Click **Components** and manually delete RTDService.

Step 4 Manually add the RTDService service again.

----End

Related Information

None

2.4.24 Solr

2.4.24.1 Solr Client Fails to Write Index in Real Time

Symptom

The Solr client fails to write the index file. The exception information is as follows:

```
Error from server at https://192.168.152.14:21104/solr/col_test_shard1_replica2: Exception writing document id 6907a8e1154a4bdb9a4238cd7bb874c4 to the index; possible analysis error., retry? 0
```

Possible Causes

- The index file is damaged.
- The disk or file system where the index file resides is faulty.

Fault Locating

1. Choose **Cluster** > *Name of the desired cluster* > **Service** > **Solr** > **Configuration > All Configurations**. In the search box, type **21104**, the port number in the exception information, to check parameters of the **SolrServer1** instance.
2. Log in to the host whose IP address is **192.168.152.14** as user **root**. Check the **solr-host name.log** file of **SolrServer1** in the **/var/log/Bigdata/solr** directory. In the log file, search for the keyword **IndexWriter AlreadyCloseException**.

Procedure

- If the abnormal stack at the bottom layer is **java.nio.file.FileSystemException: Too many open files in system**, new files cannot be opened because no file handle of the OS is available.
  a. To rectify the fault, see section "ALM-12053 Host File Handle Usage Exceeds the Threshold". After the fault is rectified, wait until the Solr service is running properly. It means that the statuses of all collection copies are **Active** on the SolrAdminUI portal.
  b. Run the **solrctl collection --reload col_test** command on the solrctl command line tool or restart the **SolrServer1** instance (choose **Cluster** >

Name of the desired cluster **> Service** > **Solr** > **Instance** and select the **SolrServer1** instance whose IP address is **192.168.152.14**. Click **More** > **Restart Instance**).

- If the abnormal stack at the bottom layer is **java.io.IOException:Input/output error:**, the disk to which the data directory of the SolrServer instance is mounted is faulty.
  a. To rectify the fault, see section "MRS Tenant-Plane Emergency Cases > Disk Issues > Handling a Hard Disk Fault in a Physical Machine Cluster > Before You Start" in the *MapReduce Service (MRS) 3.3.1-LTS Emergency Handling Guide (for Huawei Cloud Stack 8.3.1)*.
     i. After the fault is rectified, restart the **SolrServer1** instance (choose **Services** > **Solr** > **Instance** and select the **SolrServer1** instance whose IP address is **192.168.152.14**. Click **More** > **Restart Instance**) or run the **solrctl collection --reload col_test** command on the solrctl command line tool.
     ii. If the disk fault fails to be rectified, see section "Hard Disk Mounted to the Solr Data Partition Directory Is Faulty" in the *MapReduce Service (MRS) 3.3.1-LTS Emergency Handling Guide (for Huawei Cloud Stack 8.3.1)* to handle the problem.
- If the abnormal stack at the bottom layer is **java.io.IOException: Map failed: MMapIndexInput**, the instance fails to map to the index file because the virtual memory of the instance is insufficient.
  a. Adjust the JVM memory of the SolrServer1 instance (choose **Cluster** > *Name of the desired cluster* > **Service** > **Solr** > **Configuration** > **All Configurations**. Select **SolrServer1** for **Role**, select **192.168.152.14** for **Host**, and select **JVM** in the navigation tree on the left. Change the value of the **SOLR_GC_OPTS** parameter, click **Save** in the upper left corner, and click **OK**). You can also modify the **solrconfig.xml** file of the collection by changing **NRTCachingDirectoryFactory** of **DirectoryFactory** to **NIOFSDirectoryFactory**. On the solrctl command line tool, run the **solrctl collection --reload col_test** command to make the configuration collection take effect.
  b. To restart the instance, choose **Cluster** > *Name of the desired cluster* > **Service** > **Solr** > **Instance**. Select the **SolrServer1** instance whose IP address is **192.168.152.14**. Click **More** > **Restart Instance**.
- If the abnormal stack is other exception information, perform the following operations:
  a. On the solrctl command line tool, run the **solrctl collection --reload col_test** command.
  b. If the fault fails to be rectified, choose **Cluster >** *Name of the desired cluster* **> Service** > **Solr** > **Instance** and select the **SolrServer1** instance whose IP address is **192.168.152.14**. Choose **More Actions** > **Restart instance** to restart the SolrServer1 instance.
  c. If the fault fails to be rectified after the restart, add the copy of the shard to other SolrServer instances and delete the faulty copy.

Related Information

None.

2.4.24.2 Some cores still running improperly after Overseer is optimized and restarted

Symptom

In a large cluster, after Solr is restarted, the Core recovery success rate can be above 98%. As a result, a small number of cores may still run improperly.

Possible Causes

- The total number of cores is too large. When Solr is restarted, excessive messages are sent to the **/solr/overseer/queue** queue and stacked, which may exceed the limit value of the **SOLR_OVERSEER_QUEUE_MAX_NUMCHILDREN** parameter of the Overseer queue.
- When the data volume of a single core is too large, data synchronization between a copy and a leader may time out because the Overseer message is not processed in time. The timeout parameter is **SOLR_LEADER_CONFLICT_RESOLVE_WAIT**.

Fault Locating

1. Log in to the ZooKeeper client and run the **stat /solr/overseer/queue** command to check the number of **numChildren** subnodes in the Overseer queue of Solr in ZooKeeper.
2. Log in to the host IP address in the error message as user **root**. View the **solr-host name.log** log file of SolrServer under the **/var/log/Bigdata/solr** directory, and search for the keyword "Error while trying to recover" in the log file.

Procedure

When you log in to the ZooKeeper client and run the **stat /solr/overseer/queue** command to find that the number of **numChildren** subnodes exceeds the limit value of **SOLR_OVERSEER_QUEUE_MAX_NUMCHILDREN**, perform the following operations:

1. Do not restart the entire cluster with large data volume in a large cluster. Users are advised to restart a single instance one by one to reduce the peak value of the **/solr/overseer/queue** queue.
2. Before restarting the entire Solr cluster, set **SOLR_OVERSEER_QUEUE_MAX_NUMCHILDREN** to a larger value to prevent queue from being blocked.

   If the keyword "Error while trying to recover" is found in the Solr log:

   When the data volume of the Solr core is too large, the data synchronization between the copy and the leader may time out because the Overseer message is not processed in time. You are advised to increase the value of **SOLR_LEADER_CONFLICT_RESOLVE_WAIT** from 900,000 to 1,800,000, in milliseconds.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Related Information

None.

2.4.25 Spark

2.4.25.1 Spark Core

2.4.25.1.1 Error Message "java.lang.UnsatisfiedLinkError: org.apache.hadoop.util.NativeCodeLoader.buildSupportsSnappy()Z" Is Displayed When the Snappy Compression Algorithm Is Used

Symptom

UnsatisfiedLinkError is reported when the Snappy compression algorithm is used in the application programs.

```
14/09/18 20:59:50 WARN TaskSetManager: Lost task 0.0 in stage 1.0 (TID 0, vm-183):
java.lang.UnsatisfiedLinkError: org.apache.hadoop.util.NativeCodeLoader.buildSupportsSnappy()Z
org.apache.hadoop.util.NativeCodeLoader.buildSupportsSnappy(Native Method)
org.apache.hadoop.io.compress.SnappyCodec.checkNativeCodeLoaded(SnappyCodec.java:63)
org.apache.hadoop.io.compress.SnappyCodec.getDecompressorType(SnappyCodec.java:190)
org.apache.hadoop.io.compress.CodecPool.getDecompressor(CodecPool.java:176)
org.apache.hadoop.io.SequenceFile$Reader.init(SequenceFile.java:1915)
org.apache.hadoop.io.SequenceFile$Reader.initialize(SequenceFile.java:1810)
org.apache.hadoop.io.SequenceFile$Reader.<init>(SequenceFile.java:1759)
com.spark.common.format.ProtobufFileInputFormat
$ProtobufSequenceFileRecordReader.initialize(ProtobufFileInputFormat.java:76)
org.apache.spark.rdd.NewHadoopRDD$$anon$1.<init>(NewHadoopRDD.scala:117)
org.apache.spark.rdd.NewHadoopRDD.compute(NewHadoopRDD.scala:103)
org.apache.spark.rdd.NewHadoopRDD.compute(NewHadoopRDD.scala:65)
org.apache.spark.rdd.RDD.computeOrReadCheckpoint(RDD.scala:262)
org.apache.spark.rdd.RDD.iterator(RDD.scala:229)
org.apache.spark.rdd.UnionRDD.compute(UnionRDD.scala:86)
iii·
```

Or the below error displayed:

```
Error: org.apache.spark.SparkException: Job aborted due to stage failure: Task 0 in stage 1.0 failed 4 times,
most recent failure: Lost task 0.3 in stage 1.0 (TID 7, node3): java.lang.RuntimeException: native snappy
library not available: this version of libhadoop was built without snappy support.
        at org.apache.hadoop.io.compress.SnappyCodec.checkNativeCodeLoaded(SnappyCodec.java:65)
        at org.apache.hadoop.io.compress.SnappyCodec.getDecompressorType(SnappyCodec.java:193)
        at org.apache.hadoop.io.compress.CodecPool.getDecompressor(CodecPool.java:178)
        at org.apache.hadoop.io.SequenceFile$Reader.init(SequenceFile.java:1918)
        at org.apache.hadoop.io.SequenceFile$Reader.initialize(SequenceFile.java:1813)
        at org.apache.hadoop.io.SequenceFile$Reader.<init>(SequenceFile.java:1762)
        at org.apache.hadoop.io.SequenceFile$Reader.<init>(SequenceFile.java:1776)
        at org.apache.hadoop.mapred.SequenceFileRecordReader.<init>(SequenceFileRecordReader.java:49)
        at
org.apache.hadoop.mapred.SequenceFileInputFormat.getRecordReader(SequenceFileInputFormat.java:64)
        at org.apache.spark.rdd.HadoopRDD$$anon$1.<init>(HadoopRDD.scala:239)
        at org.apache.spark.rdd.HadoopRDD.compute(HadoopRDD.scala:216)
        at org.apache.spark.rdd.HadoopRDD.compute(HadoopRDD.scala:101)
        at org.apache.spark.rdd.RDD.computeOrReadCheckpoint(RDD.scala:277)
        at org.apache.spark.rdd.RDD.iterator(RDD.scala:244)
        at org.apache.spark.rdd.MapPartitionsRDD.compute(MapPartitionsRDD.scala:35)
.........
```

Possible Causes

When Spark uses the Snappy compression algorithm, no native method can be invoked.

Fault Locating

Spark depends on data in the Hadoop Distributed File System (HDFS) and depends on YARN during the computation. Compression code for Snappy cannot be found when the Snappy compression algorithm is used in the application programs.

Procedure

Step 1 Open the **$Spark_Client/conf/spark-defaults.conf** configuration file in Spark Client.

Step 2 Add values to **spark.executor.extraJavaOptions** and **spark.driver.extraJavaOptions** parameter.

```
spark.executor.extraLibraryPath= -Djava.library.path=$HADOOP_HOME/lib/native
spark.yarn.cluster.driver.extraLibraryPath= -Djava.library.path=$HADOOP_HOME/lib/native
spark.driver.extraLibraryPath= -Djava.library.path=$HADOOP_HOME/lib/native
```

NOTE

- The value of java.library.path should exist in actual environment.
- For spark.executor.extraJavaOptions and spark.driver.extraJavaOptions parameters. need to add a space after the equals sign.

----End

Reference Information

None.

2.4.25.1.2 Error Message " Not attempting to re-login since the last re-login was attempted less than 600 seconds before" Is Displayed

Symptom

When the client submits code in security mode, the following error is reported in the driver logs when a Spark task is submitted.

```
14/09/20 15:29:31 INFO SparkUI: Started SparkUI at http://linux-18:23000
14/09/20 15:29:31 WARN NativeCodeLoader: Unable to load native-hadoop library for your platform... using
builtin-java classes where applicable
14/09/20 15:29:35 WARN UserGroupInformation: Not attempting to re-login since the last re-login was
attempted less than 600 seconds before.
14/09/20 15:29:38 WARN UserGroupInformation: Not attempting to re-login since the last re-login was
attempted less than 600 seconds before.
14/09/20 15:29:43 WARN UserGroupInformation: Not attempting to re-login since the last re-login was
attempted less than 600 seconds before.
14/09/20 15:29:46 WARN UserGroupInformation: Not attempting to re-login since the last re-login was
attempted less than 600 seconds before.
```

Or report the following error:

```
Caused by: GSSException: No valid credentials provided (Mechanism level: Clock skew too great (37))
        at sun.security.jgss.krb5.Krb5Context.initSecContext(Krb5Context.java:770)
```

```
        at sun.security.jgss.GSSContextImpl.initSecContext(GSSContextImpl.java:248)
        at sun.security.jgss.GSSContextImpl.initSecContext(GSSContextImpl.java:179)
        at com.sun.security.sasl.gsskerb.GssKrb5Client.evaluateChallenge(GssKrb5Client.java:192)
        ... 80 more
Caused by: KrbException: Clock skew too great (37)
        at sun.security.krb5.KrbKdcRep.check(KrbKdcRep.java:88)
        at sun.security.krb5.KrbTgsRep.<init>(KrbTgsRep.java:87)
        at sun.security.krb5.KrbTgsReq.getReply(KrbTgsReq.java:259)
        at sun.security.krb5.KrbTgsReq.sendAndGetCreds(KrbTgsReq.java:270)
        at sun.security.krb5.internal.CredentialsUtil.serviceCreds(CredentialsUtil.java:302)
        at sun.security.krb5.internal.CredentialsUtil.acquireServiceCreds(CredentialsUtil.java:120)
        at sun.security.krb5.Credentials.acquireServiceCreds(Credentials.java:458)
        at sun.security.jgss.krb5.Krb5Context.initSecContext(Krb5Context.java:693)
        ... 83 more
```

Possible Causes

During the Kerberos authentication, the time of the client and server need to be authenticated. If the time difference exceeds the threshold (5 minutes by default), the client cannot connect to the server.

Fault Locating

Run the **date** command to check the date and the time of the client and the server. If the time difference is larger than 5 minutes, this fault is caused by time inconsistency.

Procedure

Step 1 Install the Network Time Protocol (NTP) service on the client to synchronize the time.

Step 2 Change the time of the client manually to make the time the same as that of the server.

----End

Reference Information

None.

2.4.25.1.3 Task Is Suspended and "Initial job has not accepted any resources" Error Occurs

Symptom

A task is suspended when it is submitted in yarn-client mode on the client, and error "Initial job has not accepted any resources; check your cluster UI to ensure that workers are registered and have sufficient memory" is continuously reported.

Possible Causes

When the task is run in yarn-client mode, the Driver of the Spark application is running on the client node, which will communicate with the YARN in the cluster during task execution. Check whether:

- The Spark client is in the host list of the node to which the YARN belongs. If not, the task will be incorrectly parsed. As a result, a message indicating that the job cannot be initialized is incorrectly displayed.
- The size of the Executor memory is too large so that the NodeManager memory is insufficient for a container.

Fault Locating

1. Check whether the client IP address and host name are added to the **/etc/hosts** file of each node in the cluster. If the IP address and host name are not added to the file, modify the file and execute the application again.
2. If the fault persists, check whether the **CoarseGrainedExecutorBackend** process exists on the Executor. If the process does not exist, the problem is caused by excessive Executor memory size.

Procedure

Step 1 Add the IP address and host name of the client to the **/etc/hosts** file in each node where the YARN is deployed in the cluster.

Step 2 Reduce the Executor memory size based on the available resources in the YARN.

----End

Reference Information

None.

2.4.25.1.4 "Address already in use: Service 'SparkUI' failed after 16 retries!" Error Occurs

Symptom

The following error is reported when multiple tasks are submitted at the same time.

```
2014-09-17 15:27:04,597 INFO [main] Successfully started service 'HTTP file server' on port 23503.
org.apache.spark.Logging$class.logInfo(Logging.scala:59)
2014-09-17 15:27:04,875 WARN [main] Service 'SparkUI' could not bind on port 23000. Attempting port
23001. org.apache.spark.Logging$class.logWarning(Logging.scala:71)
2014-09-17 15:27:04,942 WARN [main] Service 'SparkUI' could not bind on port 23001. Attempting port
23002. org.apache.spark.Logging$class.logWarning(Logging.scala:71)
2014-09-17 15:27:05,003 WARN [main] Service 'SparkUI' could not bind on port 23002. Attempting port
23003. org.apache.spark.Logging$class.logWarning(Logging.scala:71)
2014-09-17 15:27:05,086 WARN [main] Service 'SparkUI' could not bind on port 23003. Attempting port
23004. org.apache.spark.Logging$class.logWarning(Logging.scala:71)
2014-09-17 15:27:05,147 WARN [main] Service 'SparkUI' could not bind on port 23004. Attempting port
23005. org.apache.spark.Logging$class.logWarning(Logging.scala:71)
2014-09-17 15:27:05,213 WARN [main] Service 'SparkUI' could not bind on port 23005. Attempting port
23006. org.apache.spark.Logging$class.logWarning(Logging.scala:71)
2014-09-17 15:27:05,275 WARN [main] Service 'SparkUI' could not bind on port 23006. Attempting port
23007. org.apache.spark.Logging$class.logWarning(Logging.scala:71)
2014-09-17 15:27:05,336 WARN [main] Service 'SparkUI' could not bind on port 23007. Attempting port
23008. org.apache.spark.Logging$class.logWarning(Logging.scala:71)
2014-09-17 15:27:05,396 WARN [main] Service 'SparkUI' could not bind on port 23008. Attempting port
23009. org.apache.spark.Logging$class.logWarning(Logging.scala:71)
2014-09-17 15:27:05,461 WARN [main] Service 'SparkUI' could not bind on port 23009. Attempting port
23010. org.apache.spark.Logging$class.logWarning(Logging.scala:71)
2014-09-17 15:27:05,523 WARN [main] Service 'SparkUI' could not bind on port 23010. Attempting port
```

```
23011. org.apache.spark.Logging$class.logWarning(Logging.scala:71)
2014-09-17 15:27:05,586 WARN [main] Service 'SparkUI' could not bind on port 23011. Attempting port
23012. org.apache.spark.Logging$class.logWarning(Logging.scala:71)
2014-09-17 15:27:05,644 WARN [main] Service 'SparkUI' could not bind on port 23012. Attempting port
23013. org.apache.spark.Logging$class.logWarning(Logging.scala:71)
2014-09-17 15:27:05,704 WARN [main] Service 'SparkUI' could not bind on port 23013. Attempting port
23014. org.apache.spark.Logging$class.logWarning(Logging.scala:71)
2014-09-17 15:27:05,763 WARN [main] Service 'SparkUI' could not bind on port 23014. Attempting port
23015. org.apache.spark.Logging$class.logWarning(Logging.scala:71)
2014-09-17 15:27:05,825 WARN [main] Service 'SparkUI' could not bind on port 23015. Attempting port
23016. org.apache.spark.Logging$class.logWarning(Logging.scala:71)
2014-09-17 15:27:05,887 ERROR [main] Failed to bind SparkUI org.apache.spark.Logging
$class.logError(Logging.scala:96)
java.net.BindException: Address already in use: Service 'SparkUI' failed after 16 retries!
at sun.nio.ch.Net.bind0(Native Method)
at sun.nio.ch.Net.bind(Net.java:444)
at sun.nio.ch.Net.bind(Net.java:436)
at sun.nio.ch.ServerSocketChannelImpl.bind(ServerSocketChannelImpl.java:214)
at sun.nio.ch.ServerSocketAdaptor.bind(ServerSocketAdaptor.java:74)
at org.eclipse.jetty.server.nio.SelectChannelConnector.open(SelectChannelConnector.java:187)
at org.eclipse.jetty.server.AbstractConnector.doStart(AbstractConnector.java:316)
at org.eclipse.jetty.server.nio.SelectChannelConnector.doStart(SelectChannelConnector.java:265)
at org.eclipse.jetty.util.component.AbstractLifeCycle.start(AbstractLifeCycle.java:64)
at org.eclipse.jetty.server.Server.doStart(Server.java:293)
ii
```

Possible Causes

Each Spark task uses a driver port, that is, SparkUI, of which the port number is 23000 by default. If the port 23000 is occupied, another port is selected in random. By default, the number of port reselection retries is 16. After the 16 retries, this task is aborted.

Fault Locating

Run the ***jps*** command to check the number of tasks that are submitted on the node. If the number of tasks exceeds 16, this fault occurs.

Procedure

Rectify the fault using the following methods:

- Add the ***conf.set("spark.port.maxRetries","100")*** statement when initializing SparkConf.
- Add ***--conf spark.port.maxRetries=100*** to the command when submitting tasks by running spark-submit.
- Add ***spark.port.maxRetries 100*** to spark-defaults.conf.

The number **100** can be replaced by any number. The larger the number is, the more the tasks are allowed to run at the same time.

Reference Information

None.

2.4.25.1.5 Task Cannot Be Supported on YARN

Symptom

The following error is reported when a Spark task is submitted.

```
Exception in thread "main" org.apache.spark.SparkException: Yarn application already ended, might be
killed or not able to launch application master.
at
org.apache.spark.scheduler.cluster.YarnClientSchedulerBackend.waitForApp(YarnClientSchedulerBackend.scal
a:111)
at org.apache.spark.scheduler.cluster.YarnClientSchedulerBackend.start(YarnClientSchedulerBackend.scala:87)
at org.apache.spark.scheduler.TaskSchedulerImpl.start(TaskSchedulerImpl.scala:141)
at org.apache.spark.SparkContext.<init>(SparkContext.scala:323)
at org.apache.spark.examples.SparkPi$.main(SparkPi.scala:28)
at org.apache.spark.examples.SparkPi.main(SparkPi.scala)
at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:57)
at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
at java.lang.reflect.Method.invoke(Method.java:606)
at org.apache.spark.deploy.SparkSubmit$.launch(SparkSubmit.scala:332)
at org.apache.spark.deploy.SparkSubmit$.main(SparkSubmit.scala:79)
at org.apache.spark.deploy.SparkSubmit.main(SparkSubmit.scala)
```

Possible Causes

YARN is faulty and Spark on YARN is not supported.

Fault Locating

None.

Procedure

View the error information on the WebUI of Application Master and contact the technical support personnel of Yarn.

Reference Information

None.

2.4.25.1.6 Failed to Exit the Application Program Due to Insufficient Memory

Symptom

If the driver memory is insufficient when a developed application program is running, the spark task is suspended and the application program cannot exit. The following error exists in the container information:

```
Exception in thread "handle-read-write-executor-1" java.lang.OutOfMemoryError: Java heap space
    at java.nio.HeapByteBuffer.<init>(HeapByteBuffer.java:57)
    at java.nio.ByteBuffer.allocate(ByteBuffer.java:331)
    at org.apache.spark.network.nio.Message$.create(Message.scala:90)
    at org.apache.spark.network.nio.ReceivingConnection$Inbox.org$apache$spark$network$nio
$ReceivingConnection$Inbox$$createNewMessage$1(Connection.scala:454)
    at org.apache.spark.network.nio.ReceivingConnection$Inbox$$anonfun$1.apply(Connection.scala:464)
    at org.apache.spark.network.nio.ReceivingConnection$Inbox$$anonfun$1.apply(Connection.scala:464)
    at scala.collection.mutable.MapLike$class.getOrElseUpdate(MapLike.scala:189)
    at scala.collection.mutable.AbstractMap.getOrElseUpdate(Map.scala:91)
    at org.apache.spark.network.nio.ReceivingConnection$Inbox.getChunk(Connection.scala:464)
```

```
at org.apache.spark.network.nio.ReceivingConnection.read(Connection.scala:541)
at org.apache.spark.network.nio.ConnectionManager$$anon$6.run(ConnectionManager.scala:198)
at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1145)
at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:615)
at java.lang.Thread.run(Thread.java:745)
```

Possible Causes

The driver memory provided to the application program is insufficient, which result in full garbage collection (GC) in the memory space. Garbage Collectors, however, cannot clear the memory space promptly. Therefore, the full GC status persists and the application program cannot exit.

Fault Locating

1. Run a command to forcibly exit the task and modify the memory parameter to ensure sufficient memory for the application program so that the task is can be successfully executed.
2. To ensure that large data volume tasks are no suspended, set the related parameter so that the system displays a message indicating that the task fails to be executed when the memory is insufficient.

Procedure

Step 1 Perform the following step to exit the application program:

1. Delete the task process from the driver of Spark.

   NOTE

   Delete the task process based on the submitted application program PID. Exercise caution when performing this operation to prevent other application programs from being deleted by mistake.

   Run the **ps -ef | grep SparkSubmit** command to query the PID of the application program.

   Run the **kill** *<PID>*command to delete the process that corresponds to the PID.

2. Run the Yarn command to delete the task process:

   yarn application -kill *<App ID>*

Step 2 You can perform the following operations to resolve the problem of insufficient memory so that the task can be successfully executed:

Set the memory parameters to the maximum values when submitting the task execution command.

bin/spark-submit --master yarn-cluster --class *com.spark.test.wordcountWithSave* ***--driver-memory*** *5g* ***--executor-memory*** *4g* /opt/hadoopclient/Spark/spark/jars/spark-test.jar *hdfs://hacluster/data.txt collect*

Set the following parameters in the driver and executor:

- Driver:--driver-memory
- Executor:--executor-memory

Step 3 (Optional) When the task requires a large number of resources but the memory is insufficient, you can set the following parameter so that the system will display a message indicating that the task fails instead of suspending the task. If you do not want to set this mechanism, skip this step.

In the client installation directory, open the **$spark_client/Spark/spark/conf/spark-defaults.conf** file and add the parameter named **spark.yarn.appMasterEnv.SPARK_USE_CONC_INCR_GC**, set the value to **true**.

Example:

cd /opt/spark_client/Spark/spark/conf

vi spark-defaults.conf

Add the following:

```
spark.yarn.appMasterEnv.SPARK_USE_CONC_INCR_GC=true
```

Resubmit the application program. When the memory is insufficient, the application program is not suspended and a task execution failure message is displayed.

----End

Reference Information

None.

2.4.25.1.7 Failed to Run an Application Because of Insufficient Disk Space

Symptom

The following error occurs when an application developed using Spark is run:

```
Job aborted due to stage failure: Task 0 in stage 42.0 failed 4 times, most recent failure: Lost task 0.3 in
stage 42.0
(TID 25082, linux-245): com.esotericsoftware.kryo.KryoException: java.io.IOException: No space left on device
        com.esotericsoftware.kryo.io.Output.flush(Output.java:157)
        com.twitter.chill.Tuple2Serializer.write(TupleSerializers.scala:37)
        com.twitter.chill.Tuple2Serializer.write(TupleSerializers.scala:34)
        com.esotericsoftware.kryo.Kryo.writeClassAndObject(Kryo.java:568)
        org.apache.spark.serializer.KryoSerializationStream.writeObject(KryoSerializer.scala:119)
        org.apache.spark.storage.DiskBlockObjectWriter.write(BlockObjectWriter.scala:195)
        org.apache.spark.util.collection.ExternalSorter$$anonfun$writePartitionedFile$4$$anonfun$apply
$2.apply(ExternalSorter.scala:732)
        org.apache.spark.util.collection.ExternalSorter$$anonfun$writePartitionedFile$4$$anonfun$apply
$2.apply(ExternalSorter.scala:731)
        scala.collection.Iterator$class.foreach(Iterator.scala:727)
        org.apache.spark.util.collection.ExternalSorter$IteratorForPartition.foreach(ExternalSorter.scala:789
```

Possible Causes

During application development using Spark, if a shuffle operation is performed, shuffle data will be saved to the local computer. If the parameter spark.default.parallelism is not configured, the number of tasks generated after the shuffle operation is complete is the same as the number of tasks before the shuffle operation. If there are excessive number of concurrent tasks, the data may be lost.

Fault Locating

None.

Procedure

If this fault occurs, you can perform the following steps to rectify it:

Step 1 Modify the YARN configuration to expand the disk capacity for storing data during application development

On FusionInsight Manager, choose **Cluster** > *Name of the desired cluster* > **Service** > **Yarn** > **Configuration**, click **All Configurations**, type **yarn.nodemanager.local-dirs** in the search box to find the configuration item. Modify the configuration item to expand the disk capacity.

NOTE

- When increasing the number of disks, use commas (,) to separate disk paths.
- The specifications of disks, that is, disk capacity, must be the same; otherwise, this fault persists.

Step 2 Save the settings and restart the YARN service for the settings to take effect.

Step 3 Resubmit the application. The fault is rectified.

----End

Reference Information

None.

2.4.25.1.8 Out-of-Memory Is Displayed When A Huge Amount of Data Is Returned to the Driver

Symptom

Running the SQL in client by using JDBCServer application. The Driver exit abnormally, and the error information is displayed in JDBCServer log.

```
2015-11-24 18:29:33,393 ERROR [org.apache.spark.util.Utils] Uncaught exception in thread task-result-getter-3
java.lang.OutOfMemoryError: Java heap space
    at java.io.ObjectInputStream$HandleTable.grow(ObjectInputStream.java:3469)
    at java.io.ObjectInputStream$HandleTable.assign(ObjectInputStream.java:3275)
    at java.io.ObjectInputStream.readArray(ObjectInputStream.java:1674)
    at java.io.ObjectInputStream.readObject0(ObjectInputStream.java:1345)
    at java.io.ObjectInputStream.defaultReadFields(ObjectInputStream.java:1993)
    at java.io.ObjectInputStream.readSerialData(ObjectInputStream.java:1918)
    at java.io.ObjectInputStream.readOrdinaryObject(ObjectInputStream.java:1801)
    at java.io.ObjectInputStream.readObject0(ObjectInputStream.java:1351)
    at java.io.ObjectInputStream.readArray(ObjectInputStream.java:1707)
    at java.io.ObjectInputStream.readObject0(ObjectInputStream.java:1345)
    at java.io.ObjectInputStream.readObject(ObjectInputStream.java:371)
    at org.apache.spark.serializer.JavaDeserializationStream.readObject(JavaSerializer.scala:72)
    at org.apache.spark.serializer.JavaSerializerInstance.deserialize(JavaSerializer.scala:92)
    at org.apache.spark.scheduler.DirectTaskResult.value(TaskResult.scala:97)
    at org.apache.spark.scheduler.TaskResultGetter$$anon$2$$anonfun$run$1.apply$mcV
$sp(TaskResultGetter.scala:60)
    at org.apache.spark.scheduler.TaskResultGetter$$anon$2$$anonfun$run
```

```
$1.apply(TaskResultGetter.scala:51)
    at org.apache.spark.scheduler.TaskResultGetter$$anon$2$$anonfun$run
$1.apply(TaskResultGetter.scala:51)
    at org.apache.spark.util.Utils$.logUncaughtExceptions(Utils.scala:1701)
    at org.apache.spark.scheduler.TaskResultGetter$$anon$2.run(TaskResultGetter.scala:50)
    at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1142)
    at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:617)
    at java.lang.Thread.run(Thread.java:745)
```

In the client, the error information is shown as **Figure 2-20**.

Figure 2-20 Error in client

```
0: jdbc:hive2://ha-cluster> select imei from t11 group by imei;
15/11/24 18:30:04 INFO ZkWatcher: Get event: SyncConnected, the node was deleted successfully.
Error: org.apache.thrift.transport.TTransportException: SASL authentication not complete (state=08S01,code=0)
0: jdbc:hive2://ha-cluster> 15/11/24 18:30:04 ERROR ZkWatcher: Error in close the connection:
java.sql.SQLException: Error while cleaning up the server resources
        at org.apache.hive.jdbc.HiveConnection.close(HiveConnection.java:833)
        at org.apache.hive.jdbc.utils.ZkWatcher.process(ZkWatcher.java:58)
        at org.apache.zookeeper.ClientCnxn$EventThread.processEvent(ClientCnxn.java:592)
        at org.apache.zookeeper.ClientCnxn$EventThread.run(ClientCnxn.java:566)
Caused by: org.apache.thrift.transport.TTransportException: java.net.SocketException: Connection reset
        at org.apache.thrift.transport.TIOStreamTransport.read(TIOStreamTransport.java:129)
        at org.apache.thrift.transport.TTransport.readAll(TTransport.java:86)
        at org.apache.thrift.transport.TSaslTransport.readLength(TSaslTransport.java:376)
        at org.apache.thrift.transport.TSaslTransport.readFrame(TSaslTransport.java:453)
        at org.apache.thrift.transport.TSaslTransport.read(TSaslTransport.java:435)
        at org.apache.thrift.transport.TSaslClientTransport.read(TSaslClientTransport.java:37)
        at org.apache.thrift.transport.TTransport.readAll(TTransport.java:86)
        at org.apache.thrift.protocol.TBinaryProtocol.readAll(TBinaryProtocol.java:429)
        at org.apache.thrift.protocol.TBinaryProtocol.readI32(TBinaryProtocol.java:318)
        at org.apache.thrift.protocol.TBinaryProtocol.readMessageBegin(TBinaryProtocol.java:219)
        at org.apache.thrift.TServiceClient.receiveBase(TServiceClient.java:69)
        at org.apache.hive.service.cli.thrift.TCLIService$Client.recv_CloseSession(TCLIService.java:179)
        at org.apache.hive.service.cli.thrift.TCLIService$Client.CloseSession(TCLIService.java:166)
        at org.apache.hive.jdbc.HiveConnection.close(HiveConnection.java:831)
        ... 3 more
Caused by: java.net.SocketException: Connection reset
        at java.net.SocketInputStream.read(SocketInputStream.java:154)
        at java.net.SocketInputStream.read(SocketInputStream.java:141)
        at java.io.BufferedInputStream.fill(BufferedInputStream.java:246)
        at java.io.BufferedInputStream.read1(BufferedInputStream.java:286)
        at java.io.BufferedInputStream.read(BufferedInputStream.java:345)
        at org.apache.thrift.transport.TIOStreamTransport.read(TIOStreamTransport.java:127)
        ... 16 more
```

Possible Causes

Through log analysis, it is found that the memory is insufficient if an Out-of-Memory error occurs when the Driver runs the task-result-getter-3 thread to obtain data. This results in suspension of the JDBCServer service.

Generally, the SQL query result is returned to the Driver. If the SQL query data volume is huge, a huge amount of data will be returned to the Driver.

The size limit of the returned data is determined by **spark.driver.maxResultSize**. If the size of returned data exceeds the specified limit, the Job will generate an abnormal abort but this does not result in suspension of the JDBCServer service. In this example, the memories of the Driver and the value of **spark.driver.maxResultSize** are both 1 GB. However, other objects in the Driver process may also consume memory resources. As a result, a memory overflow occurs when the data volume obtained by the Driver has not reached 1 GB, resulting in suspension of the JDBCServer service.

Fault Locating

None.

Procedure

Two methods can be used to resolve this issue. One is to increase the memory of the Driver, and the other is to restrict the size of the data returned to the Driver.

Step 1 Use either of the following methods to modify the memory size of the Driver based on the actual situation of applications:

- Add **spark.driver.memory 20g** to the **spark-defaults.conf** file of CLASSPATH.
- Add **--driver-memory 20g** to the command when starting the Spark application.

Step 2 Set an appropriate limit for data returned to the Driver.

```
spark.driver.maxResultSize=256m
```

NOTE

A value less than the memory size of the Driver is recommended.

Step 3 Restart the Spark application for the modification to take effect.

----End

Reference Information

For the **spark.driver.maxResultSize** parameter details, see **http://spark.apache.org/docs/1.5.1/configuration.html**

2.4.25.1.9 An Application Fails Upon Startup Because Many Executors Are Lost

Symptom

When the number of executors is set to 40 and the memory is 1 GB, the jobs submitted on YARN are temporarily stopped after the JDBCServer starts. If there are no permanent Spark SQL jobs, the Spark SQL function becomes unavailable. What should I do in this case?

Possible Causes

- Check whether JDK1.8 is used in the MRS cluster server environment. Since JDK1.8, class metadata is used to replace the original control associated with permanent generation. The class metadata is divided into two parts, namely, Metaspace and Compressed Class Space. By default, the size of Compressed Class Space is 1 GB. Therefore, the virtual memory the JDK1.8 applies for may exceed the specified limit.
- The YARN monitors the virtual memory usage of each container. If the memory usage of the container exceeds the limit specified by **yarn.nodemanager.vmem-pmem-ratio** * **spark.yarn.am.memory**, then the YARN kills the container.
- Every time an executor starts, the AM needs to apply for resources from the YARN. As a result, the required memory and virtual memory significantly increases along with the number of executors. To prevent the AM from being killed by the YARN, you need to set the memory of AM to a larger value.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Fault Locating

None.

Procedure

To resolve the issue, perform the following steps:

Step 1 Run the common Spark tasks (for example, SparkPi). If many executors are lost when the number of executors is set to 40 and the memory is set to 1 GB, run the following command:

```
./spark-submit --class org.apache.spark.examples.SparkPi --master yarn --num-executors 40 --executor-memory 1G ../jars/original-spark-examples_2.11-2.1.0.jar
```

Step 2 Analyze the NodeManager log of YARN. If the virtual memory usage of container_1437473621109_0194_01_000001 exceeds the upper limit and it is killed, the log is as follows:

```
2015-07-22 15:29:59,103 | WARN  | Container Monitor | Container [pid=28855,containerID=container_1437473621109_0194_01_000001] is running beyond virtual memory limits. Current usage: 365.8 MB of 1 GB physical memory used; 2.5 GB of 2.5 GB virtual memory used. Killing container.
```

Step 3 Analyze the task run log. If container_1437473621109_0194_01_000001 is the one that maps to the AM, the executors are lost after the AM is killed.

Step 4 Change the memory of the AM to 5 GB, and run the following command to check whether the application works properly:

```
./spark-submit --class org.apache.spark.examples.SparkPi --master yarn --num-executors 40 --executor-memory 1G --conf spark.yarn.am.memory=5g ../jars/original-spark-examples_2.11-2.1.0.jar
```

Before JDBCServer startup, add the configuration item **spark.yarn.am.memory=5g**. This can ensure that the service starts properly.

----End

References

None.

2.4.25.1.10 Errors Occur When an Ultra-Large Result Set Is Being Collected to Driver

Symptom

While an ultra-large result set is being collected to Driver, the following errors are observed:

- The out of memory (OOM) error occurs, accompanied by the following log information:

```
java.lang.OutOfMemoryError: GC overhead limit exceeded
16/01/25 12:08:56 WARN AkkaRpcEndpointRef: Error sending message [message = RemoveBroadcast(69,true)] in 1 attempts
org.apache.spark.rpc.RpcTimeoutException: Recipient[Actor[akka://sparkDriver/user/BlockManagerMaster#366390194]] had
already been terminated.. This timeout is controlled by spark.rpc.askTimeout
    at org.apache.spark.rpc.RpcTimeout.org$apache$spark$rpc$RpcTimeout$$createRpcTimeoutException(RpcEnv.scala:214)
    at org.apache.spark.rpc.RpcTimeout$$anonfun$addMessageIfTimeout$1.applyOrElse(RpcEnv.scala:229)
```

```
    at org.apache.spark.rpc.RpcTimeout$$anonfun$addMessageIfTimeout
$1.applyOrElse(RpcEnv.scala:225)
    at scala.runtime.AbstractPartialFunction.apply(AbstractPartialFunction.scala:33)
    at scala.util.Failure$$anonfun$recover$1.apply(Try.scala:185)
    at scala.util.Try$.apply(Try.scala:161)
    at scala.util.Failure.recover(Try.scala:185)
    at scala.concurrent.Future$$anonfun$recover$1.apply(Future.scala:324)
    at scala.concurrent.Future$$anonfun$recover$1.apply(Future.scala:324)
    at scala.concurrent.impl.CallbackRunnable.run(Promise.scala:32)
    at org.spark-project.guava.util.concurrent.MoreExecutors
$SameThreadExecutorService.execute(MoreExecutors.java:293)
    at scala.concurrent.impl.ExecutionContextImpl$$anon$1.execute(ExecutionContextImpl.scala:133)
    at scala.concurrent.impl.CallbackRunnable.executeWithValue(Promise.scala:40)
    at scala.concurrent.impl.Promise$DefaultPromise.scala$concurrent$impl$Promise$DefaultPromise$
$dispatchOrAddCallback(Promise.scala:280)
    at scala.concurrent.impl.Promise$DefaultPromise.onComplete(Promise.scala:270)
    at scala.concurrent.Future$class.recover(Future.scala:324)
    at scala.concurrent.impl.Promise$DefaultPromise.recover(Promise.scala:153)
    at org.apache.spark.rpc.akka.AkkaRpcEndpointRef.ask(AkkaRpcEnv.scala:319)
    at org.apache.spark.rpc.RpcEndpointRef.askWithRetry(RpcEndpointRef.scala:100)
    at org.apache.spark.rpc.RpcEndpointRef.askWithRetry(RpcEndpointRef.scala:77)
```

- If data skew appears in the result set and some data blocks each is larger than 2 GB, Kryo reports the NegativeArraySizeException error during serialization. The following is the log information generated at the time of error:

```
16/02/16 16:55:13 WARN TaskSetManager: Lost task 750.0 in stage 66.0 (TID 33887, datasight-192):
com.esotericsoftware.kryo.KryoException: java.lang.NegativeArraySizeException
Serialization trace:
values (org.apache.spark.sql.catalyst.expressions.GenericRowWithSchema)
        at com.esotericsoftware.kryo.serializers.FieldSerializer$ObjectField.write(FieldSerializer.java:585)
        at com.esotericsoftware.kryo.serializers.FieldSerializer.write(FieldSerializer.java:213)
        at com.esotericsoftware.kryo.Kryo.writeClassAndObject(Kryo.java:568)
        at com.esotericsoftware.kryo.serializers.DefaultArraySerializers
$ObjectArraySerializer.write(DefaultArraySerializers.java:318)
        at com.esotericsoftware.kryo.serializers.DefaultArraySerializers
$ObjectArraySerializer.write(DefaultArraySerializers.java:293)
        at com.esotericsoftware.kryo.Kryo.writeClassAndObject(Kryo.java:568)
        at org.apache.spark.serializer.KryoSerializerInstance.serialize(KryoSerializer.scala:260)
        at org.apache.spark.executor.Executor$TaskRunner.run(Executor.scala:240)
        at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1142)
        at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:617)
        at java.lang.Thread.run(Thread.java:745)
Caused by: java.lang.NegativeArraySizeException
        at com.esotericsoftware.kryo.util.IdentityObjectIntMap.resize(IdentityObjectIntMap.java:409)
        at com.esotericsoftware.kryo.util.IdentityObjectIntMap.putStash(IdentityObjectIntMap.java:227)
        at com.esotericsoftware.kryo.util.IdentityObjectIntMap.push(IdentityObjectIntMap.java:221)
        at com.esotericsoftware.kryo.util.IdentityObjectIntMap.put(IdentityObjectIntMap.java:117)
        at com.esotericsoftware.kryo.util.IdentityObjectIntMap.putStash(IdentityObjectIntMap.java:228)
        at com.esotericsoftware.kryo.util.IdentityObjectIntMap.push(IdentityObjectIntMap.java:221)
        at com.esotericsoftware.kryo.util.IdentityObjectIntMap.put(IdentityObjectIntMap.java:117)
        at
com.esotericsoftware.kryo.util.MapReferenceResolver.addWrittenObject(MapReferenceResolver.java:23)
        at com.esotericsoftware.kryo.Kryo.writeReferenceOrNull(Kryo.java:598)
```

Possible Causes

- OOM error of Driver

  The procedure for collecting results to Driver and printing the results is divided into two phases. At phase 1, an array stores results collected from various nodes. At phase 2, the results are converted into the printable format and then printed on graphical user interface. The results are stored in memory as java objects and demand many memory resources. Moreover, many intermediate arrays are generated during format conversion, further increasing the demand for memory resources. All these factors together have led to a high risk of OOM error.

- NegativeArraySizeException error reported by Kryo during serialization

  Spark places a 2-GB limit on the size of data to be serialized at a time. If data size exceeds 2 GB, the NegativeArraySizeException error is reported.

Fault Locating

None.

Procedure

To resolve this issue, take the following methods:

- Method 1: Write the large result set into HDFS instead of collecting them to Driver, in order to avoid the OOM error.
- Method 2: If method 1 is not used, set the **spark.serializer** in the Spark client configuration file **spark-defaults.conf** to **org.apache.spark.serializer.JavaSerializer** to avoid the NegativeArraySizeException error. If you have used method 1 to mitigate the OOM error, then the NegativeArraySizeException error will not occur.

References

None.

2.4.25.1.11 Executor Log Shows that the Physical Memory Usage Exceeds the Maximal Value

Symptom

In the following scenarios, the Executor log shows that the physical memory usage exceeds the maximal value:

- When the TPC-H 21 test case is run in the 100 T-data environment, the following error information is displayed:

  The following is the Spark Executor log information generated at the time of error:

  ```
  2016-03-07 15:17:10,221 | ERROR | [SIGTERM handler] | RECEIVED SIGNAL 15: SIGTERM |
  org.apache.spark.util.SignalLoggerHandler.handle(SignalLogger.scala:57)
  ```

  The following is the YARN NodeManager log information generated at the time of error:

  ```
  ERROR | [dispatcher-event-loop-28] | Lost executor 471 on 10-196-33-3: Yarn deallocated the
  executor 471
  (container container_e04_1456978747173_0063_01_000473) | org.apache.spark.Logging
  $class.logError(Logging.scala:75)
  2016-03-07 15:05:24,704 | WARN | [Reporter] | Container killed by YARN for exceeding memory limits.
  22.0 GB of 22 GB physical
  memory used. Consider boosting spark.yarn.executor.memoryOverhead. | org.apache.spark.Logging
  $class.logWarning(Logging.scala:71)
  ```

- When the TPC-H 22 test case is run in the 100 T-data environment, the following error information is displayed:

  The following is the Spark Driver log information generated at the time of error:

  ```
  org.apache.spark.shuffle.FetchFailedException: java.lang.OutOfMemoryError: Direct buffer memory
  at
  ```

```
org.apache.spark.storage.ShuffleBlockFetcherIterator.throwFetchFailedException(ShuffleBlockFetcherIte
rator.scala:339)
at org.apache.spark.storage.ShuffleBlockFetcherIterator.next(ShuffleBlockFetcherIterator.scala:324)
at org.apache.spark.storage.ShuffleBlockFetcherIterator.next(ShuffleBlockFetcherIterator.scala:52)
at scala.collection.Iterator$$anon$14.hasNext(Iterator.scala:389)
at scala.collection.Iterator$$anon$11.hasNext(Iterator.scala:327)
at scala.collection.Iterator$$anon$13.hasNext(Iterator.scala:371)
at scala.collection.Iterator$$anon$11.hasNext(Iterator.scala:327)
at org.apache.spark.util.CompletionIterator.hasNext(CompletionIterator.scala:32)
at org.apache.spark.InterruptibleIterator.hasNext(InterruptibleIterator.scala:39)
at org.apache.spark.util.collection.ExternalSorter.insertAll(ExternalSorter.scala:217)
at org.apache.spark.shuffle.hash.HashShuffleReader.read(HashShuffleReader.scala:110)
at org.apache.spark.rdd.ShuffledRDD.compute(ShuffledRDD.scala:90)
at org.apache.spark.rdd.RDD.computeOrReadCheckpoint(RDD.scala:301)
at org.apache.spark.rdd.RDD.iterator(RDD.scala:265)
at org.apache.spark.rdd.MapPartitionsRDD.compute(MapPartitionsRDD.scala:38)
at org.apache.spark.rdd.RDD.computeOrReadCheckpoint(RDD.scala:301)
at org.apache.spark.rdd.RDD.iterator(RDD.scala:265)
at org.apache.spark.rdd.MapPartitionsRDD.compute(MapPartitionsRDD.scala:38)
at org.apache.spark.rdd.RDD.computeOrReadCheckpoint(RDD.scala:301)
at org.apache.spark.rdd.RDD.iterator(RDD.scala:265)
at org.apache.spark.scheduler.ShuffleMapTask.runTask(ShuffleMapTask.scala:75)
at org.apache.spark.scheduler.ShuffleMapTask.runTask(ShuffleMapTask.scala:42)
at org.apache.spark.scheduler.Task.run(Task.scala:90)
at org.apache.spark.executor.Executor$TaskRunner.run(Executor.scala:229)
at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1142)
at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:617)
at java.lang.Thread.run(Thread.java:745)
Caused by: io.netty.handler.codec.DecoderException: java.lang.OutOfMemoryError: Direct buffer
memory
at io.netty.handler.codec.ByteToMessageDecoder.channelRead(ByteToMessageDecoder.java:234)
at
io.netty.channel.AbstractChannelHandlerContext.invokeChannelRead(AbstractChannelHandlerContext.j
ava:308)
at
io.netty.channel.AbstractChannelHandlerContext.fireChannelRead(AbstractChannelHandlerContext.java
:294)
at io.netty.channel.DefaultChannelPipeline.fireChannelRead(DefaultChannelPipeline.java:846)
at io.netty.channel.nio.AbstractNioByteChannel$NioByteUnsafe.read(AbstractNioByteChannel.java:131)
at io.netty.channel.nio.NioEventLoop.processSelectedKey(NioEventLoop.java:511)
at io.netty.channel.nio.NioEventLoop.processSelectedKeysOptimized(NioEventLoop.java:468)
at io.netty.channel.nio.NioEventLoop.processSelectedKeys(NioEventLoop.java:382)
at io.netty.channel.nio.NioEventLoop.run(NioEventLoop.java:354)
at io.netty.util.concurrent.SingleThreadEventExecutor$2.run(SingleThreadEventExecutor.java:111)
... 1 more
Caused by: java.lang.OutOfMemoryError: Direct buffer memory
at java.nio.Bits.reserveMemory(Bits.java:658)
at java.nio.DirectByteBuffer.<init>(DirectByteBuffer.java:123)
at java.nio.ByteBuffer.allocateDirect(ByteBuffer.java:311)
at io.netty.buffer.PoolArena$DirectArena.newChunk(PoolArena.java:645)
at io.netty.buffer.PoolArena.allocateNormal(PoolArena.java:228)
at io.netty.buffer.PoolArena.allocate(PoolArena.java:212)
at io.netty.buffer.PoolArena.reallocate(PoolArena.java:358)
at io.netty.buffer.PooledByteBuf.capacity(PooledByteBuf.java:121)
at io.netty.buffer.AbstractByteBuf.ensureWritable(AbstractByteBuf.java:251)
at io.netty.buffer.AbstractByteBuf.writeBytes(AbstractByteBuf.java:849)
at io.netty.buffer.AbstractByteBuf.writeBytes(AbstractByteBuf.java:841)
at io.netty.buffer.AbstractByteBuf.writeBytes(AbstractByteBuf.java:831)
at io.netty.handler.codec.ByteToMessageDecoder$1.cumulate(ByteToMessageDecoder.java:92)
at io.netty.handler.codec.ByteToMessageDecoder.channelRead(ByteToMessageDecoder.java:228)
... 10 more
```

Possible Causes

Because the off-heap memory occupied by Executor exceeds the maximal value, NodeManager task is terminated or the error "Applying for off-heap memory fails" occurs.

Fault Locating

None.

Procedure

Add the following two parameters in the **spark-defaults.conf** configuration file of Spark client or specify the following two parameters in the submitted command by adding "--conf", to increase the value of memoryOverheads or reduce the value of executor cores.

- spark.executor.memoryOverhead: configuring off-heap Memory.
- spark.executor.cores: configuring the number of Executor cores.

Reference

None.

2.4.25.1.12 When the Big data Is Processed, the Error "Channel idle timeout" Occurs

Symptom

When the tpcds test is run in the 10-node cluster and 30 T-data environment, the following error occurs:

```
Connection to 10.10.10.1 has been quiet for 123450 ms while there are still 5 outstanding requests.
Assuming connection is dead; please adjust spark.network.timeout if this is wrong.
```

Possible Causes

When Map Server is highly occupied, the requests sent by Reduce Client are not responded. When the waiting time for the response exceeds a threshold, an error occurs. The default threshold time is 120s.

Fault Locating

None

Procedure

The error occurs when the number of requests is large, which is normal. There are following two solutions:

- Enlarge the value of spark.shuffle.io.connectionTimeout. Configure the time of TPCDS test in the 10-node and 30 T-data environment as 2000s, and running is normal. Use the parameter with spark.network.timeout, first use the parameter value configured in spark.shuffle.io.connectionTimeout. If spark.shuffle.io.connectionTimeout is not configured, use the parameter value of spark.network.timeout.
- Enlarge the value of spark.shuffle.io.serverThreads. Set the value to the double of the number of cores.

References

None.

2.4.25.1.13 Spark Job Fails and Physical Memory Overflow of ApplicationMaster

Symptom

A Spark job on YARN fails, and the physical memory of ApplicationMaster overflows. The following is the error information generated at the time of overflow:

```
2016-05-12 19:27:18,078 | WARN  | Container Monitor | Container [pid=205193,containerID=container_1462240697997_3649_01_000001] is running beyond physical memory limits. Current usage: 4.5 GB of 4.5 GB physical memory used; 6.8 GB of 22.5 GB virtual memory used. Killing container.
```

Possible Causes

Logs show that the container process is forcibly killed because NodeManager detects that ApplicationMaster has run beyond physical memory limits.

Fault Locating

None.

Procedure

Increase memoryOverhead by adjusting the values of the following parameters in the Spark client configuration file **spark-defaults.conf** or in the "--conf" option of the job submission command:

- spark.driver.memoryOverhead

  Indicates off-heap memory and used if the deploy mode of Spark is cluster.
- spark.yarn.am.memoryOverhead

  Indicates off-heap memory and used if the deploy mode of Spark is client.

References

None.

2.4.25.1.14 "BlockNotFoundException" Error Occurs and the Stage Retries During the Running of Jobs

Symptom

"**BlockNotFoundException**" error occurs and the stage retries during the running of jobs.

```
java.lang.RuntimeException: org.apache.spark.storage.BlockNotFoundException: Block rdd_2_18599 not found
        at org.apache.spark.storage.BlockManager.getBlockData(BlockManager.scala:338)
        at org.apache.spark.storage.BlockManager$$anonfun$getBlockData$2.apply(BlockManager.scala:348)
        at org.apache.spark.storage.BlockManager$$anonfun$getBlockData$2.apply(BlockManager.scala:348)
        at scala.collection.TraversableLike$$anonfun$map$1.apply(TraversableLike.scala:244)
        at scala.collection.TraversableLike$$anonfun$map$1.apply(TraversableLike.scala:244)
        at scala.collection.IndexedSeqOptimized$class.foreach(IndexedSeqOptimized.scala:33)
        at scala.collection.mutable.ArrayOps$ofRef.foreach(ArrayOps.scala:108)
        at scala.collection.TraversableLike$class.map(TraversableLike.scala:244)
        at scala.collection.mutable.ArrayOps$ofRef.map(ArrayOps.scala:108)
        at org.apache.spark.storage.BlockManager.getBlockData(BlockManager.scala:348)
        at org.apache.spark.network.netty.NettyBlockRpcServer.receive(NettyBlockRpcServer.scala:81)
        at org.apache.spark.network.server.TransportRequestHandler.processRpcRequest(TransportRequestHandler.ja
va:128)
        at org.apache.spark.network.server.TransportRequestHandler.handle(TransportRequestHandler.java:99)
        at org.apache.spark.network.server.TransportChannelHandler.channelRead0(TransportChannelHandler.java:10
```

Possible Cause

Insufficient memory of BlockManager in the Executor causes the block data dropping from the memory. The current stage cannot obtain the block data and the last stage retries and generates the corresponding block data.

Fault Locating

None.

Procedure

Log in to the FusionInsight Manager, choose **Cluster > Services > Spark > Configurations**, choose **All Configurations**, enter the parameter name **spark.executor.memory** in the search box, and then expand the Executor memory of the cluster..

References

None.

2.4.25.1.15 JobHistory Restarts Frequently

Symptom

After Spark tasks are run for multiple times, the JobHistory restarts frequently. In the log, **Full GC** is continuously printed as follows:

```
2016-08-25T19:36:45.112+0800: 418.008: [Full GC (Ergonomics) [PSYoungGen: 219648K-
>216168K(285184K)] [ParOldGen: 699130K->699130K(699392K)] 918778K->915299K(984576K),
[Metaspace: 50558K->50558K(1093632K)], 0.2660435 secs] [Times: user=6.28 sys=0.00, real=0.26 secs
```

Possible Causes

If the memory of JobHistory is the default value, that is, 4 GB, the number of stageUIData to be loaded and the size of each stageUIData are too large, the Full GC will be printed frequently, causing JobHistory frequently restarts.

Fault Locating

None

Procedure

Increase the memory parameter value of JobHistory.

On FusionInsight Manager, choose **Cluster > Services > Spark > Configurations** and click **All Configurations**. Type SPARK_DAEMON_MEMORY in the search box to find the configuration item. Modify the configuration item to adjust the JobHistory capacity.

References

None

2.4.25.1.16 During Shuffle Process, the Broken Pipe Exception or Timeout Causing Application Failure

Problem Description

In the shuffle process, stage retry attempts fail for multiple times, causing the application running failure. In the executor logs, there are a large number of **java.io.IOException:Connection timed out** and **Broken pipe** exception messages.

The timeout error logs are as follows:

```
2016-10-19 00:02:18,198 | ERROR | [shuffle-client-2] | Connection to /192.168.168.15:23301 has been quiet for 600000 ms while there are outstanding requests. Assuming connection is dead; please adjust spark.network.timeout if this is wrong. | org.apache.spark.network.server.TransportChannelHandler.userEventTriggered(TransportChannelHandler.java:128)
```

The Broken pipe error logs are as follows:

```
2016-10-19 00:03:56,864 | ERROR | [shuffle-server-4] | Error sending result RpcResponse{requestId=8767424179172197974, body=NioManagedBuffer{buf=java.nio.HeapByteBuffer[pos=0 lim=2597 cap=2597]}} to /192.168.175.14:18079; closing connection | org.apache.spark.network.server.TransportRequestHandler$2.operationComplete(TransportRequestHandler.java:170)
java.io.IOException: Broken pipe
at sun.nio.ch.FileDispatcherImpl.write0(Native Method)
at sun.nio.ch.SocketDispatcher.write(SocketDispatcher.java:47)
at sun.nio.ch.IOUtil.writeFromNativeBuffer(IOUtil.java:93)
at sun.nio.ch.IOUtil.write(IOUtil.java:65)
at sun.nio.ch.SocketChannelImpl.write(SocketChannelImpl.java:471)
at org.apache.spark.network.protocol.MessageWithHeader.copyByteBuf(MessageWithHeader.java:105)
at org.apache.spark.network.protocol.MessageWithHeader.transferTo(MessageWithHeader.java:79)
at io.netty.channel.socket.nio.NioSocketChannel.doWriteFileRegion(NioSocketChannel.java:254)
at io.netty.channel.nio.AbstractNioByteChannel.doWrite(AbstractNioByteChannel.java:237)
```

Possible Cause

In the shuffle process, a large amount of data are being exchanged. The network I/O is too high, causing high packet loss rate of network adapter or switch. The following problems occur in Spark:

TCP is unavailable and shuffle-server fails to write data blocks to the TCP link. As a result, shuffle-client fails to read the data and a large number of **Broken pipe** or **Connection timed out** exceptions occur. After the abnormality occurs, Spark timeout check mechanism is triggered and Spark re-establish a link to remotely read data blocks.

Fault Locating

None.

Procedure

Use either of the following solutions to reduce the probability of exceptions:

- Modify the **/etc/sysctl.conf** file. The recommended configurations are **net.ipv4.tcp_keepalive_time**= **15**, **net.ipv4.tcp_keepalive_probes** = **10**, and **net.ipv4.tcp_keepalive_intvl**= **30**. After parameters are configured, run the **sysctl -p** *command as the root user* to make the configuration take effect.

  NOTE

  Generally, you are advised to set parameters to meet the following conditions:

  net.ipv4.tcp_keepalive_time +**net.ipv4.tcp_keepalive_probes** ***net.ipv4.tcp_keepalive_intvl**<**spark.network.timeout**. To set the parameters, log in to FusionInsight Manager, click **Cluster > Services > Spark > Configurations**, click **All Configurations**, enter the parameter name **spark.network.timeout** in the search box, and then set the value of the parameter.

- To increase the value of the **spark.shuffle.io.maxRetries** parameter, log in to the FusionInsight Manager, choose **Cluster > Services > Spark > Configurations**, choose **All Configurations**, enter the parameter name **spark.shuffle.io.maxRetrie** in the search box, and then modify the value of the parameter. A value ranging from **5** to **10** is recommended.

Reference

None.

2.4.25.2 Spark SQL and DataFrame

2.4.25.2.1 Failed to Delete HDFS Data by Running Delete or Drop Command in the Spark SQL

Symptom

In security mode, an error occurs when the ***delete*** or ***drop*** command is run in Spark SQL to delete data of the specified files in HDFS.

```
javax.security.sasl.SaslException: GSS initiate failed [Caused by GSSException: No valid credentials provided
(Mechanism level: Failed to find any Kerberos tgt)]
        at com.sun.security.sasl.gsskerb.GssKrb5Client.evaluateChallenge(GssKrb5Client.java:211)
        at org.apache.hadoop.security.SaslRpcClient.saslConnect(SaslRpcClient.java:418)
        at org.apache.hadoop.ipc.Client$Connection.setupSaslConnection(Client.java:581)
        at org.apache.hadoop.ipc.Client$Connection.access$1900(Client.java:394)
        at org.apache.hadoop.ipc.Client$Connection$2.run(Client.java:764)
        at org.apache.hadoop.ipc.Client$Connection$2.run(Client.java:760)
```

Possible Causes

HDFS authentication credential has expired.

Fault Locating

None.

Procedure

The data of the specified files in HDFS need to be manually deleted by users.

Log in to the HDFS and delete the data of the specified path file by using ***hdfs dfs -rm*** *<path>* or ***hadoop fs -rm*** *<path>*.

NOTE

If HDFS is unavailable or the network is disconnected, check whether the data of specified files in HDFS is deleted successfully before running the ***delete*** or ***drop*** command in Spark SQL. If the data is not deleted successfully, delete it by using the ***delete*** or ***drop*** command.

References

None.

2.4.25.2.2 The select Command Returns "File Does not Exist" If the location Directory Specified During Partition Creation Is Deleted

Symptom

If a user deletes the **location** directory of a partition, which is specified while the partition is being created, the following error information is displayed after the ***select*** command is run to query information about all partitions:

```
0: jdbc:hive2://192.168.169.84:22550/default> select * from tba;
Error: java.io.FileNotFoundException: File hdfs://hacluster/test does not exist. (state=,code=0)
```

Possible Cause

The metadata of a partition is not deleted along with the **location** directory of the partition. When the ***select*** command is run to query information about all partitions, the partition that has metadata but no **location** directory should be ignored instead of being scanned. If this partition is scanned, the error information is displayed indicating that no file exists in the **location** directory of this partition.

Fault Locating

Run the ***show partitions tba;*** command to verify that the metadata of the partition whose **location** directory is deleted still exists in the tba table.

```
0: jdbc:hive2://192.168.169.84:22550/default> show partitions tba;
+----------------------+--+
|        result        |
+----------------------+--+
| date_str=2017-01-12  |
+----------------------+--+
```

Procedure

Once the **location** directory of a partition is deleted, information about the partition cannot be recovered. To avoid interrupting query in other partitions, take either of the following methods:

- Run the following command to add the **location** directory that has been deleted:

hdfs dfs -mkdir partition_location;

For example: ***hdfs dfs -mkdir hdfs://hacluster/test;***

- If the partition to which the deleted **location** directory belongs is determined, run the following command to delete the metadata of the partition from the tba table:

  Command syntax:

  alter table tablename drop partition_desc;

  Example command:

  alter table tba drop partition(date_str='2017-01-12');

NOTE

If there are a large number of partitions, running the ***mkdir*** or ***drop partition*** command makes the operation complex. In this case, you are advised to configure parameter **spark.sql.hive.verifyPartitionPath** to **true** to filter partitions without paths. After the configuration, if you run use the select statement after deleting the **location** directory specified during partition creation, no messages indicating that the file does not exist are displayed. However, this configuration must be performed during each session.

References

None.

2.4.25.2.3 "Unable to acquire" Exception

Symptom

During the running of Spark SQL statements, the error message "**java.io.IOException: Unable to acquire [...] bytes of memory**" is displayed. The detailed error messages are provided in the following:

```
WARN TaskSetManager: Lost task 578.2 in stage 30.0 (TID 228063, 8-5-203-1, 244): java.io.IOException:
Unable to acquire 16777216 bytes of memory
    at
org.apache.spark.util.collection.unsafe.sort.UnsafeExternalSorter.acquireNewPage(UnsafeExternalSorter.java:3
54)
    at org.apache.spark.util.collection.unsafe.sort.UnsafeExternalSorter.<init>(UnsafeExternalSorter.java:141)
    at org.apache.spark.util.collection.unsafe.sort.UnsafeExternalSorter.create(UnsafeExternalSorter.java:109)
    at org.apache.spark.sql.execution.UnsafeExternalRowSorter.<init>(UnsafeExternalRowSorter.java:68)
    at org.apache.spark.sql.execution.TungstenSort.org$apache$spark$sql$execution$TungstenSort$
$preparePartition$1(sort.scala:146)
    at org.apache.spark.sql.execution.TungstenSort$$anonfun$doExecute$3.apply(sort.scala:169)
    at org.apache.spark.sql.execution.TungstenSort$$anonfun$doExecute$3.apply(sort.scala:169)
    at
org.apache.spark.rdd.MapPartitionsWithPreparationRDD.prepare(MapPartitionsWithPreparationRDD.scala:50
)
    at org.apache.spark.rdd.ZippedPartitionsBaseRDD$$anonfun$tryPrepareParents
$1.applyOrElse(ZippedPartitionsRDD.scala:83)
    at org.apache.spark.rdd.ZippedPartitionsBaseRDD$$anonfun$tryPrepareParents
$1.applyOrElse(ZippedPartitionsRDD.scala:82)
    at scala.runtime.AbstractPartialFunction.apply(AbstractPartialFunction.scala:33)
    at scala.collection.TraversableLike$$anonfun$collect$1.apply(TraversableLike.scala:278)
    at scala.collection.immutable.List.foreach(List.scala:318)
    at scala.collection.TraversableLike$class.collect(TraversableLike.scala:278)
    at scala.collection.AbstractTraversable.collect(Traversable.scala:105)
    at org.apache.spark.rdd.ZippedPartitionsBaseRDD.tryPrepareParents(ZippedPartitionsRDD.scala:82)
    at org.apache.spark.rdd.ZippedPartitionsRDD2.compute(ZippedPartitionsRDD.scala:97)
    at org.apache.spark.rdd.RDD.computeOrReadCheckpoint(RDD.scala:334)
    at org.apache.spark.rdd.RDD.iterator(RDD.scala:267)
    at org.apache.spark.rdd.MapPartitionsRDD.compute(MapPartitionsRDD.scala:38)
```

```
    at org.apache.spark.rdd.RDD.computeOrReadCheckpoint(RDD.scala:334)
    at org.apache.spark.rdd.RDD.iterator(RDD.scala:267)
    at
org.apache.spark.rdd.MapPartitionsWithPreparationRDD.compute(MapPartitionsWithPreparationRDD.scala:6
3)
    at org.apache.spark.rdd.RDD.computeOrReadCheckpoint(RDD.scala:334)
    at org.apache.spark.rdd.RDD.iterator(RDD.scala:267)
    at
org.apache.spark.rdd.MapPartitionsWithPreparationRDD.compute(MapPartitionsWithPreparationRDD.scala:6
3)
    at org.apache.spark.rdd.RDD.computeOrReadCheckpoint(RDD.scala:334)
    at org.apache.spark.rdd.RDD.iterator(RDD.scala:267)
    at
org.apache.spark.rdd.MapPartitionsWithPreparationRDD.compute(MapPartitionsWithPreparationRDD.scala:6
3)
    at org.apache.spark.rdd.RDD.computeOrReadCheckpoint(RDD.scala:334)
    at org.apache.spark.rdd.RDD.iterator(RDD.scala:267)
    at org.apache.spark.rdd.ZippedPartitionsRDD2.compute(ZippedPartitionsRDD.scala:99)
    at org.apache.spark.rdd.RDD.computeOrReadCheckpoint(RDD.scala:334)
    at org.apache.spark.rdd.RDD.iterator(RDD.scala:267)
    at org.apache.spark.rdd.MapPartitionsRDD.compute(MapPartitionsRDD.scala:38)
    at org.apache.spark.rdd.RDD.computeOrReadCheckpoint(RDD.scala:334)
    at org.apache.spark.rdd.RDD.iterator(RDD.scala:267)
    at org.apache.spark.rdd.MapPartitionsRDD.compute(MapPartitionsRDD.scala:38)
    at org.apache.spark.rdd.RDD.computeOrReadCheckpoint(RDD.scala:334)
    at org.apache.spark.rdd.RDD.iterator(RDD.scala:267)
    at org.apache.spark.scheduler.ShuffleMapTask.runTask(ShuffleMapTask.scala:75)
    at org.apache.spark.scheduler.ShuffleMapTask.runTask(ShuffleMapTask.scala:42)
    at org.apache.spark.scheduler.Task.run(Task.scala:90)
    at org.apache.spark.executor.Executor$TaskRunner.run(Executor.scala:253)
    at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1142)
    at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:617)
    at java.lang.Thread.run(Thread.java:745).
```

If one task has failed for four consecutive times due to this same error, the job may fail sometimes, and the error messages are as follows:

```
org.apache.spark.SparkException: Job aborted due to stage failure: Task 537 in stage 30.0 failed 4 times,
most recent failure: Lost task 537.3 in stage 30.0 (TID 228865, 8-5-202-7, 650): java.io.IOException: Unable
to acquire 16777216 bytes of memory
    at
org.apache.spark.util.collection.unsafe.sort.UnsafeExternalSorter.acquireNewPage(UnsafeExternalSorter.java:3
54)
    at org.apache.spark.util.collection.unsafe.sort.UnsafeExternalSorter.<init>(UnsafeExternalSorter.java:141)
    at org.apache.spark.util.collection.unsafe.sort.UnsafeExternalSorter.create(UnsafeExternalSorter.java:109)
    at org.apache.spark.sql.execution.UnsafeExternalRowSorter.<init>(UnsafeExternalRowSorter.java:68)
    at org.apache.spark.sql.execution.TungstenSort.org$apache$spark$sql$execution$TungstenSort$
$preparePartition$1(sort.scala:146)
    at org.apache.spark.sql.execution.TungstenSort$$anonfun$doExecute$3.apply(sort.scala:169)
    at org.apache.spark.sql.execution.TungstenSort$$anonfun$doExecute$3.apply(sort.scala:169)
    at
org.apache.spark.rdd.MapPartitionsWithPreparationRDD.prepare(MapPartitionsWithPreparationRDD.scala:50
)
    at org.apache.spark.rdd.ZippedPartitionsBaseRDD$$anonfun$tryPrepareParents
$1.applyOrElse(ZippedPartitionsRDD.scala:83)
    at org.apache.spark.rdd.ZippedPartitionsBaseRDD$$anonfun$tryPrepareParents
$1.applyOrElse(ZippedPartitionsRDD.scala:82)
    at scala.runtime.AbstractPartialFunction.apply(AbstractPartialFunction.scala:33)
    at scala.collection.TraversableLike$$anonfun$collect$1.apply(TraversableLike.scala:278)
    at scala.collection.immutable.List.foreach(List.scala:318)
    at scala.collection.TraversableLike$class.collect(TraversableLike.scala:278)
    at scala.collection.AbstractTraversable.collect(Traversable.scala:105)
    at org.apache.spark.rdd.ZippedPartitionsBaseRDD.tryPrepareParents(ZippedPartitionsRDD.scala:82)
    at org.apache.spark.rdd.ZippedPartitionsRDD2.compute(ZippedPartitionsRDD.scala:97)
    at org.apache.spark.rdd.RDD.computeOrReadCheckpoint(RDD.scala:334)
    at org.apache.spark.rdd.RDD.iterator(RDD.scala:267)
    at org.apache.spark.rdd.MapPartitionsRDD.compute(MapPartitionsRDD.scala:38)
    at org.apache.spark.rdd.RDD.computeOrReadCheckpoint(RDD.scala:334)
    at org.apache.spark.rdd.RDD.iterator(RDD.scala:267)
    at
```

```
org.apache.spark.rdd.MapPartitionsWithPreparationRDD.compute(MapPartitionsWithPreparationRDD.scala:6
3)
    at org.apache.spark.rdd.RDD.computeOrReadCheckpoint(RDD.scala:334)
    at org.apache.spark.rdd.RDD.iterator(RDD.scala:267)
    at
org.apache.spark.rdd.MapPartitionsWithPreparationRDD.compute(MapPartitionsWithPreparationRDD.scala:6
3)
    at org.apache.spark.rdd.RDD.computeOrReadCheckpoint(RDD.scala:334)
    at org.apache.spark.rdd.RDD.iterator(RDD.scala:267)
    at
org.apache.spark.rdd.MapPartitionsWithPreparationRDD.compute(MapPartitionsWithPreparationRDD.scala:6
3)
    at org.apache.spark.rdd.RDD.computeOrReadCheckpoint(RDD.scala:334)
    at org.apache.spark.rdd.RDD.iterator(RDD.scala:267)
    at org.apache.spark.rdd.ZippedPartitionsRDD2.compute(ZippedPartitionsRDD.scala:99)
    at org.apache.spark.rdd.RDD.computeOrReadCheckpoint(RDD.scala:334)
    at org.apache.spark.rdd.RDD.iterator(RDD.scala:267)
    at org.apache.spark.rdd.MapPartitionsRDD.compute(MapPartitionsRDD.scala:38)
    at org.apache.spark.rdd.RDD.computeOrReadCheckpoint(RDD.scala:334)
    at org.apache.spark.rdd.RDD.iterator(RDD.scala:267)
    at org.apache.spark.rdd.MapPartitionsRDD.compute(MapPartitionsRDD.scala:38)
    at org.apache.spark.rdd.RDD.computeOrReadCheckpoint(RDD.scala:334)
    at org.apache.spark.rdd.RDD.iterator(RDD.scala:267)
    at org.apache.spark.scheduler.ShuffleMapTask.runTask(ShuffleMapTask.scala:75)
    at org.apache.spark.scheduler.ShuffleMapTask.runTask(ShuffleMapTask.scala:42)
    at org.apache.spark.scheduler.Task.run(Task.scala:90)
    at org.apache.spark.executor.Executor$TaskRunner.run(Executor.scala:253)
    at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1142)
    at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:617)
    at java.lang.Thread.run(Thread.java:745)
```

Possible Cause

Defects of the ShuffleMemoryManger. In principle, the ShuffleMemoryManger dynamically splits the total available memory according to the number of running tasks when allocating memory resources to tasks. If one task completes, the number of running tasks reduces and the ShuffleMemoryManger re-splits the available memory accordingly. However, before a new task is run, the memory is occupied by the running tasks entirely.

In this scenario, the overflow of memory occupied by UnsafeExternalSorter is triggered because the new task fails to apply for the memory. The task reapplies for the memory, but the application still fails because the memory occupied by the task is 0. Therefore, the "Unable to acquire" exception occurs.

The failed task will retry and the retry may succeed if there is available memory released by other tasks. In this case, the job will not fail. If no available memory is released, the retried task fails. After the task has retried for four consecutive times, the job fails.

Fault Locating

None.

Procedure

On the Spark client, enter the **$Spark_Client/conf/spark-defaults.conf** configuration file and modify the related configurations using either of the following methods:

- Method 1: Set **spark.executor.cores** to **1**, that is, set the degree of parallelism of a single Executor to **1**.

- Method 2: Increase the value of **spark.sql.shuffle.partitions** to reduce the probability of the exception.
- Method 3: Decrease the value of **spark.buffer.pageSize** to reduce the probability of the exception.

Reference

None.

2.4.25.2.4 The joinedRow.isNullAt Exception Occurs When Spark SQL Is Executed

Symptom

The **joinedRow.isNullAt** exception occurs when Spark SQL is executed. The error log is as follows:

```
6/09/08 11:04:11 WARN TaskSetManager: Lost task 1.0 in stage 7.0 (TID 10, vm1, 1):
java.lang.NullPointerException
        at org.apache.spark.sql.catalyst.expressions.JoinedRow.isNullAt(JoinedRow.scala:70)
        at org.apache.spark.sql.catalyst.expressions.GeneratedClass$SpecificMutableProjection.apply(Unknown
Source)
        at org.apache.spark.sql.execution.aggregate.TungstenAggregationIterator$$anonfun
$generateProcessRow$1.apply(TungstenAggregationIterator.scala:194)
        at org.apache.spark.sql.execution.aggregate.TungstenAggregationIterator$$anonfun
$generateProcessRow$1.apply(TungstenAggregationIterator.scala:192)
        at
org.apache.spark.sql.execution.aggregate.TungstenAggregationIterator.processInputs(TungstenAggregationIte
rator.scala:372)
        at
org.apache.spark.sql.execution.aggregate.TungstenAggregationIterator.start(TungstenAggregationIterator.scal
a:626)
        at org.apache.spark.sql.execution.aggregate.TungstenAggregate$$anonfun$doExecute$1.org$apache
$spark$sql$execution$aggregate$TungstenAggregate$$anonfun$$executePartition
$1(TungstenAggregate.scala:135)
        at org.apache.spark.sql.execution.aggregate.TungstenAggregate$$anonfun$doExecute$1$$anonfun
$3.apply(TungstenAggregate.scala:144)
        at org.apache.spark.sql.execution.aggregate.TungstenAggregate$$anonfun$doExecute$1$$anonfun
$3.apply(TungstenAggregate.scala:144)
        at
org.apache.spark.rdd.MapPartitionsWithPreparationRDD.compute(MapPartitionsWithPreparationRDD.scala:6
4)
        at org.apache.spark.rdd.RDD.computeOrReadCheckpoint(RDD.scala:334)
        at org.apache.spark.rdd.RDD.iterator(RDD.scala:267)
        at org.apache.spark.rdd.MapPartitionsRDD.compute(MapPartitionsRDD.scala:38)
        at org.apache.spark.rdd.RDD.computeOrReadCheckpoint(RDD.scala:334)
        at org.apache.spark.rdd.RDD.iterator(RDD.scala:267)
        at org.apache.spark.scheduler.ShuffleMapTask.runTask(ShuffleMapTask.scala:75)
        at org.apache.spark.scheduler.ShuffleMapTask.runTask(ShuffleMapTask.scala:42)
        at org.apache.spark.scheduler.Task.run(Task.scala:90)
        at org.apache.spark.executor.Executor$TaskRunner.run(Executor.scala:253)
        at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1142)
        at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:617)
        at java.lang.Thread.run(Thread.java:745)
```

Possible Causes

The error log indicates that the exception is caused by insufficient memory. If buffer fails to apply for memory, the null is returned. The null pointer exception is returned after operations on null.

If the configuration about memory in a cluster is set to a too small value, the null exception occurs when memory fails to be applied. For example, the memory configurations as follows are too small:

spark.executor.cores = 8

spark.executor.memory = 512M

spark.buffer.pageSize = 16M

The error log is as follows:

```
6/09/08 11:04:11 WARN TaskSetManager: Lost task 1.0 in stage 7.0 (TID 10, vm1, 1):
java.lang.NullPointerException
        at org.apache.spark.sql.catalyst.expressions.JoinedRow.isNullAt(JoinedRow.scala:70)
```

Fault Locating

When using the Spark SQL, ensure that the following conditions are met:

spark.executor.memory x 0.16 / (num x spark.executor.cores) > spark.buffer.pageSize

The default value of **spark.buffer.pageSize** is **16M** (M indicates the unit MB).

The common value of **num** is **8**, which may vary depending on Spark SQL statements.

Generally, setting **num** to **8** can avoid the preceding error in most scenarios. The maximum value of **num** is **16** because each task can apply for pageSize for a maximum of 16 times. If you want to avoid the **joinedRow.isNullAt** errors caused by insufficient memory, set **num** to **16**.

Procedure

Configure the values of the following parameters to solve this problem. Configure the following parameters in the **spark-defaults.conf** file on the client:

- spark.executor.memory: increase the value to increase the memory of Executor as required. Ensure that the value complies with this equation: spark.executor.memory > spark.buffer.pageSize x (num x spark.executor.cores) / 0.16
- spark.executor.cores: decrease the value to reduce the number of Executor cores.

  Ensure that the value complies with this equation: spark.executor.cores < spark.executor.memory / spark.buffer.pageSize / num x 0.16

Ensure that the value of preceding parameters comply with this formula: spark.executor.memory x 0.16 / (num x spark.executor.cores) > spark.buffer.pageSize. If the memory is sufficient, you are advised to set the value of num to 16 to avoid this error.

References

None

2.4.25.3 Spark Streaming

2.4.25.3.1 Out of Memory Error Occurs While Spark Streaming Application Is Running

Symptom

A Spark Streaming application attempts to carry out wordcount for batches of data, and each batch is no larger than 3000 MB. Even if the executor is allocated 30 GB memory, the out of memory (OOM) error occurs after the wordcount is run for a while.

Log information generated at the time of OOM error:

```
2016-02-04 20:19:43,458 | ERROR | [Thread-29] | Uncaught exception in thread Thread[Thread-29,5,main] |
org.apache.spark.Logging$class.logError(Logging.scala:96)
java.lang.OutOfMemoryError: Java heap space
        at java.util.Arrays.copyOf(Arrays.java:3236)
        at java.io.ByteArrayOutputStream.grow(ByteArrayOutputStream.java:118)
        at java.io.ByteArrayOutputStream.ensureCapacity(ByteArrayOutputStream.java:93)
        at java.io.ByteArrayOutputStream.write(ByteArrayOutputStream.java:153)
        at java.io.BufferedOutputStream.flushBuffer(BufferedOutputStream.java:82)
        at java.io.BufferedOutputStream.write(BufferedOutputStream.java:126)
        at java.io.ObjectOutputStream$BlockDataOutputStream.drain(ObjectOutputStream.java:1877)
        at java.io.ObjectOutputStream
$BlockDataOutputStream.setBlockDataMode(ObjectOutputStream.java:1786)
        at java.io.ObjectOutputStream.writeObject0(ObjectOutputStream.java:1189)
        at java.io.ObjectOutputStream.writeObject(ObjectOutputStream.java:348)
        at org.apache.spark.serializer.JavaSerializationStream.writeObject(JavaSerializer.scala:43)
        at org.apache.spark.serializer.SerializationStream.writeAll(Serializer.scala:153)
        at org.apache.spark.storage.BlockManager.dataSerializeStream(BlockManager.scala:1190)
        at org.apache.spark.storage.BlockManager.dataSerialize(BlockManager.scala:1199)
        at
org.apache.spark.streaming.receiver.WriteAheadLogBasedBlockHandler.storeBlock(ReceivedBlockHandler.scal
a:173)
```

Possible Causes

Spark Streaming receives data from Kafka in following two approaches:

- Receiver-based approach
- Direct approach (no receivers)

The OOM error only occurs when the receiver-based approached is used.

Each batch is dealt with by a separate job. If a job spends more time than the batch interval (predefined on the Spark Streaming application) to deal with the data, data from the data source (Kafka) will be accumulated, resulting in jobs being buffered in memory. This ultimately causes the executor to run out of memory.

Fault Locating

None.

Procedure

To resolve this issue, take either or both of the following methods:

- Reduce the batch interval so that the amount of data received within the batch interval will not be enormous.

- Increase memory so that jobs can be finished before the batch interval expires.

References

None.

2.4.25.4 Incorrect GLIBC Version

Symptom

The following error is reported when a Spark task runs.

```
Caused by: java.lang.UnsatisfiedLinkError: /tmp/snappy-1.0.5-libsnappyjava.so: /usr/lib64/libstdc++.so.6:
version `GLIBCXX_3.4.11' not found (required by /tmp/snappy-1.0.5-libsnappyjava.so)
at java.lang.ClassLoader$NativeLibrary.load(Native Method)
at java.lang.ClassLoader.loadLibrary1(ClassLoader.java:1965)
at java.lang.ClassLoader.loadLibrary0(ClassLoader.java:1890)
at java.lang.ClassLoader.loadLibrary(ClassLoader.java:1851)
at java.lang.Runtime.load0(Runtime.java:795)
at java.lang.System.load(System.java:1062)
at org.xerial.snappy.SnappyNativeLoader.load(SnappyNativeLoader.java:39)
```

Possible Causes

The version of the system where the task runs and the version of the system where the compilation environment locates are different, resulting in the incompatibility of GLIBC versions.

Fault Locating

Run the ***strings /usr/lib64/libstdc++.so.6 | grep*** command to check whether the GLIBC version is too early.

Procedure

If the GLIBC version is too early, use the file of a later version (3.4.11) to replace **libstdc++.so.6**. (This is a link file. You need to replace only the file that is linked to this link file.)

Reference Information

None.

2.4.25.5 Failed to Execute Spark Tasks After the YARN Active/Standby Switchover

Symptom

When users run the Spark application, the HDFS write operations are performed. During this process, the following error occurs:

```
Exception in thread "Driver" org.apache.hadoop.mapred.FileAlreadyExistsException: Output directory
hdfs://hacluster/testsave already exists
at org.apache.hadoop.mapred.FileOutputFormat.checkOutputSpecs(FileOutputFormat.java:132)
```

```
at org.apache.spark.rdd.PairRDDFunctions.saveAsHadoopDataset(PairRDDFunctions.scala:1021)
at org.apache.spark.rdd.PairRDDFunctions.saveAsHadoopFile(PairRDDFunctions.scala:931)
at org.apache.spark.rdd.PairRDDFunctions.saveAsHadoopFile(PairRDDFunctions.scala:840)
at org.apache.spark.rdd.RDD.saveAsTextFile(RDD.scala:1177)
at com.spark.test.wordcountWithSave$.main(wordcountWithSave.scala:30)
at com.spark.test.wordcountWithSave.main(wordcountWithSave.scala)
at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:57)
at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
at java.lang.reflect.Method.invoke(Method.java:606)
at org.apache.spark.deploy.yarn.ApplicationMaster$$anon$2.run(ApplicationMaster.scala:460)
```

Possible Causes

The possible error causes are as follows:

- Cause 1: Before running the Spark application, the directory which used for written data is existed in HDFS.
- Cause 2: The Yarn active/standby switchover occurs when data is to be written to HDFS before the application is run.

Fault Locating

Use the following method to determine whether cause 2 results in the problem:

1. On the FusionInsight Manager portal, check whether the active/standby state changes. If the state changes, the active/standby switchover occurs.
2. Check whether the following information exists Yarn logs. If the following information exists, the active/standby switchover occurs.

```
Checking for any old active which needs to be fenced...
No old node to fence
Writing znode /yarn-leader-election/yarncluster/ActiveBreadCrumb to indicate that the local node is
the most recent active...
found resource yarn-site.xml at file:/opt/huawei/Bigdata/FusionInsight_HD_xxx/
1_10_ResourceManager/etc/yarn-site.xml
USER=mapredOPERATION=refreshAdminAclsTARGET=AdminServiceRESULT=SUCCESS
Transitioning to active state
```

Procedure

- Cause: The HDFS directory already exists.

  Change the HDFS data write directory defined in the application or delete the existing HDFS directory.
- Cause: Yarn active/standby switchover, use either of the following methods:
  - Delete the exist HDFS folder or change the HDFS folder path in application, then submit the application again.

    NOTE

    Deleting a file or folder is a high-risk operation. Ensure that the file or folder is no longer required before performing this operation.
  - On the client, open the **$Spark_Client/conf/spark-defaults.conf** file and set **spark.hadoop.validateOutputSpecs** to **false**. The fault is rectified.

    NOTE

    After setting **spark.hadoop.validateOutputSpecs** to **false** and saving the file, the existing HDFS directory is overwritten. You are advised to use method 1 and set this parameter to **true**.

Reference Information

None.

2.4.25.6 "No space left on device" Is Displayed Constantly During the Running of Spark Tasks

Symptom

"No space left on device" is displayed constantly during the running of Spark tasks, as shown in **Figure 2-21**. However, the ***df -h*** command shows that a large amount of disk space is free.

Figure 2-21 No space left on device

```
application_1467918139601_0032  spark  wordcountWithshufflemapstatus  SPARK  default  Wed Jul 13 09:46:16 +0800 2016  Wed Jul 13 15:57:29 +0800 2016  FINISHED  SUCCEEDED  N/A  N/A  N/A  History
linux-63:/opt/xudong/shufflemapstatus # cat driver-20g-4cores-application_1467918139601_0039.log | grep "No space left on device" | grep linux-7
linux-63:/opt/xudong/shufflemapstatus # cat driver-20g-4cores-application_1467918139601_0039.log | grep "No space left on device" | grep linux-8
linux-63:/opt/xudong/shufflemapstatus #
linux-63:/opt/xudong/shufflemapstatus # cat driver-20g-4cores-application_1467918139601_0039.log | grep "No space left on device" | grep linux-63
linux-63:/opt/xudong/shufflemapstatus #
linux-63:/opt/xudong/shufflemapstatus # cat driver-20g-4cores-application_1467918139601_0039.log | grep "No space left on device" | grep linux-9
16/07/13 12:47:30 WARN TaskSetManager: Lost task 8820472.0 in stage 0.0 (TID 8820472, linux-9, 8): java.io.FileNotFoundException: /export11/BigData/hadoop/data1/nm/localdir/usercache/spark/appcache/app
ion_1467918139601_0039/blockmgr-1a389d56-f9b5-4771-ad41-96e18eab47f1/21/shuffle_0_8820472_0.data (No space left on device)
16/07/13 12:47:30 WARN TaskSetManager: Lost task 8820470.0 in stage 0.0 (TID 8820470, linux-9, 8): java.io.FileNotFoundException: /export11/BigData/hadoop/data1/nm/localdir/usercache/spark/appcache/app
ion_1467918139601_0039/blockmgr-1a389d56-f9b5-4771-ad41-96e18eab47f1/1b/shuffle_0_8820470_0.data (No space left on device)
16/07/13 12:47:30 WARN TaskSetManager: Lost task 8820469.0 in stage 0.0 (TID 8820469, linux-9, 5): java.io.FileNotFoundException: /export11/BigData/hadoop/data1/nm/localdir/usercache/spark/appcache/app
ion_1467918139601_0039/blockmgr-c2517216-8d1d-4057-b310-7d55fa8c7162/17/shuffle_0_8820469_0.index (No space left on device)
16/07/13 12:47:30 WARN TaskSetManager: Lost task 8820478.0 in stage 0.0 (TID 8820478, linux-9, 8): java.io.FileNotFoundException: /export11/BigData/hadoop/data1/nm/localdir/usercache/spark/appcache/app
ion_1467918139601_0039/blockmgr-1a389d56-f9b5-4771-ad41-96e18eab47f1/3d/shuffle_0_8820478_0.index (No space left on device)
16/07/13 12:47:30 WARN TaskSetManager: Lost task 8820474.0 in stage 0.0 (TID 8820474, linux-9, 5): java.io.FileNotFoundException: /export11/BigData/hadoop/data1/nm/localdir/usercache/spark/appcache/app
ion_1467918139601_0039/blockmgr-c2517216-8d1d-4057-b310-7d55fa8c7162/27/shuffle_0_8820474_0.data (No space left on device)
16/07/13 12:47:30 WARN TaskSetManager: Lost task 8820485.0 in stage 0.0 (TID 8820485, linux-9, 8): java.io.FileNotFoundException: /export11/BigData/hadoop/data1/nm/localdir/usercache/spark/appcache/app
ion_1467918139601_0039/blockmgr-1a389d56-f9b5-4771-ad41-96e18eab47f1/1b/shuffle_0_8820485_0.index (No space left on device)
16/07/13 12:47:30 WARN TaskSetManager: Lost task 8820491.0 in stage 0.0 (TID 8820491, linux-9, 5): java.io.FileNotFoundException: /export11/BigData/hadoop/data1/nm/localdir/usercache/spark/appcache/app
ion_1467918139601_0039/blockmgr-c2517216-8d1d-4057-b310-7d55fa8c7162/18/shuffle_0_8820491_0.data (No space left on device)
16/07/13 12:47:30 WARN TaskSetManager: Lost task 8820470.1 in stage 0.0 (TID 8820492, linux-9, 5): java.io.FileNotFoundException: /export11/BigData/hadoop/data1/nm/localdir/usercache/spark/appcache/app
ion_1467918139601_0039/blockmgr-c2517216-8d1d-4057-b310-7d55fa8c7162/1b/shuffle_0_8820470_0.data (No space left on device)
16/07/13 12:47:30 WARN TaskSetManager: Lost task 8820474.1 in stage 0.0 (TID 8820493, linux-9, 8): java.io.FileNotFoundException: /export11/BigData/hadoop/data1/nm/localdir/usercache/spark/appcache/app
ion_1467918139601_0039/blockmgr-1a389d56-f9b5-4771-ad41-96e18eab47f1/27/shuffle_0_8820474_0.data (No space left on device)
16/07/13 12:47:30 WARN TaskSetManager: Lost task 8820469.1 in stage 0.0 (TID 8820494, linux-9, 8): java.io.FileNotFoundException: /export11/BigData/hadoop/data1/nm/localdir/usercache/spark/appcache/app
ion_1467918139601_0039/blockmgr-1a389d56-f9b5-4771-ad41-96e18eab47f1/17/shuffle_0_8820469_0.index (No space left on device)
16/07/13 12:47:30 WARN TaskSetManager: Lost task 8820485.1 in stage 0.0 (TID 8820496, linux-9, 5): java.io.FileNotFoundException: /export11/BigData/hadoop/data1/nm/localdir/usercache/spark/appcache/app
ion_1467918139601_0039/blockmgr-c2517216-8d1d-4057-b310-7d55fa8c7162/1b/shuffle_0_8820485_0.index (No space left on device)
16/07/13 12:47:30 WARN TaskSetManager: Lost task 8820478.1 in stage 0.0 (TID 8820497, linux-9, 5): java.io.FileNotFoundException: /export11/BigData/hadoop/data1/nm/localdir/usercache/spark/appcache/app
```

Possible Causes

- The disk uses a separate inode to store metadata of every file. The number of inodes is specified after the disk is mounted. The error occurs if you attempt to create a new file after all inodes are exhausted.
- If there are too many small files, the disk may run out of inodes but a large amount of disk space is free.

Fault Locating

Use the following methods to locate the error:

- Run the ***df -h*** command to check whether the disk space is used up.
- Run the ***df -i*** command to check whether inodes are used up.

Procedure

1. Delete unnecessary files and check whether the symptom persists.
   - If the symptom disappears, no further operation is required.
   - If the symptom persists, go to **2**.
2. Add a new disk.

References

None.

2.4.25.7 Spark yarn-client Task Failure When the Client Is Deployed Outside the Cluster

Symptom

If the client is installed on a node outside the cluster, an error message is displayed when running the Spark yarn-client task. The following figure shows the log on Yarn.

```
2019-08-01 07:33:57,811 | WARN  | [main] | Exception encountered while connecting to the server : org.apache.hadoop.ipc.RemoteException(org.apache.hadoop.ipc.StandbyException)
2019-08-01 07:33:57,990 | INFO  | [main] | ApplicationAttemptId: appattempt_1563936960166_0095_000001 | org.apache.spark.internal.Logging$class.logInfo(Logging.scala:54)
2019-08-01 07:33:58,238 | INFO  | [main] | Waiting for Spark driver to be reachable. | org.apache.spark.internal.Logging$class.logInfo(Logging.scala:54)
2019-08-01 07:33:58,258 | ERROR | [main] | Failed to connect to driver at 8-5-203-8:22816, retrying ... | org.apache.spark.internal.Logging$class.logError(Logging.scala:70)
2019-08-01 07:33:58,359 | ERROR | [main] | Failed to connect to driver at 8-5-203-8:22816, retrying ... | org.apache.spark.internal.Logging$class.logError(Logging.scala:70)
2019-08-01 07:33:58,461 | ERROR | [main] | Failed to connect to driver at 8-5-203-8:22816, retrying ... | org.apache.spark.internal.Logging$class.logError(Logging.scala:70)
2019-08-01 07:33:58,562 | ERROR | [main] | Failed to connect to driver at 8-5-203-8:22816, retrying ... | org.apache.spark.internal.Logging$class.logError(Logging.scala:70)
2019-08-01 07:33:58,663 | ERROR | [main] | Failed to connect to driver at 8-5-203-8:22816, retrying ... | org.apache.spark.internal.Logging$class.logError(Logging.scala:70)
2019-08-01 07:33:58,764 | ERROR | [main] | Failed to connect to driver at 8-5-203-8:22816, retrying ... | org.apache.spark.internal.Logging$class.logError(Logging.scala:70)
2019-08-01 07:33:58,865 | ERROR | [main] | Failed to connect to driver at 8-5-203-8:22816, retrying ... | org.apache.spark.internal.Logging$class.logError(Logging.scala:70)
2019-08-01 07:33:58,966 | ERROR | [main] | Failed to connect to driver at 8-5-203-8:22816, retrying ... | org.apache.spark.internal.Logging$class.logError(Logging.scala:70)
2019-08-01 07:33:59,067 | ERROR | [main] | Failed to connect to driver at 8-5-203-8:22816, retrying ... | org.apache.spark.internal.Logging$class.logError(Logging.scala:70)
2019-08-01 07:33:59,168 | ERROR | [main] | Failed to connect to driver at 8-5-203-8:22816, retrying ... | org.apache.spark.internal.Logging$class.logError(Logging.scala:70)
```

Possible Causes

URL of the driver is in the hostname:port format. The compute node cannot recognize the host name. As a result, the connection fails.

Procedure

Step 1 Query the IP address of the client (possibly multiple NICs). Find the IP address that can communicate with the cluster compute node, for example, 10.8.3.4. Add the following configuration to **spark-defaults.conf** on the Spark client:

spark.driver.host = 10.8.3.4

Step 2 Run the Spark yarn-client task again.

----End

Reference

None.

2.4.26 Yarn

2.4.26.1 Link on the ResourceManager Native Page Is Unavailable

Symptom

The node information is displayed after the ResourceManager native page login.

Cluster Metrics

Apps Submitted	Apps Pending	Apps Running	Apps Completed	Containers Running	Memory Used	Memory Total	Memory Reserved	VCores Used	VCores Total
0	0	0	0	0	0 B	24 GB	0 B	0	24

Show 20 entries

Rack	Node State	Node Address	Node HTTP Address	Last health-update	Health-report
/default-rack	RUNNING	hghoulaslx413:26009	hghoulaslx413:26010	8-Jan-2015 15:37:59	
/default-rack	RUNNING	hghoulaslx414:26009	hghoulaslx414:26010	8-Jan-2015 15:37:59	
/default-rack	RUNNING	hghoulaslx412:26009	hghoulaslx412:26010	8-Jan-2015 15:38:00	

Showing 1 to 3 of 3 entries

The node cannot be accessed by clicking the node link.

Possible Causes

- The mapping relationship between HostName and IP of every node in the cluster must be configured on the local host.
- The related port is disabled in the cluster.

Fault Locating

Check whether the mapping relationship between HostName and IP is configured in the local **hosts** files. Check whether the related port is enabled in the cluster.

Procedure

Step 1 Log in to the FusionInsight Manager system, click **Host**, and check the mapping relationship between Host Name and IP.

Step 2 Modify the local host file based on the relationship between the HostName and IP address.

Directory containing local hosts files:

- In the Windows system: **C:\Windows\System32\drivers\etc\hosts**
- In the Linux system: **/etc/hosts**

Step 3 If this port is disabled (using the firewall or iptables), you must enable this port. You can view the HTTPS port number of NodeManager Webapp through the **yarn.nodemanager.webapp.https.port** parameter on FusionInsight Manager.

----End

Reference Information

None.

2.4.26.2 ResourceManager Node Faults

Symptom

- One or all ResourceManager nodes are in the **Restoring** state.
- If no ResourceManager in the Active state exists, alarms indicating that the MapReduce service is unavailable occur.
- Use the client to submit a MapReduce task. During the MapReduce task process, faults occur on the active ResourceManager node, which may cause task failures.

Possible Causes

- The server is faulty.
- The ZooKeeper service is abnormal.
- The ResourceManager process in this node is abnormal. (The abnormal ResourceManager process can be caused by high CPU usage, node agent exceptions, and manual or accidental operations.)

Fault Locating

1. Check whether alarms indicating that the YARN service is unavailable occur and the alarm cause is No active instance. For details, see the alarm description.
2. Check the status of the ZooKeeper service. If no alarm occurs, the ZooKeeper service is running properly.
3. Check the network status.
4. Collect and view the logs.

Procedure

Step 1 Log in to the FusionInsight Manager system.

Step 2 Click **O&M > Alarm > Alarms** to check whether alarms related to Yarn and ZooKeeper services exist.

- If yes, handle the alarms according to related description.
- If no, go to **Step 3**.

Step 3 Choose **Cluster >** *Name of the desired cluster* **> Services** > **Yarn**, and go to the abnormal ResourceManager page.

Step 4 Restart the abnormal ResourceManager instance, and check whether the fault is rectified.

- If yes, no further operation is required.
- If no, go to **Step 5**.

Step 5 Choose **System** > **Log > Download,** select **Resource Manager** from the **Service**.

Step 6 Select a time range in the upper right corner, or click to specify **Start Date** and **End Date**, and click **Download**.

Step 7 Contact thetechnical support, and send collected fault logs.

----End

Reference Information

None.

2.4.26.3 NodeManager Node Faults

Symptom

- One or multiple NodeManager nodes are in the **Restoring** state.
- The NodeManager Unhealthy alarm or NodeManager Heartbeat Lost alarm is reported.
- During the MapReduce task process, faults occur in the NodeManager node, which may cause task failures or the slow running.

Possible Causes

- The network in this node is abnormal.
- The ZooKeeper service is abnormal.
- The NodeManager process is abnormal.

Fault Locating

1. Check whether the ZooKeeper service is normal.
2. Check the exception information displayed on the ResourceManager page.

Procedure

Step 1 Log in to the FusionInsight Manager system.

Step 2 Click **O&M > Alarm > Alarms** to check whether ZooKeeper alarms exist.

- If yes, handle the alarms according to related description.
- If no, go to **Step 3**.

Step 3 Choose **Cluster >** *Name of the desired cluster* **> Services** > **Yarn** > **ResourceManager(Active)**, and go to the active ResourceManager page. Check the abnormal node, and rectify faults based on the information.

Step 4 Choose **System** > **Log > Download**, select **NodeManager** from the **Service**.

Step 5 Select a time range in the upper right corner, or click to specify **Start Date** and **End Date**, and click **Download**.

Step 6 Contact the technical support, and send collected fault logs.

----End

Reference Information

None.

2.4.26.4 NodeManager Unable to Start with DBException

Symptoms

NodeManager unable to start. The following exception is logged in the NodeManager logs.

```
org.fusesource.leveldbjni.internal.NativeDB$DBException: Corruption: 1 missing files;
```

Possible Cause

This exception is encountered when **yarn.nodemanager.recovery.enabled**=**true** and **levelDB** used as NodeManager recovery store is corrupted because of either less disk space or file handler exhaust.

Procedure

Step 1 Delete the folder represented by **{yarn.nodemanager.recovery.dir}/yarn-nm-state** in **yarn-site.xml**.

The impact is shown below:

- Log Aggregation might be affected for already finished applications on this node as result aggregated does not contain the attempt logs run in this NodeManager. Stale files/folders can be cleaned up after the application is **FINISHED**, go to **{yarn.nodemanager.log-dirs}** and find the folder with **<applicationID>** and delete it.
- Localized resources and container temp files may not be cleaned up on this node. Stale files/folders can be cleaned up after the application is **FINISHED,** go to **{yarn.nodemanager.local-dirs}** and find the folders with **<applicationID>** and delete them.
- Current container may fail as Container-tokens are not refreshed after the crash.

Step 2 Start the NodeManager.

----End

Reference Information

None.

2.4.26.5 Spark Task Failure Caused by OutOfMemoryError on NodeManager

Symptom

When Spark dynamic scheduling is enabled and millions of Spark tasks are running, the Spark tasks fail in the Reduce phase after multiple retries. The message "java.lang.OutOfMemoryError: Direct buffer memory" is displayed and the error log is as follows.

```
2016-07-06 19:05:15,794 | WARN | shuffle-server-37 | Exception in connection from /10.16.0.130:49654 |
TransportChannelHandler.java:79
io.netty.handler.codec.DecoderException: java.lang.OutOfMemoryError: Direct buffer memory
at io.netty.handler.codec.ByteToMessageDecoder.channelRead(ByteToMessageDecoder.java:153)
at
io.netty.channel.AbstractChannelHandlerContext.invokeChannelRead(AbstractChannelHandlerContext.java:33
3)
at
io.netty.channel.AbstractChannelHandlerContext.fireChannelRead(AbstractChannelHandlerContext.java:319)
at io.netty.channel.DefaultChannelPipeline.fireChannelRead(DefaultChannelPipeline.java:787)
at io.netty.channel.nio.AbstractNioByteChannel$NioByteUnsafe.read(AbstractNioByteChannel.java:130)
at io.netty.channel.nio.NioEventLoop.processSelectedKey(NioEventLoop.java:511)
at io.netty.channel.nio.NioEventLoop.processSelectedKeysOptimized(NioEventLoop.java:468)
at io.netty.channel.nio.NioEventLoop.processSelectedKeys(NioEventLoop.java:382)
at io.netty.channel.nio.NioEventLoop.run(NioEventLoop.java:354)
at io.netty.util.concurrent.SingleThreadEventExecutor$2.run(SingleThreadEventExecutor.java:116)
at java.lang.Thread.run(Thread.java:745)
Caused by: java.lang.OutOfMemoryError: Direct buffer memory
at java.nio.Bits.reserveMemory(Bits.java:693)
at java.nio.DirectByteBuffer.<init>(DirectByteBuffer.java:123)
at java.nio.ByteBuffer.allocateDirect(ByteBuffer.java:311)
at io.netty.buffer.PoolArena$DirectArena.newChunk(PoolArena.java:434)
at io.netty.buffer.PoolArena.allocateNormal(PoolArena.java:179)
at io.netty.buffer.PoolArena.allocate(PoolArena.java:168)
```

```
at io.netty.buffer.PoolArena.reallocate(PoolArena.java:277)
at io.netty.buffer.PooledByteBuf.capacity(PooledByteBuf.java:108)
at io.netty.buffer.AbstractByteBuf.ensureWritable(AbstractByteBuf.java:251)
at io.netty.buffer.AbstractByteBuf.writeBytes(AbstractByteBuf.java:849)
at io.netty.buffer.AbstractByteBuf.writeBytes(AbstractByteBuf.java:841)
at io.netty.buffer.AbstractByteBuf.writeBytes(AbstractByteBuf.java:831)
at io.netty.handler.codec.ByteToMessageDecoder.channelRead(ByteToMessageDecoder.java:146)
```

Possible Cause

When Spark dynamic scheduling is enabled, NodeManager consumes a large amount of memory resources to process spark shuffle data. If the value of memory parameter about NodeManager is not large enough, the message **"java.lang.OutOfMemoryError: Direct buffer memory"** is displayed.

Fault Locating

Check whether the error message **"OutOfMemoryError"** exists in the NodeManager log.

Procedure

If the error message OutOfMemoryError exists in the NodeManager log, either of the following two methods can be used to rectify the error:

- Leave the MaxDirectMemorySize parameter of NodeManager unspecified, so that the memory is not limited.

  Log in to the FusionInsight Manager WebUI, choose **Cluster >** *Name of the desired cluster* **> Services > Yarn** > **Configurations**, and click **All Configurations**. Select **NodeManager** for the **Role**, click **System**, and modify the configurations of the **GC_OPTS** parameter.

  NOTE

  By default, **-XX:MaxDirectMemorySize** is not configured in the **GC_OPTS** parameter. To configure it, you need to add it to the **GC_OPTS** parameter as an custom option.

- You can configure the memory parameters about NodeManager as required before running tasks.

  When Spark dynamic scheduling is enabled, the required memory of NodeManager can be roughly calculated using the following formulas:

  Off-heap memory (MB) = (Maximum number of tasks for a single stage in Spark/Number of available NodeManagers) x 32 x Number of cores of the VM/1024/1024

  Heap memory (MB) = (Maximum number of tasks for a single stage in Spark/Number of available NodeManagers) x 512/1024/1024

  NOTE

  Many factors, such as the number of stages running at the same time or messages stacking are not taken into account in the preceding formulas. The actual value may be one to five times larger than the calculated value.

  You can log in to the FusionInsight Manager WebUI, select **NodeManager** > **GC_OPTS**, and configure the following parameters:

- MaxDirectMemorySize: indicates the maximum size of off-heap memory. The parameter can be configured to the value of "Off-heap memory (MB)" in the preceding formula.
- Xmx: indicates the maximum heap memory. The parameter can be configured to the sum of "Off-heap memory (MB)" and "Heap memory (MB)" calculated in the preceding formulas.

References

None.

2.4.26.6 Tenant Functions Become Abnormal When the Yarn Service Is Set to the Superior Scheduler Mode During Installation

Symptom

When the superior scheduler mode is set during installation of the MRS cluster or Yarn service, tenants fail to be added and resources of the default tenant are displayed abnormally.

Possible Cause

An error occurred when initializing the default tenant data in the database. The TENANT_RESOURCES tag indicates that the default TENANTID of the root queue is incorrect.

Fault Locating

Check the TENANTID column of the root queue to determine whether a data error exists in the table.

Procedure

Step 1 Log in to the active management node as user **root**.

Step 2 Run the **su - omm** command to switch to user **omm**.

Step 3 Run the following command to disable logout upon session timeout:

TMOUT=0

NOTE

After the operations in this section are complete, run the **TMOUT=***Timeout interval* command to restore the timeout interval in a timely manner. For example, **TMOUT=600** indicates that a user is logged out if the user does not perform any operation within 600 seconds.

Step 4 Run the following command to log in to the database:

gsql -p 20015 -d omm -U ommdba -W *password*

NOTE

In the preceding command, *password* indicates the database password of the **ommdba** user. For details about the default password of user **hdfs**, see ***Huawei Cloud Stack 8.3.1 Account List*** or consult the system administrator.

Step 5 Run the following command to check whether the value exists in the **TENANTID** column:

select * from TENANT_RESOURCES where RESOURCENAME='root';

```
OMM=# select * from TENANT_RESOURCES where RESOURCENAME='root';
         RESOURCEID          | SERVICENAME | RESOURCENAME | RESOURCEFULLNAME | SERVICEID | RESOURCETYPE |      SUBTYPE       |      TENANTID      | STATUS
-----------------------------+-------------+--------------+------------------+-----------+--------------+--------------------+--------------------+---------
 000002-fi-tenant-resource-1 | Yarn        | root         | root             |           | parentQueue  | Superior Scheduler | 000000-fi-tenant-1 | constant
(1 row)
```

- If yes, go to **Step 6**.
- If no, contact the technical support.

Step 6 Run the following command to restore data:

update TENANT_RESOURCES set TENANTID='' where RESOURCENAME='root';

Step 7 Run the following command to check whether the value is cleared in the **TENANTID** column:

select * from TENANT_RESOURCES where RESOURCENAME='root';

```
OMM=# select * from TENANT_RESOURCES where RESOURCENAME='root';
         RESOURCEID          | SERVICENAME | RESOURCENAME | RESOURCEFULLNAME | SERVICEID | RESOURCETYPE |      SUBTYPE       | TENANTID | STATUS
-----------------------------+-------------+--------------+------------------+-----------+--------------+--------------------+----------+---------
 000002-fi-tenant-resource-1 | Yarn        | root         | root             |           | parentQueue  | Superior Scheduler |          | constant
(1 row)
```

- If yes, go to **Step 8**.
- If no, contact technical support.

Step 8 Log in to FusionInsight Manager and check whether the tenant functions related to the superior scheduler are normal.

- If yes, no further action is required.
- If no, contact technical support.

----End

2.4.26.7 A Job Fails to Be Submitted Because the Launcher-job Queue Fails to Be Created During Cluster Provisioning

Symptom

Failed to submit the job when a new cluster is provisioned. The failure cause is that the launcher-job queue does not exist.

Possible Cause

The ResourceManager fails to synchronize the configuration when creating a queue.

Fault Locating

1. Check whether the launcher-job tenant is successfully created.
2. Check whether launcher-job can be found on the native page.
3. Check whether the ResourceManager configuration status is Failed.

Procedure

Step 1 Log in to FusionInsight Manager.

Step 2 Choose **Audit** > **Audit**, click **Advanced Search**, set **Operation Type** to **Add tenant**, enter **executor** in the **User**, and click **Search** to check whether the launcher-job tenant is successfully created.

- If yes, go to **Step 3**.
- If no, go to **Step 8**.

Step 3 Choose **Cluster** > **Services** > **Yarn** and click the link next to **ResourceManager WebUI**. The native page is displayed. In the navigation tree on the left, choose **Cluster** > **Scheduler**. In the **Application Queues** area, check whether the launcher-job queue exists.

- If yes, go to **Step 8**.
- If no, go to **Step 4**.

Step 4 On FusionInsight Manager, choose **Cluster** > **Services** > **Yarn** > **Instance** and check whether the ResourceManager **Configuration Status** is **Failed**.

- If yes, go to **Step 5**.

Step 5 Click the name of the ResourceManager whose **Configuration Status** is **Failed**. The ResourceManager instance page is displayed. In the upper right corner, choose **More** > **Synchronize Configuration**. Check whether the configuration is successfully synchronized.

- If yes, go to **Step 6**.
- If no, go to **Step 8**.

Step 6 Choose **Cluster** > **Services** > **Yarn** > **Dashboard**. In the upper right corner, choose **More** > **Refresh Queue**. Check whether the queue is refreshed successfully.

- If yes, go to **Step 7**.
- If no, go to **Step 8**.

Step 7 On the **Dashboard** page of Yarn, click the link next to **ResourceManager WebUI**. The native page is displayed. In the navigation tree on the left, choose **Cluster** > **Scheduler**. On the **Application Queues** page, check whether the launcher-job queue exists.

- If yes, the repair is complete.
- If no, go to **Step 8**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 8 Contact technical support., and send the collected fault logs.

----End

2.4.27 ZooKeeper

2.4.27.1 ZooKeeper Instance Always in Restoring Status

Symptom

On the ZooKeeper window, the ZooKeeper instance is always in **Restoring** status.

Possible Causes

- The space of the disk where ZooKeeper is located is insufficient.
- ZooKeeper service data files are damaged.

Fault Locating

1. Check the space of the disk where ZooKeeper is located.
2. Delete the damaged ZooKeeper service data files.

Procedure

Step 1 Log in to the FusionInsight Manager portal.

Step 2 Click **O&M** > **Alarm** > **Alarm** to check whether alarms indicating that the space of the disk where the faulty ZooKeeper instance is located is insufficient exist.

- If yes, handle the alarm based on related processes.
- If no, go to **Step 3**.

Step 3 After confirming that the disk space is sufficient, choose **Cluster** > *Name of the desired cluster* > **Services** > **ZooKeeper** > **Instance**, select the faulty quorumpeer instance, choose **More** > **Restart Instance** to restart the instance, and check whether it can recover.

- If yes, no further action is required.
- If no, go to **Step 4**.

Step 4 Choose **Cluster** > *Name of the desired cluster* > **Services** > **ZooKeeper** > **Configuration** to find the ZooKeeper data storage directory in the configuration parameter **dataDir**.

Step 5 Log in to the node where the faulty ZooKeeper instance is located as user **root**, and then run the following command to switch to user **omm**:

su - omm

NOTE

The current user is user **omm**.

Step 6 Run the following command to switch to the directory where the ZooKeeper data is stored (The default data directory is used as an example.)

cd ${BIGDATA_DATA_HOME}/zookeeper

Step 7 Run the following command to create an empty directory.

mkdir ${BIGDATA_DATA_HOME}/zookeeper/version-2

Step 8 Run the following command to back up version-2.

mv ${BIGDATA_DATA_HOME}/zookeeper/version-2 ${BIGDATA_DATA_HOME}/zookeeper/version-2.bak

Step 9 Log in to the FusionInsight Manager portal again, choose **Cluster >***Name of the desired cluster* **> Services > ZooKeeper > Instance**, select the faulty quorumpeer instance, choose **More** > **Restart Instance** to restart it, and check whether it can recover.

- If yes, no further operation is required.
- If no, contact the .

----End

References

None.

2.4.27.2 Unavailable ZooKeeper Service

Symptom

ZooKeeper is abnormal, and the Hadoop distributed file system (HDFS) cannot be started.

Possible Causes

- You cannot select the active ZooKeeper instance.
- The nodes where the ZooKeeper instances are located are configured with the same IP address or host name.

Fault Locating

1. Check the ZooKeeper installation, and check whether odd instances are running (for example 3 or 5).
2. Restore the services of the faulty ZooKeeper instances.

Procedure

Step 1 Log in to the FusionInsight Manager portal.

Step 2 Choose **Cluster** > *Name of the desired cluster* **>Services > ZooKeeper > Instance** to check whether odd ZooKeeper instances are installed.

- If yes, go to **Step 3**.
- If no, Configure an odd number of ZooKeeper instances as prompted.

Step 3 Click **O&M > Alarm >Alarm** to check whether ZooKeeper alarms or alarms indicating insufficient disk space exist.

- If yes, handle the alarms by following the steps provided in related sections.
- If no, go to **Step 4**.

Step 4 Check whether the nodes where the ZooKeeper instances are located are configured with the same IP address or host name.

- If yes, change the IP address and host name of the node.

  For details, see section **Planning Node Network Parameters** in the **Software Installation and Configuration**.
- If no, contact technical support.

----End

References

None

2.4.27.3 ZooKeeper Client Session is Closed

Symptom

Exception occurs on ZooKeeper client when data larger than 4MB is written to ZooKeeper nodes. The exception information is as follows:

```
2019-11-07 15:23:34,237 | WARN | NIOServerCxn.Factory:/10.18.51.157:24002 |
Exception causing close of session 0xe4985ef3128000d due to java.io.IOException: Len error 1080037 |
org.apache.zookeeper.server.NIOServerCnxn.doIO(NIOServerCnxn.java:362)
2019-11-07 15:23:34,238 | INFO | NIOServerCxn.Factory:/10.18.51.157:24002 |
Closed socket connection for client /10.18.51.156:44987 which had sessionid 0xe4985ef3128000d |
org.apache.zookeeper.server.NIOServerCnxn.closeSock(NIOServerCnxn.java:1007)
```

Possible Causes

ZooKeeper is validating the znode data size against **jute.maxbuffer** configuration value. If the data size exceeds this configured value, server will reject the request and throw this exception. By default the value is 4MB. The value of this configuration should be same in both client and the server side.

Fault Locating

None.

Procedure

You are advised not to change the value of **jute.maxbuffer**. When writing data to ZooKeeper nodes, ensure that the size of a single file does not exceed 4 MB. To ensure the ZooKeeper performance, do not write a large amount of data to ZooKeeper nodes.

References

None.

2.4.27.4 Failed to Restore a ZooKeeper File That Was Deleted by Mistake

Symptom

The ZooKeeper folder is deleted by mistake. The ZooKeeper instance is uninstalled and then reinstalled on FusionInsight Manager. After the restoration is complete, the process is in the Restoring state on the page.

Possible Causes

A user deletes the pid file of ZooKeeper, for example, **hadoop-omm-quorumpeer.pid**. But the ZooKeeper process is running in the background. After the instance restoration, the instance cannot be started and is in the **Restoring** state.

For example, before the pid file is deleted, the ZooKeeper instance PID is **6419**; after the pid file is deleted, a new pid file is generated during the ZooKeeper instance restoration and a new process whose PID is **6405** is started. The **6405** process cannot be started because the **6419** process is not cleared.

Fault Locating

None.

Procedure

Log in to the node where the ZooKeeper instance is located as user **omm**, run the ***kill -9*** *old_pid* command to delete the process.

old_pid indicates the PID before the error occurs. You can run the ***jps*** command to view the PID.

References

None.

2.4.27.5 ZooKeeper Service Abnormal After DNS Installation

Symptom

On the FusionInsight Manager portal, the ZooKeeper service status automatically switches between **Faulty** and **Normal**, and the ZooKeeper instance running status also switches between **Restoring** and **Normal**.

Possible Causes

- The configuration of **/etc/hosts** on the node where the ZooKeeper locates is incorrect.
- The DNS is deployed on the node where ZooKeeper locates.

Fault Locating

1. Check whether the IP address and host name configuration is correct in **/etc/hosts**, that is, whether one IP address corresponds to multiple host names or one host name corresponds to multiple IP addresses.
2. Check whether the DNS is installed on the node where ZooKeeper locates.

Procedure

Step 1 Log in to the FusionInsight Manager portal.

Step 2 Choose **Cluster > Services** > *Name of the desired cluster* **> ZooKeeper** > **Instance** to check the faulty ZooKeeper instance.

Step 3 Log in to the node where the faulty ZooKeeper locates as user **root.**

Step 4 Check whether the configuration in **/etc/hosts** is correct.

- If yes, go to **Step 5**.
- If no, correct the configuration in **/etc/hosts** and restart the ZooKeeper service. The fault can be rectified.

Step 5 Run the following command to check whether the DNS server is installed on the node:

service named status

The following information indicates that the DNS server is installed and enabled.

```
Checking for nameserver BIND
version: 9.6-ESV-R7-P4
CPUs found: 8
worker threads: 8
number of zones: 17
debug level: 0
xfers running: 0
xfers deferred: 0
soa queries in progress: 0
query logging is ON
recursive clients: 4/0/1000
tcp clients: 0/100
server is up and running
```

Step 6 If the DNS server is installed and enabled on the node, run the following command to disable the DNS server:

service named stop

The following information indicates that the DNS server disabled.

```
Shutting down name server BIND waiting for named to shut down (28s)
```

Step 7 Run the following command to check whether the DNS client is installed on the node:

cat /etc/resolv.conf

The following information indicates that the DNS client is installed and enabled.

```
nameserver 10.10.8.8
nameserver 10.10.4.4
```

Step 8 If the DNS client is installed and enabled on the node, run the following command to disable the DNS client:

vi /etc/resolv.conf

Comment all the content by "#" and save the file.

```
# nameserver 10.10.8.8
# nameserver 10.10.4.4
```

Step 9 Log in to FusionInsight Manager, choose **Cluster >** *Name of the desired cluster* **> Services** > **ZooKeeper** > **Instance**, select the faulty ZooKeeper instance, choose **More** > **Restart Instance** to restart the instance, and check whether ZooKeeper is restored.

- If yes, no further action is required.
- If no, contact thetechnical support.

----End

Reference Information

None.

2.4.27.6 Emergency Restoration Upon a Service Exception Caused by Metadata Abnormalities (older than the last zxid)

Symptom

A ZooKeeper instance is always in the Restoring state.

Possible Causes

View the run log of the ZooKeeper instance in the Restoring state (**/var/log/Bigdata/zookeeper/quorumpeer/zookeeper-omm-server-***host name***.log**). It is found that **Unable to load database on disk** or **is older than the last zxid** is printed in the log. Therefore, the ZooKeeper metadata is abnormal.

```
2015-12-19 14:34:16,770 | ERROR | main | Unable to load database on disk |
org.apache.zookeeper.server.quorum.QuorumPeer.loadDataBase(Quoru mPeer.java:725)
java.io.IOException: The current epoch, 9, is older than the last zxid, 42949672963
at org.apache.zookeeper.server.quorum.QuorumPeer.loadDataBase(QuorumPeer.java:707)
2015-12-19 14:34:16,773 | ERROR | main | Unexpected exception, exiting abnormally |
org.apache.zookeeper.server.quorum.QuorumPeerMain.main( QuorumPeerMain.java:111)
java.lang.RuntimeException: Unable to run quorum server
at org.apache.zookeeper.server.quorum.QuorumPeer.loadDataBase(QuorumPeer.java:726)
```

Fault Locating

1. Delete the ZooKeeper metadata file of the malfunctioning instance (by backing up the file to another directory).
2. When no metadata is available, ZooKeeper automatically synchronizes metadata from the leader node during start.

Procedure

Step 1 Log in as user **omm** to the node where the malfunctioning ZooKeeper instance resides. If you log in as user **root**, run the **su-omm** command to switch to user **omm**.

Step 2 Back up the data of the malfunctioning ZooKeeper instance.

mv /srv/BigData/zookeeper/version-2 /srv/BigData/zookeeper/version-2-bk

NOTE

/srv/BigData/zookeeper is the default data directory of ZooKeeper and is specified by the **dataDir** parameter. The data directory varies depending on the cluster.

Step 3 After 4 minutes, check whether the ZooKeeper status is normal on the FusionInsight Manager page.

Step 4 Log in to node where the original malfunctioning ZooKeeper instance resides and run the following command to check the directory. If the directory is not blank, the instance has been restored.

ls -l /srv/BigData/zookeeper/version-2/

Example:

```
-rw------- 1 omm wheel        1 Mar  5 18:24 acceptedEpoch
-rw------- 1 omm wheel        1 Mar  5 18:24 currentEpoch
-rw------- 1 omm wheel 67108880 Mar  5 18:31 log.600000001
-rw------- 1 omm wheel      873 Feb 27 02:47 snapshot.50000000d
-rw------- 1 omm wheel      665 Mar  5 18:13 snapshot.60000001d
-rw------- 1 omm wheel      849 Mar  5 18:24 snapshot.70000000c
```

Step 5 After ZooKeeper is restored, observe the ZooKeeper status for a period of time or check whether the disk space is insufficient, and then run the following command to delete the backup file:

rm -rf /srv/BigData/zookeeper/version-2-bk

NOTICE

The operations are risky. Ensure that the operations are correct. The backup file to be deleted is in the preceding backup path.

----End

2.4.28 OS

2.4.28.1 The Operating System Command Execution is Slow in SUSE 12.x

Symptom

In the SUSE 12.x system, running the operating system command is slow, for example, the **su** command.

Possible Causes

The **pam_systemd.so** plug-in is configured in the **/etc/pam.d/common-session** file of the SUSE 12.x system.

Procedure

Step 1 Log in to the faulty node as user **root** and check whether the **pam_systemd.so** configuration exists in the **/etc/pam.d/common-session** file.

```
session optional pam_systemd.so
```

Step 2 If yes, comment out the **session optional pam_systemd.so** content in the **/etc/pam.d/common-session** file.

Step 3 Go to the **/sys/fs/cgroup/pids/system.slice/sshd.service** directory and check the values of **pids.current** and **pids.max**. Check the values of the two parameters. Ensure that the value of **pids.max** is sufficient. If the value of **pids.max** is too small, you cannot log in to the node using SSH after the **reboot** command is executed.

You can modify the **DefaultTasksMax** parameter in **/etc/systemd/system.conf** and the **kernel.pid_max** parameter in **/etc/sysctl.conf** to change the value of **pids.max**. The reference values are as follows:

```
DefaultTasksMax=512000
kernel.pid_max=1024000
```

Step 4 Restart the operating system to check whether the commands related to the operating system are running properly.

----End

References

None.

2.4.28.2 systemd Restarting Services Causes Other Associated Services to Restart in SUSE 12.2

Symptom

In the SUSE 12.2 operating system, when the systemd restarts services, all services started by the restarted service are restarted, such as cron and sshd.

Possible Causes

If the KillMode of a service is control-group, stopping or restarting the service will stop all processes that belong to the cgroup service.

Procedure

Step 1 Log in to the node as user root. Use the cron service as an example. Run the following command to check whether KillMode is control-group:

systemctl show cron.service | grep KillMode

- If yes, go to **Step 2**.
- If no, contact the technical support.

Step 2 Edit and view the **/usr/lib/systemd/system/cron.service** file to change the KillMode mode of the cron service.

Add KillMode=process to the description field of [Service].

For example, the configuration is similar to the following:

```
[Unit]
Description=Command Scheduler
After=ypbind.service nscd.service network.target
After=postfix.service sendmail.service exim.service
[Service]
ExecStart=/usr/sbin/cron -n
ExecReload=/usr/bin/kill -s SIGHUP $MAINPID
Restart=on-abort
KillMode=process
[Install]
WantedBy=multi-user.target
```

Step 3 Run the following commands in sequence for the settings to take effect:

systemctl daemon-reload

systemctl restart cron.service

----End

References

None.

2.5 Appendix

2.5.1 Logging In to Service OM

Step 1 Log in to ManageOne Maintenance Portal using a browser.

- Login with the URL: **https://***Domain name of ManageOne Maintenance Portal***:31943**. Alternatively, access **https://***Address for accessing the ManageOne unified portal* to log in to the ManageOne unified portal and choose OperationCenter to access ManageOne Maintenance Portal.

  Obtain the domain name of ManageOne Maintenance Portal on the "2.3 Portal" sheet of the deployment parameter table exported from HCC Turnkey during the installation of Huawei Cloud Stack basic services.
- Login using a password: Enter the username and password.

  Default account: bss_admin. To obtain the default password, contact the system administrator or refer to the default password of the ManageOne Maintenance Portal account on the "Type A (Portal)" sheet in ***Huawei Cloud Stack 8.3.1 Account List*** .

  NOTE

  For ManageOne upgraded from 8.2.0 or an earlier version, the default account name is **admin**.
- Login using a USB key: Insert a USB key with preset user certificates, select the required device and certificate, and enter a PIN.

Step 2 On the maintenance portal homepage, click Service_OM in **Common Links**. Select a region to switch to the **Service OM** page.

----End

2.5.2 Logging In to an MRS Management Node

Huawei Cloud Stack provides a security O&M channel through the CLI terminal (an optional module). When you install the security O&M channel, the way of logging in to backend nodes changes. This section describes how to log in to a backend node in different scenarios.

The module provides security O&M capabilities for ManageOne Maintenance Portal, including SSH login without password, command execution or interception, file upload and download, and O&M command audit. The module provides a unified O&M portal. This enhances O&M management, control, and audit, simplifies the remote O&M access process, improves O&M efficiency, and enhances account and password security.

The module is selected by default and can be deselected. It is not upgraded by default and can be added after the upgrade.

NOTE

The CLI supports the following accounts in different scenarios:

- Accounts of cloud services where the security O&M channel is not installed can only be used to log in to nodes over SSH.
- Accounts of cloud services where the security O&M channel is installed but that are not reclaimed can only be used to log in to nodes over SSH.
- Accounts of cloud services where the secure O&M channel is installed and that are reclaimed can be used to log in to nodes over SSH by applying for a password because its password has been changed to a random one after reclamation.
- Accounts of cloud services where the secure O&M channel is installed, that are reclaimed, and that have obtained the one-click login permission can be used to log in to nodes through the CLI terminal or over SSH by applying for a password.

Prerequisites

- You have logged in to ManageOne Maintenance Portal as a system administrator.
- You have obtained the permission to perform operations on the CLI.
- If the command whitelist is enabled, only whitelisted commands can be executed on the CLI. If the function is disabled, any commands can be executed on the CLI.

Logging In to an MRS Management Node Through the CLI Terminal

Step 1 Check whether secure O&M channel has been installed.

Choose **O&M** from the main menu and check whether the CLI terminal is displayed in the navigation pane.

- If yes, the secure O&M channel has been installed. Go to **Step 2**.
- If no, the secure O&M channel is not installed. In this case, log in to a management node over SSH. For details, see **Logging In to an MRS Management Node Over SSH**.

Step 2 Check whether the account has been managed by an external system.

1. Choose **O&M** > **Accounts** from the main menu.

2. Check whether the account for logging in to the backend node has been remotely managed based on information displayed in the **Application/Cloud Service**, **Resource Name**, and **Account Management Party** columns.
   - If yes, use an SSH client, such as PuTTY, to log in to a node.
   - If no, go to **Step 3**.

Step 3 Use either of the following methods to log in to a backend node:

- Login using SSH

  Apply for permission to use an account password to log in to the node over SSH. For details, see section "Account Request" > "Creating a Request for Obtaining Passwords" in the **Huawei Cloud Stack 8.3.1 O&M Guide**.
- One-click login on the CLI
  a. Choose **O&M** > **CLI** from the main menu.
  b. In the navigation pane on the left, expand the corresponding nodes one by one and check whether the account for logging in to the backend node is displayed.
     - If yes, the account has obtained the permission for one-click login. Go to **Step 4**.
     - If no, apply for the one-click login permission to log in to the node. For details, see section "Account Request" > "Creating a Request for Obtaining Passwords" in the **Huawei Cloud Stack 8.3.1 O&M Guide**. Then, go to **Step 4**.

Step 4 Click **Execute Command** to log in to the backend node. Then, proceed with other operations.

NOTE

Only commands in the trustlist can be executed. If the following error message is displayed during the execution, contact the administrator to add the commands to the trustlist. For details, see the **Huawei Cloud Stack 8.3.1 O&M Guide**.
Your command is highly risky. Please check the whitelisted commands.

----End

Logging In to an MRS Management Node Over SSH

Step 1 Log in to ManageOne Maintenance Portal as the system administrator. In the **Common Links** navigation tree, click Service_OM and select a region to go to the Service OM page.

Step 2 Choose **Services** > **Resource** > **Compute Resource**.

Step 3 Click the **VMs** tab, enter a keyword in the search box to search for the VM name, for example, **EICommon-Region-Master**, **MRS_DB**, **Console-DB**, or **Console-Static**, and record the IP address of the VM.

Step 4 Use PuTTY to log in to any VM whose **Status** is **Running** as user **opsadmin**. For example, log in to the **EICommon-Region-Master-01**, **MRS_DB-01**, **Console-DB-01**, or **Console-Static-01** VM.

Obtain the default password by referring to ***Huawei Cloud Stack 8.3.1 Account List*** or contacting the system administrator.

NOTE

If **Status** of all VMs is not **Running**, contact the cluster administrator.

----End